SonicOS 7

High Availability

Administration Guide

SONICWALL®

Contents

1

High Availability

This section provides conceptual information about High Availability (HA) in SonicOS and describes how to connect the Security Appliances for HA.

Topics:

About High Availability

High Availability (HA) is a redundancy design that allows two identical SonicWall Security Appliances running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One SonicWall SuperMassive is configured as the Primary unit, and an identical Security Appliance is configured as the Secondary unit. If the Primary Security Appliance fails, the Secondary Security Appliance takes over to secure a reliable connection between the protected network and the Internet. Two Security Appliances configured in this way are also known as a High Availability Pair (HA Pair).

High Availability provides a way to share SonicWall licenses between two SonicWall Security Appliances when one is acting as a high-availability system for the other. Both Security Appliances must be the same SonicWall model.

To use this feature, you must register the SonicWall Security Appliances on MySonicWall as Associated Products.

ⓘ **NOTE:** HA is not supported on TZ series Security Appliances with wireless enabled. Stateful HA and Active/Active DPI are supported on TZ500 Series and above Security Appliances. See Active/Standby and Active/Active DPI Prerequisites.

Topics:

- High Availability Terminology
- High Availability Modes
- High Availability Encryption
- Crash Detection
- Virtual MAC Address
- Dynamic WAN Interfaces with PPPoE HA
- Stateful Synchronization with DHCP
- Stateful Synchronization with DNS Proxy
- About HA Monitoring

High Availability Terminology

HIGH AVAILABILITY TERMINOLOGY

Active	The operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Secondary hardware unit.
Failover	The actual process in which the Standby 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 in Configuring High Availability.
HA	High Availability: non-state, hardware failover capability.
IDV	Interface Disambiguation through VLAN.
PoE	Power over Ethernet is a technology that lets network cables carry electrical power.
PPP	Point-to-point protocol that provides a standard method for transporting multi-protocol diagrams over point-to-point links.
PPPoE	A method for transmitting PPP over ethernet.
PPPoE HA	HA PPPoE support function without State.
Preempt	Applies to a post-failover condition in which the Primary unit has failed, and the Secondary unit has assumed the Active role. Enabling Preempt causes the Primary unit to seize the Active role from the Secondary after the Primary has been restored to a verified operational state.
Primary	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.
Secondary (Backup)	The subordinate hardware unit itself. The Secondary identifier is a relational designation and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Secondary unit operates in a Standby mode. Upon failure of the Primary unit, the Secondary unit assumes the Active role.
SHF	State Hardware Failover, a SonicOS feature that allows existing network flows to remain active when the primary Security Appliance fails and the backup Security Appliance takes over.
Standby (Idle)	The passive condition of a hardware unit. The Standby identifier is a logical role that can be assumed by either a Primary or Secondary hardware unit. The Standby unit assumes the Active role upon a determinable failure of the Active unit.

STP	Spanning Tree Protocol.

High Availability Modes

High Availability has several operation modes, which can be selected on **DEVICE | High Availability > Settings**.

- **None**—Selecting None activates a standard high availability configuration and hardware failover functionality, with the option of enabling Stateful HA and Active/Active DPI.
- **Active/Standby**—Active/Standby mode provides basic high availability with the configuration of two identical Security Appliances as a High Availability Pair. The Active unit handles all traffic, while the Standby unit shares its configuration settings and can take over at any time to provide continuous network connectivity if the Active unit stops working.

  By default, Active/Standby mode is stateless, meaning that network connections and VPN tunnels must be re-established after a failover. To avoid this, Stateful Synchronization can be licensed and enabled with Active/Standby mode. In this Stateful HA mode, the dynamic state is continuously synchronized between the Active and Standby units. When the Active unit encounters a fault condition, stateful failover occurs as the Standby Security Appliance takes over the Active role with no interruptions to the existing network connections.

  > ⓘ **NOTE:** Stateful HA is:
  >
  > - Included on NSA 4600 and higher NSA platforms.
  > - Supported on the NSA 2600 and NSA 3600 platforms with a SonicOS Expanded License or a High Availability License.
  > - Supported on the TZ500 and higher TZ platforms with a SonicOS Expanded License or a High Availability (Stateful) Upgrade License.
  >
  > For licensing information, see *SonicOS 7 Settings* document.

- **Active/Active DPI**—The Active/Active Deep Packet Inspection (DPI) mode can be used along with the Active/Standby mode. When Active/Active DPI mode is enabled, the processor intensive DPI services, such as Intrusion Prevention (IPS), Gateway Anti-Virus (GAV), and Anti-Spyware are processed on the standby Security Appliance, while other services, such as firewall, NAT, and other types of traffic are processed on the Active Security Appliance concurrently.

  > ⓘ **NOTE:** Active/Active DPI is:
  >
  > - Supported on the NSA 5600 and above platforms with a SonicOS Expanded License or a High Availability (Stateful) License.
  >
  > For licensing information, see *SonicOS 7 Settings* document.

- **Active/Active Clustering**—In this mode, multiple Security Appliances are grouped together as cluster nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI and sharing the network load. Each cluster node consists of two units acting as a Stateful HA pair. Active/Active Clustering provides Stateful Failover support in addition to load-sharing. Optionally, each cluster node can also consist of a single unit, in which case Stateful Failover and Active/Active DPI are not available.

  > ⓘ **NOTE:** Active/Active Clustering is:
  >
  > - Supported on NSA 3600 and above platforms only with the purchase of a SonicOS Expanded License.
  >
  > For licensing information, see *SonicOS 7 Settings* document.

- **Active/Active DPI Clustering**—This mode allows for the configuration of up to four HA cluster nodes for failover and load sharing, where the nodes load balance the application of DPI security services to network traffic. This mode can be enabled for additional performance gain, utilizing the standby units in each cluster node.

> ⓘ **NOTE:** Active/Active DPI Clustering is:
>
> - Supported on NSA 3600 and above platforms only with the purchase of a SonicOS Expanded License.
>
> For licensing information, see *SonicOS 7 Settings* document.

High Availability Encryption

High Availability encryption adds security to the communication between appliances in a HA pair. HA control messages between active and standby firewalls, such as heartbeats, configuration sync and HA state information, are encrypted to ensure security for inter-node communication.

This option is available in Active-Standby HA mode only and does not apply to messages exchanged for stateful synchronization even in Active-Standby mode. Discovery messages (find-peer and found-peer) are transmitted without encryption. After the discovery stage, however, all control messages are encrypted between the firewalls:

- Heartbeats
- Messages used for incremental config updates
- prefSync messages
- Various messages for sending HA commands between the firewall pair
- Firmware sync messages

Crash Detection

The HA feature has a thorough self-diagnostic mechanism for both the Active and Standby Security Appliances. The failover to the standby unit occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Security Appliance loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the Security Appliance. The diagnostics check internal system status, system process status, and network connectivity. There is a weighting mechanism on both sides to decide which side has better connectivity 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.

Virtual MAC Address

The Virtual MAC address allows the High Availability 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 high availability.

