

Active/Active Unified Threat Management

Document Scope

This document describes how to configure and use the *Active/Active UTM* feature in SonicOS Enhanced. This document contains the following sections:

- [“Feature Overview” section on page 1](#)
- [“Configuring Active/Active UTM” section on page 3](#)
- [“Verifying Active/Active UTM Configuration” section on page 7](#)
- [“Related Features” section on page 9](#)

Feature Overview

This section provides an introduction to the *Active/Active UTM* feature. This section contains the following subsections:

- [“What is Active/Active UTM?” section on page 1](#)
- [“Benefits of Active/Active UTM” section on page 2](#)
- [“How Does Active/Active UTM Work?” section on page 2](#)
- [“Supported Platforms” section on page 2](#)

What is Active/Active UTM?

The High Availability feature on versions of SonicOS Enhanced prior to 5.5 uses an active-idle model that requires the active firewall to perform all Unified Threat Management (UTM), firewall, NAT, and other processing, while the idle firewall is not utilized until failover occurs. In an active/active model, both firewalls share the processing.

As a first step towards complete Active/Active High Availability, this release migrates Deep Packet Inspection (DPI) UTM services to an Active/Active model, referred to as Active/Active UTM. The following DPI UTM services are affected:

- Gateway Anti-Virus (GAV)
- Anti-Spyware
- Intrusion Protection (IPS)
- Application Firewall

When Active/Active UTM is enabled on a Stateful HA pair, these DPI UTM services can be processed concurrently with firewall, NAT, and other modules on both the active and idle firewalls. Processing of all modules other than DPI UTM services is restricted to the active unit.

Benefits of Active/Active UTM

The benefits of the Active/Active UTM feature include the following:

- Both the firewalls in the HA pair are utilized to derive maximum throughput
- GAV, IPS, Anti-Spyware, and Application Firewall services are the most processor intensive, and concurrent processing of these services on the idle firewall while the active firewall performs other processing provides the most throughput gain

How Does Active/Active UTM Work?

To use the Active/Active UTM feature, the administrator must configure an additional interface as the **HA Data Interface**. Certain packet flows on the active unit are selected and offloaded to the idle unit on the HA data interface. DPI UTM is processed on the idle unit and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

After configuring Stateful High Availability on the appliances in the HA pair, connecting and configuring the HA data interface is the only additional configuration required to enable Active/Active UTM.

Supported Platforms

Active/Active UTM is available in the SonicOS Enhanced 5.5 release on the following SonicWALL security appliances:

- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500

Configuring Active/Active UTM

To configure the Active/Active UTM feature, you must perform the following tasks:

- Physically connect an additional interface between the two appliances in your Stateful HA pair. The interface must be the same number on both appliances. For example, connect X4 on the Primary unit to X4 on the Backup.
- Configure this interface as the HA Data Interface, and enable Active/Active UTM in the SonicOS management interface.

This section contains the following subsections:

- “Prerequisites” section on page 3
- “Connecting the HA Data Interface” section on page 3
- “Configuring Active/Active UTM in the Management Interface” section on page 5

Prerequisites

Before you can configure Active/Active UTM, you must configure two SonicWALL security appliances as a Stateful High Availability pair and enable Stateful Synchronization in the SonicOS management interface.



Note

Enabling Stateful Synchronization may require the purchase of an additional license.

You can view system licenses on the System > Licenses page of the management interface. This page also provides a way to log into MySonicWALL and obtain the license.

For more information about configuring Stateful HA, see the *SonicOS Enhanced Administrator's Guide* for SonicWALL NSA Series, available online at:

<http://www.sonicwall.com/us/Support.html>

Connecting the HA Data Interface

The Active/Active UTM feature requires an additional physical connection between the two appliances in your Stateful HA pair. Perform the following steps:

-
- Step 1** Decide which interface to use for the additional connection between the appliances. The same interface must be selected on each appliance. For example, you could connect X4 on the Primary unit to X4 on the Backup, in which case X4 would be the HA Data Interface.

Step 2 In the SonicOS Enhanced management interface, navigate to the Network > Interfaces page and ensure that the **Zone** is **Unassigned** for the intended HA Data Interface.

