CHAPTER 37

Configuring Failover

The Failover page provides access to failover settings for the selected security appliance. The available settings and the overall appearance of the Failover page may change slightly, depending upon the type of device selected, its mode of operation (routed or transparent), and its context mode (single or multiple).

In other words, how you configure failover depends upon both the operating mode and the security context of the security appliance.

Please note the following caveats when assigning an interface as a failover link:

- You can define the interface in the Using the Add/Edit Interface Dialog Box, page 35-6, but do not configure it. In particular, **do not specify an interface Name**, as this parameter disqualifies the interface from being used as the failover link.
- On an ASA 5505, an interface assigned as the backup for another interface cannot be used as a failover link (although no checking is performed to prevent this).
- Do not assign a PPPoE-enabled interface as a failover link. PPPoE and Failover should not be configured on the same device interface (although no checking is performed to prevent this).
- A failover interface cannot use the same IP address as another interface, especially the Management IP address (although no checking is performed to prevent this).

Note also that after you assign an interface as a failover link, the interface is listed on the Interfaces page, but you cannot edit or delete the interface from that page. The only exception is if you set a physical interface to be the stateful failover link—you can configure its speed and duplex.

This chapter contains the following topics:

Understanding Failover

Failover lets you set up two identical security appliances such that one will take over firewall operations if the other fails. Using a pair of security appliances, you can provide high system availability without operator intervention.

The linked security appliances communicate failover information over a dedicated link. This failover link can be either a LAN-based connection or, on PIX security appliances, a dedicated serial failover cable. The following information is communicated over the failover link:

- Current failover state (active or standby)
- "Hello" messages (keep-alives)
- Network link status
- MAC address exchange
- Configuration replication

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords, and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing failover communications with a failover key, particularly if you are using the security appliance to terminate VPN tunnels.

Cisco security appliances support two types of failover:

- **Active/Standby** – The *active* security appliance inspects all network traffic, while the *standby* security appliance remains idle until a failure occurs on the active appliance. Changes to the configuration of the active security appliance are transmitted over the failover link to the standby security appliance.

  When failover occurs, the standby security appliance becomes the active unit, and it assumes the IP and MAC addresses of the previously active unit. Because other devices on the network do not see any changes in the IP or MAC addresses, ARP entries do not change or time-out anywhere on the network.

  Active/Standby failover is available to security appliances operating in single- or multiple-context mode. In single-context mode, only Active/Standby failover is available, and all failover configuration is by means of the Failover page.

  Note When using Active/Standby failover, you must make all configuration changes on the active unit. The active unit automatically replicates the changes to the standby unit. The standby unit should not be imported or added to the Security Manager device list.

  Also, you must manually copy the authentication certificate from the active device to the standby device. See Additional Steps for an Active/Standby Failover Configuration, page 37-7 for additional information.

- **Active/Active** – Both security appliances inspect network traffic by alternating their roles—such that one is active and one is standby—on a per context basis. This means Active/Active failover is available only on security appliances operating in multiple-context mode.

  However, Active/Active failover is not required in multiple-context mode. That is, on a device operating in multiple-context mode, you can configure Active/Standby or Active/Active failover. In either case, you provide system-level failover settings in the system context, and context-level failover settings in the individual security contexts.

  See Active/Active Failover, page 37-3 for additional information about this topic.

In addition, failover can be stateless or stateful:

- **Stateless** – Also referred to as *regular* failover. With stateless failover, all active connections are dropped when failover occurs. Clients need to re-establish connections when the new active unit takes over.

- **Stateful** – The active unit in the failover pair continually passes per-connection state information to the standby unit. When failover occurs, the same connection information is available on the new active unit. Supported end-user applications are not required to reconnect to maintain the current communication session.

  See Stateful Failover, page 37-4 for more information.

Active/Active Failover

Active/Active failover is available only on security appliances operating in multiple-context mode. In an Active/Active failover configuration, both security appliances inspect network traffic, on a per-context basis. That is, for each context, one of the appliances is the active device, while the other is the standby device.

The active and standby roles are assigned over the complete set of security contexts, more or less arbitrarily.

To enable Active/Active failover on the security appliance, you must assign the security contexts to one of two failover groups. A failover group is a simply a logical group of one or more security contexts. You should specify failover group assignments on the unit that will have failover group 1 in the active state. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.

As in Active/Standby failover, each unit in an Active/Active failover pair is given a primary or secondary designation. Unlike Active/Standby failover, this designation does not indicate which unit is active when both units start simultaneously. Each failover group in the configuration is given a primary or secondary role preference. This preference determines the unit on which the contexts in the failover group appear in the active state when both units start simultaneously. You can have 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, balancing the traffic across the devices.

Note To reliably manage security contexts in Active/Active failover mode, Cisco Security Manager requires an IP address for the management interface of each context so that it can communicate directly with the active security context of a failover pair.

