TechNote

SonicOS

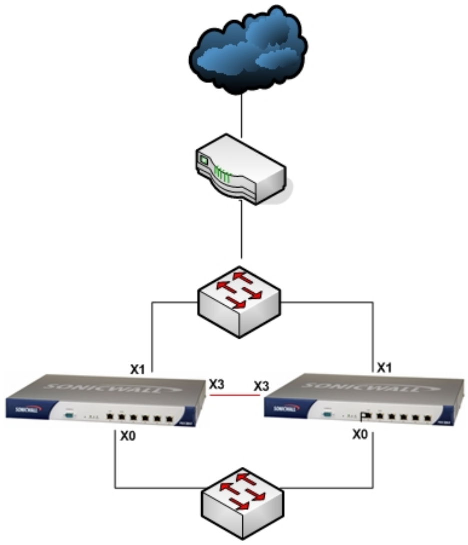
How to Configure Hardware Failover in SonicOS Enhanced 2.5 and 3.0

Introduction

This document provides a step-by-step example for configuring this feature for **SonicOS Enhanced 2.5.0.5** through **3.0**. SonicOS Enhanced 2.5 included significant changes to the method for Hardware Failover (HF). Please review the applicable *SonicOS Enhanced Administration Guide* for a full explanation of functionality and requirements.

SonicWALL Hardware Failover provides firewall redundancy. When the primary loses functionality or connectivity, the backup unit assumes the active role. If preempt is enabled, the role will fail back to the primary unit. 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.

Hardware Failover can be configured with only 1 Public WAN IP address (Virtual IP only) or 3 IP addresses (Virtual IP, Primary management IP and Backup management IP). Using 3 WAN addresses allows management access to either Primary or Backup unit whether they are the active unit or not. This can assist in some remote troubleshooting scenarios. If only 1 public IP is defined, the management interface of the unit running in *idle* mode will not be accessible via the WAN interface. The scenario in this document uses 3 WAN IP addresses (Virtual IP and Management IPs), but notes for using 1 WAN IP is included.



Scenario: PRO2040 HF Pair running SonicOS 2.5.0.5e or 3.0.0.8e.

The Primary and Backup SonicWALLs are connected with a crossover cable to a designated interface (X3 for 2040, X5 for 3060, 4060, and 5060) to create the Hardware Failover Link. All synchronization information and the HF heartbeat are passed through this Hardware Failover Link.

Requirements

The following are basic requirements for Hardware Failover with SonicOS Enhanced 2.5 and 3.0:

- SonicWALL PRO series models that run SonicOS Enhanced
- Primary and Backup must be the same model
- The same firmware versions must be installed on both units.
- Static IP addresses are required for the WAN Virtual IP and interfaces; you cannot use dynamic addressing from an ISP.
- Requires 3 LAN IP addresses (Virtual IP, Primary management IP and Backup management IP)
- Configuration option of only 1 Public WAN IP address (Virtual IP only) or 3 IP addresses (Virtual IP, Primary management IP and Backup management IP)

Additional requirements are listed in the SonicOS Enhanced Admin Guide. Please review them prior to installing SonicOS HF at your site.

The first time HF is configured, you must have the same SonicOS Enhanced version of firmware on both units. The ‘Synchronize Firmware’ feature will not work if firmware prior to SonicOS 2.5.0.5e is installed on the Backup unit. After a Hardware Failover pair has been configured, subsequent firmware upgrades only require upgrading the Primary SonicWALL and selecting ‘Synchronize Firmware’.

> ***Note**: Hardware Failover is only available for PRO models running SonicOS Enhanced. HF is not available on the TZ170.*

Physical Cabling

The WAN interfaces must be connected to the hub or switch port in the same subnet. The LAN interfaces must be connected to the same hub or switch in the same subnet. The SonicWALL HF designated interface must be connected with a crossover cable.

