11

Failover

Terms you’ll need to understand:

✓ Primary firewall

✓ Secondary firewall

✓ Serial cable failover

✓ LAN-based failover

✓ Non-stateful failover

✓ Stateful failover

✓ Replication

✓ Primary firewall

Techniques you’ll need to master:

✓ Configuring stateful firewalls

✓ Failing back

Previous chapters have talked about several features the PIX firewall can provide. These features can protect systems from access and reconnaissance attacks and enable you to control user access with AAA services. These features are excellent at what they do; however, they rely on one firewall connection. Therefore, that firewall must be functioning and online to allow traffic to flow. If that one firewall were to fail, all traffic would cease.

The PIX firewall addresses this single point of failure with a technology called *failover*. Failover enables two firewalls to work together to provide basic fault tolerance in the event the primary firewall fails. This chapter provides an overview of the failover feature offered by the PIX firewall.

Introduction to Failover

The PIX firewall provides the capability to support a backup-generator-style of fault tolerance. If the primary unit goes down, the secondary unit comes online to take its place. However, the secondary does not provide load-balancing capabilities, but rather a hot standby approach if the primary fails.

To support failover, firewalls are interconnected with a cable to provide a means of monitoring and configuring each other. This interconnection is provided by special serial cables or via a dedicated Ethernet interface cable called a *LAN-based* cable. Figure 11.1 displays a typical configuration of a primary and secondary firewall configuration.

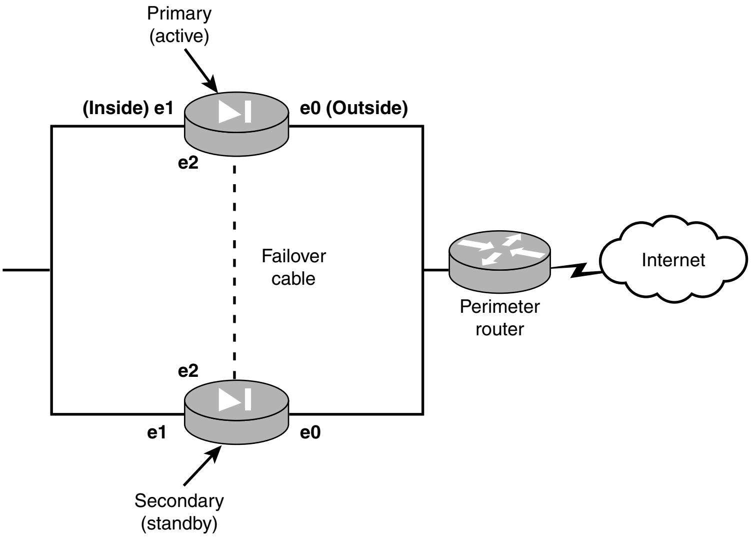

Figure 11.1 A basic failover configuration.

Non-stateful Failover

Non-stateful failover is the most basic solution of the failover options. When two firewalls are interconnected with either a serial cable or dedicated Ethernet interface, they send only RAM configuration information and session information across. If the primary (active) firewall cannot be detected across any interface, the secondary (standby) firewall assumes the active role, subsequently inheriting the primary's IP addresses and MAC address, and effectively become the operating firewall.

The primary, on the other hand, assumes the IP address and MAC address of the secondary firewall and stops passing traffic. When this happens, all xlate and connection table entries are lost and will have to be reestablished. For example, if Jack had an FTP connection through the firewall, when failover occurred Jack would have to reestablish a connection through the firewall to make his FTP operational. Figure 11.1 is a non-stateful failover configuration.

When a primary interface fails (unplugged or broken cable), the secondary becomes the active firewall and inherits the primary's IP addresses. The primary moves into a fail or standby state and assumes the secondary firewall's IP addresses.

Stateful Failover

Stateful failover behaves in a similar way to non-stateful when a failover occurs. However, xlate and connection table information is maintained continually across a second dedicated Ethernet connection between the firewalls. When failover occurs, the secondary already contains the xlate and connection table information, providing users with a seamless failover. For example, if Jack had an FTP connection before the failover, that connection would still be maintained in the xlate and connection tables when the secondary took over. Figure 11.2 shows a stateful failover configuration.