Without Virtual MAC enabled, the Active and Standby Security Appliances each have their own MAC addresses. Because the Security 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 Secondary Security 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 Security 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 Secondary Security Appliances. When a failover occurs, all routes to and from the Primary Security Appliance are still valid for the Secondary Security 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 firmware and is different from the physical MAC address of either the Primary or Secondary Security 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 DEVICE | High Availability > Monitoring.

The Virtual MAC setting is available even if Stateful High Availability is not licensed. When Virtual MAC is enabled, it is always used even if Stateful Synchronization is not enabled.

Dynamic WAN Interfaces with PPPoE HA

ⓘ **NOTE:** Dynamic WAN interfaces with PPPoE HA is not supported on the SuperMassive 9800. Only the DHCP Server dynamic WAN mode is supported.

PPPoE can be enabled on interfaces in non-stateful mode, HA Active/Standby mode. PPPoE HA provides HA where a Secondary Security Appliance assumes connection to the PPPoE server when the Active Security Appliance fails.

ⓘ **NOTE:** One WAN interface must be configured as PPPoE; see Configuring a WAN Interface section in the *SonicOS 7.0 Firewall Network* document available at https://www.sonicwall.com/support/technical-documentation/.

After the Active unit connects to the PPPoE server, the Security Appliance synchronizes the PPPoE session ID and server name to the Secondary unit.

When the Active Security Appliance fails, it terminates the PPPoE HA connection on the client side by timing out. The Secondary Security Appliance connects to the PPPoE server, terminates the original connection on the server side, and starts a new PPPoE connection. All pre-existing network connections are rebuilt, the PPPoE sessions are re-established, and the PPP process is renegotiated.

Stateful Synchronization with DHCP

DHCP can be enabled on interfaces in both Active/Standby (non-stateful) and Stateful Synchronization modes.

Only the Active Security Appliance can get a DHCP lease. The Active Security Appliance synchronizes the DHCP IP address along with the DNS and gateway addresses to the Secondary Security Appliance. The DHCP client ID is also synchronized, allowing this feature to work even without enabling Virtual MAC.

During a failover, the Active Security Appliance releases the DHCP lease and, as it becomes the Active unit, the Secondary Security Appliance renews the DHCP lease using the existing DHCP IP address and client ID. The IP address does not change, and network traffic, including VPN tunnel traffic, continues to pass.

If the Active Security Appliance does not have an IP address when failover occurs, the Secondary Security Appliance starts a new DHCP discovery.

Stateful Synchronization with DNS Proxy

DNS Proxy supports stateful synchronization of DNS cache. When the DNS cache is added, deleted, or updated dynamically, it synchronizes to the idle Security Appliance.

About HA Monitoring

On **DEVICE | High Availability > Monitoring**, you can configure both physical and logical interface monitoring:

- By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability.
- Logical monitoring involves configuring the SonicWall to monitor a reliable device on one or more of the connected networks.

Failure to periodically communicate with the device by the Active unit in the HA Pair triggers a failover to the Standby unit. If neither unit in the HA Pair can connect to the device, no action is taken.

The Primary and Secondary IP addresses configured on **DEVICE | High Availability > Monitoring** can be configured on LAN or WAN interfaces, and are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Secondary Security Appliances' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN needs to use the virtual LAN IP address as their gateway.

If WAN monitoring IP addresses are configured, then X0 monitoring IP addresses are not required. If WAN monitoring IP addresses are not configured, then X0 monitoring IP addresses are required, because in such a scenario the Standby unit uses the X0 monitoring IP address to connect to the licensing server with all traffic routed through the Active unit.

The management IP address of the Secondary/Standby unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-Security Appliance basis (not per-HA Pair). Even if the Secondary unit was already registered on MySonicWall before creating the HA association, you must use the link on **Device | Settings > Licenses** to connect to the SonicWall server while accessing the Secondary Security Appliance through its management IP address (for more information, see *SonicOS 7 Settings* document).

When using logical monitoring, the HA Pair pings the specified Logical Probe IP address target from the Primary as well as from the Secondary unit. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as SonicOS assumes that the problem is with the target, and not the Security Appliances. If one Security Appliance can ping the target but the other cannot, however, the HA Pair failovers to the unit that can ping the target.

The configuration tasks on **DEVICE | High Availability > Monitoring** are performed on the Primary unit and then are automatically synchronized to the Secondary.

About Active/Standby HA

HA allows two identical Security Appliances running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One Security Appliance is configured as the Primary unit, and an identical Security Appliance is configured as the Secondary unit. In the event of the failure of the Primary Security Appliance, the Secondary Security Appliance takes over to secure a reliable connection between the protected network and the Internet. Two Security Appliances configured in this way are also known as a High Availability Pair (HA Pair).

Active/Standby HA provides standard, high availability, and hardware failover functionality with the option of enabling stateful HA and Active/Active DPI.

HA provides a way to share licenses between two Security Appliances when one is acting as a high availability system for the other. To use this feature, you must register the Security Appliances on MySonicWall as Associated Products. Both Security Appliances must be the same SonicWall model.

Topics:

- Benefits of Active/Standby HA
- Working of Active/Standby HA

Benefits of Active/Standby HA

- **Increased network reliability** – In a High Availability configuration, the Secondary Security Appliance assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant Security Appliances. You do not need to purchase a second set of licenses for the Secondary unit in a High Availability Pair.
- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA 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 high availability. By default, the Virtual MAC address is provided by the SonicWall firmware and is different from the physical MAC address of either the Primary or Secondary Security Appliances.

Working of Active/Standby HA

HA requires one SonicWall Security Appliance configured as the Primary SonicWall, and an identical Security Appliance configured as the Secondary SonicWall. During normal operation, the Primary SonicWall is in an Active state and the Secondary SonicWall in an Standby state. If the Primary device loses connectivity, the Secondary SonicWall transitions to Active mode and assumes the configuration and role of Primary, including the interface IP addresses of the configured interfaces.

Basic Active/Standby HA provides stateless high availability. After a failover to the Secondary Security Appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated. Stateful Synchronization can be licensed and enabled separately. For more information, see About Stateful Synchronization.

The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWall. The failover to the Secondary SonicWall occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary SonicWall loses power. The Primary and Secondary SonicWall devices are currently only capable of performing Active/Standby High Availability or Active/Active DPI – complete Active/Active high availability is not supported at present.

There are two types of synchronization for all configuration settings:

- **Incremental** – If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Standby unit.
- **Complete** –If the timestamps are out of sync and the Standby unit is available, a complete synchronization is pushed to the Standby unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

About Stateful Synchronization

Stateful Synchronization provides dramatically improved failover performance. When enabled, the network connections and VPN tunnel information is continuously synchronized between the two units so that the Secondary can seamlessly assume all network responsibilities if the Primary Security Appliance fails, with no interruptions to existing network connections.

ⓘ **NOTE:** Stateful HA is supported on the TZ500 and higher TZ platforms with an Extended or Stateful HA upgrade license. For licensing information, see *SonicOS7 Settings* document.

