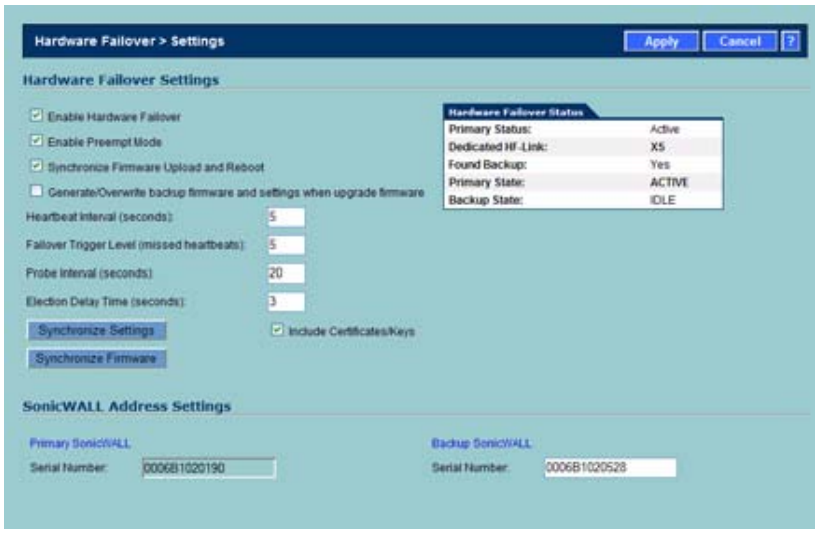
CHAPTER

51

Setting Up Hardware Failover

Hardware Failover > Settings

Hardware Failover allows two identical SonicWALL PRO Series security appliances running SonicOS Enhanced to be configured to provide a reliable, continuous connection to the public Internet. In the event of the failure of the Primary SonicWALL, the Backup SonicWALL takes over to secure a reliable connection between the protected network and the Internet.



How Hardware Failover Works

Hardware Failover requires one SonicWALL device configured as the Primary SonicWALL, and an identical SonicWALL device configured as the Backup SonicWALL. During normal operation, the Primary SonicWALL is in an Active state and the Backup SonicWALL in an Idle state. When a failure on the Primary SonicWALL occurs, the Backup SonicWALL transitions to Active mode and assumes the configuration and role of Primary. The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWALL.

SonicWALL security appliance configuration is performed on only the Primary SonicWALL, with no need to perform any configuration on the Backup SonicWALL. The Backup SonicWALL contains a real-time mirrored configuration of the Primary SonicWALL via a dedicated Ethernet link. If the firmware configuration becomes corrupted on the Primary SonicWALL, the Backup SonicWALL

automatically refreshes the Primary SonicWALL with the last-known-good copy of the configuration preferences.

The Primary and Backup SonicWALL appliances have unique MAC addresses and communicate via the X3 interface on the PRO2040 series, and via the X5 interface on the PRO3060/4060/5060 series. The dedicated HF interface link transmits all synchronization information from the Primary SonicWALL to the Backup SonicWALL.

There are two types of synchronization: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental sync is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete sync is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

Crash Detection

The Hardware Failover feature has a thorough self-diagnostic mechanism for both the Primary and Backup SonicWALL security appliances. The failover to the Backup SonicWALL occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the SonicWALL loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the SonicWALL device. The diagnostics check internal system status, system process status, and both internal and external network connectivity. For example, if a network topology has three levels, then diagnostics are performed on the router/switch/hub connectivity on the first, second, and third level. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

Before Configuring Hardware Failover

Before attempting to configure two SonicWALL appliances as a **Hardware Failover** pair, check the following requirements:

- Hardware Failover is only supported on the SonicWALL PRO 2040, PRO 3060, PRO 4060 and PRO 5060 security appliances running SonicOS Enhanced. It is not supported in any version of SonicOS Standard, or on any SonicWALL TZ 170 series product running the version of SonicOS Enhanced
- The Primary and Backup SonicWALL security appliances must be same hardware model – mixing and matching SonicWALLs of different hardware types is not currently supported.
- The Hardware Failover feature requires three unique LAN IP addresses to operate – the first IP address is used as a virtual gateway IP address, the second is used as the unique LAN IP address for the Primary device, and the third is used as the unique LAN IP address for the Backup device. You have at least one (1) valid, static IP address available from your Internet Service Provider (ISP). Two (2) valid, static IP addresses are required to remotely manage both the primary SonicWALL and the backup SonicWALL.

