

PIX/ASA: Active/Active Failover Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Related Products](#)

[Conventions](#)

[Active/Active Failover](#)

[Active/Active Failover Overview](#)

[Primary/Secondary Status and Active/Standby Status](#)

[Device Initialization and Configuration Synchronization](#)

[Command Replication](#)

[Failover Triggers](#)

[Failover Actions](#)

[Regular and Stateful Failover](#)

[Regular Failover](#)

[Stateful Failover](#)

[Failover Configuration Limitations](#)

[Unsupported Features](#)

[Cable-Based Active/Active Failover Configuration](#)

[Prerequisites](#)

[Network Diagram](#)

[Configurations](#)

[LAN-Based Active/Active Failover Configuration](#)

[Network Diagram](#)

[Primary Unit Configuration](#)

[Secondary Unit Configuration](#)

[Configurations](#)

[Verify](#)

[Use of the show failover Command](#)

[View of Monitored Interfaces](#)

[Display of the Failover Commands in the Running Configuration](#)

[Failover Functionality Tests](#)

[Forced Failover](#)

[Disabled Failover](#)

[Restoration of a Failed Unit](#)

[Replace the Failed Unit with a New Unit](#)

[Troubleshoot](#)

[Failover System Messages](#)

[Primary Lost Failover communications with mate on interface interface_name](#)

[Debug Messages](#)

[SNMP](#)

[Failover Polltime](#)

[WARNING: Failover message decryption failure.](#)

[Related Information](#)

[Introduction](#)

The failover configuration requires two identical security appliances connected to each other through a dedicated failover link and, optionally, a stateful failover link. The health of the active interfaces and units is monitored to determine if specific failover conditions are met. If those conditions are met, failover occurs.

The security appliance supports two failover configurations, **Active/Active Failover** and **Active/Standby Failover**. Each failover configuration has its own method to determine and perform failover. With Active/Active Failover, both units can pass network traffic. This lets you configure load balancing on your network. Active/Active Failover is only available on units that run in multiple context mode. With Active/Standby Failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby Failover is available on units that run in either single or multiple context mode. Both failover configurations support stateful or stateless (regular) failover.

This document focuses on how to configure an Active/Active Failover in Cisco PIX/ASA Security Appliance.

Refer to [PIX/ASA 7.x Active/Standby Failover Configuration Example](#) in order to learn more information about the Active/Standby Failover configurations.

Note: VPN failover is not supported on units that run in multiple context mode as VPN is not supported in multiple context. VPN failover is available only for **Active/Standby Failover** configurations in single context configurations.

This configuration guide provides a sample configuration to include a brief introduction to the PIX/ASA 7.x Active/Active technology. Refer to the [Cisco Security Appliance Command Reference, Version 7.2](#) for a more in-depth sense of the theory based behind this technology.

[Prerequisites](#)

[Requirements](#)

Hardware Requirement

The two units in a failover configuration must have the same hardware configuration. They must be the same model, have the same number and types of interfaces, and the same amount of RAM.

Note: The two units do not need to have the same size Flash memory. If you use units with different Flash memory sizes in your failover configuration, make sure the unit with the smaller Flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger Flash memory to the unit with the smaller Flash memory fails.

Software Requirement

The two units in a failover configuration must be in the operational modes (routed or transparent, single or multiple context). They must have the same major (first number) and minor (second number) software version, but you can use different versions of the software within an upgrade process; for example, you can upgrade one unit from Version 7.0(1) to Version 7.0(2) and have failover remain active. Cisco recommends that you upgrade both units to the same version to ensure long-term compatibility.

Refer to [Performing Zero Downtime Upgrades for Failover Pairs](#) for more information about upgrading the software on a failover pair.

License Requirements

On the PIX/ASA Security appliance platform, at least one of the units must have an **unrestricted (UR) license**. The other unit can have a Failover Only Active-Active (FO_AA) license, or another UR license. Units with a Restricted license cannot be used for failover, and two units with FO_AA licenses cannot be used together as a failover pair.

Note: You might need to upgrade the licenses on a failover pair in order to obtain additional features and benefits. For more information on upgrade, refer to [License Key Upgrade on a Failover Pair](#)

Note: The licensed features, such as SSL VPN peers or security contexts, on both security appliances that participate in failover must be identical.

Note: The FO license does not support Active/Active Failover.

[Components Used](#)

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

- PIX Security Appliance with 7.x version 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 these hardware and software versions:

- ASA with 7.x version and later

Note: Active/Active failover is not available on the ASA 5505 series adaptive security appliance.

[Conventions](#)

Refer to the [Cisco Technical Tips Conventions](#) for more information document conventions.

[Active/Active Failover](#)

This section describes Active/Standby Failover and includes these topics:

- [Active/Active Failover Overview](#)
- [Primary/Secondary Status and Active/Standby Status](#)
- [Device Initialization and Configuration Synchronization](#)
- [Command Replication](#)
- [Failover Triggers](#)
- [Failover Actions](#)

[Active/Active Failover Overview](#)

Active/Active failover is only available to security appliances in multiple context mode. In an Active/Active failover configuration, both security appliances can pass network traffic.

In Active/Active failover, you divide the security contexts on the security appliance into failover groups. A failover group is simply a logical group of one or more security contexts. You can create a maximum of two failover groups on the security appliance. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.

The failover group forms the base unit for failover in Active/Active failover. Interface failure monitoring, failover, and active/standby status are all attributes of a failover group rather than the unit. When an active failover group fails, it changes to the standby state while the standby failover group becomes active. The interfaces in the failover group that becomes active assume the MAC and IP addresses of the interfaces in the failover group that failed. The interfaces in the failover group that is now in the standby state take over the standby MAC and IP addresses.

Note: A failover group failing on a unit does not mean that the unit has failed. The unit may still have another failover group passing traffic on it.