Topics:

- Benefits of Stateful Synchronization
- How Does Stateful Synchronization Work?
- Example of Stateful Synchronization

Benefits of Stateful Synchronization

- **Improved reliability** - By synchronizing most critical network connection information, Stateful Synchronization prevents down time and dropped connections in case of Security Appliance failure.
- **Faster failover performance** - By maintaining continuous synchronization between the Primary and Secondary Security Appliances, Stateful Synchronization enables the Secondary Security 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 Synchronization Work?

Stateful Synchronization is not load-balancing. It is an active-standby configuration where the Primary Security Appliance handles all traffic. When Stateful Synchronization is enabled, the Primary Security Appliance actively communicates with the Secondary to update most network connection information. As the Primary Security Appliance creates and updates network connection information (such as VPN tunnels, active users, connection cache entries), it immediately informs the Secondary Security Appliance. This ensures that the Secondary Security 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 Security Appliance and automatically propagated to the Secondary Security Appliance. The High Availability pair uses the same LAN and WAN IP addresses—regardless of which Security Appliance is currently Active.

When using SonicWall Global Management System (GMS) to manage the Security 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 Security Appliance are not logged out; however, **Get** and **Post** commands may result in a time out with no reply returned.

Synchronized and non-synchronized information table lists the information that is synchronized and information that is not currently synchronized by Stateful Synchronization.

SYNCHRONIZED AND NON-SYNCHRONIZED INFORMATION

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 time outs
Dynamic Address Objects	Active wireless client information
DHCP server information	Wireless client packet statistics
Multicast and IGMP	Rogue AP list

Information that is Synchronized	Information that is not Synchronized
Active users	
ARP	
SonicPoint status	
Wireless guest status	
License information	
Weighted Load Balancing information	
RIP and OSPF information	

Example of Stateful Synchronization

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

1. A PC user connects to the network, and the Primary Security Appliance creates a session for the user.
2. The Primary Security Appliance synchronizes with the Secondary Security Appliance. The Secondary now has all of the user's session information.
3. The administrator restarts the Primary unit.
4. The Secondary unit detects the restart of the Primary unit and switches from Standby to Active.
5. The Secondary Security 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 Security Appliance. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a Web page, the Secondary Security Appliance has all of the user's session information and is able to continue the user's session without interruption.

Active/Standby and Active/Active DPI Prerequisites

This section lists the supported platforms, provides recommendations and requirements for physically connecting the units, and describes how to register, associate, and license the units for High Availability.

Topics:

- Supported Platforms and Licensing for HA
- Physically Connecting Your Security Appliances
- Connecting the Active/Active DPI Interfaces for Active/Active DPI

Supported Platforms and Licensing for HA

Licenses included with the purchase of a SonicWall Security Appliance are shown in **HA licenses available with SonicWall Security Appliances** table. Some platforms require additional licensing to use the HA features.

ⓘ **NOTE:** HA licenses must be activated on each Security Appliance, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

The HA licenses included with the purchase of the SonicWall Security Appliance are shown in **HA licenses available with SonicWall Security Appliances**. Some platforms require additional licensing to use the Stateful Synchronization or Active/Active DPI features. SonicOS Expanded licenses or High Availability licenses can be purchased on MySonicWall or from a SonicWall reseller.

ⓘ **NOTE:** Stateful High Availability licenses must be activated on each Security Appliance, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

HA LICENSES AVAILABLE WITH SONICWALL SECURITY APPLIANCES

Platform	Active/Standby HA	Stateful HA	A/A Clustering	A/A DPI
TZ600/TZ600 P	Included	Expanded License Stateful HA License	N/A	N/A
TZ500/TZ500 W	Included	Expanded License Stateful HA License	N/A	N/A

You can view system licenses on **DEVICE | Settings > Licenses**. This page also provides a way to log into MySonicWall and to apply licenses to a Security Appliance. For further information, see *SonicOS7 Settings* document.

There is also a way to synchronize licenses for an HA pair whose Security Appliances do not have Internet access. When live communication with SonicWall's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your Security Appliances. When you register a Security Appliance on MySonicWall, a license keyset is generated for the Security Appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the Security Appliance, it cannot perform the licensed services.

ⓘ **IMPORTANT:** In a High Availability deployment without Internet connectivity, you must apply the license keyset to both of the Security Appliances in the HA pair.

You can view system licenses on **DEVICE | Settings > Licenses**. This page also provides a way to log into MySonicWall. For information about licensing, see *SonicOS 7 Settings* document.

ⓘ **IMPORTANT:** Even if you first register your Security Appliances on MySonicWall, you must individually register both the Primary and the Secondary Security Appliances from the SonicOS management interface while logged into the individual management IP address of each Security Appliance. This allows the Secondary unit to synchronize with the SonicWall license server and share licenses with the associated Primary Security Appliance. When Internet access is restricted, you can manually apply the shared licenses to both Security Appliances.

Physically Connecting Your Security Appliances

ⓘ **NOTE:** For complete procedures for connecting your Security Appliances, see the Quick Start Guide for your Security Appliance.

ⓘ **NOTE:** If you are connecting the Primary and Secondary Security Appliances to an Ethernet switch that uses the spanning tree protocol, be aware that it may be necessary to adjust the link activation time on the switch port to which the SonicWall interfaces connect. 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.

High Availability requires additional physical connections among the affected SonicWall Security Appliances. For all modes, you need connections for HA Control and HA Data. Active/Active DPI requires an additional connection.

In any High Availability deployment, you must physically connect the LAN and WAN ports of all units to the appropriate switches.

It is important that the X0 interfaces from all units be connected to the same broadcast domain. Otherwise, traffic failover does not work. Also, X0 is the default redundant HA port; if the normal HA Control link fails, X0 is used to communicate heartbeats between units. Without X0 in the same broadcast domain, both units would become active if the HA Control link fails.

ⓘ **TIP:** SonicOS Security Appliances now allow heartbeats to be exchanged between an HA pair across the MGMT interface in addition to the HA control interface.

A WAN connection to the Internet is useful for registering your Security Appliances on MySonicWall and for synchronizing licensing information. Unless live communication with SonicWall's licensing server is not permitted due to network policy, the WAN (X1) interface should be connected before registration and licensing are performed.

Connecting the Active/Active DPI Interfaces for Active/Active DPI

For Active/Active DPI, you must physically connect at least one additional interface, called the **Active/Active DPI** Interface, between the two Security Appliances in each HA pair, or Cluster Node. The connected interfaces must be the same number on both Security Appliances, and must initially appear as unused, unassigned interfaces in **Network | System > Interfaces**. For example, you could connect X5 on the Primary unit to X5 on the Secondary if X5 is an unassigned interface. After enabling Active/Active DPI, the connected interface has a Zone assignment of **HA Data-Link**.

Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit and then the results are returned to the active unit over the same interface.

Optionally, for port redundancy with Active/Active DPI, you can physically connect a second Active/Active DPI Interface between the two Security Appliances in each HA pair. This interface takes over transferring data between the two units during Active/Active DPI processing if the first Active/Active DPI Interface has a fault.

