



SonicOS Enhanced 4.0: Stateful Hardware Failover

Document Scope

This solutions document describes how to plan, design, implement, and manage the Stateful Hardware Failover feature. This document contains the following sections:

- [“Feature Overview” section on page 1](#)
 - [“Benefits” section on page 2](#)
 - [“How Does Stateful Hardware Failover Work?” section on page 2](#)
 - [“Platforms” section on page 4](#)
- [“Using Stateful Hardware Failover” section on page 5](#)
 - [“Prerequisites” section on page 5](#)
 - [“Configuration Procedure” section on page 7](#)
 - [“Verifying Stateful Hardware Failover Configuration” section on page 10](#)
- [“Related Features” section on page 10](#)

Feature Overview

This section provides an introduction to the Stateful Hardware Failover feature. This section contains the following subsections:

- [“What is a Stateful Hardware Failover?” section on page 1](#)
- [“Benefits” section on page 2](#)
- [“How Does Stateful Hardware Failover Work?” section on page 2](#)
- [“Platforms” section on page 4](#)

What is a Stateful Hardware Failover?

The original version of SonicOS Enhanced provided a basic Hardware Failover feature where a backup firewall assumes the interface IP addresses of the configured interfaces when the primary unit fails. Upon failover layer 2 broadcasts are issued (ARP) to inform the network that the IP addresses are now owned by the backup unit. All pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

SonicOS Enhanced release 4.0 introduces Stateful Hardware Failover (SHF), which provides dramatically improved failover performance. The primary and backup appliances are continuously synchronized so that the backup can seamlessly assume all network responsibilities if the primary appliance fails, with no interruptions to existing network connections.

Benefits

Stateful Hardware Failover provides the following benefits:

- **Improved reliability** - By synchronizing most critical network connection information, Stateful Hardware Failover prevents down time and dropped connections in case of appliance failure.
- **Faster failover performance** - By maintaining continuous synchronization between the primary and backup appliances, Stateful Hardware Failover enables the backup appliance to take over in case of a failure with virtually no down time or loss of network connections.
- **Minimal impact on CPU performance** - Typically less than 1% usage.
- **Minimal impact on bandwidth** - Transmission of synchronization data is throttled so as not interfere with other data.

How Does Stateful Hardware Failover Work?

Stateful Hardware Failover is not load-balancing. It is an active-passive configuration where the primary appliance handles all traffic. When Stateful Hardware Failover is enabled, the primary appliance actively communicates with the backup to update most network connection information. As the primary appliance creates and updates network connection information (VPN tunnels, active users, connection cache entries, etc.), it immediately informs the backup appliance. This ensures that the backup appliance is always ready to transition to the active state without dropping any connections.

The synchronization traffic is throttled to ensure that it does not interfere with regular network traffic. All configuration changes are performed on the primary appliance and automatically propagated to the backup appliance. The hardware failover pair uses the same LAN and WAN IP addresses—regardless of which appliance is currently active.

When using SonicWALL Global Management System (GMS) to manage the appliances, GMS logs into the shared WAN IP address. In case of a failover, GMS administration continues seamlessly, and GMS administrators currently logged into the appliance will not be logged out, however **Get** and **Post** commands may result in a timeout with no reply returned.

[Table 1](#) lists the types of information that currently are and are not synchronized by Stateful Hardware Failover.

Table 1 *Information Synchronized by Stateful Hardware Failover*

| Information that is Synchronized | Information that is not Synchronized |
|----------------------------------|---|
| VPN information | Dynamic WAN clients (L2TP, PPPoE, and PPTP) |
| Basic connection cache | Deep Packet Inspection (GAV, IPS, and Anti Spyware) |
| FTP | IPHelper bindings (such as NetBIOS and DHCP) |
| Oracle SQL*NET | SYNFlood protection information |
| Real Audio | Content Filtering Service information |
| RTSP | VoIP protocols |
| GVC information | Dynamic ARP entries and ARP cache timeouts |
| Dynamic Address Objects | Active wireless client information |

Table 1 Information Synchronized by Stateful Hardware Failover

| Information that is Synchronized | Information that is not Synchronized |
|-------------------------------------|--------------------------------------|
| DHCP server information | wireless client packet statistics |
| Multicast and IGMP | Rogue AP list |
| Active users | |
| ARP | |
| SonicPoint status | |
| Wireless guest status | |
| RIP and OSPF information | |
| License information | |
| Weighted Load Balancing information | |

Virtual MAC Address

The Stateful Hardware Failover feature introduces the virtual MAC address. The virtual MAC address allows the hardware failover pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by hardware failover.