The second Ethernet connection used for stateful failover must be a dedicated link between the two firewalls. The link can be FDDI, 100Mbps Fast Ethernet, or Gigabit Ethernet. When using 100Mbps Fast Ethernet, the connection is made using either a CAT 5 crossover cable or a dedicated full-duplex VLAN switch connection. Figure 11.2 shows the stateful connection using Ethernet 2 interfaces.

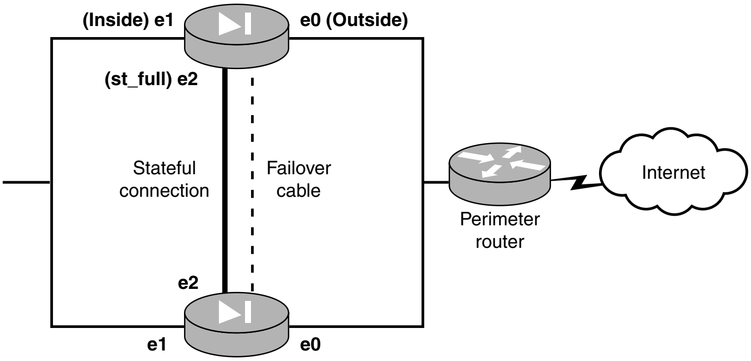

Figure 11.2 A stateful failover configuration.

ALERT

Stateful failover requires an extra interface to connect the two firewalls. This interface carries stateful information to keep the firewall's xlate and connection tables in sync.

Cable-based and LAN-based Configurations

Cable-based (serial) and LAN-based configurations dictate how the primary and secondary firewalls are linked together to provide failover support. The following provides an overview of each.

ALERT

Both cable-based and LAN-based configurations support stateful failover solutions.

Cable-based Configurations

A cable-based configuration—also known as serial-based—requires a special serial cable from Cisco to connect the firewalls. The cable can be up to 6 feet in length and connects the dedicated failover port on the PIX models 515 and above. Before software version 5.2, the maximum speed that software provided across the serial cable was only 9.6Kbps; however, it's now 115Kbps.

This connection provides a means to replicate RAM information from the active to the standby firewall and provides detection of power loss on the other side. However, the limiting factor for this setup is that the distance between the firewalls can be only 6 feet.

The special Cisco serial cable allows the detection of power on the other firewall. The cable is also labeled with the words “primary” and “secondary” to make installation easy.

LAN-based Configurations

A LAN-based configuration has been introduced in version 6.2 of the PIX firewall software. This enables the use of a dedicated Ethernet interface to perform the same functions as the serial cable-based configuration does. However, you are no longer restricted by the 6-foot distance limitation.

Some restrictions do exist when using LAN-based configurations. The two interfaces dedicated for LAN-based failover must be on the same subnet, so the two firewalls can’t travel through a router. Another limitation is that the interface is completely dedicated to the failover monitoring and configuration and therefore should not be on the same LAN/broadcast domain as any other device. When linking the two firewalls, you must use a dedicated hub, switch, or VLAN. Please note that you cannot use a CAT 5 crossover cable for this connection. Figure 11.3 shows a typical LAN-based failover configuration.

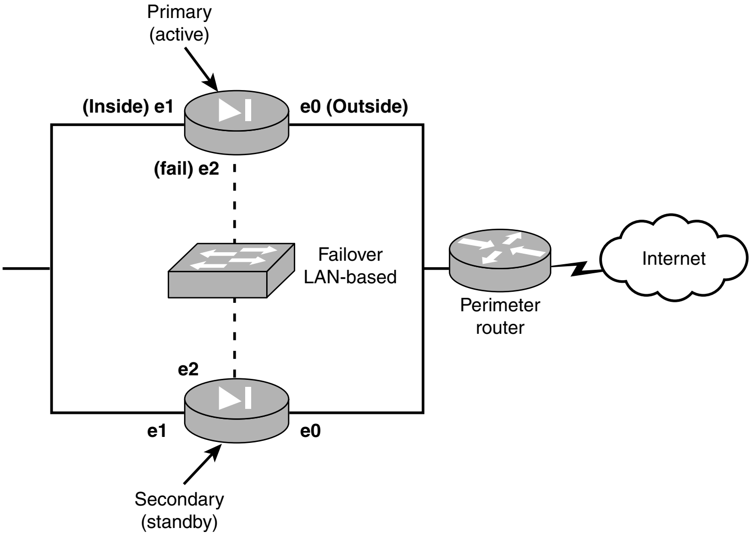

Figure 11.3 A LAN-based configuration.