Initial configuration synchronization occurs when one or both units start. This synchronization occurs as follows:

- When both units start simultaneously, the configuration is synchronized from the primary unit to the secondary unit.
- When one unit starts while the other unit is already active, the unit that is starting up receives the configuration from the already active unit.

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

- 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 A 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.

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

Note When bootstrapping the peer devices in an Active/Active Failover configuration, the bootstrap configurations are only applied to the system contexts of the respective failover peer devices.

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, 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.

Stateful Failover

Note Stateful failover is not supported on the ASA 5505 appliance.

When stateful failover is enabled, the active unit in the failover pair continually updates the current connection-state information on the standby unit. When failover occurs, supported end-user applications are not required to reconnect to maintain the current communication session.

Note The IP and MAC addresses for the state and LAN failover links do not change at failover.

To employ stateful failover, you must configure a link to pass all state information to the standby unit. If you are using a LAN failover connection rather than the serial failover interface (which is available only on the PIX platform), you can use the same interface for the state link and the failover link. However, we recommend that you use a dedicated interface for passing state information to the standby unit.

The following information is passed to the standby unit when stateful failover is enabled:

- NAT translation table
- TCP connection table (except for HTTP), including the timeout connection
- HTTP connection states (if HTTP replication is enabled)
- H.323, SIP and MGCP UDP media connections
- The system clock
- The ISAKMP and IPsec SA table

The following information is not copied to the standby unit when stateful failover is enabled:

- HTTP connection table (unless HTTP replication is enabled)
- The user authentication (uauth) table
- The ARP table
- Routing tables

Basic Failover Configuration

The following steps describe basic failover configuration. Please note the following caveats when assigning an interface as a failover link:

- You can define the interface in the Using the Add/Edit Interface Dialog Box, page 35-6, but do not configure it. In particular, **do not specify an interface Name**, as this parameter disqualifies the interface from being used as the failover link.
- On an ASA 5505, an interface assigned as the backup for another interface cannot be used as a failover link (although no checking is performed to prevent this).
- Do not assign a PPPoE-enabled interface as a failover link. PPPoE and Failover should not be configured on the same device interface (although no checking is performed to prevent this).
- A Failover interface cannot use the same IP address as another interface, especially the Management IP address (although no checking is performed to prevent this).

Note When you save a failover configuration, it is applied to both the security appliance and the failover peer.

Related Topics

- Additional Steps for an Active/Standby Failover Configuration, page 37-7
- Failover Policies, page 37-8

Step 1 Ensure Device View is your present application view; if necessary, click the **Device View** button on the toolbar.

Note For more information on using the Device View to configure device policies, see Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-27.

Step 2 Select the appliance you want to configure.

Step 3 Expand the **Platform** entry in the Device Policy selector, then expand **Device Admin** and select **Failover**.

The Failover page is displayed.

Step 4 (PIX only) Choose the Failover Method: **Serial Cable** or **LAN Based**.

Step 5 Select **Enable Failover** to enable failover on this appliance.

Step 6 Click the Bootstrap button to open the Bootstrap configuration for LAN failover dialog box, which provides bootstrap configurations that can be applied to the primary and secondary devices in a LAN failover configuration. See Bootstrap Configuration for LAN Failover Dialog Box, page 37-24 for more information.

Step 7 (Multiple-context devices only) In the Configuration section, select the failover mode: **Active/Active** or **Active/Standby**.

Step 8 (Optional) Click the Settings button to open the Settings dialog box for the selected device. The contents of the Settings dialog box depend on the type of device, and whether it is operating in single or multiple mode—some options may not be available. Refer to the following sections:

- Settings Dialog Box, page 37-18 (ASA/PIX 7+)
- Advanced Settings Dialog Box, page 37-14 (FWSM)

Step 9 (Optional) Follow these steps to configure an interface for **LAN Failover** communications between the two devices:

a. Assign a device **Interface** for LAN-based communications, and then press the Tab key on your keyboard to update the page.

On PIX and ASA devices, this drop-down list displays the interfaces defined on the device. You can type in a port ID (e.g., *gigabitethernet1*), or you can choose the port if you have already defined the interface (see Using the Add/Edit Interface Dialog Box, page 35-6).

On an FWSM, the Interface list is not populated with VLAN IDs; you must enter the numeric ID of the VLAN you wish to use.

Note In both cases, this cannot be a Named interface, nor can the interface be configured for PPPoE.

b. Provide a **Logical Name** for this failover interface.

c. Enter the **Active IP** address for failover communications.

d. Enter a **Standby IP** address for failover communications. The Standby IP address is used on the security appliance that is currently the standby unit.

e. Enter the **Subnet Mask** for both IP addresses. Both must be on the same subnet.

Step 10 (Optional) Follow these steps to enable and configure an interface for **Stateful Failover** communications between the two devices:

a. Assign a device **Interface** for update communications, and then press the Tab key on your keyboard to update the page.

