SonicWall® SonicOS 6.4.1.1

Release Notes

July 2019

These release notes provide information about the SonicWall® SonicOS 6.4.1.1 release.

Topics:

About SonicOS 6.4.1.1

SonicOS 6.4.1.1 is a feature release on SuperMassive 9800 and NS*sp* 12000 series and also fixes certain vulnerabilities. For more information, see the Key Features, Security Advisory and Resolved Issues sections.

SonicOS 6.4.1.1 provides all the features and resolved issues that were included in previous releases of SonicOS 6.4. For more information about other releases, see the previous release notes, available on MySonicWall at: https://www.mysonicwall.com/.

Security Advisory

Ensuring the security of our customers is a responsibility we take seriously at SonicWall. Please review the security advisory and update your SonicWall firewall per the advisory.

Security Advisory: https://www.sonicwall.com/support/product-notification/?sol_id=190717234810906

Supported Platforms

SonicOS 6.4.1.1 is supported on the following SonicWall platforms:

- SuperMassive 9800
- NS*sp* 12400
- NS*sp* 12800

Feature Support Information

The SuperMassive 9800 and NS*sp* 12000 series running SonicOS 6.4.1.1 support many of the same features provided in SonicOS 6.2 releases for other platforms, but not all features are supported.

The following features are *not supported* on the SuperMassive 9800 and NS*sp* 12000 series with SonicOS 6.4.1.1:

- 3G/4G (WWAN)
- Comprehensive Anti-Spam Service (CASS)
- Dynamic WAN protocols, except for DHCP Client (IPv4 and IPv6)
- SonicWave access points
- VPN Manual Key

Refer to the *SonicOS 6.4 Administration Guide* or online help for more information about supported or unsupported features.

Key Features

This section describes the key features in SonicOS 6.4.1.1:

- SNMP Support for SonicOS Performance Monitoring and Reporting
- DNS Doctoring
- DPI Engine CPU Cycles Per Packet and Per Flow Limit
- NAT Utilization Visualization

SNMP Support for SonicOS Performance Monitoring and Reporting

This feature provides support for SonicOS performance monitoring and supporting. This feature allows users to monitor several types of polling and trap information.

Topics:

- Session Usage Traps
- Dynamic NAT Translation Count Polling
- Dynamic NAT Translation Count Traps
- Management CPU Polling

- Management CPU Traps
- Forwarding/Inspection CPU Polling
- Network Interface Usage Polling
- Network Interface Usage Trap
- Firewall Throughput Trap

Session Usage Traps

Session usage traps can be configured to send trap information using internal options. Contact SonicWall Technical Support for more information.

Dynamic NAT Translation Count Polling

Dynamic NAT translation count polling retrieves the number of current connections that meet Network Address Translation (NAT).

Dynamic NAT Translation Count Traps

Dynamic NAT translation count traps send trap information once the current NATed connection exceeds 50% of the maximum defined value.

Management CPU Polling

Management CPU polling retrieves the percentage of management CPU utilization.

Management CPU Traps

Management CPU traps sends trap information once the current trap exceeds the configured threshold.

Forwarding/Inspection CPU Polling

Forwarding/Inspection CPU polling retrieves the CPU usage of Forwarding/Inspection plane.

NOTE: Forwarding/Inspection CPU means CPU usage on all data processors.

Network Interface Usage Polling

Network interface usage polling retrieves data on interface usage for a table that contains "sonicIfStatEntry" entries that correspond to specific interfaces. The table entries include:

- Name of an interface
- Usage for an interface

Network Interface Usage Trap

Network interface usage trap sends trap information when any physical interface utilization is greater than 80% of the maximum rated tolerance (for the interface) for more than 10 seconds.

Firewall Throughput Trap

Firewall throughput trap sends trap information once the total firewall throughput is greater than 50% of the maximum rated tolerance for more than 10 seconds.