In traditional stateless hardware failover, the active and passive appliances each have their own MAC addresses. Because the appliances are using the same IP address, when a failover occurs, it breaks the mapping between the IP address and MAC address in the ARP cache of all clients and network resources. The backup appliance must issue an ARP request, announcing the new MAC address/IP address pair. Until this ARP request propagates through the network, traffic intended for the primary appliance's MAC address can be lost.

The virtual MAC address greatly simplifies this process by using the same MAC address for both the primary and backup appliances. When a failover occurs, all routes to and from the primary appliance are still valid for the backup appliance. All clients and remote sites continue to use the same virtual MAC address and IP address without interruption.

By default, this virtual MAC address is provided by the SonicWALL backend and is different from the physical MAC address of either the primary or backup appliances. This eliminates the possibility of configuration errors and ensures the uniqueness of the virtual MAC address, which prevents possible conflicts. Optionally, you can manually configure the virtual MAC address on the **Hardware Failover > Monitoring** page. SonicWALL recommends that you manually configure the virtual MAC address only if the appliances do not have Internet access (for example, in secure network environments).

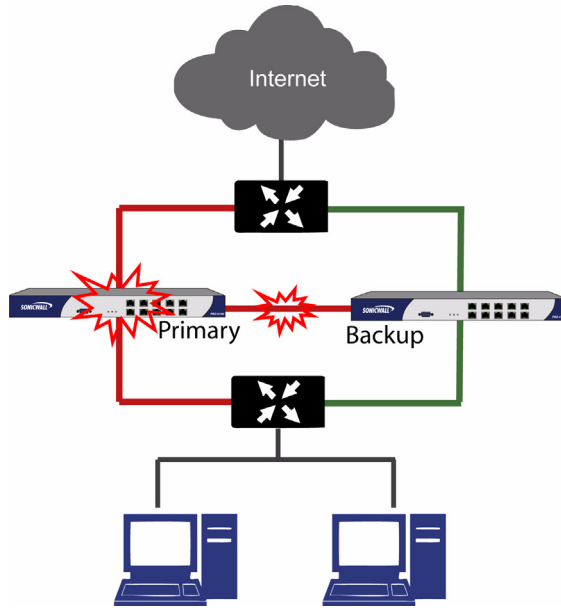
Security Services and Stateful Hardware Failover

Hardware Failover pairs share a single set of security services licenses. These licenses are synchronized between the active and passive appliances in the same way that all other information is synchronized between the two appliances. For information on security service license synchronization, see the *SonicWALL Hardware Failover License Synchronization* feature module, which is available at <http://www.sonicwall.com/us/Support.html>.

Stateful Hardware Failover Example

Figure 1 shows a sample Stateful Hardware Failover network.

Figure 1 *Stateful Hardware Failover Example*



In case of a failover, the following sequence of events occurs:

1. A PC user connects to the network, and the primary SonicWALL security appliance creates a session for the user.
2. The primary appliance synchronizes with the backup appliance. The backup now has all of the user's session information.
3. The power is unplugged from the primary appliance and it goes down.
4. The backup unit does not receive heartbeat messages from the primary appliance and switches from passive to active mode.
5. The backup appliance begins to send gratuitous ARP messages to the LAN and WAN switches using the same virtual MAC address and IP address as the primary appliance. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a webpage, the backup appliance has all of the user's session information and is able to continue the user's session without interruption.

Platforms

Stateful Hardware Failover is available on the SonicWALL PRO 4060, PRO 4100, and PRO 5060 security appliances running SonicOS version 4.0 or later.