[Primary/Secondary Status and Active/Standby Status](#)

As in Active/Standby failover, one unit in an Active/Active failover pair is designated the primary unit, and the other unit the secondary unit. Unlike Active/Standby failover, this designation does not indicate which unit becomes active when both units start simultaneously. Instead, the primary/secondary designation does two things:

- Determines which unit provides the running configuration to the pair when they boot simultaneously.
- Determines on which unit each failover group appears in the active state when the units boot simultaneously. Each failover group in the configuration is configured with a primary or secondary unit preference. You can configure both failover groups be in the active state on a single unit in the pair, with the other unit containing the failover groups in the standby state. However, a more typical configuration is to assign each failover group a different role preference to make each one active on a different unit, distributing the traffic across the

devices. **Note:** The security appliance **does not** provide load balancing services. Load balancing must be handled by a router passing traffic to the security appliance.

Which unit each failover group becomes active on is determined as shown

- When a unit boots while the peer unit is not available, both failover groups become active on the unit.
- When a unit boots while the peer unit is active (with both failover groups in the active state), the failover groups remain in the active state on the active unit regardless of the primary or secondary preference of the failover group until one of the following:
A failover occurs. You manually force the failover group to the other unit with the **no failover active** command
You configured the failover group with the **preempt** command, which causes the failover group to automatically become active on the preferred unit when the unit becomes available.
- When both units boot at the same time, each failover group becomes active on its preferred unit after the configurations have been synchronized.

Device Initialization and Configuration Synchronization

Configuration synchronization occurs when one or both units in a failover pair boot. The configurations are synchronized as shown:

- When a unit boots while the peer unit is active (with both failover groups active on it), the booting unit contacts the active unit to obtain the running configuration regardless of the primary or secondary designation of the booting unit.
- When both units boot simultaneously, the secondary unit obtains the running configuration from the primary unit.

When the replication starts, the security appliance console on the unit sending the configuration displays the message "**Beginning configuration replication: Sending to mate,**" and when it is complete, the security appliance displays the message "**End Configuration Replication to mate.**" During replication, commands entered on the unit sending the configuration may not replicate properly to the peer unit, and commands entered on the unit receiving the configuration may be overwritten by the configuration being received. Avoid entering commands on either unit in the failover pair during the configuration replication process. Depending upon the size of the configuration, replication can take from a few seconds to several minutes.

On the unit receiving the configuration, the configuration exists only in running memory. To save the configuration to Flash memory after synchronization enter the **write memory all** command in the system execution space on the unit that has failover group 1 in the active state. The command is replicated to the peer unit, which proceeds to write its configuration to Flash memory. Using the **all** keyword with this command causes the system and all context configurations to be saved.

Note: Startup configurations saved on external servers are accessible from either unit over the network and do not need to be saved separately for each unit. Alternatively, you can copy the contexts configuration files from the disk on the primary unit to an external server, and then copy them to disk on the secondary unit, where they become available when the unit reloads.

Command Replication

After both units are running, commands are replicated from one unit to the other as shown:

- Commands entered within a security context are replicated from the unit on which the security

context appears in the active state to the peer unit.**Note:** context is considered in the active state on a unit if the failover group to which it belongs is in the active state on that unit.

- Commands entered in the system execution space are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state.
- Commands entered in the admin context are replicated from the unit on which failover group 1 is in the active state to the unit on which failover group 1 is in the standby state.

All configuration and file commands (**copy, rename, delete, mkdir, rmdir**, and so on) are replicated, with the following exceptions. The **show, debug, mode, firewall, and failover lan unit** commands are not replicated.

Failure to enter the commands on the appropriate unit for command replication to occur causes the configurations to be out of synchronization. Those changes may be lost the next time the initial configuration synchronization occurs.

You can use the **write standby** command to resynchronize configurations that have become out of sync. For Active/Active failover, the **write standby** command behaves as shown:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the security appliance is written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.**Note:** If there are security contexts in the active state on the peer unit, the **write standby** command causes active connections through those contexts to be terminated. Use the **failover active** command on the unit providing the configuration to make sure all contexts are active on that unit before entering the **write standby** command.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.

Replicated commands are not saved to the Flash memory when replicated to the peer unit. They are added to the running configuration. To save replicated commands to Flash memory on both units, use the **write memory** or **copy running-config startup-config** command on the unit that you made the changes on. The command is replicated to the peer unit and cause the configuration to be saved to Flash memory on the peer unit.

[Failover Triggers](#)

In Active/Active failover, failover can be triggered at the unit level if one of the following events occurs:

- The unit has a hardware failure.
- The unit has a power failure.
- The unit has a software failure.
- The **no failover active** or the **failover active** command is entered in the system execution space.

Failover is triggered at the failover group level when one of these events occurs:

- Too many monitored interfaces in the group fail.

- The **no failover active group group_id** or **failover active group group_id** command is entered.

Failover Actions

In an Active/Active failover configuration, failover occurs on a failover group basis, not a system basis. For example, if you designate both failover groups as active on the primary unit, and failover group 1 fails, then failover group 2 remains active on the primary unit while failover group 1 becomes active on the secondary unit.

Note: When configuring Active/Active failover, make sure that the combined traffic for both units is within the capacity of each unit.

This table shows the failover action for each failure event. For each failure event, the policy (whether or not failover occurs), actions for the active failover group, and actions for the standby failover group are given.

Failure Event	Policy	Active Group Action	Standby Group Action	Notes
A unit experiences a power or software failure	Failover	Become standby Mark as failed	Become standby. Mark active as failed	When a unit in a failover pair fails, any active failover groups on that unit are marked as failed and become active on the peer unit.
Interface failure on active failover group above threshold	Failover	Mark active group as failed	Become active	None
Interface failure on standby failover group above threshold	No failover	No action	Mark standby group as failed	When the standby failover group is marked as failed, the active failover group does not attempt to fail over, even if the interface failure threshold is surpassed.
Formerly active failover group recovers	No failover	No action	No action	Unless configured with the preempt command, the failover groups remain active on their current unit.