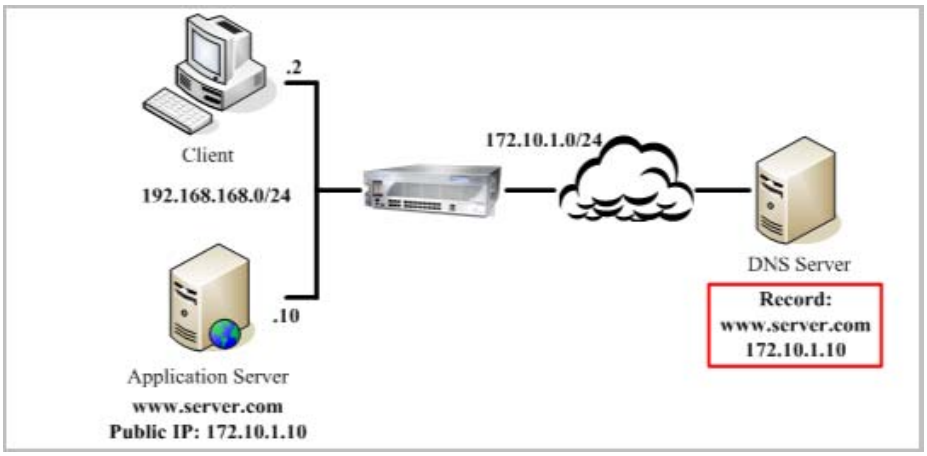
DNS Doctoring

DNS doctoring allows the Network Security Appliance (NSA) to change the embedded IP addresses in Domain Name System (DNS) responses, so that clients can connect to the correct server IP addresses. DNS Doctoring mainly performs two functions:

- Translates a public address in a DNS reply to a private address when the DNS client is on a private interface.
- Translates a private address to a public address when the DNS client is on the public interface.

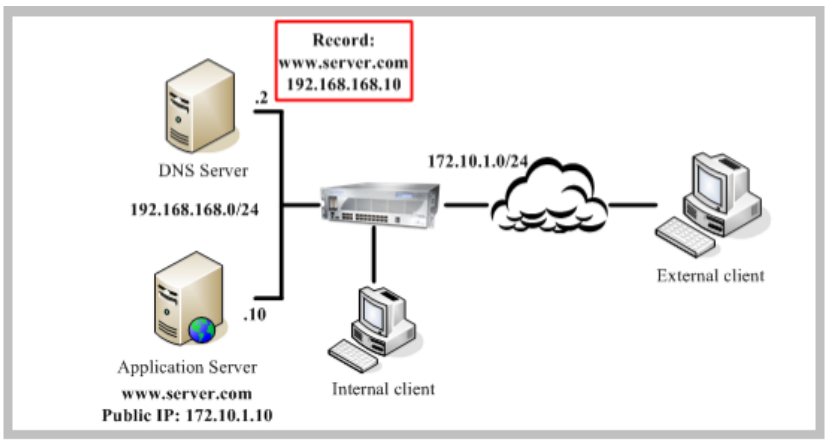
Use cases for DNS doctoring include:

- **Use Case 1:** The local client and the local application server are both located on the inside interface of the appliance, while the DNS server that the client uses is located on another public network. When the client wants to access the server with its URL, the DNS server returns the public address of the application server to the client. The client cannot access the local server with its public address.