The LAN-based connection must be through a dedicated hub, switch, or VLAN on a switch—do not use a crossover cable.

Hardware and Software Requirements

Providing firewall failover capabilities involves several basic hardware and software requirements. The firewalls must have the following:

- Same PIX firewall hardware models
- Same amount of RAM memory
- Same amount of flash memory
- Same type and number of interfaces
- Special serial cable (optional)
- Same version of software
- Same activation keys for DES or 3DES

When configuring for failover, firewall models need to be exactly the same all the way down to their memory sizes.

Hardware

The PIX firewalls need to have the same hardware models for failover to work properly, but failover support is not available on all models. The 501, 506, and 506E do not support failover functionality; only the 515 and above models do.

Software

Software on the two firewalls also needs to be the same version number; otherwise, failover might not work properly.

Every model of the PIX firewall, including the 501, uses the same software—activation keys just enable extra features within the software. However, you still cannot use failover on the lower models.

Licensing

Activations keys also need to be installed to enable the failover functionality of the software. Cisco has several licensing features for failover, as listed in Table 11.1.

Table 11.1 Licenses

License	Description
UR	The unrestricted license must be used on the primary (active) firewall and can optionally be used on the secondary (standby) firewall.
FO	The failover license is used for secondary standby modes only.
R	The restricted license cannot be used for either the primary or secondary firewall.

Now that you have seen the various licenses available, Table 11.2 displays the possible primary and secondary licensing combinations.

Table 11.2 Licensing Combinations

	Primary (Active)	Secondary (Standby)
Combination 1	UR	UR
Combination 2	UR	FO

The PIX does not have separate software for failover protection. Only activation keys are necessary to enable the features.

Replication

When two firewalls are interconnected for failover, replication of the RAM configuration file (`running config`) occurs, keeping the standby firewall in sync with the primary firewall.

The following lists the methods by which the primary replicates its running configuration file across to the secondary firewall:

- When the standby starts, it obtains the latest configuration from the active firewall.
- When commands are entered into the active firewall, they are automatically replicated to the secondary firewall's RAM (the running configuration).

- The `write standby` command can be used to force a replication of the entire configuration in memory to the standby firewall.

One important item to note is that replication sends only the running configuration to the standby's RAM; the startup configuration is not sent to flash. Therefore, to save configuration on the standby to flash, you must issue the `write memory` command.

Replication of Stateful Failover

In non-stateful failover configuration, only one cable is used to replicate the running configuration file. Conversely, in stateful failover, two cables are necessary—one for the normal running configuration file replication and another for the xlate table and other such stateful information. The following is a list of what is replicated across in a stateful failover configuration:

- The translation xlate table
- The connection table
- The negotiated fixup protocol ports

However, not all stateful information is sent across. This list of items is not replicated and, as such, is lost when failover occurs:

- The user authentication (`uauth`) table used by AAA services
- The ARP table
- Routing information
- ISAKMP and IPSec security association (SA) tables

Lastly, the following list shows what is sent across the serial or LAN-based failover cables:

- The running configuration replication
- MAC address exchanges
- The status (active or standby)
- The network interface status
- Hello keepalive messages

Together both cables help keep the firewall in sync to provide failover fault tolerance.

Failover Detection

The PIX can detect several types of failovers. One mechanism it uses is the hello message. This message is sent every 3–15 seconds out every interface to test communication. The default is 15 seconds, but it can be changed with the `firewall poll` command.

If a firewall unit doesn't see a hello message in two updates (30 seconds), both firewalls start to initiate failover tests to determine and confirm which of the firewalls has failed. If the primary is confirmed down, the standby moves into the active role; if the secondary firewall has failed, the primary continues to operate with no failover.

Make sure you understand that Hello messages are sent across all interfaces, including the serial or LAN-based cable. By default, hello messages are sent every 15 seconds, and if two messages are missed, the failover process begins.

Causes for Failovers

Failovers occur for many reasons. When a failover does occur, both firewalls work together to promote the standby firewall to the active state if possible. If the primary firewall detects an interface going down, it tells the secondary to move into the active state. On the other hand, the secondary promotes itself if it notices that the primary is offline. The following events cause failovers:

- The primary firewall is turned off or the power supply fails.
- The primary firewall is rebooted.
- An interface on the active firewall goes down or the serial interface cable fails.
- The primary firewall experiences a block memory exhaustion condition.