Failover link failed at startup	No failover	Become active	Become active	If the failover link is down at startup, both failover groups on both units become active.
Stateful Failover link failed	No failover	No action	No action	State information becomes out of date, and sessions are terminated if a failover occurs.
Failover link failed during operation	No failover	n/a	n/a	Each unit marks the failover interface as failed. You should restore the failover link as soon as possible because the unit cannot fail over to the standby unit while the failover link is down.

[Regular and Stateful Failover](#)

The security appliance supports two types of failover, regular and stateful. This section includes these topics:

- [Regular Failover](#)
- [Stateful Failover](#)

[Regular Failover](#)

When a failover occurs, all active connections are dropped. Clients need to re-establish connections when the new active unit takes over.

[Stateful Failover](#)

When stateful failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

The state information passed to the standby unit includes these:

- The NAT translation table
- The TCP connection states
- The UDP connection states
- The ARP table
- The Layer 2 bridge table (when it runs in the transparent firewall mode)
- The HTTP connection states (if HTTP replication is enabled)
- The ISAKMP and IPSec SA table
- The GTP PDP connection database

The information that is not passed to the standby unit when stateful failover is enabled includes these:

- The HTTP connection table (unless HTTP replication is enabled)
- The user authentication (uauth) table
- The routing tables
- State information for security service modules

Note: If failover occurs within an active Cisco IP SoftPhone session, the call remains active because the call session state information is replicated to the standby unit. When the call is terminated, the IP SoftPhone client loses connection with the Call Manager. This occurs because there is no session information for the CTIQBE hang-up message on the standby unit. When the IP SoftPhone client does not receive a response back from the Call Manager within a certain time period, it considers the Call Manager unreachable and unregisters itself.

Failover Configuration Limitations

You cannot configure failover with these types of IP addresses:

- IP addresses obtained through DHCP
- IP addresses obtained through PPPoE
- IPv6 addresses

Additionally, these restrictions apply:

- Stateful Failover is not supported on the ASA 5505 adaptive security appliance.
- Active/Active failover is not supported on the ASA 5505 adaptive security appliance.
- You cannot configure failover when Easy VPN Remote is enabled on the ASA 5505 adaptive security appliance.
- VPN failover is not supported in multiple context mode.

Unsupported Features

Multiple context mode does not support these features:

- Dynamic routing protocolsSecurity contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.
- VPN
- Multicast

Cable-Based Active/Active Failover Configuration

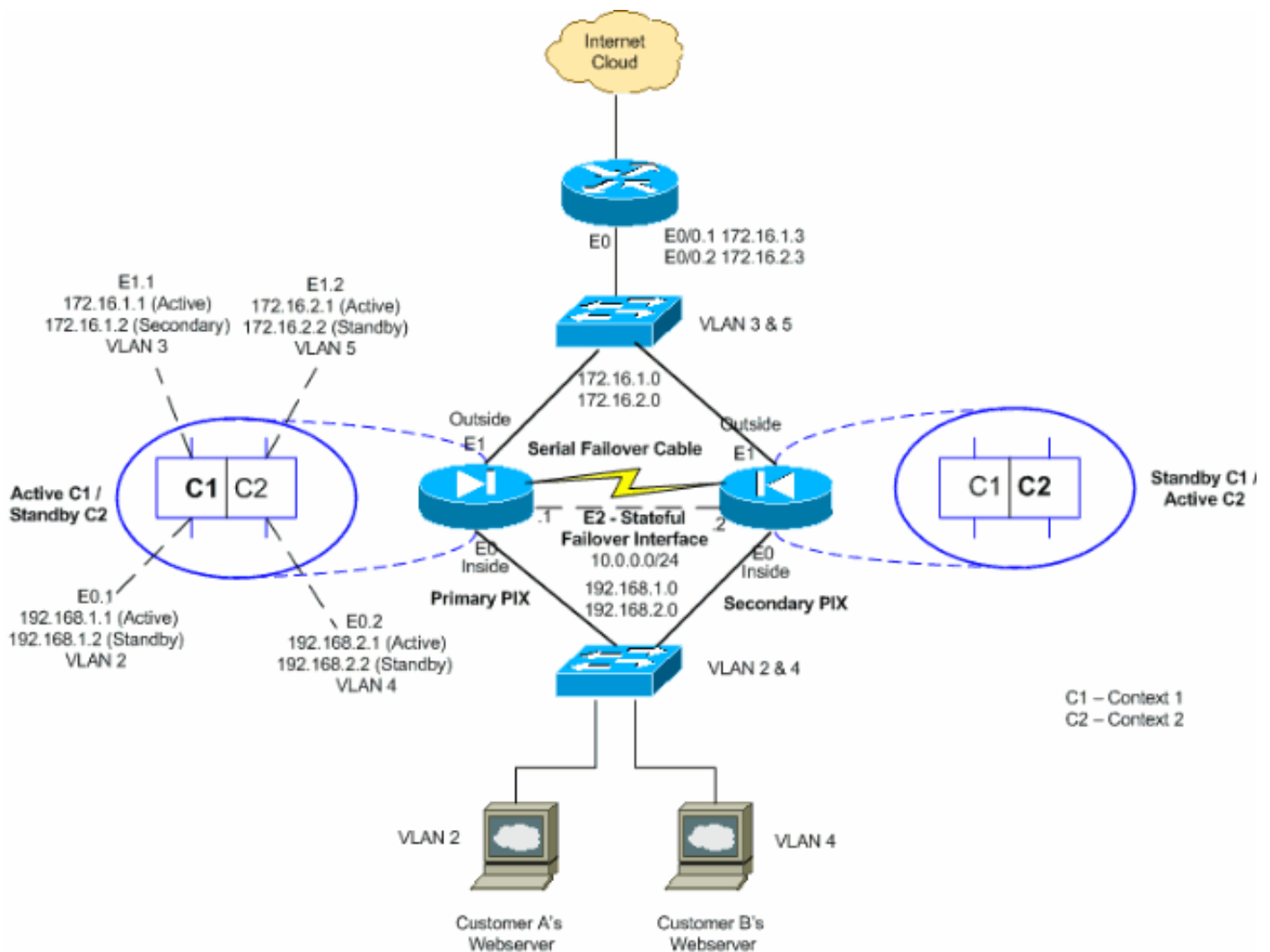
Prerequisites

Before you begin, verify the following:

- Both units have the same hardware, software configuration, and proper license.
- Both units are in the same mode (single or multiple, transparent or routed).