- Connect the **X3 (HF Link)** interfaces of the PRO2040s with a **crossover cable** (use X5 interface for PRO3060, 4060, or 5060 pairs).
- Connect the **X0 (LAN)** interface on each unit to your LAN subnet hub or switch with a straight-through cable.
- Connect the **X1 (WAN)** interface on each unit to the WAN hub or switch with a straight-through cable. The gateway router will also connect to this subnet hub or switch.

***Note:** 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 spanning tree port fast on a Cisco Catalyst-series switch, for each port connecting to the SonicWALL’s interfaces.*

Firmware Setup

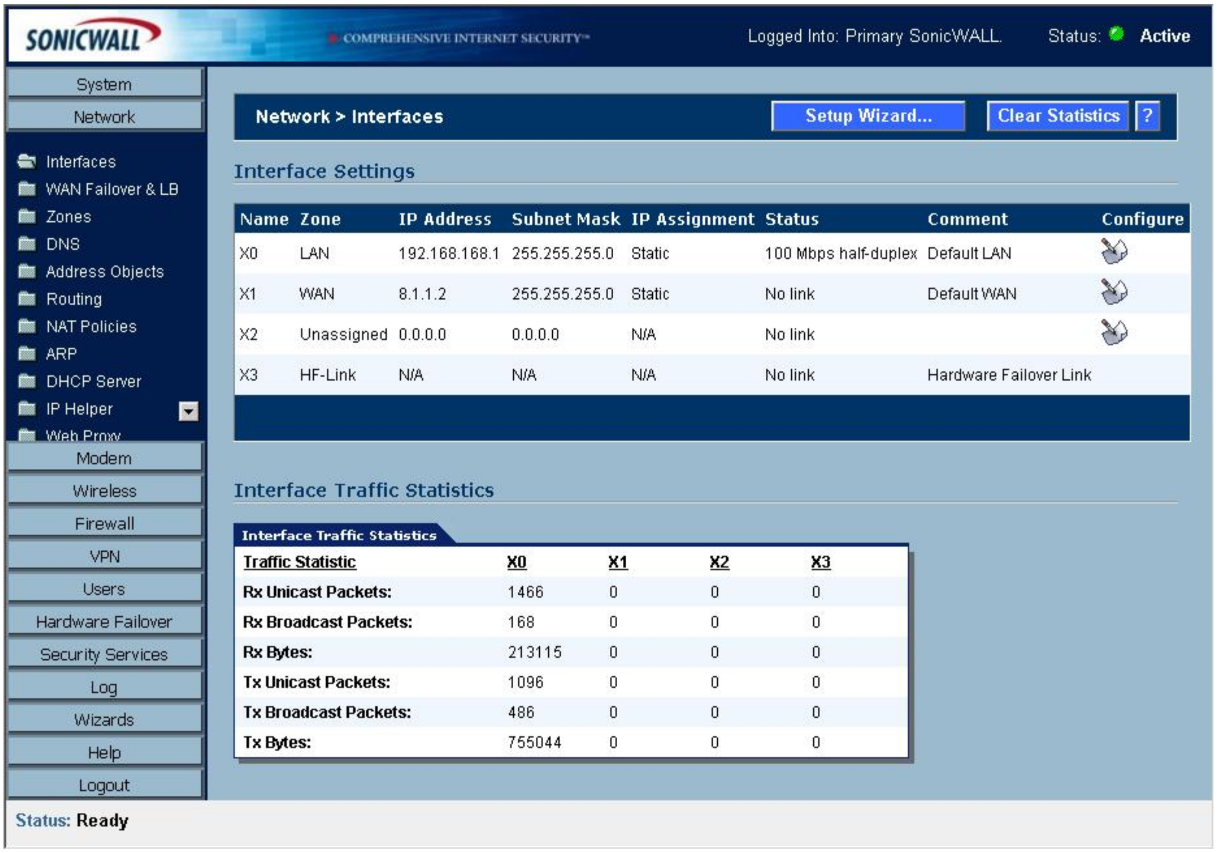
Step 1: Primary SonicWALL Basic Configuration

On the **Network > Interface** page:

- Configure the interfaces with the IP addresses. The interface IP address assigned in this step will become the '**Virtual IP**' addresses used for the HF pair and will be used as the LAN gateway for nodes on the X0 interface.