When using the serial cable as the failover link between the firewalls, power off detection can take place. If the primary firewall's power is turned off, the secondary firewall starts to promote itself to active state within 15 seconds. If a LAN-based cable is used, the power failure cannot be detected.

The Four Interface Tests

The PIX firewall issues four tests to determine whether the active firewall is truly faulty before promoting the secondary to active. As stated previously, hello messages are sent to detect interfaces on the opposite firewall. If two messages are missed, a series of tests is initiated to probe more deeply and help justify a failover. Table 11.3 explains the failover tests.

Table 11.3 Four Failover Tests

Test	Function
NIC status test	This tests the up/down status of the interface. If the link is down or unplugged, or the intermediate switch is turned off or plugged in to a switch-performing spanning tree, the interface is detected as a failure and the active firewall becomes the standby firewall. However, if the link is determined to be up, the test succeeds and the PIX searches more deeply during the second test to test for other possible problems that caused the missing hello messages.
Network activity	The PIX monitors the activity of the link for 5 seconds; if valid frames are detected, the failover testing is aborted. If no valid frames are detected, meaning the test failed, the PIX moves on to the third test.
ARP test	This test sends ARP requests to the last 10 IP addresses queued in the ARP table. If any response comes back, the testing is aborted and the firewall is considered operational. However, if no responses come back, the PIX moves to the fourth test.
Ping test	This is the last-chance test. A broadcast ping of 255.255.255.255 is sent, and if any device (host, router, and so on) replies, the test is considered a success and failover is aborted. However, if no requests come back, the failover to the standby takes place.

During the testing, if any valid frames are received from the other PIX, the testing is aborted and the systems are deemed operational. The results of each test are passed back and forth between the primary and secondary firewalls to determine which firewall is operational. For example, the primary might determine that the secondary interfaces are down and thus not promote the secondary firewall to the active state.

EXAM ALERT

The network activity test monitors for traffic for 5 seconds. If no traffic is found, the PIX moves to the next test, instead of to standby mode.

Failed State

When a firewall is deemed as failed, it disables all its network interfaces. However, every 15 seconds the failed PIX tries to test all the interfaces and automatically moves into the standby state. If problems still exist, it fails again.

To manually move the failed firewall back into the standby state, the `failover reset` command can be issued. For example, if Jack unplugs an interface, the PIX moves into the failed state. After Jack plugs the interface back in, the PIX automatically moves into the standby state in 15 seconds, as long as everything else is functioning correctly. Or Jack could issue the `failover reset` command if he doesn't want to wait 15 seconds. If a problem still exists after the command has been issued, the PIX again moves into the failed state.

Fail Back

After the secondary has been set to the active state, it will not fail back to the standby state until manually told to do so. For example, if Jack's primary firewall is turned off, the secondary moves to the active state. After Jack's primary comes back online, he will have to manually force the secondary to go into standby state, thus making the primary active again. This can be done from either unit. Table 11.4 lists the two commands used to force active or standby state.

Table 11.4 Failover Commands

Command	Description
failover active	You use this command on the primary firewall to set the primary to active mode.
no failover active	You use this command on the secondary to force it back into standby mode.

If the firewalls are set up in a stateful configuration, stateful information is kept when the new active firewall takes over. Otherwise, the users will have to reconnect.

Failover Configuration

The failover configuration is actually quite simple. Only a handful of commands are necessary to fully configure failover, and cable-based failover takes even fewer commands than LAN-based. The following is an overview of some of the basic commands:

```
pixfirewall(config)# failover [active]
pixfirewall(config)# failover IP address <if_name> <IP_address>
pixfirewall(config)# failover link [stateful_if_name]
pixfirewall(config)# failover mac address <if_name>
<active_mac> <standby_mac>
pixfirewall(config)# failover replicate http
```

Table 11.5 displays several of the configuration failover commands used to set up failover.

Table 11.5 Failover Configuration Commands

Command	Description
failover [active]	This enables failover. The **[active]** option manually forces the standby to be active.
failover ip address	This specifies the IP address of the standby firewall. When failover occurs, this is the IP address the firewall will be changed to.
failover link	This defines which FastEthernet interface is used for stateful failover.
failover mac address	This specifies the MAC addresses for the primary and standby firewalls. This is available in case you want to override the burned-in address (BIA) of the firewall.
failover replicate http	By default, HTTP connections are not replicated in stateful replication. This enables HTTP replication.