Network Diagram

This document uses this network setup:



Follow these steps in order to configure Active/Active failover using a serial cable as the failover link. The commands in this task are entered on the primary unit in the failover pair. The primary unit is the unit that has the end of the cable labeled "Primary" plugged into it. For devices in multiple context mode, the commands are entered in the system execution space unless otherwise noted.

You do not need to bootstrap the secondary unit in the failover pair when you use cable-based failover. Leave the secondary unit powered off until instructed to power it on.

Note: Cable-based failover is only available on the PIX 500 series security appliance.

Complete these steps in order to configure cable-based, Active/Active failover:

1. Connect the failover cable to the PIX 500 series security appliances. Make sure that you attach the end of the cable marked "Primary" to the unit you use as the primary unit, and that you attach the end of the cable marked "Secondary" to the unit you use as the secondary unit.
2. Power on the primary unit.
3. If you have not done so already, configure the active and standby IP addresses for each data interface (routed mode), for the management IP address (transparent mode), or for the management-only interface. The standby IP address is used on the security appliance that is currently the standby unit. It must be in the same subnet as the active IP address. You must configure the interface addresses from within each context. Use the **changeto context** command to switch between contexts. The command prompt changes to

hostname/context (config-if)#, where context is the name of the current context. You must enter a management IP address for each context in transparent firewall multiple context mode. **Note:** Do not configure an IP address for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the **failover interface ip** command to configure a dedicated Stateful Failover interface in a later step. hostname/context (config-if)#ip address active_addr netmask standby standby_addr In the example, the outside interface for context1 of the primary PIX is configured this way: PIX1/context1 (config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2 For Context2: PIX1/context2 (config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2 In routed firewall mode and for the management-only interface, this command is entered in interface configuration mode for each interface. In transparent firewall mode, the command is entered in global configuration mode.

- In order to enable Stateful Failover, configure the Stateful Failover link. Specify the interface to be used as Stateful Failover link: hostname (config)#failover link if_name phy_if In this example, the Ethernet2 interface is used to exchange the stateful failover link state information. failover link stateful Ethernet2 The if_name argument assigns a logical name to the interface specified by the phy_if argument. The phy_if argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. This interface should not be used for any other purpose (except, optionally, the failover link). Assign an active and standby IP address to the Stateful Failover

link: hostname (config)#failover interface ip if_name ip_addr mask standby ip_addr In this example, 10.0.0.1 is used as an active, and 10.0.0.2 is used as a standby IP address for the stateful failover link. PIX1 (config)#failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2 The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby IP address subnet mask. The Stateful Failover link IP address and MAC address do not change at failover except for when Stateful Failover uses a regular data interface. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit. Enable the interface: hostname (config)#interface phy_if hostname (config-if)#no shutdown

- Configure the failover groups. You can have at most two failover groups. The **failover group** command creates the specified failover group if it does not exist and enters the failover group configuration mode. For each failover group, you need to specify whether the failover group has primary or secondary preference using the **primary** or **secondary** command. You can assign the same preference to both failover groups. For load balancing configurations, you should assign each failover group a different unit preference. The following example assigns failover group 1 a primary preference and failover group 2 a secondary

```
preference: hostname (config)#failover group 1 hostname (config-fover-group)#primary
hostname (config-fover-group)#exit hostname (config)#failover group 2 hostname (config-fover-
group)#secondary hostname (config-fover-group)#exit
```

- Assign each user context to a failover group using the **join-failover-group** command in context configuration mode. Any unassigned contexts are automatically assigned to failover group 1. The admin context is always a member of failover group 1. Enter these commands to assign each context to a failover group:

```
hostname (config)#context context_name
hostname (config-context)#join-failover-group {1 | 2} hostname (config-context)#exit
```

- Enable failover: hostname (config)#failover

- Power on the secondary unit and enable failover on the unit if it is not already enabled: hostname (config)#failover The active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages "Beginning

configuration replication: Sending to mate" and "End Configuration Replication to mate" appear on the primary console. **Note:** Issue the **failover** command on the primary device first, and then issue it on the secondary device. After you issue the **failover** command on the secondary device, the secondary device immediately pulls the configuration from the primary device and sets itself as *standby*. The primary ASA stays up and passes traffic normally and marks itself as the *active* device. From that point on, whenever a failure occurs on the active device, the standby device comes up as active.

9. Save the configuration to Flash memory on the Primary unit. Because the commands entered on the primary unit are replicated to the secondary unit, the secondary unit also saves its configuration to Flash memory. `hostname(config)#copy running-config startup-config`
10. If necessary, force any failover group that is active on the primary to the active state on the secondary. To force a failover group to become active on the secondary unit, issue this command in the system execution space on the primary unit: `hostname#no failover active group group_id` The `group_id` argument specifies the group you want to become active on the secondary unit.