Complete the configuration of all other settings (Rules, NAT Policies, VPN policies, etc).

Network > Interface



Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	192.168.168.1	255.255.255.0	Static	100 Mbps half-duplex	Default LAN	🔧
X1	WAN	8.1.1.2	255.255.255.0	Static	No link	Default WAN	🔧
X2	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		🔧
X3	HF-Link	N/A	N/A	N/A	No link	Hardware Failover Link	

Interface Traffic Statistics

Interface Traffic Statistics

Traffic Statistic	X0	X1	X2	X3
Rx Unicast Packets:	1466	0	0	0
Rx Broadcast Packets:	168	0	0	0
Rx Bytes:	213115	0	0	0
Tx Unicast Packets:	1096	0	0	0
Tx Broadcast Packets:	486	0	0	0
Tx Bytes:	755044	0	0	0

Status: **Ready**

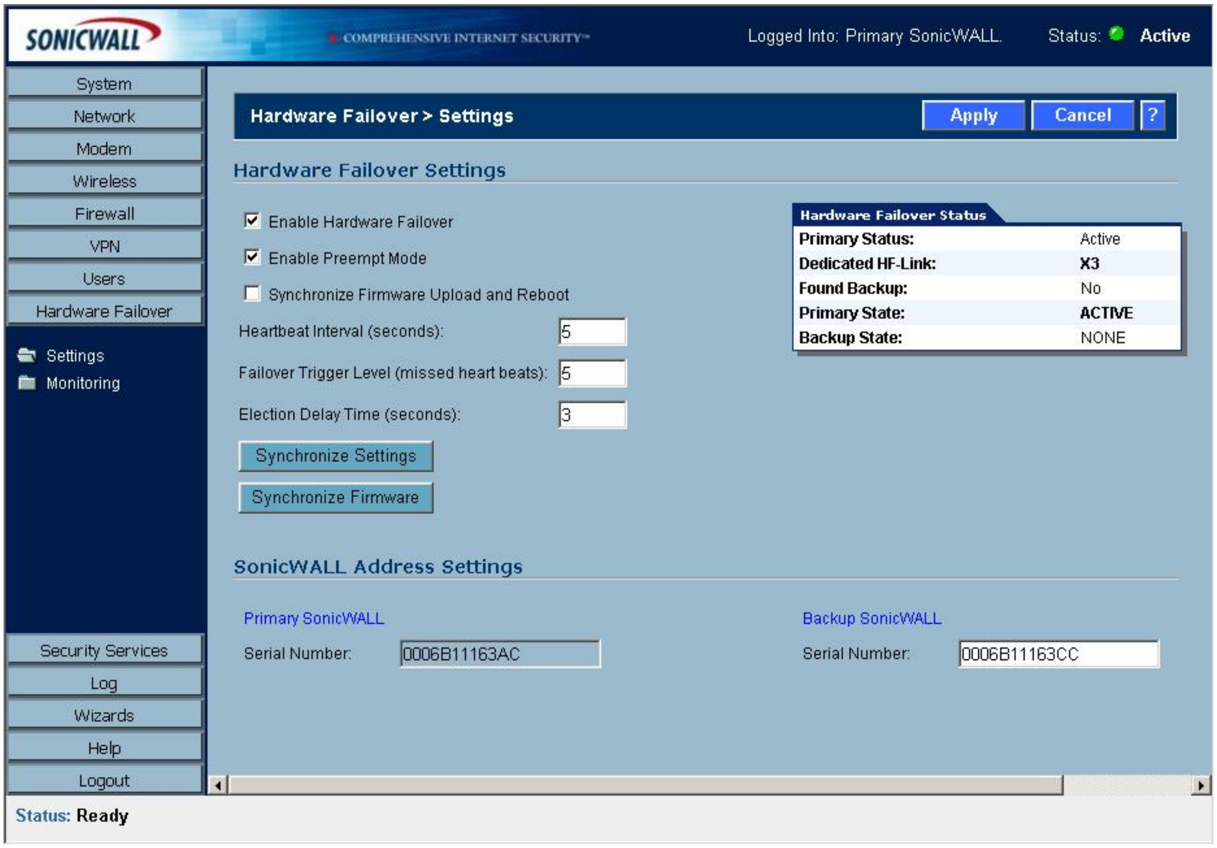
Note*: The X3 interface will show up as an HF-Link on the Pro2040. The X5 interface will show up as an HF-Link on the Pro 3060, 4060 or 5060.*