The commands listed in Table 11.5 are the basic commands needed to perform cable-based stateful failover capability. To support LAN-based failover, the following additional commands are necessary:

```
pixfirewall(config)# failover lan enable
pixfirewall(config)# failover lan unit primary¦secondary
pixfirewall(config)# failover lan interface <if_name>
pixfirewall(config)# failover lan key <secret_key>
```

Table 11.6 displays a list of LAN-based commands used to configure the PIX firewall for failover.

Table 11.6 LAN-based Failover Commands

Command	Description
failover lan enable	Enables LAN-based failover instead of cable-based.
failover lan unit	Unlike the serial cable that helps define which firewall is the primary or secondary, the **lan unit** command specifies the function of the firewall.
failover lan interface	Defines which interface is used for LAN-based connections.
failover lan key	This gives you the ability to specify an encryption key to use for protected failover messages.

Configuring for Cable-based Failover

The following example demonstrates how to configure two PIX firewalls for serial cable-based failover. The first step attaches the serial cable, which has primary and secondary labels on its ends and is provided by Cisco. Be sure you install them in the correct order. Next, you configure a stateful failover system based on Figure 11.4.

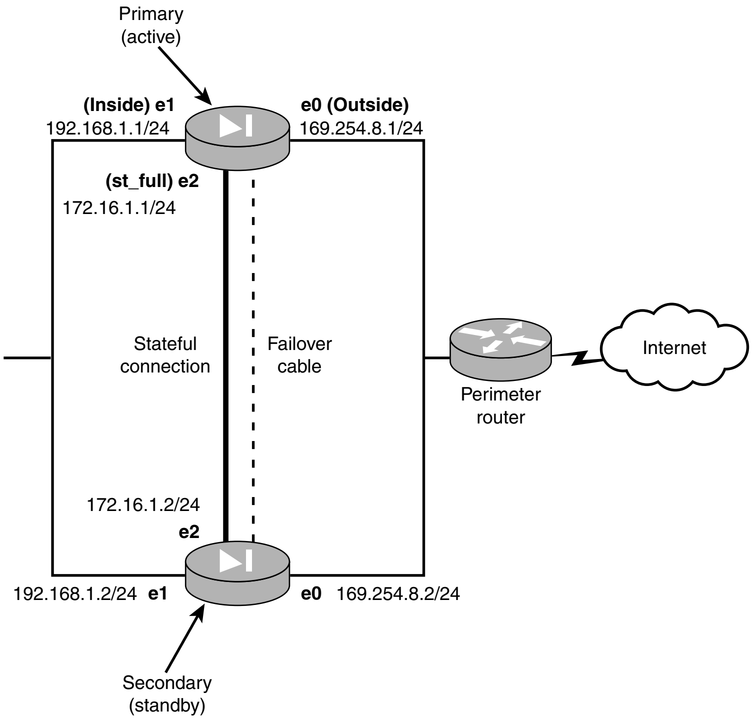

Figure 11.4 Cable-based stateful failover example.

Follow these steps, which are discussed in more detail in the following sections:

1. Configure the clock.
2. Configure the system addresses.
3. Enable failover.
4. Configure the failover addresses.
5. Enable stateful failover.
6. Finish the process.

Configuring the Clock

First, you must configure the clock on the primary firewall. The clock settings are replicated to the secondary firewall after the secondary firewall is enabled. The following is the command used to configure the clock's date and time values:

```
primaryfirewall(config)# clock set 16:00 August 31, 2003
```

Configuring the System Addresses

Now, you need to set the system addresses on the firewall. Be sure you force flow control and do not use autosensing. Listing 11.1 shows the commands needed to configure the system settings on the primary firewall.