You can type in a port ID (e.g., *gigabitethernet1*), or you can choose the port if you have already defined the interface (see Using the Add/Edit Interface Dialog Box, page 35-6; note that this cannot be a Named interface).

Note On an FWSM, this is a **VLAN** interface.

b. Provide a **Logical Name** for this interface.

c. Enter the **Active IP** address for connection updates.

d. Enter a **Standby IP** address for update communications.

e. Enter the **Subnet Mask** for both IP addresses. Both must be on the same subnet.

f. Select **Enable HTTP Replication** to preserve HTTP connection information.

Connection information is communicated to the standby unit for all TCP protocols except HTTP, because HTTP connections are generally short-lived. Select this option to maintain HTTP connections during failover.

Step 11 Provide a communications-encryption key: enter a **Shared Key** and then repeat it in the **Confirm** field. Be sure to enter the same key on both devices. (Not available on FWSM versions prior to 3.1)

The Shared Key can be any arbitrary string of up to 63 alphanumeric characters. If **HEX** is checked, the Shared Key is an arbitrary string of exactly 32 hexadecimal characters. (The HEX option is available only on PIX/ASA version 7.0.5 and later, and FWSM versions 3.1.3 and later.)

Note This step is optional, but we strongly recommend encrypting failover communications.

Step 12 To specify a failover reconnect timeout value for asymmetrically routed sessions, enter a length of time in the **Timeout** field, in the form hh:mm:ss (the minutes and seconds values are optional). If the field is blank (the default), or contains a zero, reconnections are prevented. Setting this value to -1 disables the timeout, allowing connections to reconnect after any amount of time.

Step 13 (FWSM only) – Configured interfaces are listed in the Interface Configuration table. To edit the failover configuration for a listed interface, select it and click the Edit Row button to open the Edit Failover Interface Configuration Dialog Box (FWSM), page 37-15.

Additional Steps for an Active/Standby Failover Configuration

Cisco Security Manager lets you authenticate a PIX/ASA/FWSM device by validating the certificate installed on the device. When configuring firewalls in an active/standby failover configuration, you must manually copy the certificate from the active device to the standby device so that Security Manager can communicate with the standby device after a failover occurs.

The following procedures describe how to export or display the identity certificate, CA certificate, and keys for a security appliances in your network using ASDM, and then import that information onto a standby device using ASDM.

- Exporting the Certificate to a File or PKCS12 data, page 37-7
- Importing the Certificate onto the Standby Device, page 37-8

Exporting the Certificate to a File or PKCS12 data

To export a trustpoint configuration, follow these steps using ASDM:

Step 1 Go to Configuration > Features > Device Administration > Certificate > Trustpoint > Export.

Step 2 Fill in the Trustpoint Name, Encryption Passphrase, and Confirm Passphrase fields. For information on these fields, click Help.

Step 3 Select a method for exporting the trustpoint configuration.

- Export to a File—Type the filename or browse for the file.
- Display the trustpoint configuration in PKCS12 format—Display the entire trustpoint configuration in a text box and then copy it for importing. For more information, click Help.

Step 4 Click **Export**.

Importing the Certificate onto the Standby Device

To import a trustpoint configuration, follow these steps using ASDM:

Step 1 Go to Configuration > Features > Device Administration > Certificate > Trustpoint > Import.

Step 2 Fill in the Trustpoint Name, Decryption Passphrase, and Confirm Passphrase fields. For information on these fields, click Help. The decryption passphrase is the same as the encryption passphrase used when the trustpoint configuration was exported.

Step 3 Select a method for importing the trustpoint configuration.

- Import from a File—Type the filename or browse for the file.
- Enter the trustpoint configuration in PKCS12 format—Paste the entire trustpoint configuration from the exported source into a text box. For more information, click Help.

Failover Policies

This section lists the pages that describe configuring failover on various types of security appliances; the pages are organized by device type.

PIX 6.x Firewalls

- Failover Page (PIX 6.x), page 37-9
  - Edit Failover Interface Configuration Dialog Box (PIX 6.x), page 37-10
  - Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Firewall Services Modules

- Failover Page (FWSM), page 37-11
  - Advanced Settings Dialog Box, page 37-14
  - Add Interface MAC Address Dialog Box, page 37-23
  - Edit Failover Interface Configuration Dialog Box (FWSM), page 37-15
  - Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Adaptive Security Appliances and PIX 7.0 Firewalls

- Failover Page (ASA/PIX 7.x), page 37-16
  - Settings Dialog Box, page 37-18
  - Add Failover Group Dialog Box, page 37-21
  - Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x), page 37-22
  - Add Interface MAC Address Dialog Box, page 37-23
  - Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Failover Page (PIX 6.x)

Use the Failover page to configure failover settings for a PIX 6.x Firewall.