Step 2: Configure Hardware Failover Settings

On the **Hardware Failover > Settings** page:

- Check the ***Enable Hardware Failover*** box.
- Check the ***Enable Preempt Mode*** box if you want the primary unit to reassume the *active* role when it becomes available after a failover.
- Keep the recommended default settings for Heartbeat Interval, Failover trigger Level, and Election Delay Time as shown.

Hardware Failover > Settings



Logged Into: Primary SonicWALL. Status: Active

Hardware Failover > Settings

Hardware Failover Settings

☑ Enable Hardware Failover

☑ Enable Preempt Mode

☐ Synchronize Firmware Upload and Reboot

Heartbeat Interval (seconds): 5

Failover Trigger Level (missed heart beats): 5

Election Delay Time (seconds): 3

Hardware Failover Status

Primary Status:	Active
Dedicated HF-Link:	**X3**
Found Backup:	No
Primary State:	**ACTIVE**
Backup State:	NONE

SonicWALL Address Settings

Primary SonicWALL

Serial Number: 0006B11163AC

Backup SonicWALL

Serial Number: 0006B11163CC

Status: Ready

The **Heartbeat Interval** on this screen refers to the amount of time (seconds) between system checks.

The **Failover Trigger Level** refers to the number of missed heartbeats that will occur before a failover happens.

If the Heartbeat Interval is set to 5 seconds, and the Failover Trigger Level is set to 5 seconds, a failover will occur after 25 seconds.

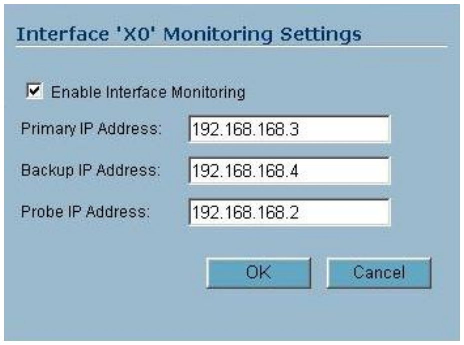
Step 3: Configure the Management & Monitoring IP Addresses

The WAN IP address (8.1.1.2) assigned earlier on the **Network > Interface** page will become the 'floating' or WAN 'Virtual IP' address. The LAN IP address (192.168.168.1) assigned on the **Network > Interface** page will become the LAN 'Virtual IP' address. Hosts on the LAN will use the LAN 'Virtual IP' as their default gateway. This section will configure additional addresses used for management access and network probing on the individual SonicWALL appliances.

- On the **Hardware Failover > Monitoring page:**
- Select the Configure Icon for interface ***X0 (LAN)***.
- Configure the ***Primary and Backup IP Addresses for X0***. These are the LAN addresses for management access via the LAN interface of the primary and backup units.
- Configure the ***Probe IP Address for X0***. This will be system on the LAN that is always up and will respond to pings. If you don't want to configure probing leave blank. Recommendations would be a down stream router or server.
- Select the Configure Icon for interface ***X1 (WAN)***.
- Configure the ***Primary and Backup IP Addresses for X1***. These are the WAN addresses for management access via the WAN interface of the primary and backup units.
- Configure the ***Probe IP Address for X1***. This will be an IP on the WAN that is always up and will respond to pings. If you don't want to configure probing leave blank. Recommendations would be to use your upstream router or an IP within your ISP.