Alert: *SonicWALL Hardware Failover does not support dynamic IP address assignment from your ISP.*

- Each SonicWALL security appliance in the **Hardware Failover** pair must have the same firmware version installed.
- SonicWALL Security Services licenses are not shared between Primary and Backup SonicWALL devices -- the Backup SonicWALL must have separate licenses. Each SonicWALL security appliance in the **Hardware Failover** pair must have the same SonicWALL Security Services

enabled. If the Backup SonicWALL security appliance does not have the same upgrades and subscriptions enabled, these functions are not supported in the event of a failure of the Primary SonicWALL appliance.

- All SonicWALL ports being used must be connected together with a hub or switch. If each SonicWALL has a unique WAN IP Address for remote management, the WAN IP Addresses must be in the same subnet.

✓ **Tip:** *The two SonicWALLs in the Hardware Failover pair send "heartbeats" on their X5 Interfaces*—on the PRO3060/4060/5060 series—*as a dedicated-HF link. However, the PRO2040 series uses the X3 Interface as the dedicated-HF link.*

- If using new single WAN IP method, please note that the Backup device, when in offline 'Idle' mode, will not be able to use NTP to synchronize its internal clock, nor will it be able to contact the backend services licensing servers. It is also unable to perform device registration with the backend licensing servers.
- Hardware Failover can be used with dual WAN ports, but only if both WAN interfaces use static IP addressing; the current firmware does not support either WAN interface using dynamic IP addressing.
- Once Hardware Failover has been configured and activated, upon first preferences synchronization, the Backup SonicWALL security appliance automatically reboots in order to load the mirrored preferences – this is normal behavior.
- At present, the monitor feature utilizes ICMP pings on designated probe targets, and can only be used on interfaces that have been assigned unique IP addresses (at present, LAN and WAN only).
- The Primary and Backup SonicWALL security appliance's unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.
- The Primary and Backup SonicWALL devices are currently only capable of performing active/passive Hardware Failover – active/active failover is not supported at present.
- Session state is not currently synchronized between the Primary and Backup SonicWALL security appliances. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.
- If shifting a previously assigned interface to act as the Secondary WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.
- It's strongly recommended that Primary and Backup SonicWALL security appliances run the exact same version of firmware; system instability may result if firmware versions are out of sync.
- Successful Hardware Failover synchronization is not logged, only failures.
- If you are connecting the Primary and Backup device to an Ethernet switch running the spanning-tree protocol, please be aware that it may be necessary to adjust the link activation time on the switch port that the SonicWALL interfaces connect to. As an example, it would be necessary to activate spantree portfast on a Cisco Catalyst-series switch, for each port connecting to the SonicWALL's interfaces.
- If you will not be using the unique WAN IP address feature, make sure each entry field is set to '0.0.0.0' – the SonicWALL will report an error if the field is left blank.

Hardware Failover Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - The actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

Initial Hardware Failover Setup

Before you begin the configuration of Hardware Failover on the Primary SonicWALL security appliance, perform the following initial setup procedures.

- On the back of the Backup SonicWALL security appliance, local the serial number and write the number down. You need to enter this number in the **Hardware Failover>Settings** page.
- Check to make sure the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions, and running the same SonicWALL Security services.
- Make sure Primary SonicWALL and Backup SonicWALL security appliance's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the X5 ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT6-rated crossover cable. The Primary and Backup SonicWALL security appliances must have a dedicated connection between each other using the X3 (PRO2040) or X5 (PRO3060/4060/5060) interface. SonicWALL recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable.
- Power up the Primary SonicWALL security appliance, and then power on the Backup SonicWALL security appliance.
- Do not make any configuration to the Primary's X3 (PRO 2040) or X5 (PRO 3060/4060/5060) interface; the Hardware Failover programming in an upcoming step takes care of this issue. When done, disconnect the workstation.

Configuring Hardware Failover

The first task in setting up hardware failover after initial setup is configuring the **Hardware Failover>Settings** page on the Primary SonicWALL security appliance. Once you configure hardware failover on the Primary SonicWALL security appliance, you push out the settings to the Backup SonicWALL security appliance.