Navigation Path

To access this feature, select a firewall device in Device View and then select **Platform > Device Admin > Failover** from the Device Policy selector.

Related Topics

- Failover Policies, page 37-8
- Additional Steps for an Active/Standby Failover Configuration, page 37-7
- Edit Failover Interface Configuration Dialog Box (PIX 6.x), page 37-10
- Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Field Reference

Table 37-1 Failover Page (PIX 6.x)

Element	Description
Failover	
Failover Method	Choose the type of failover link: Serial Cable or LAN Based.
Enable Failover	Check this box to enable failover on this device. **Note** To enable failover, you must ensure that both devices have the same software version, activation key type, Flash memory, and RAM.
Failover Poll Time	Specifies how long failover waits before determining if other devices remain available between primary and standby devices over all network interfaces and failover cable. Values can range from 3 to 15 seconds; default is 15.
LAN-Based Failover	
Interface	Choose the interface to be used for LAN-based failover. If “Not Selected” is chosen, LAN-Based Failover is disabled.
Shared Key	Used to encrypt communication between primary and standby devices. Value can be any string.
Confirm	Re-enter the Shared Key.
Stateful Failover	
Interface	Choose the interface to be used for Stateful Failover. If “Not Selected” is chosen, Stateful Failover is disabled. **Note** You must choose a fast LAN link from the list (for example, 100full, 1000full, or 1000sxfull).
Enable HTTP Replication	Enables stateful failover to copy active HTTP sessions to standby PIX Firewall.

Table 37-1 Failover Page (PIX 6.x) (Continued)

Element	Description
Failover Interface Table	
Interface	Displays the name of the interface on the active firewall device to be used for communication with standby device for failover. When configured for stateful failover, the interface is connected directly to the standby device.
Active IP Address	Displays the IP address of the active interface. This address is used by the standby device to communicate with the active device. The address must be on the same network as the system IP address. **Tip** You can use this IP address with the ping tool to check the status of the active device.
Standby IP Address	Displays the IP address of the standby interface. This address is used by the active device to communicate with the standby device. The address must be on same network as system IP address. **Tip** You can use this IP address with the ping tool to check the status of the standby device.
Active MAC Address	Displays the MAC address of the active interface in hexadecimal format (for example, 0123.4567.89ab).
Standby MAC Address	Displays the MAC address of the standby interface in hexadecimal format (for example, 0123.4567.89ab).
Edit Row button	Click to display the Edit Failover Interface Configuration dialog box.

Edit Failover Interface Configuration Dialog Box (PIX 6.x)

Use the Edit Failover Interface Configuration dialog box to configure a failover interface for PIX 6.x devices.

Note The failover interface cannot be configured for PPPoE.

Navigation Path

You can access the Edit Failover Interface Configuration dialog box from the Failover page. For more information about the Failover page, see Failover Page (PIX 6.x), page 37-9.

Related Topics

- Failover Policies, page 37-8
- Failover Page (PIX 6.x), page 37-9

Field Reference

Table 37-2 Edit Failover Interface Configuration Dialog Box (PIX 6.x)

Element	Description
Interface	Displays the name of the interface on the active firewall device to be used for communication with standby device for failover. When configured for stateful failover, the interface is connected directly to the standby device.
Active IP Address	Displays the IP address of the active interface. This address is used by the standby device to communicate with the active device. The address must be on the same network as the system IP address. **Tip** You can use this IP address with the ping tool to check the status of the active device.
Netmask	Displays the netmask of the active device.
Standby IP Address	Specify the IP address of the standby interface. This address is used by the active device to communicate with the standby device. The address must be on the same network as the system IP address. **Tip** You can use this IP address with the ping tool to check the status of the standby device.
Failover MAC Addresses	
Active MAC Address	Specifies the MAC address of the active interface in hexadecimal format (for example, 0123.4567.89ab).
Standby MAC Address	Specifies the MAC address of the standby interface in hexadecimal format (for example, 0123.4567.89ab).

Failover Page (FWSM)

Use the Failover page to configure basic failover settings for FWSMs.

Navigation Path

To access this feature, select a FWSM in Device View and then select **Platform > Device Admin > Failover** from the Device Policy selector.