Note: *If you are configuring with only 1 public IP address, enter 0.0.0.0 in the X1 (WAN) Primary and X1 (WAN) Backup IP Address fields. You will get an error if you leave the fields blank. The WAN Interface IP address configured under* ***Network > Interface*** *settings (8.1.1.2 in this example) will be used to access the active SonicWALL from the WAN. The SonicWALL that is in the idle state will not be accessible from the WAN.*

Hardware Failover > Monitoring > X0



Interface 'X0' Monitoring Settings

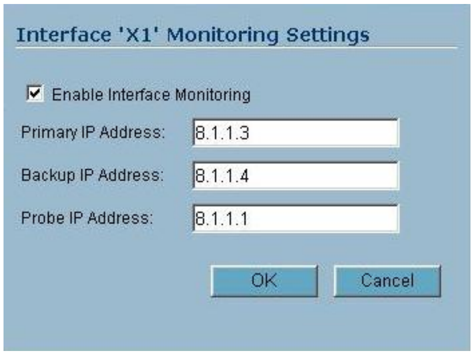
☑ Enable Interface Monitoring

Primary IP Address: 192.168.168.3

Backup IP Address: 192.168.168.4

Probe IP Address: 192.168.168.2

Hardware Failover > Monitoring > X1



Interface 'X1' Monitoring Settings

☑ Enable Interface Monitoring

Primary IP Address: 8.1.1.3

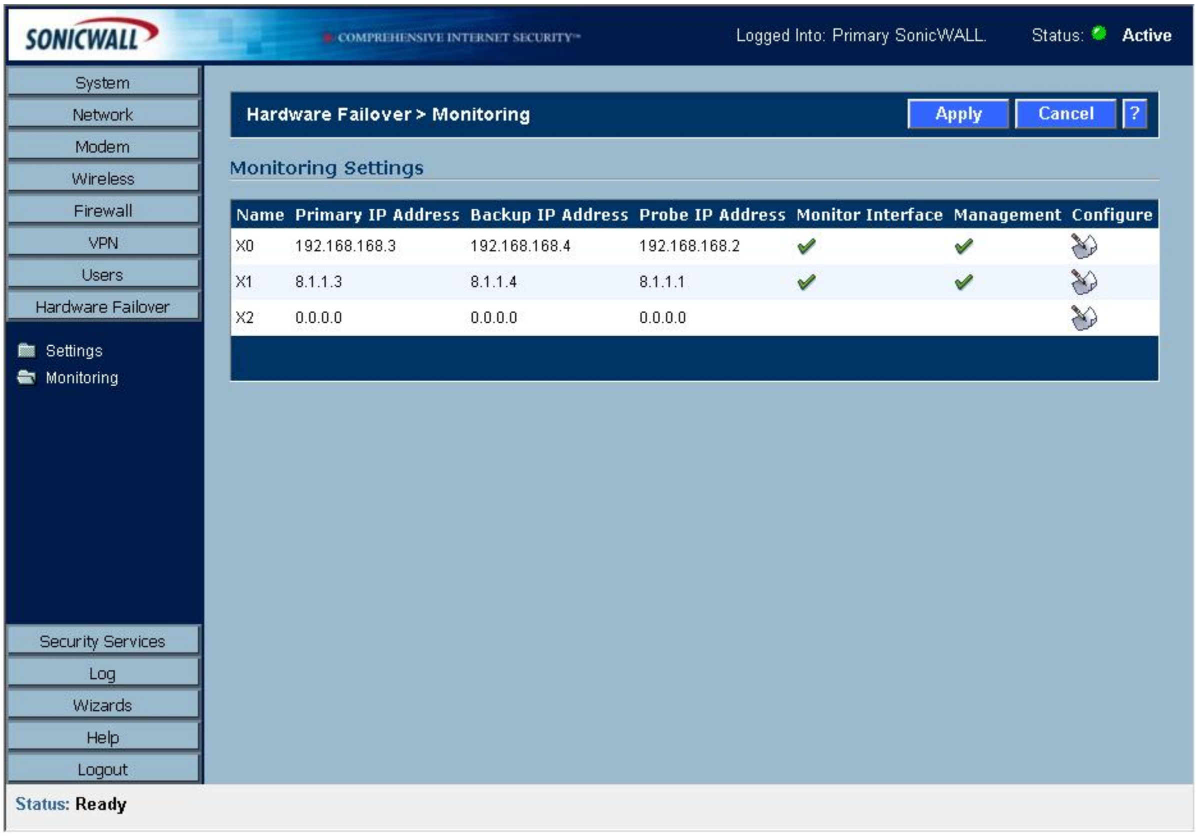
Backup IP Address: 8.1.1.4

Probe IP Address: 8.1.1.1

The ***Primary*** **and** ***Backup IP Addresses*** that you configure for **X0 (LAN)** and **X1 (WAN)** will be the IP addresses that you can always use for management access to each unit (regardless of which is currently the active unit). You will also be able to access the **active** SonicWALL with the 'Virtual IP' assigned on the **Network > Interface** page.

The SonicWALL uses probing to determine whether the active unit is still available. The ***Probe IP Address*** is a machine on the LAN or WAN that is known to be active. The SonicWALLs will ping the configured ***Probe IP Address*** to verify connectivity. If the non-active SonicWALL can ping the ***Probe IP Address*** but the Active unit cannot, a failover or preempt will occur. If neither unit can ping the ***Probe IP Address***, no failover will occur.

Hardware Failover > Monitoring



Monitoring Settings

Name	Primary IP Address	Backup IP Address	Probe IP Address	Monitor Interface	Management	Configure
X0	192.168.168.3	192.168.168.4	192.168.168.2	✓	✓	
X1	8.1.1.3	8.1.1.4	8.1.1.1	✓	✓	
X2	0.0.0.0	0.0.0.0	0.0.0.0			

The **Hardware Failover > Monitoring** page will show your Primary, Backup, and Probe IP Addresses for each interface.

Step 4: Synchronize Firmware and Settings to Backup

Once the Primary unit has been configured, power on the Backup unit. Make sure the X3 interfaces are connected with a crossover cable.