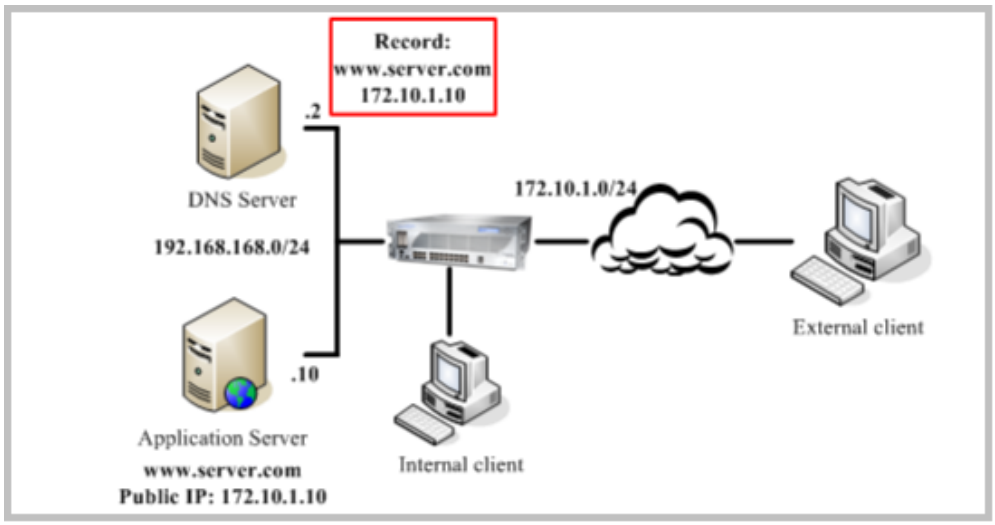
- **Use Case 2:** The DNS server and the application server are located on the inside interface of the appliance. For this scenario, the DNS server records either a private or public IP address.
  - **Private IP Addresses**

    In this case, the internal clients can get the correct IP (private) addresses from the DNS server. However, external clients can't access to the application server's private IP address. In this scenario, the NSA performs DNS Doctoring, allowing the external clients access to the public IP addresses.



- **Public IP Addresses**

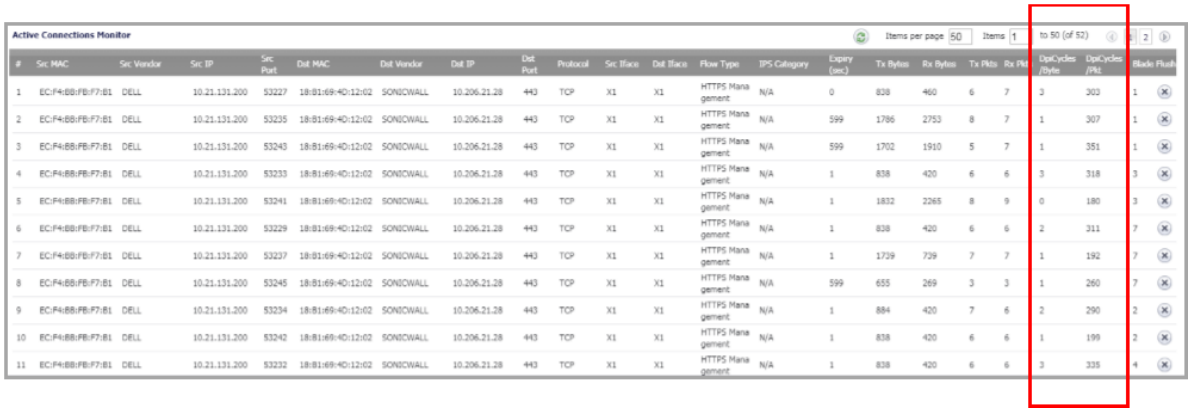
  In this case, the internal and external clients can get the correct IP (public) addresses from the DNS server. In this scenario, the NSA performs DNS Doctoring, to provide the internal clients with direct access to the application servers, without passing through appliances.



DPI Engine CPU Cycles Per Packet and Per Flow Limit

NOTE: This feature now only supports IPv4 addresses and does not support VPN tunnels. The original destination and translated destination can be either address objects or address groups.