Related Topics

- Failover Policies, page 37-8
- Additional Steps for an Active/Standby Failover Configuration, page 37-7
- Advanced Settings Dialog Box, page 37-14
- Edit Failover Interface Configuration Dialog Box (FWSM), page 37-15
- Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Field Reference

Table 37-3 Failover Page (FWSM)

Element	Description
Enable Failover	Specifies whether failover is enabled on this device. You must configure the logical LAN failover interface and, optionally, the stateful failover interface. **Note** To enable failover, you must ensure that both devices have the same software version, activation key type, Flash memory, and RAM.
Configuration (FWSM 3.x only)	
Active/Active option (FWSM 3.x only)	In an Active/Active failover configuration, both security appliances pass network traffic. Active/Active failover is only available to security appliances in multiple context mode. To enable Active/Active failover on the security appliance, you must create failover groups. If you enable failover without creating failover groups, you are enabling Active/Standby failover. A failover group is a logical group of one or more security contexts. You can create two failover groups on the security appliance. You should create the failover groups on the unit that will have failover group 1 in the active state. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.
Active/Standby option (FWSM 3.x only)	In an Active/Standby configuration, the active security appliance handles all network traffic passing through the failover pair. The standby security appliance does not handle network traffic until a failure occurs on the active security appliance. Whenever the configuration of the active security appliance changes, it sends configuration information over the failover link to the standby security appliance. When a failover occurs, the standby security appliance becomes the active unit. It assumes the IP and MAC addresses of the previously active unit. Because the other devices on the network do not see any changes in the IP or MAC addresses, ARP entries do not change or time out anywhere on the network. Active/Standby failover is available to security appliances in single mode or multiple mode.
Settings button	Click to display the Advance Settings dialog box. See Advanced Settings Dialog Box, page 37-14 for more information.
LAN Failover	
VLAN	Enter the numeric ID of the VLAN interface you are using for the failover link; for example, 11. This list is not automatically populated with VLAN IDs.
Logical Name	The logical name of the VLAN interface on the active firewall device that communicates with the standby device for failover. When configured for stateful failover, the interface is directly connected to the standby device.
Active IP Address	Specifies the IP address of the active interface.

Table 37-3 Failover Page (FWSM) (Continued)

Element	Description
Standby IP Address	Specifies the IP address of the standby interface.
Subnet Mask	Mask that corresponds with active and standby IP addresses.
State Failover	
VLAN	Enter the numeric ID of the VLAN interface you are using for the failover link; for example, 12. This list is not automatically populated with VLAN IDs.
Logical Name	The logical name of the interface on active firewall device that communicates with the standby device for failover. When configured for stateful failover, the interface is directly connected to the standby device.
Active IP Address	Specifies the IP address of the active interface.
Standby IP Address	Specifies the IP address of the standby interface.
Subnet Mask	Mask that corresponds with active and standby IP addresses.
Enable HTTP Replication check box	Enables stateful failover to copy active HTTP sessions to a standby firewall.
Suspend Configuration Synchronization (FWSM 2.3 only)	When selected, configurations between the active and standby device are no longer synchronized. **Note** You cannot disable this feature using the Security Manager user interface. To disable this feature after enabling it in Security Manager, issue the **no failover suspend-config-sync** command directly on the device, or by using the FlexConfig feature. For more information on FlexConfigs, see Understanding FlexConfig Policies and Policy Objects, page 7-1.
Shared Key (FWSM 3.x only)	To encrypt and authenticate the communication between failover peers, specify a shared secret in the Shared Key field for the active unit of an Active/Standby failover pair or on the unit that has failover group 1 in the active state of an Active/Active failover pair. The shared key can be from 1 to 63 characters and can be any combination of numbers, letters, or punctuation. **Caution** All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If FWSM is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using FWSM to terminate VPN tunnels.

Advanced Settings Dialog Box

The Advanced Settings dialog box lets you configure additional failover settings for FWSMs.

Note The following reference table presents all fields that can be presented in the Advanced Settings dialog box. The fields actually presented depend on operating mode (routed or transparent) and whether the device is hosting single or multiple contexts.

Navigation Path

You can access the Advance dialog box by clicking the Settings button on the Failover page. See Failover Page (FWSM), page 37-11 for more information.

Related Topics

- Failover Policies, page 37-8
- Failover Page (FWSM), page 37-11
- Add Interface MAC Address Dialog Box, page 37-23

Field Reference

Table 37-4 Advance Dialog Box

Element	Description
Interface Policy	
Number of failed interfaces	When the number of failed monitored interfaces exceeds this value, the security appliance fails over. The range is between 1 and 250 failures.
Percentage of failed interfaces	When the number of failed monitored interfaces exceeds this percentage, the security appliance fails over.
Failover Poll Time	
Unit Failover	The amount of time between hello messages among units. The range is between 1 and 15 seconds, or between 500 and 999 milliseconds if the msec option is checked.
Unit Hold Time	Sets the time during which a unit must receive a hello message on the failover link, or the unit begins the testing process for peer failure. The range is between 3 and 45 seconds. You cannot enter a value that is less than 3 times the Unit Failover value.
Monitored Interface	The amount of time between polls among interfaces. The range is between 3 and 15 seconds.
Management IP Address	
Active	The IP address of the management interface.
Netmask	The subnet mask for the Active and Standby addresses.
Standby	The management IP address on the standby unit, which must be on the same subnet as the Active IP address. You do not need to identify the Standby address subnet mask.