Using Stateful Hardware Failover

This section contains the following subsections:

- “Prerequisites” section on page 5
- “Configuration Procedure” section on page 7
- “Verifying Stateful Hardware Failover Configuration” section on page 10

Prerequisites

Your network environment must me the following prerequisites before configuring Stateful Hardware Failover:

- The primary and backup appliances must be associated as a Hardware Failover pair on mySonicWALL.com. There are several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. Or, you can associate two units that are both already registered. Or, you can start the process by selecting a registered unit and adding a new appliance with which to associate it.



Note On mysonicwall.com, the primary appliance is referred to as HF Primary and the backup appliance is referred to as HF Secondary.

- To use Stateful Hardware Failover, you must purchase a **Stateful High Availability Upgrade** license for the primary unit. Stateful Hardware Failover is a licensed service that must be activated for the primary appliance on mySonicWALL.com.

| GATEWAY SERVICES | | | | |
|--|------|------------------------------|-------------------------|---|
| Service Name | Info | Status | Options | |
| Gateway AV/Anti-Spyware/Intrusion Prevention | » | Expiry: 08 May 2008 | Buy Now | Enter Key |
| Content Filtering: Standard Edition | » | - | Buy Now | Try Enter Key |
| Content Filtering: Premium Edition | » | Expiry: 08 Jun 2007 | Buy Now | Enter Key |
| VPN Upgrade | » | gift-ammo-roll-mop-tony-lacy | | |
| SonicOS Enhanced | » | drew-tint-fell-san-ask-pam | | |
| Stateful High Availability Upgrade | » | - | | Enter Key |

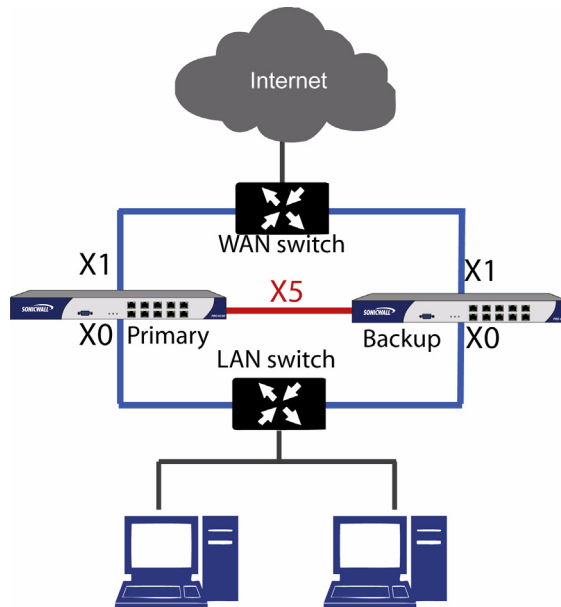
You must purchase a single set of security services licenses for the HF Primary appliance. For information on registering a Hardware Failover pair on mySonicWALL.com and on configuring license synchronization, see the *SonicWALL Hardware Failover License Synchronization* feature module, which is available at <http://www.sonicwall.com/us/Support.html>.

- The primary and backup appliances must be the same model.
- The primary and backup appliances must be running the same version of SonicOS Enhanced firmware.
- The primary and backup appliances must have the same security services enabled.
- The WAN virtual IP address and interfaces must use static IP addresses.
- You must purchase licenses for Stateful Hardware Failover on both the primary and backup appliances. To do so, go to mysonicwall.com and click on the name of the appliance. Under the **Gateway Services** heading, click **Buy Now** for the **Stateful High Availability Upgrade** services.