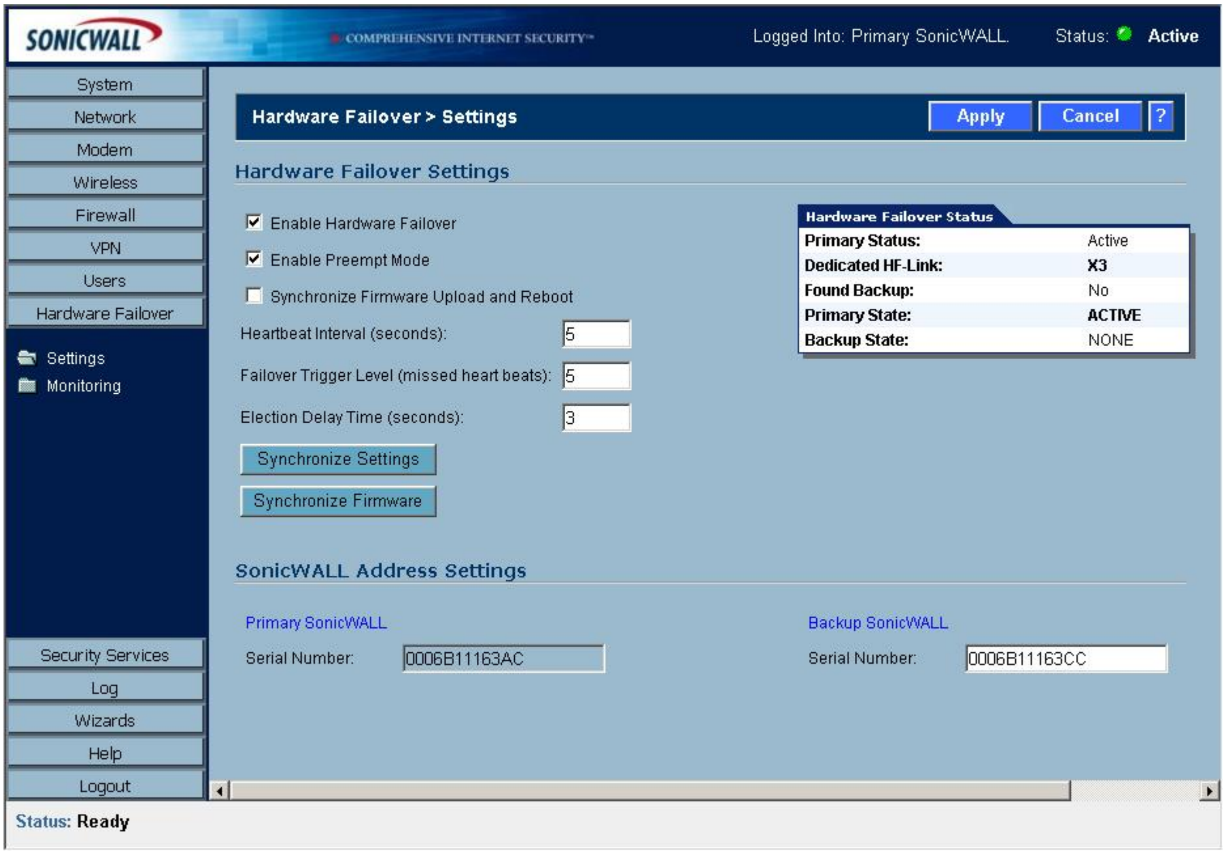
On the **Hardware > Failover Settings** page:

- Click the **Synchronize Firmware** button. This will push the firmware to the Backup unit.
- Click the **Synchronize Settings** button. This will push the configuration to the Backup Unit.

Note: *Successful Hardware Failover synchronization is not logged, only failures.*

The Backup unit will reboot after the Synchronize Settings has completed.

Hardware Failover > Settings



Logged Into: Primary SonicWALL. Status: ● Active

Hardware Failover > Settings

Hardware Failover Settings

☑ Enable Hardware Failover

☑ Enable Preempt Mode

☐ Synchronize Firmware Upload and Reboot

Heartbeat Interval (seconds): 5

Failover Trigger Level (missed heart beats): 5

Election Delay Time (seconds): 3

Hardware Failover Status

Primary Status:	Active
Dedicated HF-Link:	**X3**
Found Backup:	No
Primary State:	**ACTIVE**
Backup State:	NONE