To connect the Active/Active DPI interfaces for Active/Active DPI:

1. Decide which interface to use for the additional connection between the Security Appliances in the HA pair. The same interface must be selected on each Security Appliance.
2. In the SonicOS Management Interface, navigate to **Network | System > Interfaces** and ensure that the **Zone** is **Unassigned** for the intended Active/Active DPI Interface.
3. Using a standard Ethernet cable, connect the two interfaces directly to each other.
4. Optionally, for port redundancy with Active/Active DPI, physically connect a second Active/Active DPI Interface between the two Security Appliances in each HA pair.

Maintenance

Topics:

- Removing an HA Association
- Replacing a SonicWall Security Appliance

Removing an HA Association

You can remove the association between two SonicWall Security Appliances on MySonicWall at any time. You might need to remove an existing HA association if you replace a Security Appliance or reconfigure your network. For example, if one of your SonicWall Security Appliances fails, you need to replace it. Or, you might need to switch the HA Primary Security Appliance with the Secondary, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association, and then create a new association that uses a new Security Appliance or changes the parent-child relationship of the two units (see Replacing a SonicWall Security Appliance).

To remove the association between two registered SonicWall Security Appliances:

1. Log in to MySonicWall.
2. In the left navigation bar, navigate to **My Workspace > Tenant Products**.
3. Scroll down to find the secondary Security Appliance from which you want to remove associations. Click the **serial number**.
4. On the **Products Details** page, scroll down to the **Parent Products** section, just below the **Associated Products** section.

5. Under **Parent Products**, to remove the association for this Security Appliance:
    a. Click **Remove** under **ACTIONS**.
    b. Wait for the page to reload.
    c. Scroll down.
    d. Click **Remove** again.

Replacing a SonicWall Security Appliance

If your SonicWall Security Appliance has a hardware failure while still under warranty, SonicWall replaces it. In this case, you need to remove the HA association containing the failed Security Appliance in MySonicWall, and add a new HA association that includes the replacement. If you contact SonicWall Technical Support to arrange the replacement (known as an RMA), Support often takes care of this for you.

After replacing the failed Security Appliance in your equipment rack with the new unit, you can update MySonicWall and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing an HA Secondary unit. Both procedures are provided in these sections:

- Replacing an HA Primary Unit
- Replacing an HA Secondary Unit

Replacing an HA Primary Unit

To replace an HA Primary unit:

1. In the SonicOS management interface of the remaining SonicWall Security Appliance (the Secondary unit), on the High Availability page, uncheck **Enable High Availability** to disable it.
2. Check **Enable High Availability**.
   The old Secondary unit now becomes the Primary unit. Its serial number is automatically displayed in the Primary SonicWall Serial Number field.
3. Type the serial number for the replacement unit into the `Secondary SonicWall Serial Number` field.
4. Click **Synchronize Settings**.
5. On MySonicWall, remove the old HA association. See Removing an HA Association.
6. On MySonicWall, register the replacement SonicWall Security Appliance and create an HA association with the new Primary (original Secondary) unit as the HA Primary, and the replacement unit as the HA Secondary.
7. Contact SonicWall Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.

   This step is required when the HA Primary unit has failed because the licenses are linked to the Primary unit in an HA Pair.

Replacing an HA Secondary Unit

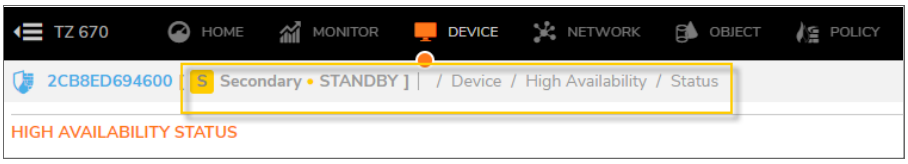
To replace an HA Secondary unit:

1. On MySonicWall, remove the old HA association as described in Removing an HA Association.
2. On MySonicWall, register the replacement SonicWall Security Appliance.
3. Create an HA association with the original HA Primary, using the replacement unit as the HA Secondary as described in Replacing an HA Primary Unit.

High Availability Status

The **DEVICE | High Availability > Status** page displays the current status of the High Availability pair, including state of primary and secondary units, mode and link configuration, and licenses.

At the top of the page, you can see which unit you are logged into, **Primary** or **Secondary**, and whether the unit is in the **Active** or **Standby** state.



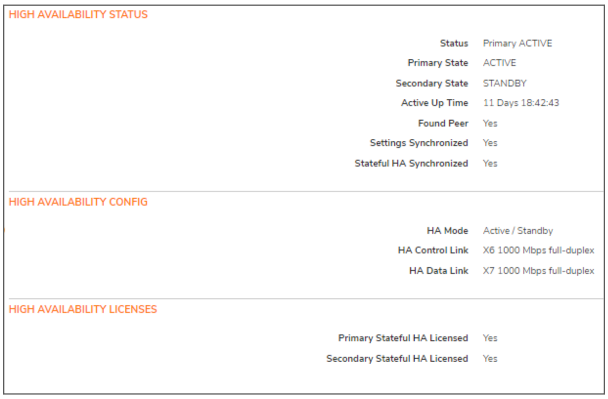
In the event that the Primary unit has a failure, you can view the status by accessing the management interface of the Secondary unit at the Primary unit virtual LAN IP address or the Secondary unit unique LAN IP address. When the Primary unit restarts after a failure, it is accessible using the unique IP address created on the **DEVICE | High Availability > Monitoring** page. If preempt mode is enabled, the Primary unit immediately takes over as the Active firewall and the Secondary unit returns to Standby status.

Topics:

- Active/Standby High Availability Status
- Active/Active High Availability Status

Active/Standby High Availability Status

Active/Standby High Availability provides basic high availability with the configuration of two identical firewalls as a High Availability pair. On a firewall that belongs to an Active/Standby HA pair, the **DEVICE | High Availability > Status** page displays information about the state, configuration, and licenses on the HA pair.