Table 37-4 Advance Dialog Box (Continued)

Element	Description
Failover Groups	
Group table	This table lists failover groups on the device, with the following information: • Group Number – Numeric identifier for the group. • Preferred Role – Primary or Secondary. • Preempt Enabled – True or false.
Edit row button	Click this button to edit the selected entry in the Failover Groups table; the Edit Failover Group dialog box opens.

Edit Failover Interface Configuration Dialog Box (FWSM)

Use the Edit Failover Interface Configuration dialog box to configure a failover interface for FWSMs.

Note The failover interface cannot be configured for PPPoE.

Navigation Path

You can access the Edit Failover Interface Configuration dialog box from the Failover page. For more information about the Failover page, see Failover Page (FWSM), page 37-11.

Related Topics

- Failover Policies, page 37-8
- Failover Page (FWSM), page 37-11

Field Reference

Table 37-5 Edit Failover Interface Configuration Dialog Box (FWSM)

Element	Description
Interface Name	Identifies the interface name; not editable.
Active IP Address	Identifies the IP address for this interface. This field does not appear if an IP address has not been assigned to the interface.
Standby IP Address	Specifies the IP address of the corresponding interface on the standby failover unit. This field does not appear if an IP address has not been assigned to the interface.

Table 37-5 Edit Failover Interface Configuration Dialog Box (FWSM) (Continued)

Element	Description
Monitor this interface for failure	Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds). Monitored failover interfaces can have the following status: • Unknown—Initial status. This status can also mean the status cannot be determined. • Normal—The interface is receiving traffic. • Testing—Hello messages are not heard on the interface for five poll times. • Link Down—The interface is administratively down. • No Link—The physical link for the interface is down. • Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Failover Page (ASA/PIX 7.x)

Use the Failover page to configure basic failover settings for ASAs and PIX 7.x firewalls.

Navigation Path

To access this feature, select an ASA or PIX 7.x firewall device in Device View and then select **Platform > Device Admin > Failover** from the Device Policy selector.

Related Topics

- Failover Policies, page 37-8
- Additional Steps for an Active/Standby Failover Configuration, page 37-7
- Settings Dialog Box, page 37-18
- Add Failover Group Dialog Box, page 37-21
- Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x), page 37-22
- Add Interface MAC Address Dialog Box, page 37-23
- Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Field Reference

Table 37-6 Failover Page (ASA/PIX 7.x)

Element	Description
Enable Failover	Specifies whether failover is enabled on this device. You must configure the logical LAN failover interface and, optionally, the stateful failover interface. **Note** To enable failover, you must ensure that both devices have the same software version, activation key type, Flash memory, and RAM.
Configuration	
Active/Active option	In an Active/Active failover configuration, both security appliances pass network traffic. Active/Active failover is only available to security appliances in multiple context mode. To enable Active/Active failover on the security appliance, you must create failover groups. If you enable failover without creating failover groups, you are enabling Active/Standby failover. A failover group is a logical group of one or more security contexts. You can create two failover groups on the security appliance. You should create the failover groups on the unit that will have failover group 1 in the active state. The admin context is always a member of failover group 1. Any unassigned security contexts are also members of failover group 1 by default.
Active/Standby option	In an Active/Standby configuration, the active security appliance handles all network traffic passing through the failover pair. The standby security appliance does not handle network traffic until a failure occurs on the active security appliance. Whenever the configuration of the active security appliance changes, it sends configuration information over the failover link to the standby security appliance. When a failover occurs, the standby security appliance becomes the active unit. It assumes the IP and MAC addresses of the previously active unit. Because the other devices on the network do not see any changes in the IP or MAC addresses, ARP entries do not change or time out anywhere on the network. Active/Standby failover is available to security appliances in single mode or multiple mode.
Settings button	Click to display the Settings dialog box. See Settings Dialog Box, page 37-18 for more information.
LAN Failover	
Interface	Interface you are using for the failover link.
Logical Name	The logical name of the interface on the active firewall device to communicate with standby device for failover. When configured for stateful failover, the interface is directly connected to the standby device.
Active IP Address	Specifies the IP address of the active interface.
Standby IP Address	Specifies the IP address of the standby interface.
Subnet Mask	Netmask that corresponds with active and standby IP addresses.

Table 37-6 Failover Page (ASA/PIX 7.x) (Continued)

Element	Description
Bootstrap button	Click to display the Bootstrap Configuration for LAN Failover dialog box. See Bootstrap Configuration for LAN Failover Dialog Box, page 37-24 for more information.
State Failover	
Interface	Interface you are using for the stateful failover link.
Logical Name	The logical name of the interface on the active firewall device to communicate with standby device for failover. When configured for stateful failover, the interface is directly connected to the standby device.
Active IP Address	Specifies the IP address of the active interface.
Standby IP Address	Specifies the IP address of the standby interface.
Subnet Mask	Netmask that corresponds with active and standby IP addresses.
Enable HTTP Replication	When selected, enables stateful failover to copy active HTTP sessions to standby firewall.
Shared Key	Used to encrypt communication between primary and standby devices. Value can be any string.