- Three LAN IP addresses are required:
 - **LAN virtual IP address** - Configured on the X0 interface of the primary unit. This is the default gateway for all devices configured on the LAN.
 - **Primary management IP address** - Configured under **Hardware Failover > Monitoring**. This is the IP address used for managing the primary unit over the LAN interface, regardless of the active or idle status of the unit.
 - **Backup Management P Address** - Configured under **Hardware Failover > Monitoring**. This is the IP address used for managing the backup unit over the LAN interface, regardless of the active or idle status of the unit.
- At least one WAN IP addresses are required:
 - **WAN Virtual IP** - Configured on the X1 Interface of the Primary Unit. Accessing Management Interface with this IP address will log you into the Firewall that is Active whether it is the Primary Unit or Backup unit
 - **Primary WAN Management IP (Optional)** - Configured under **Hardware Failover > Monitoring**. This is the IP address used for managing the primary unit over the WAN interface, regardless of the active or idle status of the unit. This requires that you have an additional routable IP address available. This is an Optional Configuration.
 - **Backup Management IP Address (Optional)** - Configured under **Hardware Failover > Monitoring**. This is the IP address used for managing the backup unit over the WAN interface, regardless of the active or idle status of the unit. This requires that you have an additional routable IP address available. This is an Optional Configuration

Figure 2 shows an example of how to connect two SonicWALL security appliances for Stateful Hardware Failover.

Figure 2 Stateful Hardware Failover Cabling Example



The LAN (X0) interfaces are connected to a switch on the LAN network. The WAN (X1) interfaces are connected to another switch, which connects to the Internet. The hardware failover (X5) interfaces are connected directly to each other using a crossover cable.

**Note**

If you are connecting the Primary and Backup appliances to an Ethernet switch that uses 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. For example, on a Cisco Catalyst-series switch, it is necessary to activate **spanning tree port fast** for each port connecting to the SonicWALL security appliance's interfaces.

Configuration Procedure

The following sections describe how to configure Stateful Hardware Failover:

- [Configuring Stateful Hardware Failover, page 7](#)
- [Configuring Interface Monitoring Between the Primary and Backup Appliances, page 9](#)

Configuring Stateful Hardware Failover

To configure Stateful Hardware Failover, perform the following steps:

Step 1 In the left navigation pane, click **Hardware Failover > Settings**.

| Hardware Failover Status | |
|--------------------------|--------|
| Primary Status: | Active |
| Dedicated HF-Link: | X5 |
| Found Backup: | No |
| My HA Licensed: | No |
| Peer HA Licensed: | No |
| Setting Synced: | No |
| State Synced: | No |
| Primary State: | ACTIVE |
| Backup State: | NONE |

Step 2 Check **Enable Hardware Failover**.

Step 3 Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance. You can find the serial number on the back of the SonicWALL security appliance, or in the **System > Status** screen of the backup unit. The serial number for the Primary SonicWALL is automatically populated.

Step 4 Click **Apply** to retain these settings.

Step 5 In the left navigation pane, click **Hardware Failover > Advanced**.

The screenshot shows the 'Hardware Failover > Advanced' settings window. It includes checkboxes for 'Enable Stateful Synchronization' (checked), 'Enable Preempt Mode' (unchecked), 'Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware' (checked), and 'Enable Virtual MAC' (unchecked). Below these are input fields for 'Heartbeat Interval (milliseconds):' (5000), 'Failover Trigger Level (missed heartbeats):' (5), 'Probe Interval (seconds):' (20), 'Election Delay Time (seconds):' (3), and 'Dynamic Route Hold-Down Time (seconds):' (45). There are buttons for 'Synchronize Settings' and 'Synchronize Firmware', and a checkbox for 'Include Certificates/Keys' (checked). A 'Windows Internet Explorer' dialog box is open, showing a warning icon and text: 'Stateful Synchronization recommended settings: 1000 milliseconds for Heartbeat Interval, 5 seconds for Probe Interval.' with an 'OK' button.

Step 6 In the Hardware Failover > Advanced screen, select **Enable Stateful Synchronization**. A dialog box is displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings it shows are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWALL is under a heavy load. You can use higher values if your SonicWALL handles a lot of network traffic.

Step 7 Click **OK** in the dialog box.

Step 8 For Stateful Hardware Failover, ensure that the **Enable Preempt Mode** setting is disabled.



Tip

SonicWALL recommends disabling preempt mode when using Stateful Hardware Failover. This is because preempt mode can be over-aggressive about failing over to the backup appliance. For example if both devices are idle, preempt mode may prompt a failover.

Step 9 To back up the firmware and settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.

Step 10 Check the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network routing tables when a failover occurs. Only the WAN switch that the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.