HIGH AVAILABILITY STATUS

Status	Primary ACTIVE
Primary State	ACTIVE
Secondary State	STANDBY
Active Up Time	11 Days 18:42:43
Found Peer	Yes
Settings Synchronized	Yes
Stateful HA Synchronized	Yes

HIGH AVAILABILITY CONFIG

HA Mode	Active / Standby
HA Control Link	X6 1000 Mbps full-duplex
HA Data Link	X7 1000 Mbps full-duplex

HIGH AVAILABILITY LICENSES

Primary Stateful HA Licensed	Yes
Secondary Stateful HA Licensed	Yes

Topics:

- High Availability Status
- High Availability Config
- High Availability Licenses

High Availability Status

The **High Availability Status** section on the **DEVICE | High Availability > Status** page displays the following information:

- **Status** – Indicates the High Availability status of the current firewall. The possible values are:
  - **Primary Active** – Indicates that the current appliance is the Primary unit in the ACTIVE state.
  - **Primary Standby** – Indicates that the current appliance is the Primary unit in the STANDBY state.
  - **Primary Disabled** – Indicates that the current appliance is the Primary unit, but High Availability has not been enabled.
  - **Primary not in a steady state** – Indicates that the current appliance is the Primary unit, HA is enabled, and the appliance is neither in the ACTIVE nor the STANDBY state.
- **Primary State** - Indicates the current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Secondary appliances. The possible values are:
  - **ACTIVE** – Indicates that the Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the standby unit.
  - **STANDBY** – Indicates that the Primary unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Primary and Secondary units are negotiating which should be the ACTIVE unit.
  - **SYNC** – Indicates that the Primary unit is synchronizing settings or firmware to the Secondary.
  - **ERROR** – Indicates that the Primary unit has reached an error condition.
  - **REBOOT** – Indicates that the Primary unit is rebooting.
  - **NONE** – When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Secondary unit, **NONE** indicates that the Secondary unit is not receiving heartbeats from the Primary unit.
- **Secondary State** - Indicates the current state of the Secondary appliance as a member of an HA

Pair. The Secondary State field is displayed on both the Primary and the Secondary appliances. The possible values are:

  - **ACTIVE** – Indicates that the Secondary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the standby unit.
  - **STANDBY** – Indicates that the Secondary unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Secondary and Primary units are negotiating which should be the ACTIVE unit.
  - **SYNC** – Indicates that the Secondary unit is synchronizing settings or firmware with the Primary.
  - **ERROR** – Indicates that the Secondary unit has reached an error condition.
  - **REBOOT** – Indicates that the Secondary unit is rebooting.
  - **NONE** – When viewed on the Secondary unit, NONE indicates that HA is not enabled on the Secondary. When viewed on the Primary unit, NONE indicates that the Primary unit is not receiving heartbeats from the Secondary unit.

- **Active Up Time** - Indicates how long the current Active firewall has been Active, since it last became Active. If the unit is not part of an HA pair, this line displays High Availability Disabled.
- **Found Peer** - Indicates if the Primary unit has discovered the Secondary unit. Possible values are **Yes** and **No**.
- **Settings Synchronized** - Indicates if HA settings are synchronized between the Primary and Secondary units. Possible values are **Yes** and **No**.
- **Stateful HA Synchronized** - Indicates if stateful synchronization settings are synchronized between the Primary and Secondary units. Possible values are **Yes** and **No**.

High Availability Config

The **High Availability Config** section on the **DEVICE | High Availability > Status** page provides the following information:

- **HA Mode** - Indicates one of:
  - **None** – High Availability is not enabled on the unit.
  - **Active/Standby** – Active/Standby mode provides basic high availability with the configuration of two identical firewalls as a High Availability Pair. By default, Active/Standby mode is stateless, meaning that network connections and VPN tunnels must be re-established after a failover. To avoid this, Stateful Synchronization can be licensed and enabled with Active/Standby mode.
- **HA Control Link** – Indicates the port, speed, and duplex settings of the HA control link, such as **X6 1 Gbps Full Duplex**. When High Availability is not enabled, the field displays **N/A**. The HA control link is used to communicate heartbeats and other control traffic between the units. If the HA control link fails, X0 is used to communicate heartbeats between units; therefore X0 on both units should be in the same broadcast domain.
- **HA Data Link** – Indicates the port, speed, and duplex settings of the HA data link, such as **X7 1 Gbps Full Duplex**. When High Availability is not enabled, the field displays **N/A**. The HA data link is used to transfer data necessary to keep settings and firmware synchronized between the units.

High Availability Licenses

The **High Availability Licenses** section on the **DEVICE | High Availability > Status** page provides the following information:

- **Primary Stateful HA Licensed** - Indicates if the Primary appliance is licensed for Stateful HA. Possible values are **Yes** or **No**. With Stateful HA licensed and enabled, the dynamic state is continuously synchronized between the Active and Standby units. When the Active unit encounters a fault condition, stateful failover occurs as the Standby firewall takes over the Active role with no interruptions to the existing network connections.
- **Secondary Stateful HA Licensed** - Indicates if the Secondary appliance has a Stateful HA license. Possible values are Yes or No. Note that the Stateful HA license is shared with the Primary, but that you must access MySonicWall at https://www.mysonicwall.com while logged into the unique LAN management IP address of the Secondary unit in order to synchronize with the SonicWall licensing server.
- **Primary Active/Active Licensed** - Indicates if the Primary appliance has an Active/Active license. Possible values are **Yes** or **No**.

Configuring High Availability

IMPORTANT: High Availability cannot be used along with PortShield except with the SonicWall X-Series/N-Series Solution. Before configuring HA, remove any existing PortShield configuration from **NETWORK | System > PortShield Groups**. For more information, go to https://www.sonicwall.com/support/technical-documentation/ and search for the SonicWall TZ Series in the Select A Product field.

TIP: For a description of High Availability in SonicOS, see About High Availability and Active/Active Clustering.

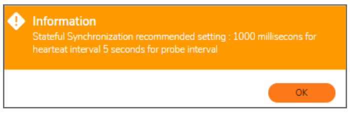
Configuring Active/Standby High Availability Settings

The configuration tasks on **DEVICE | High Availability > Settings** are performed on the Primary firewall and then are automatically synchronized to the Secondary firewall.

To configure Active/Standby:

1. Navigate to **DEVICE | High Availability > Settings**.
2. In **GENERAL SETTINGS** section, do the following:
   a. select **Active / Standby** from the **Mode** drop-down field.
   b. Select **Enable Stateful Synchronization.** This option is not selected by default.

      When Stateful High Availability is not enabled, session state is not synchronized between the Primary and Secondary firewalls. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.
   c. Click **OK** in the information dialog displayed.



Information

Stateful Synchronization recommended setting : 1000 millisecons for hearteat interval 5 seconds for probe interval

   d. To configure the High Availability Pair so that the Primary firewall takes back the Primary role when it restarts after a failure, select **Enable Preempt Mode**. This option is not selected by default.

ⓘ | **TIP:** It is recommended that preempt mode be disabled when enabling Stateful High Availability because preempt mode can be over-aggressive about failing over to the Secondary firewall.

e. Click **OK**.

f. Select **Enable Virtual MAC** to allow the Primary and Secondary firewalls to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. This option is not selected by default.

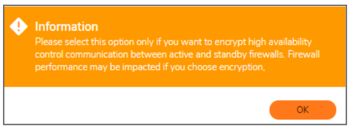
ⓘ | **IMPORTANT:** If PPPoE Unnumbered is configured, you must select Enable Virtual MAC.

Only the switch to which the two firewalls are connected needs to be notified. All outside devices continue to route to the single shared MAC address.

g. To encrypt HA control communication between the active and standby firewalls, select Enable Encryption for Control Communication. This option is not selected by default.

ⓘ | **IMPORTANT:** Firewall performance may be affected if you choose encryption.