To configure Hardware Failover on the Primary SonicWALL, perform the following steps:

1 Select the **Hardware Failover > Settings** page on the Primary SonicWALL.

2 In the **Serial Number** field under **Backup SonicWALL**, enter the Backup SonicWALLs Serial number (this can be found on the back of the device).

3 Leave the **Heartbeat Interval (seconds)**, **Failover Trigger Level (missed heart beats)**, **Probe Interval (seconds)**, and **Election Delay Time (seconds)** timers to their default settings. These timers can be tuned later as necessary for your specific network environment. A description of these timers and their effects are covered in the "**Adjusting Hardware Failover Settings**" section.

4 Check the **Enable Hardware Failover** and the **Enable Preempt Mode** checkboxes. If everything is configured and cabled correctly, the Primary SonicWALL automatically contacts the Backup SonicWALL over the dedicated link and configures all necessary settings. The Backup SonicWALL then reboots with its new settings and come back online in Idle mode.

5 Check the **Generate/Overwrite backup firmware and settings when upgrade firmware** checkbox if you want the SonicWALL to backup the firmware and system settings when upgrading to a new firmware version. This will overwrite the current backup file when the firmware is upgraded. If you prefer to manually manage backup settings, leave this checkbox unchecked.

6 Click the **Apply** button to save the changes.

Synchronize Settings

Once you've configured the hardware failover setting on the Primary SonicWALL security appliance, click the **Synchronize Settings** button. You should see a **HA Peer Firewall has been updated** message at the bottom of the Management Interface page. Also note that the Management Interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the primary and backup units. When Local Certificates are copied to the backup unit, the associated Private Keys are also copied. Because the connection between the primary and backup units is

typically protected, this is generally not a security concern.

Tip: *A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the* ***Include Certificate/Keys*** *setting and manually synchronize the settings, and then disable* ***Include Certificate/Keys****.*

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWALL device. The Backup SonicWALL security appliance should quickly take over.

From your Management Workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. If this SonicWALL security appliance has not been registered at mySonicWALL.com, register it. The Management Interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the Management Interface. The Management GUI should again display **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure everything is working correctly.

Forcing Transitions

In some cases, it may be necessary to force a transition from one active SonicWALL to another – for example, to force the primary SonicWALL to become active again after a failure when **Preempt Mode** has not been enabled, or to force the backup SonicWALL to become active in order to do preventive maintenance on the primary SonicWALL.

To force such a transition, it is necessary to interrupt the heartbeat from the currently active SonicWALL. This may be accomplished by disconnecting the active SonicWALL's LAN port, by shutting off power on the currently active unit, or by restarting it from the Web Management Interface. In all of these cases, heartbeats from the active SonicWALL are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the active SonicWALL, log into the primary SonicWALL LAN IP Address and click **Tools** on the left side of the browser window and then click **Restart** at the top of the window.

Click **Restart SonicWALL**, then **Yes** to confirm the restart. Once the active SonicWALL restarts, the other SonicWALL in the **Hardware Failover** pair takes over operation.

Alert: *If the Preempt Mode checkbox has been checked for the primary SonicWALL, the primary unit takes over operation from the backup unit after the restart is complete.*

Adjusting Hardware Failover Settings

On the **Hardware Failover>Settings** page, there are four user-configurable timers that can be adjusted to suit your network's needs:

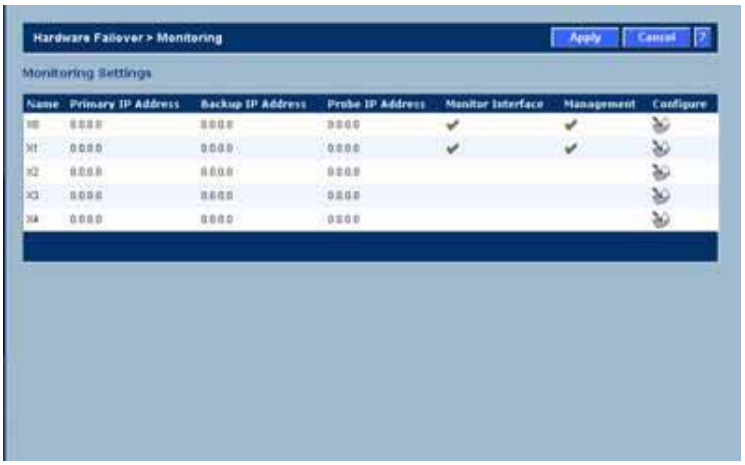
- **Heartbeat Interval (seconds)** – This timer is the length of time between status checks. By default this timer is set to 5 seconds; using a longer interval will result in the SonicWALL taking more time to detect when/if failures have occurred.
- **Failover Trigger Level (missed heart beats)** – This timer is the number of heartbeats the SonicWALL will miss before failing over. By default, this time is set to 5 missed heart beats.This timer is linked to the Heartbeat Interval timer – for example, if you set the Heartbeat Interval to 10 seconds, and the Failover Trigger Level timer to 5, it will be 50 seconds before the SonicWALL fails over.
- **Probe Interval** – This timer controls the path monitoring speed. Path monitoring sends pings to specified IP addresses to monitor that the network critical path is still reachable. The default is 20 seconds, and the allowed range is from 5 to 255 seconds.
- **Election Delay Time** – This timer can be used to specify an amount of time the SonicWALL will wait to consider an interface up and stable, and is useful when dealing with switch ports that have a spanning-tree delay set.

Synchronizing Firmware

Checking the **Synchronize Firmware Upload and Reboot** checkbox allows the Primary And Backup SonicWALL security appliances in Hardware Failover mode to have firmware uploaded on both devices at once, in staggered sequence to ensure security is always maintained. During the firmware upload and reboot, you are notified via a message dialog box that the firmware is loaded on the Backup SonicWALL security appliance, and then the Primary SonicWALL security appliance. You initiate this process by clicking on the **Synchronize Firmware** button.

Monitoring Links

On the **Hardware Failover > Monitoring** page, you can specify IP addresses that the SonicWALL security appliance performs an ICMP ping on to determine link viability.



When using logical monitors, the SonicWALL will ping the defined Probe IP Address target from the Primary as well as the Backup SonicWALL. If both can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWALLs will assume that the problem is with the target, and not the SonicWALLs. But, if one SonicWALL can ping the target but the other SonicWALL cannot, it will failover to the SonicWALL that can ping the target.

Clicking the edit icon in the **Configure** column of the Monitoring Settings table displays the **Edit HA Monitoring** window for monitoring hardware failover for the individual interface.

Hardware Failover Status

If failure of the primary SonicWALL occurs, the backup SonicWALL assumes the primary SonicWALL LAN and WAN IP Addresses. There are three primary methods to check the status of the High

Availability pair: the Hardware Failover Status window, E-mail Alerts and View Log. These methods are described in the following sections.

- **Hardware Failover Status** - One method to determine which SonicWALL is active is to check the Hardware Failover Settings Status indicator on the Hardware Failover>Settings page. If the primary SonicWALL is active, the first line in the page indicates that the primary SonicWALL is currently Active. It is also possible to check the status of the backup SonicWALL by logging into the LAN IP Address of the backup SonicWALL. If the primary SonicWALL is operating normally, the status indicates that the backup SonicWALL is currently Idle. If the backup has taken over for the primary, the status indicates that the backup is currently Active. In the event of a failure in the primary SonicWALL, you can access the Management Interface of the backup SonicWALL at the primary SonicWALL LAN IP Address or at the backup SonicWALL LAN IP Address. When the primary SonicWALL restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the primary SonicWALL becomes the active firewall and the backup firewall returns to Idle status.
- **E-mail Alerts Indicating Status Change** - If you have configured the primary SonicWALL to send E-mail alerts, you receive alert e-mails when there is a change in the status of the Hardware Failover pair. For example, when the backup SonicWALL takes over for the primary after a failure, an e-mail alert is sent indicating that the backup has transitioned from Idle to Active. If the primary SonicWALL subsequently resumes operation after that failure, and Preempt Mode has been enabled, the primary SonicWALL takes over and another e-mail alert is sent to the administrator indicating that the primary has preempted the backup.
- **View Log** - The SonicWALL also maintains an event log that displays the Hardware Failover events in addition to other status messages and possible security threats. This log may be viewed with a browser using the SonicWALL Management Interface or it may be automatically sent to the administrator's E-mail address. To view the SonicWALL log, click Log on the left side of the management interface.