Network /
Interfaces

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	10.0.0.2	255.255.0.0	Static	100 Mbps full-duplex	Default LAN	
X1	WAN	67.115.118.49	255.255.255.192	Static	100 Mbps full-duplex	Corp DSJ	
X2	WAN	206.160.221.34	255.255.255.224	Static	100 Mbps full-duplex	Sprint T1	
X3	WLAN	172.17.2.1	255.255.255.0	Static	100 Mbps full-duplex	SWBeta	
X3:V403	eng_peap	172.17.3.1	255.255.255.0	Static	VLAN Sub-Interface	ENG PEAP	
X3:V404	eng_sslvpn	172.17.4.1	255.255.255.0	Static	VLAN Sub-Interface	ENG SSLVPN	
X3:V405	eng_guest	172.17.5.1	255.255.255.0	Static	VLAN Sub-Interface	ENG GUEST	
X3:V406	eng_gvc	172.17.6.1	255.255.255.0	Static	VLAN Sub-Interface	ENG GVC	
X4	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X5	HA-Link	N/A	N/A	N/A	1000 Mbps full-duplex	High Availability Link	

Step 3 Using a standard Ethernet cable, connect the two interfaces directly to each other.

Configuring Active/Active UTM in the Management Interface

After physically connecting the HA Data Interface as described in [“Connecting the HA Data Interface” on page 3](#), you are ready to configure Active/Active UTM in the SonicOS management interface. To configure your Stateful HA pair to use Active/Active UTM, perform the following steps:

- Step 1** Navigate to the **High Availability > Advanced** page and select the **Enable Stateful Synchronization** checkbox if it is not yet enabled.

High Availability /
Advanced

Accept Cancel

High Availability Advanced Settings

Enable Stateful Synchronization

Enable Active/Active UTM

HA Data Interface:



Note Your system must be licensed for Stateful High Availability, as noted in the [“Prerequisites” section on page 3](#).

- Step 2** Select the **Enable Active/Active UTM** checkbox.
- Step 3** Select an interface in the **HA Data Interface** drop-down list. This interface will be used for transferring data between the two units during Active/Active UTM processing. Only unassigned, available interfaces appear in the list.

High Availability /
Advanced

Accept Cancel

High Availability Advanced Settings

Enable Stateful Synchronization

Enable Active/Active UTM

HA Data Interface:

Enable Preempt Mode

X4

- Step 4** Click **Accept**.

On the **Network > Interfaces** page, the selected interface now belongs to the **HA Data-Link** zone.

Network /

Interfaces

Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN	10.0.0.2	255.255.0.0	Static	100 Mbps full-duplex	Default LAN	
X1	WAN	67.119.118.49	255.255.255.192	Static	100 Mbps full-duplex	Corp DS3	
X2	WAN	206.160.221.34	255.255.255.224	Static	100 Mbps full-duplex	Sprint T1	
X3	WLAN	172.17.2.1	255.255.255.0	Static	100 Mbps full-duplex	SWBeta	
X3:V403	eng_peap	172.17.3.1	255.255.255.0	Static	VLAN Sub-Interface	ENG PEAP	
X3:V404	eng_sslvpn	172.17.4.1	255.255.255.0	Static	VLAN Sub-Interface	ENG SSLVPN	
X3:V405	eng_guest	172.17.5.1	255.255.255.0	Static	VLAN Sub-Interface	ENG GUEST	
X3:V406	eng_gvc	172.17.6.1	255.255.255.0	Static	VLAN Sub-Interface	ENG GVC	
X4	HA Data-Link	N/A	N/A	N/A	1000 Mbps full-duplex	High Availability Data Link	
X5	HA-Link	N/A	N/A	N/A	1000 Mbps full-duplex	High Availability Link	

Verifying Active/Active UTM Configuration

This section describes two methods of verifying the correct configuration of Active/Active UTM, and two “false negatives” that might give the impression that the idle unit is not contributing.

See the following:

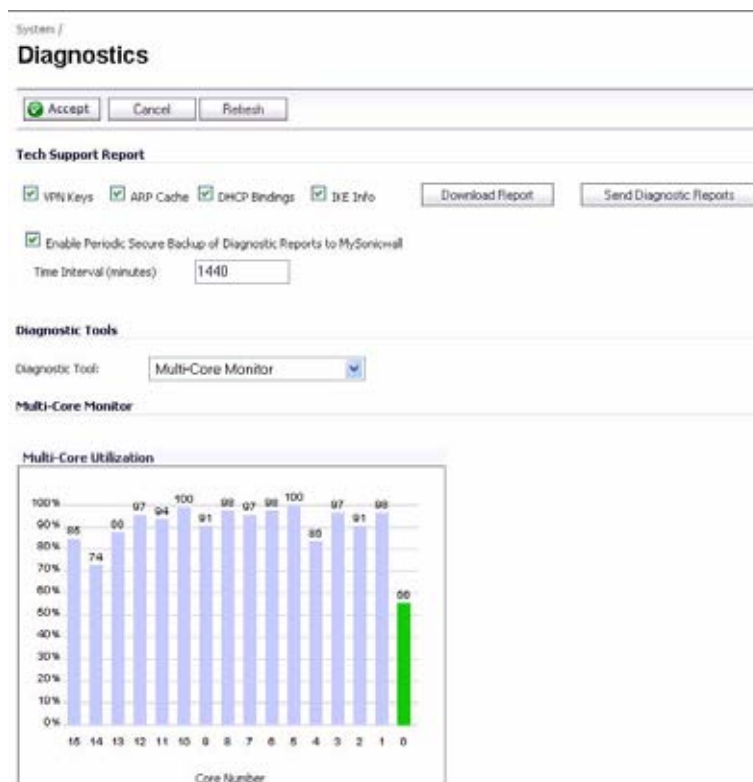
- “Comparing CPU Activity on Both Appliances” on page 7
- “Additional Parameters in TSR” on page 8
- “Responses to DPI UTM Matches” on page 8
- “Logging” on page 8