A confirmation message displays:



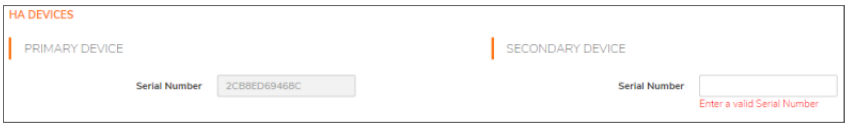
Information

Please select this option only if you want to encrypt high availability control communication between active and standby firewalls. Firewall performance may be impacted if you choose encryption.

h. Click **OK**.

3. In the **HA DEVICES** section, enter the `Serial Number` of the **SECONDARY DEVICE**.

   The serial number for the Primary Device is displayed, but the field is dimmed and cannot be edited.



HA DEVICES

PRIMARY DEVICE

Serial Number 2CB8ED69468C

SECONDARY DEVICE

Serial Number

Enter a valid Serial Number

4. In the **HA INTERFACES** section:

   a. Select the interface for the **HA Control Interface**.

   This option is dimmed and the interface displayed if the firewall detects that the interface is already configured.

   b. Select the interface for the **HA Data Interface**.

   c. When finished with all High Availability configuration, click **Accept**. All settings are synchronized to the Secondary firewall, and the Secondary firewall reboots.

Configuring HA with Dynamic WAN Interfaces

The configuration tasks on **DEVICE | High Availability > Settings** are performed on the Primary firewall and then are automatically synchronized to the Secondary firewall.

To configure HA with a dynamic WAN interface:

1. Navigate to **NETWORK | System > Interfaces**.
2. Configure a WAN interface as PPPoE, as described in *Configuring a WAN Interface* in the *SonicOS 7.0 Firewall Network* document available at https://www.sonicwall.com/support/technical-documentation/.
3. Navigate to **DEVICE | High Availability > Settings**.
4. In **GENERAL SETTINGS** section, do the following:
    a. select **HA mode** from the **Mode** drop-down field.

       If you chose **Active/Active DPI** or **Active/Active Clustering**, a message about license and signature updates displays.

    b. Click **OK**.

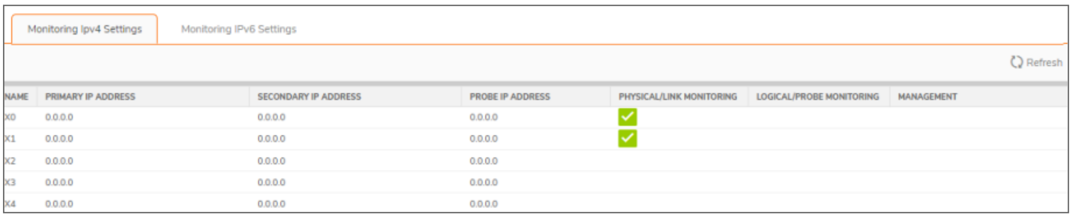
    c. Ensure **Enable Stateful Synchronization** is not selected. This option is not selected by default.

    d. Ensure **Enable Preempt Mode** is not selected. This option is not selected by default.

    e. Select **Enable Virtual MAC** to allow the Primary and Secondary firewalls to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. This option is not selected by default.

       ⓘ | **IMPORTANT:** If PPPoE Unnumbered is configured, you must select Enable Virtual MAC.

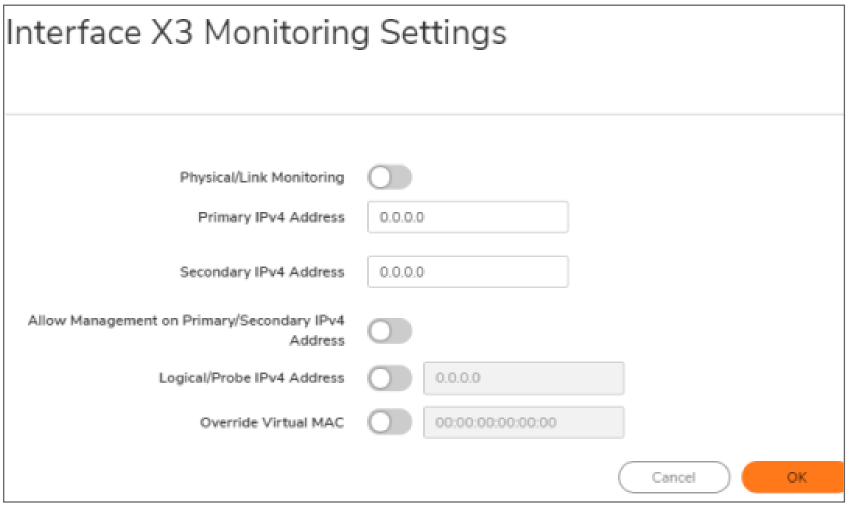
       Only the switch to which the two firewalls are connected needs to be notified. All outside devices continue to route to the single shared MAC address.
5. Configure HA Devices and HA Interfaces options as described in Configuring Active/Standby High Availability Settings.
6. Click **Accept**.
7. Navigate to **DEVICE | High Availability > Monitoring**.



NAME	PRIMARY IP ADDRESS	SECONDARY IP ADDRESS	PROBE IP ADDRESS	PHYSICAL/LINK MONITORING	LOGICAL/PROBE MONITORING	MANAGEMENT
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			

8. Hover over the PPPoE interface and click **Edit** icon.

   Interface Monitoring Settings dialog is displayed.



Interface X3 Monitoring Settings

Physical/Link Monitoring	○
Primary IPv4 Address	0.0.0.0
Secondary IPv4 Address	0.0.0.0
Allow Management on Primary/Secondary IPv4 Address	○
Logical/Probe IPv4 Address	○ 0.0.0.0
Override Virtual MAC	○ 00:00:00:00:00:00

9. Enable **Physical/Link Monitoring**. This option is not selected by default.
10. Ensure the **Primary IPv4 Address** and **Secondary IPv4 Address** fields are set to 0.0.0.0.
11. Ensure none of the other options are selected.
12. Click **OK**.

Configuring Network DHCP and Interface Settings

When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off and cannot be enabled. Networks needing a DHCP server can use an external DHCP server. The SonicOS DHCP server should be disabled in the management interface before enabling Active/Active Clustering, and all DHCP server lease scopes deleted.

On **Network | System > Interfaces**, you can configure additional virtual IP addresses for interfaces in a Virtual Group, and redundant ports for interfaces.

For information about performing these tasks, see:

- Disabling the SonicOS DHCP Server
- Configuring Virtual IP Addresses

Disabling the SonicOS DHCP Server

To disable the SonicOS DHCP server and delete all DHCP server lease scopes:

1. Log in to the Primary unit of the Cluster Node.
2. Navigate to the **NETWORK | System > DHCP Server**.
3. Choose IP version: **IPv4** or **IPv6**.
4. Clear **Enable DHCPv4/6 Server**.
5. Under **DHCP Server Lease Scopes**, select **All** for the **View** Style to select all lease scopes in the

table.

6. Select the checkbox in the header of the table.
7. Click **Delete**.
8. Click **OK** in the confirmation dialog.
9. Click **OK** in the success dialog.