Listing 11.1 Primary Firewall Cable-based Commands

```
primaryfirewall(config)# interface Ethernet0 100full
primaryfirewall(config)# interface Ethernet1 100full
primaryfirewall(config)# interface Ethernet2 100full

primaryfirewall(config)# nameif ethernet0 outside sec0
primaryfirewall(config)# nameif ethernet1 inside sec100
primaryfirewall(config)# nameif ethernet2 st_ful sec50

primaryfirewall(config)# IP address outside 169.254.8.1 255.255.255.0
primaryfirewall(config)# IP address inside 192.168.1.1 255.255.255.0
primaryfirewall(config)# IP address st_ful 172.16.1.1 255.255.255.0

primaryfirewall(config)# clear xlate
```

Now, you use the `show ip address` command to display the system and current address information, like so:

```
primaryfirewall(config)# show ip address
System IP Addresses:
     ip address outside 169.254.8.1 255.255.255.0
     ip address inside 192.168.1.1 255.255.255.0
     ip address st_ful 172.16.1.1 255.255.255.0
Current IP Addresses:
     ip address outside 169.254.8.1 255.255.255.0
     ip address inside 192.168.1.1 255.255.255.0
     ip address st_ful 172.16.1.1 255.255.255.0
```

EXAM ALERT

When the primary is in active mode, it uses the system IP addresses and media access control (MAC) addresses. On the other hand, when the primary is in standby mode, it uses the failover IP addresses and the MAC addresses.

Enabling Failover

After the system addresses are configured, failover can be enabled. The following command enables failover on the primary:

```
primaryfirewall(config)# failover active
```

The command to enable failover can be used before you set the system addresses, but I like to do it just after to ensure that the addresses are configured prior to failover activation.

Make sure you remember that the **failover active** command is used to enable failover on the PIX firewall.

Configuring the Failover Addresses

Configuring the failover addresses enables you to define what the secondary address will be and what the primary will become in the event of a failover. Listing 11.2 displays the commands needed on the primary firewall to define which secondary IP address will be used and which interface is the stateful interface.

Listing 11.2 Configuring Primary Cable-based Failover IP Addresses

```
primaryfirewall(config)# failover ip address outside 169.254.8.2
primaryfirewall(config)# failover ip address inside 192.168.1.2
primaryfirewall(config)# failover ip address st_ful 172.16.1.2
```

To verify the configuration, you can use the `show failover` command as shown here:

```
primaryfirewall(config)# show failover
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
     This host: primary - Active
                 Active time: 240 (sec)
                 Interface st_ful (172.16.1.1): Normal (Waiting)
                 Interface outside (169.254.8.1): Normal (Waiting)
                 Interface inside (192.168.1.1): Normal (Waiting)
     Other host: secondary - Standby
                 Active time: 0 (sec)
                 Interface st_ful (172.16.1.2): Unknown (Waiting)
                 Interface outside (168.254.8.2): Unknown (Waiting)
                 Interface inside (192.168.1.2): Unknown (Waiting)
```

The `Other host` in the previous code is the secondary host. The status of `Unknown` is displayed if you have the secondary off, as I did in this case.

Enabling Stateful Failover

In this example, you are using stateful failover on the 172.16.1.1-to-172.16.1.2 link. The following command enables the stateful failover on the interface named st_ful. At this point, you must turn on the secondary firewall, using the following:

```
primaryfirewall(config)# failover link st_ful
primaryfirewall(config)# show failover
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
     This host: primary - Active
                 Active time: 251 (sec)
                 Interface st_ful (172.16.1.1): Normal
                 Interface outside (169.254.8.1): Normal
                 Interface inside (192.168.1.1): Normal
     Other host: secondary - Standby
                 Active time: 11 (sec)
                 Interface st_ful (172.16.1.2): Normal
                 Interface outside (168.254.8.2): Normal
                 Interface inside (192.168.1.2): Normal

Stateful Failover Logical Update Statistics
    Link : failover
    Stateful Obj     xmit     xerr     rcv     rerr
    General          1201     0        0       0
    sys cmd          1130     0        0       0
    up time          0        0        0       0
    xlate            0        0        0       0
    tcp conn         0        0        0       0
    udp conn         0        0        0       0
    ARP tbl          0        0        0       0
    RIP Tbl          0        0        0       0

    Logical Update Queue Information

            Cur     Max     Total
    Recv Q: 0       0       0
    Xmit Q: 0       0       1201
```

Finishing Up

Now that the primary has been configured, the commands will be replicated to the secondary firewall when it is powered on or reloaded. The firewall will start with the Sync Started message; the Sync Completed message displays when the firewall replication has finished. After all the changes have been made on the primary and the secondary has been synchronized, use the write memory command on both firewalls to save the configuration to flash.

With cable-based topology, the primary firewall automatically replicates the configuration and setup information to the secondary unit.