Settings Dialog Box

The Settings dialog box lets you define criteria for when failover should occur on an ASA or PIX 7.x appliance.

Navigation Path

You can access the Settings dialog box by clicking the Settings button on the Failover page. For more information, see Failover Page (ASA/PIX 7.x), page 37-16.

Note The following reference table presents all fields that can be presented in the Settings dialog box. The fields actually presented depend on operating mode (routed or transparent) and whether the device is hosting single or multiple contexts.

Related Topics

- Failover Policies, page 37-8
- Failover Page (ASA/PIX 7.x), page 37-16
- Add Failover Group Dialog Box, page 37-21
- Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x), page 37-22
- Add Interface MAC Address Dialog Box, page 37-23
- Bootstrap Configuration for LAN Failover Dialog Box, page 37-24

Field Reference

Table 37-7 Settings Dialog Box

Element	Description
Interface Policy	
Number of failed interfaces	When the number of failed monitored interfaces exceeds this value, the security appliance fails over. The range is between 1 and 250 failures.
Percentage of failed interfaces	When the number of failed monitored interfaces exceeds this percentage, the security appliance fails over.
Failover Poll Time	
Unit Failover	The amount of time between hello messages among units. The range is between 1 and 15 seconds, or between 200 and 999 milliseconds if the msec option is checked.
Unit Hold Time	Sets the time during which a unit must receive a hello message on the failover link, or the unit begins the testing process for peer failure. The range is between 3 and 45 seconds, or between 800 and 999 milliseconds if the msec option is checked. You cannot enter a value that is less than three times the Unit Failover value.
Monitored Interface	The amount of time between polls among interfaces. The range is between 3 and 15 seconds, or between 500 and 999 milliseconds if the msec option is checked.
Interface Hold Time	Sets the time during which a data interface must receive a hello message, after which the peer is declared failed. Valid values are from 5 to 75 seconds.
Failover Groups	
Group Number	Specifies the failover group number. This number is used when assigning contexts to failover groups.
Preferred Role	Specifies the unit in the failover pair, primary or secondary, on which the failover group appears in the active state when both units start up simultaneously or when the preempt option is selected. You can have both failover groups 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, balancing the traffic across the devices.
Preempt Enabled	Specifies whether the unit that is the preferred failover device for this failover group should become the active unit after rebooting.
Preempt Delay	Specifies the number of seconds that the preferred failover device should wait after rebooting before taking over as the active unit for this failover group. The range is between 0 and 1200 seconds.
Interface Policy	Specifies either the number of monitored interface failures or the percentage of failures that are allowed before the group fails over. The range is between 1 and 250 failures or 1 and 100 percent.
Interface Poll Time	Specifies the amount of time between polls among interfaces. The range is between 3 and 15 seconds.

Table 37-7 Settings Dialog Box (Continued)

Element	Description
Replicate HTTP	Identifies whether Stateful Failover should copy active HTTP sessions to the standby firewall for this failover group. If you do not allow HTTP replication, HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link. This setting overrides the HTTP replication setting on the Setup tab.
MAC Address	Identifies the MAC address of the active interface.
MAC Address Mapping	
Physical Interface	Specifies the physical interface for which failover virtual MAC addresses are configured.
Active MAC Address	Specifies the MAC address of the active interface in hexadecimal format (for example, 0123.4567.89ab).
Standby MAC Address	Specifies the MAC address of the standby interface in hexadecimal format (for example, 0123.4567.89ab).
Monitor Interface Configuration	
Interface Name	Displays the name of the interface.
Is Monitored	Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds). Monitored failover interfaces can have the following status: • Unknown—Initial status. This status can also mean the status cannot be determined. • Normal—The interface is receiving traffic. • Testing—Hello messages are not heard on the interface for five poll times. • Link Down—The interface is administratively down. • No Link—The physical link for the interface is down. • Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.
Edit Row button	Click to display the Edit Failover Interface Configuration dialog box to edit a failover interface configuration.
Management IP Address	
Active	Specifies the management IP address of the active device.
Netmask	Specifies the netmask that corresponds with the active and standby IP addresses.
Standby	Specifies the management IP address of the standby device.

Add Failover Group Dialog Box

Use the Add Failover Group dialog box to define failover groups for an Active/Active failover configuration.

Navigation Path

You can access the Add Failover Group dialog box from the Failover page. For more information, see Failover Page (ASA/PIX 7.x), page 37-16.