Configuring Virtual IP Addresses

When Active/Active Clustering is enabled for the first time, the configured IP addresses for the interfaces on that Security Appliance are automatically converted to virtual IP addresses for Virtual Group 1. Thus, Virtual Group 1 includes virtual IP addresses for X0, X1, and any other interfaces which are configured and assigned to a zone.

Active/Active Clustering requires additional configuration of virtual IP addresses for additional Virtual Groups. You can assign multiple virtual IP addresses to each interface, one per Virtual Group. Each additional virtual IP address is associated with one of the other Virtual Groups in the cluster. Each interface can have up to a maximum of four virtual IP addresses. VLAN interfaces can also have up to four virtual IP addresses.

ⓘ **NOTE:** A packet cannot be forwarded on an interface if a virtual IP address is not configured on it for the Virtual Group handling that traffic flow.

To configure a virtual IP address on an interface:

1. Log in to the Primary unit of the Cluster Node.
2. Navigate to **Network | System > Interfaces**.
3. In the **Interface Settings** table, click the **Edit** icon for the interface you want to configure.
4. In the **Edit Interface** dialog, type the virtual IP address into the **IP Address (Virtual Group X)** field, where X is the virtual group number.

   ⓘ **NOTE:** The new virtual IP address must be in the same subnet as any existing virtual IP address for that interface.
5. Click **OK**. The configured virtual IP address appears in the **Interface Settings** table.

Configuring Redundant Ports

Redundant ports can be used along with Active/Active Clustering. You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. If there is a physical link failure on the primary interface, the redundant interface can continue processing traffic without any interruption. One advantage of this feature is that in case of a physical link failure, there is no need to do a device failover.

You can configure a redundant port on **Network | System > Interfaces > Edit Interface > Advanced** dialog. The **Redundant Port** field is only available when Active/Active Clustering is enabled.

ⓘ **NOTE:** Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

To configure a redundant port for an interface::

1. Log in to the Primary unit of the Cluster Node.
2. Navigate to **Network | System > Interfaces**.
3. In the **Interface Settings** table, click the **Edit** icon for the primary interface for which you want to create a redundant port. For example, click the Edit icon for X2. The Edit Interface dialog displays.
4. Click **Advanced**.
5. From **Redundant/Aggregate Ports**, select **Port Redundancy**. The options on the dialog change.
6. From **Redundant Port**, select the redundant port. Only unused interfaces are available for selection. For example, select X4 for the redundant port.
7. Click **OK**.

   The selected interface is dimmed in the **Interface Settings** table. A note indicates that it is a redundant Port and lists the primary interface. The interface also appears in the **Redundant Port** field in the Edit **Interface dialog** of the primary port.

   ⓘ **NOTE:** The primary and redundant ports must be physically connected to the same switch, or preferably, to redundant switches in the network.
8. On each Cluster Node, replicate the redundant physical connections using the same interface numbers for primary and redundant ports. All Cluster Nodes share the same configuration as the Master node.

Fine Tuning High Availability

Topics:

- Advanced Settings
- Configuring Advanced High Availability Settings

Advanced Settings

DEVICE | High Availability > Advanced provides the ability to fine-tune the High Availability configuration as well as synchronize setting and firmware among the High Availability Security Appliances. **High Availability > Advanced** is identical for both Active/Standby and Active/Active configurations.

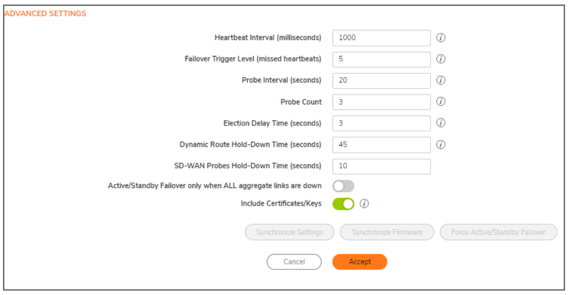
The **Heartbeat Interval** and **Failover Trigger Level (missed heartbeats)** settings apply to both the SVRRP heartbeats (Active/Active Clustering heartbeat) and HA heartbeats. Other settings on High **Availability > Advanced** apply only to the HA pairs within the Cluster Nodes.

For more information on High Availability, see About High Availability and Active/Standby and Active/Active DPI Prerequisites.

Configuring Advanced High Availability Settings

To configure advanced settings:

1. Log in as an administrator to the SonicOS Management Interface on the Master Node, that is, on the Virtual Group1 IP address (on X0 or another interface with HTTP management enabled).
2. Navigate to **DEVICE | High Availability > Settings**.



ADVANCED SETTINGS

Heartbeat Interval (milliseconds)	1000
Failover Trigger Level (missed heartbeats)	5
Probe Interval (seconds)	20
Probe Count	3
Election Delay Time (seconds)	3
Dynamic Route Hold-Down Time (seconds)	45
SD-WAN Probes Hold-Down Time (seconds)	10
Active/Standby Failover only when ALL aggregate links are down	○
Include Certificates/Keys	●

3. Optionally adjust the **Heartbeat Interval** to control how often the Security Appliances in the Active/Active cluster communicate. This setting applies to all units in the Active/Active cluster. The default is **1,000 milliseconds (1 second)**, the minimum value is 1,000 milliseconds, and the maximum is 300000.

   ⓘ | **NOTE:** SonicWall recommends that you set the Heartbeat Interval to at least 1000.

   You can use higher values if your deployment handles a lot of network traffic. Lower values may cause unnecessary failovers, especially when the Security Appliance is under a heavy load.

   This timer is linked to the **Failover Trigger Level (missed heartbeats)** timer.

4. Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. This setting applies to all units in the Active/Active cluster. The default is **5**, the minimum is 4, and the maximum is 99.

   This timer is linked to the Heartbeat Interval timer. If the **Failover Trigger Level** is set to 5 and the **Heartbeat Interval** is set to 10000 milliseconds (10 seconds), it takes 50 seconds without a heartbeat before a failover is triggered.

5. Set the **Probe Interval** to the interval, in seconds, between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This interval is used in logical monitoring for the local HA pair. The default is **20** seconds, and the allowed range is 5 to 255 seconds.

   ⓘ | **TIP:** SonicWall recommends that you set the interval for at least 5 seconds.

   You can set the Probe IP Address(es) on **DEVICE | High Availability > Advanced**. See Monitoring High Availability.

6. Set the **Probe Count** to the number of consecutive probes before SonicOS concludes that the network critical path is unavailable or the probe target is unreachable. This count is used in logical monitoring for the local HA pair. The default is **3**, and the allowed range is 3 to 10.

7. Set the **Election Delay Time** to the number of seconds the Primary Security Appliance waits to consider an interface up and stable. The default is 3 seconds, the minimum is **3** seconds, and the maximum is 255 seconds.

   This timer is useful with switch ports that have a spanning-tree delay set.

8. Set the **Dynamic Route Hold-Down Time** to the number of seconds the newly-active Security Appliance keeps the dynamic routes it had previously learned in its route table. The default value is **45** seconds, the minimum is 0 seconds, and the maximum is 1200 seconds (20 minutes).