Configurations

This document uses these configurations:

- [PIX1 - System Configuration](#)
- [PIX1 - Context1 Configuration](#)
- [PIX1 - Context2 Configuration](#)

PIX1 - System Configuration

```
PIX1#show running-config : Saved PIX Version 7.2(2)
<system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-addresses auto !---
Enable the physical and logical interfaces in the system
execution !--- space by giving "no shutdown" before
configuring the same in the contexts ! interface
Ethernet0 ! interface Ethernet0.1 vlan 2 ! interface
Ethernet0.2 vlan 4 ! interface Ethernet1 ! interface
Ethernet1.1 vlan 3 ! interface Ethernet1.2 vlan 5 ! !---
Configure "no shutdown" in the stateful failover
interface !--- of both Primary and secondary PIX.
interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 shutdown ! interface Ethernet4
shutdown ! interface Ethernet5 shutdown ! class default
limit-resource All 0 limit-resource ASDM 5 limit-
resource SSH 5 limit-resource Telnet 5 ! ftp mode
passive pager lines 24 !--- Command to enable the
failover feature failover !--- Command to assign the
interface for stateful failover failover link stateful
Ethernet2 !--- Command to configure the active and
standby IP's for the !--- stateful failover failover
interface ip stateful 10.0.0.1 255.255.255.0 standby
10.0.0.2 !--- Configure the group 1 as primary failover
group 1 !--- Configure the group 1 as secondary failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! !--- Command to
create a context called "context1" context context1 !---
Command to allocate the logical interfaces to the
contexts allocate-interface Ethernet0.1 inside_context1
```

```
allocate-interface Ethernet1.1 outside_context1 config-  
url flash:/context1.cfg !--- Assign this context to the  
failover group 1 join-failover-group 1 ! context  
context2 allocate-interface Ethernet0.2 inside_context2  
allocate-interface Ethernet1.2 outside_context2 config-  
url flash:/context2.cfg join-failover-group 2 ! prompt  
hostname context  
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

PIX1 - Context1 Configuration

```
PIX1/context1(config)#show running-config : Saved : PIX  
Version 7.2(2) <context> ! hostname context1 enable  
password 8Ry2YjIyt7RRXU24 encrypted names ! interface  
inside_context1 nameif inside security-level 100 !---  
Configure the active and standby IP's for the logical  
inside !--- interface of the context1. ip address  
192.168.1.1 255.255.255.0 standby 192.168.1.2 !  
interface outside_context1 nameif outside security-level  
0 !--- Configure the active and standby IP's for the  
logical outside !--- interface of the context1. ip  
address 172.16.1.1 255.255.255.0 standby 172.16.1.2 !  
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100  
extended permit tcp any host 172.16.1.1 eq www pager  
lines 24 mtu inside 1500 mtu outside 1500 monitor-  
interface inside monitor-interface outside icmp  
unreachable rate-limit 1 burst-size 1 no asdm history  
enable arp timeout 14400 static (inside,outside)  
172.16.1.1 192.168.1.5 netmask 255.255.255.255 access-  
group 100 in interface outside route outside 0.0.0.0  
0.0.0.0 172.16.1.3 1 timeout xlate 3:00:00 timeout conn  
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp  
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media  
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00  
timeout uauth 0:05:00 absolute no snmp-server location  
no snmp-server contact telnet timeout 5 ssh timeout 5 !  
class-map inspection_default match default-inspection-  
traffic ! ! policy-map type inspect dns preset_dns_map  
parameters message-length maximum 512 policy-map  
global_policy class inspection_default inspect dns  
preset_dns_map inspect ftp inspect h323 h225 inspect  
h323 ras inspect netbios inspect rsh inspect rtsp  
inspect skinny inspect esmtp inspect sqlnet inspect  
sunrpc inspect tftp inspect sip inspect xdmcp ! service-  
policy global_policy global  
Cryptochecksum:00000000000000000000000000000000 : end
```

PIX1 - Context2 Configuration