Configuring for LAN-based Failover

In the previous example, you configured a cable-based firewall that required a special 6-foot serial cable from Cisco. For this example, you will use the new LAN-based configuration to set up a failover system. The LAN-based failover uses dedicated Ethernet interfaces that interconnect the two firewalls. This interconnect must go through a dedicated hub, a switch, or a VLAN on a switch. In this example, you will use a switch, as shown in Figure 11.5. You will also use a stateful link to interconnect the firewalls for session state information replication. This connection can be a crossover cable, which is shown with a straight line in Figure 11.5. Be sure you don't cable them together until the last step.

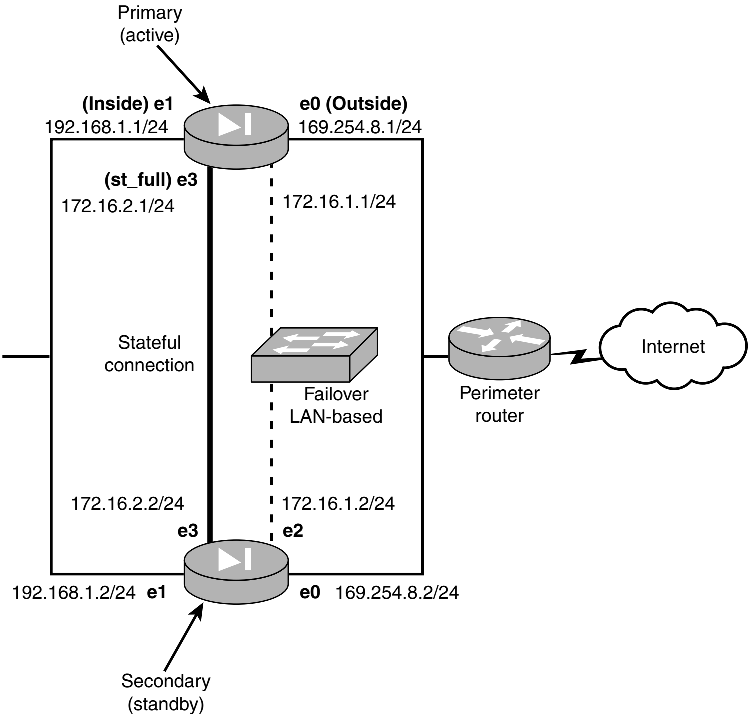

Figure 11.5 LAN-based stateful failover example.

The following steps, which are discussed in the following sections, are required to configure LAN-based failover:

1. Configure the clock.
2. Configure the primary system address.
3. Enable failover.

4. Configure the failover addresses.
5. Configure the primary LAN-based connections.
6. Enable stateful failover.
7. Configure the standby firewall.
8. Finish the process.

Configuring the Clock

You must first configure the clock on the primary firewall. The clock is replicated to the secondary firewall after it's enabled. Here's the code used to accomplish this:

```
primaryfirewall(config)# clock set 16:00 August 31, 2003
```

Configuring the Primary System Addresses

Now you have to set the system addresses on the primary firewall. Listing 11.3 shows the commands needed to configure the system settings on the primary firewall.

Listing 11.3 Primary Firewall LAN-based Commands

```
primaryfirewall(config)# interface Ethernet0 100full
primaryfirewall(config)# interface Ethernet1 100full
primaryfirewall(config)# interface Ethernet2 100full
primaryfirewall(config)# interface Ethernet3 100full

primaryfirewall(config)# nameif ethernet0 outside sec0
primaryfirewall(config)# nameif ethernet1 inside sec100
primaryfirewall(config)# nameif ethernet2 fl_ovr sec75
primaryfirewall(config)# nameif ethernet3 st_ful sec50

primaryfirewall(config)# IP address outside 169.254.8.1 255.255.255.0
primaryfirewall(config)# IP address inside 192.168.1.1 255.255.255.0
primaryfirewall(config)# IP address fl_ovr 172.16.1.1 255.255.255.0
primaryfirewall(config)# IP address st_ful 172.16.2.1 255.255.255.0

primaryfirewall(config)# clear xlate
```