Step 11 Optionally adjust the **Heartbeat Interval** to control how often the two units communicate. The default is 5000 milliseconds; the minimum recommended value is 1000 milliseconds. Less than this may cause unnecessary failovers, especially when the SonicWALL is under a heavy load.

Step 12 Set the **Probe Level** for the interval in seconds between communication with upstream or downstream systems. SonicWALL recommends that you set the interval for at least 5 seconds. You can set the Probe IP Address(es) on the **Hardware Failover > Monitoring** screen.

- Step 13** Typically, SonicWALL recommends leaving the **Failover Trigger Level (missed heart beats)**, **Election Delay Time (seconds)**, and **Dynamic Route Hold-Down Time** timers to their default settings. These timers can be tuned later as necessary for your specific network environment.
- The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over.
 - The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role.
 - The **Dynamic Route Hold-Down Time** setting is used when a failover occurs on a hardware failover pair that is using either RIP or OSPF dynamic routing. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is 45 seconds. In large or complex networks, a larger value may improve network stability during a failover.
- Step 14** Check the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
- Step 15** Click **Synchronize Settings** to synchronizes the settings between the primary and backup appliances.
- Step 16** Click **Synchronize Firmware** if you previously uploaded new firmware to your primary unit while the secondary unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your secondary appliance offline while you test a new firmware version on the primary unit before upgrading both units to it.
- Step 17** Click **Apply** to retain the settings on this screen.

Configuring Interface Monitoring Between the Primary and Backup Appliances

To configure interface monitoring between the primary and backup appliances, perform the following steps:

- Step 1** Navigate to the **Hardware Failover > Monitoring** page.

| Name | Primary IP Address | Backup IP Address | Probe IP Address | Monitor Interface | Management | Configure |
|------|--------------------|-------------------|------------------|-------------------|------------|-----------|
| X0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | ✓ | ✓ | |
| X1 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | ✓ | ✓ | |
| X2 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | ✓ | | |
| X3 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | | | |
| X4 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | | | |

- Step 2** Click on the configure icon for the X0 interface. The **Interface X0 Monitoring Settings** window displays.

Interface 'X0' Monitoring Settings

☒ Enable Interface Monitoring

Primary IP Address: 192.168.165.50

Backup IP Address: 192.168.165.100

Probe IP Address: 0.0.0.0

☐ Manual Virtual MAC: 00:00:00:00:00:00

OK Cancel

- Step 3** Enter the LAN management IP address for the primary appliance in the **Primary IP Address** field.
- Step 4** Enter the LAN management IP address for the backup appliance in the **Backup IP Address** field.
- Step 5** (Optional) Check the **Enable Interface Monitoring** checkbox and enter the IP address of a reliable device on the LAN network in the **Probe IP Address** field. This should be a downstream router or server. The primary and backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the SonicWALL appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.
- Step 6** (Optional) To manually specify the virtual MAC address, check the **Manual Virtual MAC** checkbox and enter a MAC address. SonicWALL recommends that you manually configure the virtual MAC address only if the appliances do not have Internet access (for example, in secure network environments). Allowing the appliances to retrieve the virtual MAC address from the SonicWALL backend eliminates the possibility of configuration errors and ensures the uniqueness of the virtual MAC address, which prevents possible conflicts.
- Step 7** Click **OK**.
- Step 8** Click on the configure icon for the X1 interface and repeat steps 3 through 7 for the WAN IP addresses on the primary and backup appliances.

Verifying Stateful Hardware Failover Configuration

To determine the current status of Stateful Hardware Failover, view the **Hardware Failover Status** table on the **Hardware Failover > Settings** page. When the primary appliance has successfully synchronized with the backup appliance, the **Found Backup** row will state **yes**.

Related Features

All SonicWALL documentation can be found on the SonicWALL support page:
<http://www.sonicwall.com/us/Support.html>

- For more information on Hardware Failover, see the Hardware Failover chapter of the *SonicOS Enhanced Administrator's Guide*.
- For information on registering a Hardware Failover pair on mySonicWALL.com and on configuring license synchronization, see the *SonicWALL Hardware Failover License Synchronization* feature module.