```
PIX1/context2(config)#show running-config : Saved : PIX  
Version 7.2(2) <context> ! hostname context2 enable  
password 8Ry2YjIyt7RRXU24 encrypted names ! interface  
inside_context2 nameif inside security-level 100 !---  
Configure the active and standby IP's for the logical  
inside !--- interface of the context2. ip address  
192.168.2.1 255.255.255.0 standby 192.168.2.2 !  
interface outside_context2 nameif outside security-level  
0 !--- Configure the active and standby IP's for the  
logical outside !--- interface of the context2. ip  
address 172.16.2.1 255.255.255.0 standby 172.16.2.2 !  
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100  
extended permit tcp any host 172.16.2.1 eq www pager  
lines 24 mtu inside 1500 mtu outside 1500 monitor-  
interface inside monitor-interface outside icmp  
unreachable rate-limit 1 burst-size 1 no asdm history
```


This section describes how to configure Active/Active failover using an Ethernet failover link. When configuring LAN-based failover, you must bootstrap the secondary device to recognize the failover link before the secondary device can obtain the running configuration from the primary device.

Note: Instead of using a crossover Ethernet cable to directly link the units, Cisco recommends that you use a dedicated switch between the primary and secondary units.

This section includes the topics as shown:

- [Primary Unit Configuration](#)
- [Secondary Unit Configuration](#)

Primary Unit Configuration

Complete these steps in order to configure the primary unit in an Active/Active failover configuration:

1. If you have not done so already, configure the active and standby IP addresses for each data interface (routed mode), for the management IP address (transparent mode), or for the management-only interface. The standby IP address is used on the security appliance that is currently the standby unit. It must be in the same subnet as the active IP address. You must configure the interface addresses from within each context. Use the **changeto context** command to switch between contexts. The command prompt changes to `hostname/context(config-if)#`, where `context` is the name of the current context. In transparent firewall mode, you must enter a management IP address for each context. **Note:** Do not configure an IP address for the Stateful Failover link if you are going to use a dedicated Stateful Failover interface. You use the **failover interface ip** command to configure a dedicated Stateful Failover interface in a later step. `hostname/context(config-if)#ip address active_addr netmask standby standby_addr` In the example, the outside interface for context1 of the primary PIX is configured this way: `PIX1/context1(config)#ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2` For Context2: `PIX1/context2(config)#ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2` In routed firewall mode and for the management-only interface, this command is entered in interface configuration mode for each interface. In transparent firewall mode, the command is entered in global configuration mode.
2. Configure the basic failover parameters in the system execution space. (PIX security appliance only) Enable LAN-based failover: `hostname(config)#failover lan enable` Designate the unit as the primary unit: `hostname(config)#failover lan unit primary` Specify the failover link: `hostname(config)#failover lan interface if_name phy_if` In this example, we use the interface ethernet 3 as LAN based failover interface. `PIX1(config)#failover lan interface LANFailover ethernet3` The `if_name` argument assigns a logical name to the interface specified by the `phy_if` argument. The `phy_if` argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. On the ASA 5505 adaptive security appliance, the `phy_if` specifies a VLAN. This interface should not be used for any other purpose (except, optionally, the Stateful Failover link). Specify the failover link active and standby IP addresses: `hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr` For this example, we use 10.1.0.1 as active and 10.1.0.2 as standby IP addresses for failover interface. `PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2` The standby IP address must be in the same subnet as the

active IP address. You do not need to identify the standby IP address subnet mask. The failover link IP address and MAC address do not change at failover. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit.

3. To enable Stateful Failover, configure the Stateful Failover link: Specify the interface to be used as Stateful Failover link:
`hostname(config)#failover link if_name`

`phy_if` `PIX1(config)#failover link stateful ethernet2` The `if_name` argument assigns a logical name to the interface specified by the `phy_if` argument. The `phy_if` argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. This interface should not be used for any other purpose (except, optionally, the failover link). **Note:** If the Stateful Failover link uses the failover link or a regular data interface, then you only need to supply the `if_name` argument. Assign an active and standby IP address to the Stateful Failover link. **Note:** If the Stateful Failover link uses the failover link or a regular data interface, skip this step. You have already defined the active and standby IP addresses for the interface.
`hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr`
`PIX1(config)#failover interface ip stateful 10.0.0.1 255.255.255.0 standby 10.0.0.2` The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask. The state link IP address and MAC address do not change at failover. The active IP address always stays with the primary unit, while the standby IP address stays with the secondary unit. Enable the interface. **Note:** If the Stateful Failover link uses the failover link or regular data interface, skip this step. You have already enabled the interface.
`hostname(config)#interface phy_if hostname(config-if)#no shutdown`

4. Configure the failover groups. You can have at most two failover groups. The **failover group** command creates the specified failover group if it does not exist and enters the failover group configuration mode. For each failover group, specify whether the failover group has **primary** or **secondary** preference using the `primary` or `secondary` command. You can assign the same preference to both failover groups. For load balancing configurations, you should assign each failover group a different unit preference. The following example assigns failover group 1 a primary preference and failover group 2 a secondary preference:
`hostname(config)#failover group 1 hostname(config-fover-group)#primary hostname(config-fover-group)#exit hostname(config)#failover group 2 hostname(config-fover-group)#secondary hostname(config-fover-group)#exit`

5. Assign each user context to a failover group using the **join-failover-group** command in context configuration mode. Any unassigned contexts are automatically assigned to failover group 1. The admin context is always a member of failover group 1. Enter these commands to assign each context to a failover group:
`hostname(config)#context context_name hostname(config-context)#join-failover-group {1 | 2} hostname(config-context)#exit`

6. Enable failover.
`hostname(config)#failover`

Secondary Unit Configuration

When configuring LAN-based Active/Active failover, you need to bootstrap the secondary unit to recognize the failover link. This allows the secondary unit to communicate with and receive the running configuration from the primary unit.

Complete these steps in order to bootstrap the secondary unit in an Active/Active failover configuration:

1. (PIX security appliance only) Enable LAN-based failover.`hostname(config)#failover lan enable`
2. Define the failover interface. Use the same settings as you used for the primary unit:Specify the interface to be used as the failover interface.`hostname(config)#failover lan interface if_name phy_if``PIX1(config)#failover lan interface LANFailover ethernet3`The `if_name` argument assigns a logical name to the interface specified by the `phy_if` argument. The `phy_if` argument can be the physical port name, such as Ethernet1, or a previously created subinterface, such as Ethernet0/2.3. On the ASA 5505 adaptive security appliance, the `phy_if` specifies a VLAN.Assign the active and standby IP address to the failover link:`hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr``PIX1(config)#failover interface ip LANFailover 10.1.0.1 255.255.255.0 standby 10.1.0.2` **Note:** Enter this command exactly as you entered it on the primary unit when you configured the failover interface.The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask.Enable the interface.`hostname(config)#interface phy_if` `hostname(config-if)#no shutdown`
3. Designate this unit as the secondary unit:`hostname(config)#failover lan unit secondary` **Note:** This step is optional because by default units are designated as secondary unless previously configured otherwise.
4. Enable failover.`hostname(config)#failover` After you enable failover, the active unit sends the configuration in running memory to the standby unit. As the configuration synchronizes, the messages **Beginning configuration replication: Sending to mate and End Configuration Replication to mate** appear on the active unit console.**Note:** Issue the **failover** command on the primary device first, and then issue it on the secondary device. After you issue the **failover** command on the secondary device, the secondary device immediately pulls the configuration from the primary device and sets itself as *standby*. The primary ASA stays up and passes traffic normally and marks itself as the *active* device. From that point on, whenever a failure occurs on the active device, the standby device comes up as active.
5. After the running configuration has completed replication, enter this command to save the configuration to Flash memory:`hostname(config)#copy running-config startup-config`
6. If necessary, force any failover group that is active on the primary to the active state on the secondary unit. To force a failover group to become active on the secondary unit, enter this command in the system execution space on the primary unit:`hostname#no failover active group group_id` The `group_id` argument specifies the group you want to become active on the secondary unit.

Configurations

This document uses these configurations:

Primary PIX

```
PIX1(config)#show running-config : Saved : PIX Version
7.2(2) <system> ! hostname PIX1 enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !
interface Ethernet0 ! interface Ethernet0.1 vlan 2 !
interface Ethernet0.2 vlan 4 ! interface Ethernet1 !
interface Ethernet1.1 vlan 3 ! interface Ethernet1.2
vlan 5 ! !--- Configure "no shutdown" in the stateful
failover interface as well as !--- LAN Failover
interface of both Primary and secondary PIX/ASA.
interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 description LAN Failover Interface
```