Related Topics

- Failover Policies, page 37-8
- Failover Page (ASA/PIX 7.x), page 37-16

Field Reference

Table 37-8 Add Failover Group Dialog Box

Element	Description
Preferred Role	Specifies the unit in the failover pair, primary or secondary, on which the failover group appears in the active state when both units start up simultaneously or when the preempt option is selected. You can have both failover groups 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, balancing the traffic across the devices.
"Preempt after booting with optional delay of"	Specifies the number of seconds that the preferred failover device should wait after rebooting before taking over as the active unit for this failover group. The range is between 0 and 1200 seconds.
Interface Policy	Select the failover policy for this interface: • Number of failed interfaces that triggers failover • Percentage of failed interfaces that triggers failover • Use system failover interface policy
Poll time interval for monitored interfaces	Specifies the amount of time between polls among interfaces. The range is between 3 and 15 seconds.
Enable HTTP Replication	Identifies whether Stateful Failover should copy active HTTP sessions to the standby firewall for this failover group. If you do not allow HTTP replication, HTTP connections are disconnected at failover. Disabling HTTP replication reduces the amount of traffic on the state link. This setting overrides the HTTP replication setting on the Setup tab.
Interface Table	
Physical Interface	Specifies the physical interface for which failover virtual MAC addresses are configured.
Active MAC Address	Specifies the MAC address of the active interface in hexadecimal format (for example, 0123.4567.89ab).
Standby MAC Address	Specifies the MAC address of the standby interface in hexadecimal format (for example, 0123.4567.89ab).

Table 37-8 Add Failover Group Dialog Box (Continued)

Element	Description
Add	Click to display the dialog box to define a failover interface association.
Edit	Click to display the dialog box to edit a failover interface association.
Delete	Click to delete the selected failover interface association.

Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x)

Use the Edit Failover Interface Configuration dialog box to define the standby IP address for an interface and to specify whether the status of the interface should be monitored.

Note The failover interface cannot be configured for PPPoE.

Navigation Path

You can access the Edit Failover Interface Configuration dialog box from the Failover page. For more information, see Failover Page (ASA/PIX 7.x), page 37-16.

Related Topics

- Failover Policies, page 37-8
- Failover Page (ASA/PIX 7.x), page 37-16
- Add Failover Group Dialog Box, page 37-21

Field Reference

Table 37-9 Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x)

Element	Description
Interface Name	Identifies the interface name.
Active IP Address	Identifies the IP address for this interface. This field does not appear if an IP address has not been assigned to the interface.
Standby IP Address	Specifies the IP address of the corresponding interface on the standby failover unit. This field does not appear if an IP address has not been assigned to the interface.

Table 37-9 Edit Failover Interface Configuration Dialog Box (ASA/PIX 7.x) (Continued)

Element	Description
Monitor this interface for failure	Specifies whether this interface is monitored for failure. The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged between the security appliance failover pair during every interface poll time period. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds). Monitored failover interfaces can have the following status: • Unknown—Initial status. This status can also mean the status cannot be determined. • Normal—The interface is receiving traffic. • Testing—Hello messages are not heard on the interface for five poll times. • Link Down—The interface is administratively down. • No Link—The physical link for the interface is down. • Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Add Interface MAC Address Dialog Box

The Add Interface MAC Address dialog box allows you to define the MAC addresses of interfaces for ASA, FWSM 3.x and PIX 7.x security appliances that are configured for failover.

Related Topics

- Failover Policies, page 37-8
- Failover Page (ASA/PIX 7.x), page 37-16
- Settings Dialog Box, page 37-18

Field Reference

Table 37-10 Add Interface MAC Address Dialog Box

Element	Description
Physical Interface	Specifies the physical interface for which failover virtual MAC addresses are configured.
MAC Address	
Active Interface	Specifies the MAC address of the active interface in hexadecimal format (for example, 0123.4567.89ab).
Standby Interface	Specifies the MAC address of the standby interface in hexadecimal format (for example, 0123.4567.89ab).

Bootstrap Configuration for LAN Failover Dialog Box

The Bootstrap Configuration for LAN Failover dialog box provides you with bootstrap configuration that can be applied to the primary and secondary devices in a LAN failover configuration.

Navigation Path

You can access the Bootstrap Configuration for LAN Failover dialog box from the Failover page. For more information about the Failover page, see:

- Failover Page (PIX 6.x), page 37-9
- Failover Page (FWSM), page 37-11
- Failover Page (ASA/PIX 7.x), page 37-16

Related Topics

- Failover Policies, page 37-8
- Additional Steps for an Active/Standby Failover Configuration, page 37-7

Field Reference

Table 37-11 Bootstrap Configuration for LAN Failover Dialog Box

Element	Description
Primary	Contains the bootstrap configuration for the primary device. Open a console connection to the primary device and then paste this configuration to activate failover on the device.
Secondary	Contains the bootstrap configuration for the secondary device. After the primary device becomes active, open a console connection to the secondary device and then paste this configuration to activate failover on the device.

Note For Active/Active Failover, the bootstrap configurations are only applied to the system contexts of the respective failover peer devices.