SonicWALL Address Settings

Primary SonicWALL

Serial Number: 0006B11163AC

Backup SonicWALL

Serial Number: 0006B11163CC

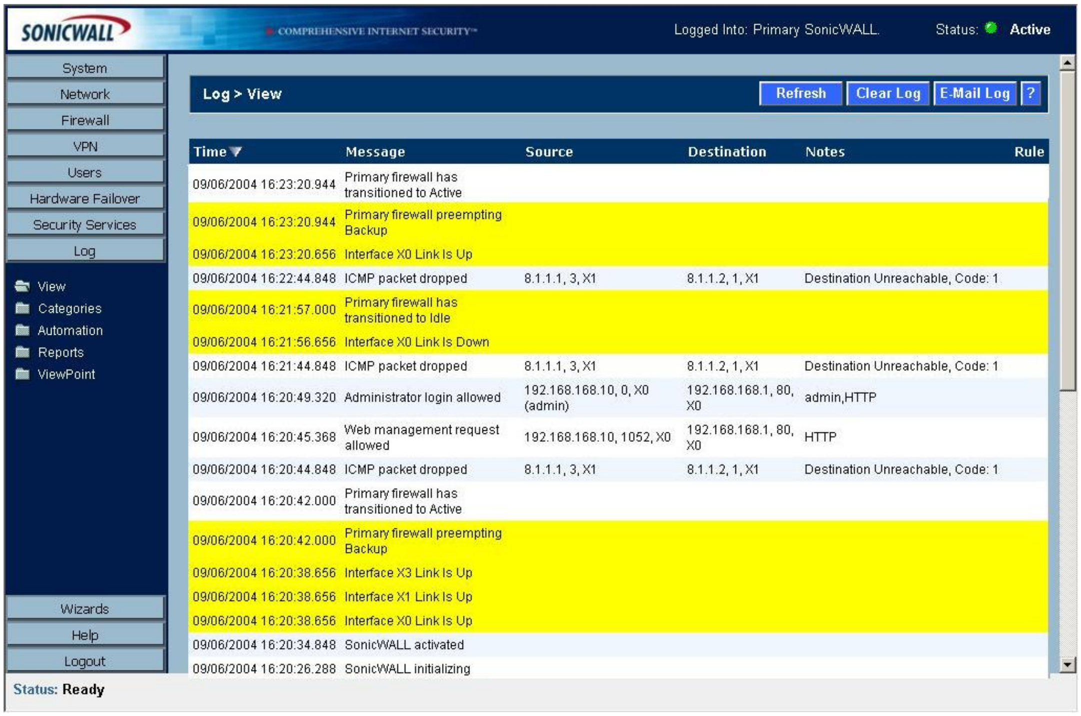
Status: **Ready**

Failover Function Test

The status of the HF unit is shown in the upper right corner of the management GUI. When an initial failover occurs, the Primary unit will transition to *Idle (***Status: Idle).** The Primary unit will transition back to *Active* (**Status: Active**) and the Backup unit will transition back to *Idle* when the Primary comes back online if preempt is enabled.

The screen shot below shows the log messages generated when HF pair failover and preempt events occur.

Log > View



Logged Into: Primary SonicWALL. Status: ● Active

Time ▼	Message	Source	Destination	Notes	Rule
09/06/2004 16:23:20.944	Primary firewall has transitioned to Active				
09/06/2004 16:23:20.944	Primary firewall preempting Backup				
09/06/2004 16:23:20.656	Interface X0 Link Is Up				
09/06/2004 16:22:44.848	ICMP packet dropped	8.1.1.1, 3, X1	8.1.1.2, 1, X1	Destination Unreachable, Code: 1	
09/06/2004 16:21:57.000	Primary firewall has transitioned to Idle				
09/06/2004 16:21:56.656	Interface X0 Link Is Down				
09/06/2004 16:21:44.848	ICMP packet dropped	8.1.1.1, 3, X1	8.1.1.2, 1, X1	Destination Unreachable, Code: 1	
09/06/2004 16:20:49.320	Administrator login allowed	192.168.168.10, 0, X0 (admin)	192.168.168.1, 80, X0	admin,HTTP	
09/06/2004 16:20:45.368	Web management request allowed	192.168.168.10, 1052, X0	192.168.168.1, 80, X0	HTTP	
09/06/2004 16:20:44.848	ICMP packet dropped	8.1.1.1, 3, X1	8.1.1.2, 1, X1	Destination Unreachable, Code: 1	
09/06/2004 16:20:42.000	Primary firewall has transitioned to Active				
09/06/2004 16:20:42.000	Primary firewall preempting Backup				
09/06/2004 16:20:38.656	Interface X3 Link Is Up				
09/06/2004 16:20:38.656	Interface X1 Link Is Up				
09/06/2004 16:20:38.656	Interface X0 Link Is Up				
09/06/2004 16:20:34.848	SonicWALL activated				
09/06/2004 16:20:26.288	SonicWALL initializing				

Status: Ready

Log Messages for Successful Failover & Preempt