```

! interface Ethernet4 shutdown ! interface Ethernet5
shutdown ! class default limit-resource All 0 limit-
resource ASDM 5 limit-resource SSH 5 limit-resource
Telnet 5 ! ftp mode passive pager lines 24 failover
failover lan unit primary !--- Command to assign the
interface for LAN based failover failover lan interface
LANFailover Ethernet3 !--- Command to enable the LAN
based failover failover lan enable !--- Configure the
Authentication/Encryption key failover key *****
failover link stateful Ethernet2 !--- Configure the
active and standby IP's for the LAN based failover
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2 failover interface ip stateful 10.0.0.1
255.255.255.0 standby 10.0.0.2 failover group 1 failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! context context1
allocate-interface Ethernet0.1 inside_context1 allocate-
interface Ethernet1.1 outside_context1 config-url
flash:/context1.cfg join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end

```

Note: Refer the Cable based Failover Configuration section, [PIX1 - Context1 Configuration](#) and [PIX1 - Context2 Configuration](#) for context configuration in LAN based failover scenario.

Secondary PIX

```

PIX2#show running-config failover failover lan unit
secondary failover lan interface LANFailover Ethernet3
failover lan enable failover key ***** failover
interface ip LANFailover 10.1.0.1 255.255.255.0 standby
10.1.0.2

```

Verify

Use of the show failover Command

This section describes the **show failover** command output. On each unit, you can verify the failover status with the **show failover** command.

Primary PIX

```

PIX1(config-subif)#show failover Failover On Cable status: N/A - LAN-based failover
enabled Failover unit Primary Failover LAN Interface: LANFailover Ethernet3 (up) Unit
Poll frequency 15 seconds, holdtime 45 seconds Interface Poll frequency 5 seconds,
holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 250 maximum Version:
Ours 7.2(2), Mate 7.2(2) Group 1 last failover at: 06:12:45 UTC Apr 16 2007 Group 2
last failover at: 06:12:43 UTC Apr 16 2007 This host: Primary Group 1 State: Active
Active time: 359610 (sec) Group 2 State: Standby Ready Active time: 3165 (sec)
context1 Interface inside (192.168.1.1): Normal context1 Interface outside
(172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2
Interface outside (172.16.2.2): Normal Other host: Secondary Group 1 State: Standby
Ready Active time: 0 (sec) Group 2 State: Active Active time: 3900 (sec) context1
Interface inside (192.168.1.2): Normal context1 Interface outside (172.16.1.2):
Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside

```

```
(172.16.2.1): Normal Stateful Failover Logical Update Statistics Link : stateful
Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 48044 0 48040 1 sys cmd 48042
0 48040 1 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0 ARP
tbl 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv
Q: 0 1 72081 Xmit Q: 0 1 48044
```

Secondary PIX

```
PIX1(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled
Failover unit Secondary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll
frequency 15 seconds, holdtime 45 seconds Interface Poll frequency 5 seconds,
holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 250 maximum Version:
Ours 7.2(2), Mate 7.2(2) Group 1 last failover at: 06:12:46 UTC Apr 16 2007 Group 2
last failover at: 06:12:41 UTC Apr 16 2007 This host: Secondary Group 1 State:
Standby Ready Active time: 0 (sec) Group 2 State: Active Active time: 3975 (sec)
context1 Interface inside (192.168.1.2): Normal context1 Interface outside
(172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2
Interface outside (172.16.2.1): Normal Other host: Primary Group 1 State: Active
Active time: 359685 (sec) Group 2 State: Standby Ready Active time: 3165 (sec)
context1 Interface inside (192.168.1.1): Normal context1 Interface outside
(172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2
Interface outside (172.16.2.2): Normal Stateful Failover Logical Update Statistics
Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 940 0 942 2
sys cmd 940 0 940 2 up time 0 0 0 0 RPC services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0
0 0 0 ARP tbl 0 0 2 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max
Total Recv Q: 0 1 1419 Xmit Q: 0 1 940
```

Use the **show failover state** command to verify the state.

Primary PIX

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host -
Primary Group 1 Active None Group 2 Standby Ready None Other host - Secondary Group 1
Standby Ready None Group 2 Active None ====Configuration State=== Sync Done
====Communication State=== Mac set
```

Secondary unit

```
PIX1(config)#show failover state State Last Failure Reason Date/Time This host -
Secondary Group 1 Standby Ready None Group 2 Active None Other host - Primary Group 1
Active None Group 2 Standby Ready None ====Configuration State=== Sync Done - STANDBY
====Communication State=== Mac set
```

In order to verify the IP addresses of the failover unit, use the **show failover interface** command.

Primary unit

```
PIX1(config)#show failover interface interface stateful Ethernet2 System IP Address:
10.0.0.1 255.255.255.0 My IP Address : 10.0.0.1 Other IP Address : 10.0.0.2 interface
LANFailover Ethernet3 System IP Address: 10.1.0.1 255.255.255.0 My IP Address :
10.1.0.1 Other IP Address : 10.1.0.2
```

Secondary unit

```
PIX1(config)#show failover interface interface LANFailover Ethernet3 System IP
Address: 10.1.0.1 255.255.255.0 My IP Address : 10.1.0.2 Other IP Address : 10.1.0.1
interface stateful Ethernet2 System IP Address: 10.0.0.1 255.255.255.0 My IP Address
: 10.0.0.2 Other IP Address : 10.0.0.1
```

[View of Monitored Interfaces](#)

In order to view the status of monitored interfaces: In single context mode, enter the `show monitor-interface` command in global configuration mode. In multiple context mode, enter the `show monitor-interface` within a context.