Comparing CPU Activity on Both Appliances

As soon as Active/Active UTM is enabled on the Stateful HA pair, you can observe a change in CPU utilization on both appliances. CPU activity goes down on the active unit, and goes up on the idle unit.

To view and compare CPU activity:

- Step 1** In two browser windows, log into the **Monitoring** IP address of each unit, active and idle. For information about configuring HA Monitoring, including individual IP addresses, see the *SonicOS Enhanced Administrator's Guide*.
- Step 2** Navigate to the **System > Diagnostics** page in both SonicOS management interfaces.
- Step 3** On both appliances, select **Multi-Core Monitor** from the **Diagnostic Tool** drop-down list. The active unit is displayed below with the real-time Multi-Core Utilization graph showing an immediate drop in CPU activity.



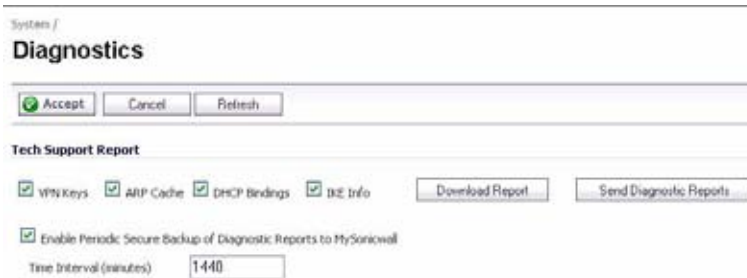
Additional Parameters in TSR

You can tell that Active/Active UTM is correctly configured on your Stateful HA pair by generating a Tech Support Report on the System > Diagnostics page. The following configuration parameters should appear with their correct values in the Tech Support Report:

- Enable Active/Active UTM
- HA Data Interface configuration

To generate a TSR for this purpose:

-
- Step 1** Log into the Stateful HA pair using the shared IP address.
 - Step 2** Navigate to the **System > Diagnostics** page.
 - Step 3** Under Tech Support Report, click **Download Report**.



Responses to DPI UTM Matches

Responses, or actions, are always sent out from the active unit of the Stateful HA pair running Active/Active UTM when DPI UTM matches are found in network traffic. Note that this does not indicate that all the processing was performed on the active unit.

Deep Packet Inspection discovers network traffic that matches virus attachments, IPS signatures, Application Firewall policies, and other malware. When a match is made, SonicOS Enhanced performs an action such as dropping the packet or resetting the TCP connection.

Some DPI match actions inject additional TCP packets into the existing stream. For example, when an SMTP session carries a virus attachment, SonicOS sends the SMTP client a “552” error response code, with a message saying “the email attachment contains a virus.” A TCP reset follows the error response code and the connection is terminated.

These additional TCP packets are generated as a result of the DPI UTM processing on the idle firewall. The generated packets are sent to the active firewall over the HA data interface, and are sent out from the active firewall as if the processing occurred on the active firewall. This ensures seamless operation and it appears as if the DPI UTM processing was done on the active firewall.

Logging

If DPI UTM processing on the idle firewall results in a DPI match action as described above, then the action is logged on the active unit of the Stateful HA pair, rather than on the idle unit where the match action was detected. This does not indicate that all the processing was performed on the active unit.

Related Features

The following features are related to the Active/Active UTM feature in SonicOS Enhanced:

SonicOS Enhanced Stateful High Availability - See the *SonicOS Enhanced Administrator's Guide* for information about Stateful High Availability.

SonicOS Enhanced High Availability License Synchronization - Information about license synchronization for HA pairs is available in the *SonicOS Enhanced Administrator's Guide* and in the following feature module:

http://www.sonicwall.com/downloads/HA_License_Sync_5.0e_Feature_Module.pdf

Solution Document Version History

Version Number	Date	Notes
1	12/18/2008	This document was created by Susan Weigand
2	7/29/09	Updated for release in SonicOS Enhanced 5.5