   ⓘ | **NOTE:** The **Dynamic Route Hold-Down Time** setting is displayed only when the **Advanced Routing Mode**option is selected on **NETWORK | System > Dynamic Routing > Settings**.

   ⓘ | **TIP:** In large or complex networks, a larger value may improve network stability during a failover.

   This setting is used when a failover occurs on a High Availability pair that is using either RIP or OSPF dynamic routing. During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, SonicOS deletes the old routes and implements the new routes it has learned from RIP or OSPF.

9. If you want Failover to occur only when ALL aggregate links are down, select **Active/Standby Failover only when ALL aggregate links are down**. This option is not selected by default.
10. To have the appliances synchronize all certificates and keys within the HA pair. select **Include Certificates/Keys**. This option is selected by default.
11. (Optional) To synchronize the SonicOS preference settings between your primary and secondary HA firewalls, click **Synchronize Settings**.
12. (Optional) To synchronize the firmware version between your primary and secondary HA firewalls, click **Synchronize Firmware**.
13. (Optional) To test the HA failover functionality is working properly by attempting an Active/Standby HA failover to the secondary Security Appliance, click **Force Active/Standby Failover**.
14. When finished with all High Availability configuration, click **Accept**. All settings are synchronized to the Secondary Security Appliance or to other units in the cluster.

Monitoring High Availability

On **DEVICE | High Availability > Monitoring**, you can configure independent management IP addresses for each unit in the HA Pair, using either LAN or WAN interfaces. You can also configure physical/link monitoring and logical/probe monitoring.

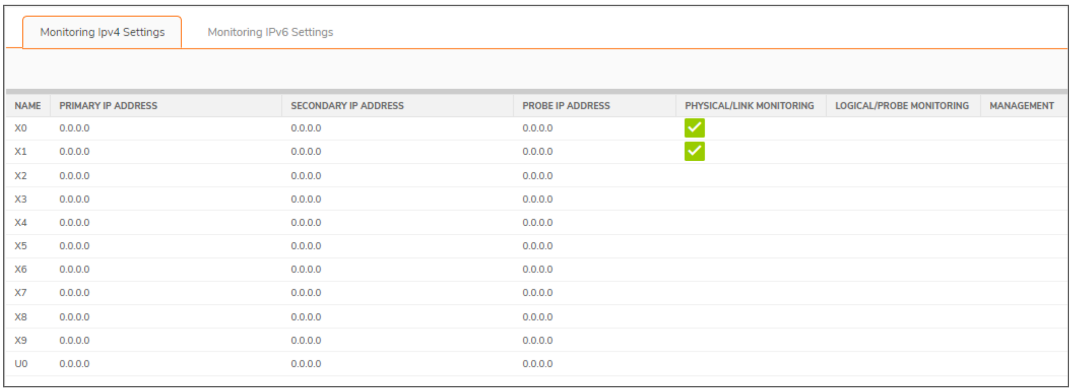
Topics:

- Configuring Active/Standby High Availability Monitoring
- IPv6 High Availability Monitoring

Configuring Active/Standby High Availability Monitoring

To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring:

1. Log in as an administrator to the SonicOS Management Interface on the Primary SonicWall Security Appliance.
2. Navigate to **DEVICE | High Availability > Monitoring**.



NAME	PRIMARY IP ADDRESS	SECONDARY IP ADDRESS	PROBE IP ADDRESS	PHYSICAL/LINK MONITORING	LOGICAL/PROBE MONITORING	MANAGEMENT
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			
X5	0.0.0.0	0.0.0.0	0.0.0.0			
X6	0.0.0.0	0.0.0.0	0.0.0.0			
X7	0.0.0.0	0.0.0.0	0.0.0.0			
X8	0.0.0.0	0.0.0.0	0.0.0.0			
X9	0.0.0.0	0.0.0.0	0.0.0.0			
U0	0.0.0.0	0.0.0.0	0.0.0.0			

3. Click the **Edit** icon for an interface on the LAN, such as X0. The **Interface Monitoring Settings** dialog is displayed.
4. To enable link detection between the designated HA interfaces on the Primary and Secondary units, leave **Physical/Link Monitoring** selected. This option is selected by default.

5. In the `Primary IPv4/v6 Address` field, enter the unique LAN management IP address of the Primary unit. The default is **0.0.0.0**.
6. In the `Secondary IPv4/v6 Address` field, enter the unique LAN management IP address of the Secondary unit. The default is **0.0.0.0**.
7. Select **Allow Management on Primary/Secondary IP Address**. When this option is enabled for an interface, a green icon appears in the interface's **Management** column in the **Monitoring Settings** table. Management is only allowed on an interface when this option is enabled. This option is not selected by default.
8. In the **Logical/ Probe IPv4/v6 Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) This option is not selected by default.

   The Primary and Secondary Security Appliances regularly ping this probe IP address. If both successfully ping the target, no failover occurs. If neither successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the Security Appliances. But, if one Security Appliance can ping the target but the other cannot, failover occurs to the Security Appliance that can ping the target.

   The `Primary IPv4/v6 Address` and `Secondary IPv4/v6 Address` fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.
9. Optionally, to manually specify the virtual MAC address for the interface, select Override Virtual MAC and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as A1:B2:C3:d4:e5:f6. This option is not selected by default.

   ⓘ **IMPORTANT:** Care must be taken when choosing the Virtual MAC address to prevent configuration errors.

   When **Enable Virtual MAC** is selected on **DEVICE | High Availability > Settings**, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.
10. Click **OK**.
11. Click **Close**.

IPv6 High Availability Monitoring

For complete information on the SonicOS implementation of IPv6, see IPv6.

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and backup Security Appliances can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs.

For easy configuration of both IP versions, toggle between IPv6 and IPv4 displays in DEVICE | High Availability > Monitoring.

The IPv6 HA Monitoring configuration page is inherited from IPv4, so the configuration procedures are almost identical. Just select IPv6 and refer to About High Availability and IPv6 HA Monitoring Considerations for configuration details.

IPv6 HA Monitoring Considerations

Consider the following when configuring IPv6 HA Monitoring:

- In the **Interface Settings** dialog, enable **Physical/Link Monitoring** and **Override Virtual MAC** are dimmed because they are layer 2 properties. That is, the properties are used by both IPv4 and IPv6, so you configure them in the IPv4 monitoring page.
- The primary/backup IPv6 address must be in the same subnet of the interface, and it can not be same as the global IP and Link-Local-IP of the primary/backup Security Appliance.
- If the primary/backup monitoring IP is set to (not ::), then they cannot be the same.
- If **Allow Management on Primary/Secondary IPv6 Address** is enabled, then primary/backup monitoring IPv6 addresses cannot be unspecified (that is, ::).
- If **Logical/Probe IPv6 Address** is enabled, then the probe IP cannot be unspecified.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

SonicOS High Availability Administration Guide
Updated - February 2021
Software Version - 7
232-005335-10 Rev A

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035