Note: In order to enable health monitoring on a specific interface, use the [monitor-interface](#) command in global configuration mode:

```
monitor-interface <if_name>
```

Primary PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Active Interface
inside (192.168.1.1): Normal Interface outside (172.16.1.1): Normal Other host:
Secondary - Standby Ready Interface inside (192.168.1.2): Normal Interface outside
(172.16.1.2): Normal
```

Secondary PIX

```
PIX1/context1(config)#show monitor-interface This host: Secondary - Standby Ready
Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Other
host: Secondary - Active Interface inside (192.168.1.1): Normal Interface outside
(172.16.1.1): Normal
```

Note: If you do not enter a failover IP address, the `show failover` command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remains in a "waiting" state. You must set a failover IP address for failover to work. For more information about different states for failover, refer to [show failover](#).

By default, monitoring of physical interfaces is enabled, and monitoring of subinterfaces is disabled.

[Display of the Failover Commands in the Running Configuration](#)

In order to view the failover commands in the running configuration, enter this command:

```
hostname(config)#show running-config failover
```

All of the **failover** commands are displayed. On units that run in multiple context mode, enter the `show running-config failover` command in the system execution space. Enter the **show running-config all failover** command to display the failover commands in the running configuration and include commands for which you have not changed the default value.

[Failover Functionality Tests](#)

In order to test failover functionality, perform these steps:

1. Test that your active unit or failover group passes traffic as expected with FTP (for example) to send a file between hosts on different interfaces.
2. Force a failover to the standby unit with this command: For Active/Active failover, enter the following command on the unit where the failover group containing the interface connecting your hosts is active: `hostname(config)#no failover active group group_id`
3. Use FTP to send another file between the same two hosts.

4. If the test was not successful, enter the **show failover command** to check the failover status.
5. When you are finished, you can restore the unit or failover group to active status with this command: For Active/Active failover, enter the following command on the unit where the failover group containing the interface connecting your hosts is

```
hostname(config)#failover active group group_id
```

Forced Failover

In order to force the standby unit to become active, enter one of these commands:

Enter this command in the system execution space of the unit where the failover group is in the standby state:

```
hostname#failover active group group_id
```

Or, enter this command in the system execution space of the unit where the failover group is in the active state:

```
hostname#no failover active group group_id
```

Entering this command in the system execution space causes all failover groups to become active:

```
hostname#failover active
```

Disabled Failover

In order to disable failover, enter this command:

```
hostname(config)#no failover
```

If you disable failover on an Active/Standby pair, it causes the active and standby state of each unit to be maintained until you restart. For example, the standby unit remains in standby mode so that both units do not start to pass traffic. In order to make the standby unit active (even with failover disabled), see the [Forced Failover](#) section.

If you disable failover on an Active/Active pair, it causes the failover groups to remain in the active state on whichever unit they are currently active on, no matter which unit they are configured to prefer. The **no failover** command can be entered in the system execution space.

Restoration of a Failed Unit

In order to restore a failed Active/Active failover group to an unfailed state, enter this command:

```
hostname(config)#failover reset group group_id
```

If you restore a failed unit to an unfailed state, it does not automatically make it active; restored units or groups remain in the standby state until made active by failover (forced or natural). An exception is a failover group configured with the **preempt** command. If previously active, a failover group becomes active if it is configured with the **preempt** command and if the unit on which it failed is its preferred unit.

Replace the Failed Unit with a New Unit

Complete these steps in order to replace a failed unit with a new unit:

1. Run the **no failover** command on the primary unit. The status of the secondary unit shows **standby unit as not detected**.
2. Unplug the primary unit, and connect the replacement primary unit.
3. Verify that the replacement unit runs the same software and ASDM version as the secondary unit.
4. Run these commands on the replacement unit:

```
ASA(config)#failover lan unit primary ASA(config)#failover lan interface failover Ethernet3
ASA(config)#failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2
ASA(config)#interface Ethernet3 ASA(config-if)#no shut ASA(config-if)#exit
```

5. Plug the replacement primary unit to the network, and run this command:ASA(config)#failover

Troubleshoot

When a failover occurs, both security appliances send out system messages. This section includes these topics:

1. [Failover System Messages](#)
2. [Debug Messages](#)
3. [SNMP](#)

Failover System Messages

The security appliance issues a number of system messages related to failover at priority level 2, which indicates a critical condition. In order to view these messages, refer to the [Cisco Security Appliance Logging Configuration and System Log Messages](#) to enable logging and to see descriptions of the system messages.

Note: Within switchover, failover logically shuts down and then brings up interfaces, which generates syslog **411001** and **411002** messages. This is normal activity.

Primary Lost Failover communications with mate on interface interface_name

This failover message is displayed if one unit of the failover pair can no longer communicate with the other unit of the pair. Primary can also be listed as Secondary for the secondary unit.

(Primary) Lost Failover communications with mate on interface interface_name

Verify that the network that is connected to the specified interface is functioning correctly.

Debug Messages

In order to see debug messages, enter the **debug fover** command. Refer to the [Cisco Security Appliance Command Reference, Version 7.2](#) for more information.

Note: Because debugging output is assigned high priority in the CPU process, it can drastically affect system performance. For this reason, use the **debug fover** commands only to troubleshoot specific problems or within troubleshooting sessions with Cisco technical support staff.

[SNMP](#)

In order to receive SNMP syslog traps for failover, configure the SNMP agent to send SNMP traps to SNMP management stations, define a syslog host, and compile the Cisco syslog MIB into your SNMP management station. Refer to the **snmp-server** and **logging** commands in the [Cisco Security Appliance Command Reference, Version 7.2](#) for more information.

[Failover Polltime](#)

In order to specify the failover unit poll and hold times, issue the **failover polltime** command in global configuration mode.

The `failover polltime unit msec [time]` represents the time interval to check the existence of the standby unit by polling hello messages.

Similarly, the `failover holdtime unit msec [time]` represents the time period during which a unit must receive a hello message on the failover link, after which the peer unit is declared to have failed.

Refer to [failover polltime](#) for more information.

[WARNING: Failover message decryption failure.](#)

Error message:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

This problem occurs due to failover key configuration. In order to resolve this issue, remove the failover key, and configure the new shared key.

[Related Information](#)

- [Cisco 500 Series PIX Support Page](#)
- [Firewall Services Module \(FWSM\) Failover Configuration](#)
- [FWSM Failover Troubleshooting](#)
- [How Failover Works on the Cisco Secure PIX Firewall](#)
- [Cisco 5500 Series Adaptive Security Appliance Support Page](#)
- [Technical Support & Documentation - Cisco Systems](#)