Next, you use the `show ip address` command to display the system and current address information, like so:

```
primaryfirewall(config)# show ip address
System IP Addresses:
     ip address outside 169.254.8.1 255.255.255.0
     ip address inside 192.168.1.1 255.255.255.0
     ip address fl_ovr 172.16.1.1 255.255.255.0
     ip address st_ful 172.16.2.1 255.255.255.0
Current IP Addresses:
     ip address outside 169.254.8.1 255.255.255.0
     ip address inside 192.168.1.1 255.255.255.0
     ip address fl_ovr 172.16.1.1 255.255.255.0
     ip address st_ful 172.16.2.1 255.255.255.0
```

Enabling Failover

After the system addresses are configured, failover can be enabled using the following command:

```
primaryfirewall(config)# failover active
```

Configuring the Failover Addresses

Configuring the failover addresses enables you to define what the secondary address will be and what the primary will become in the event of a failover. Listing 11.4 shows a configuration example.

Listing 11.4 Configuring Primary LAN-based Failover IP Addresses

```
primaryfirewall(config)# failover ip address outside 169.254.8.2
primaryfirewall(config)# failover ip address inside 192.168.1.2
primaryfirewall(config)# failover ip address fl_ovr 172.16.1.2
primaryfirewall(config)# failover ip address st_ful 172.16.2.2
```

To verify the configuration, you can use the `show failover` command, as shown here:

```
primaryfirewall(config)# show failover
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
Poll frequency 15 seconds
     This host: primary - Active
                Active time: 250 (sec)
                Interface outside (169.254.8.1): Normal (Waiting)
                Interface inside (192.168.1.1): Normal (Waiting)
                Interface fl_ovr (172.16.1.1): Normal (Waiting)
                Interface st_ful (172.16.2.1): Normal (Waiting)
     Other host: secondary - Standby
                Active time: 0 (sec)
                Interface outside (168.254.8.2): Unknown (Waiting)
                Interface inside (192.168.1.2): Unknown (Waiting)
                Interface fl_ovr (172.16.1.2): Unknown (Waiting)
                Interface st_ful (172.16.2.2): Unknown (Waiting)
```

Configuring LAN-based Connections

Because you are using a LAN-based configuration, the serial cable will not be used and you will have to tell the firewall that it is the primary unit. Listing 11.5 configures the primary firewall for LAN-based configuration.

Listing 11.5 Setting LAN-based Primary Firewall Commands

```
primaryfirewall(config)# no failover
primaryfirewall(config)# failover lan unit primary
primaryfirewall(config)# failover lan interface fl_ovr
primaryfirewall(config)# failover lan key dog
primaryfirewall(config)# failover lan enable
primaryfirewall(config)# failover active
```

Listing 11.5 configures the firewall unit as the primary firewall, disables the failover, defines the failover link to `fl_ovr`, and uses the secret key (password) of `dog` when sending data. In a later step, you will configure the secondary with the same key (password).

Enabling Stateful Failover

In this example, you are using stateful failover on the `st_ful` interface (172.16.2.0/24). The command shown here enables the stateful failover on this link:

```
primaryfirewall(config)# failover link st_ful
```

Configuring the Standby Firewall

Now that you've configured the primary, the secondary needs to have basic LAN-based configuration set on it. Be sure the secondary has no configuration before you start the next three steps.

The first thing you must do is set the interface IP address so it can receive information from the primary. Listing 11.6 configures basic settings on the Ethernet interface on the firewall.

Listing 11.6 Secondary LAN-based Basic Configuration

```
secondaryfirewall(config)# interface Ethernet2 100full
secondaryfirewall(config)# nameif ethernet2 fl_ovr sec75
secondaryfirewall(config)# IP address fl_ovr 172.16.1.2 255.255.255.0
```

The second step is to configure the LAN-based settings. Listing 11.7 enables the firewall as a secondary unit. The last two code lines save the configuration to flash and reload the PIX.

Listing 11.7 Secondary LAN-based Configuration

```
secondaryfirewall(config)# failover IP address fl_ovr 172.16.1.2
secondaryfirewall(config)# failover lan unit secondary
secondaryfirewall(config)# failover lan interface fl_ovr
secondaryfirewall(config)# failover lan key dog
secondaryfirewall(config)# failover lan enable
secondaryfirewall(config)# failoversecondaryfirewall(config)# write memory
secondaryfirewall(config)# reload
```

Finishing Up

Now that the primary and secondary have been configured, make sure you have saved both configurations before cabling them together. Then use the `show failover` command to monitor their statuses.