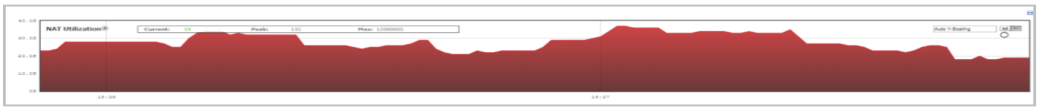
In the event of an unexpected increase in core utilization, SonicOS 6.4.1.1 provides the ability to easily identify the culprit connection with new "totalDpiCycles" 64-bit Byte and Packet counters. The new counters are displayed in the Connection Monitor. The value in each column represents the total number of CPU cycles used for DPI processing divided by total bytes/packets processed for each active connection. A dramatic increase in DPI cycle values can indicate a culprit connection.



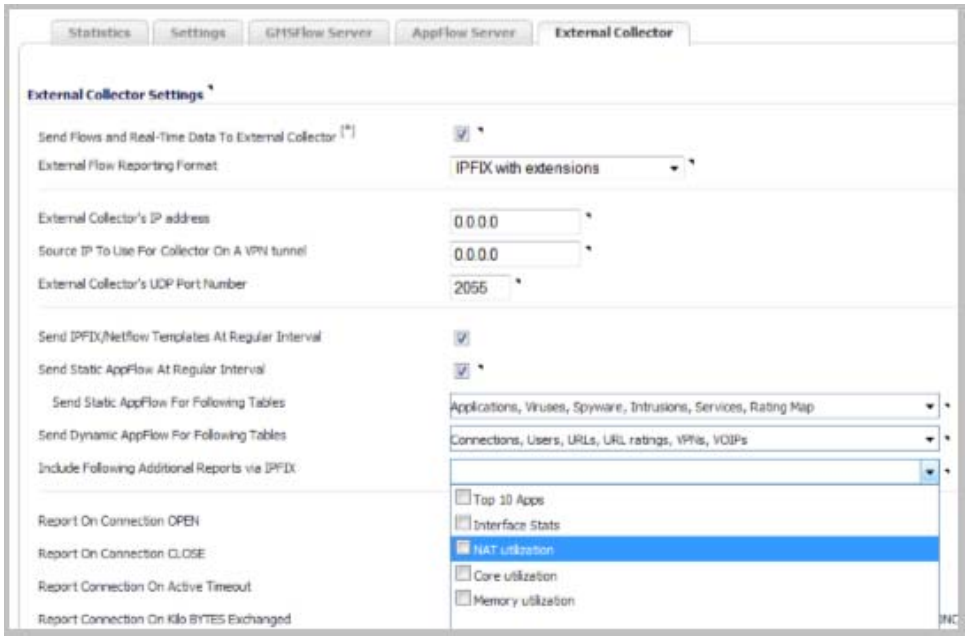
NAT Utilization Visualization

SonicOS 6.4.1.1 provides the ability to view NAT utilization status by accessing the Dashboard Real-Time Monitor, IP Flow Information Export, or Syslog pages. The following NAT utilization visualization options are available:

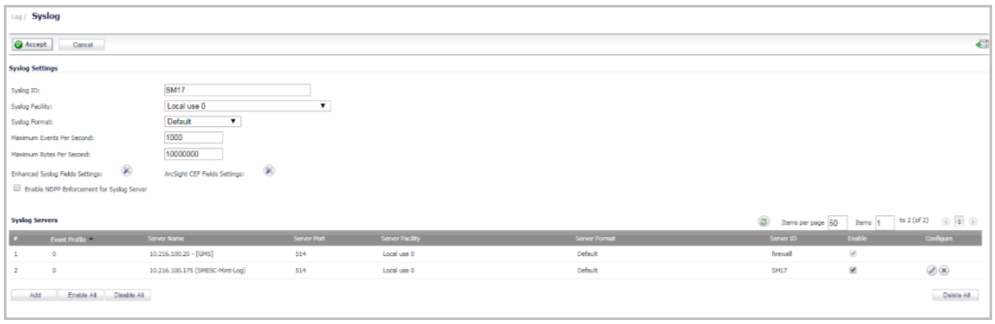
- **Dashboard Real-Time Monitor** displays the number of sessions using NAT in predefined time intervals.



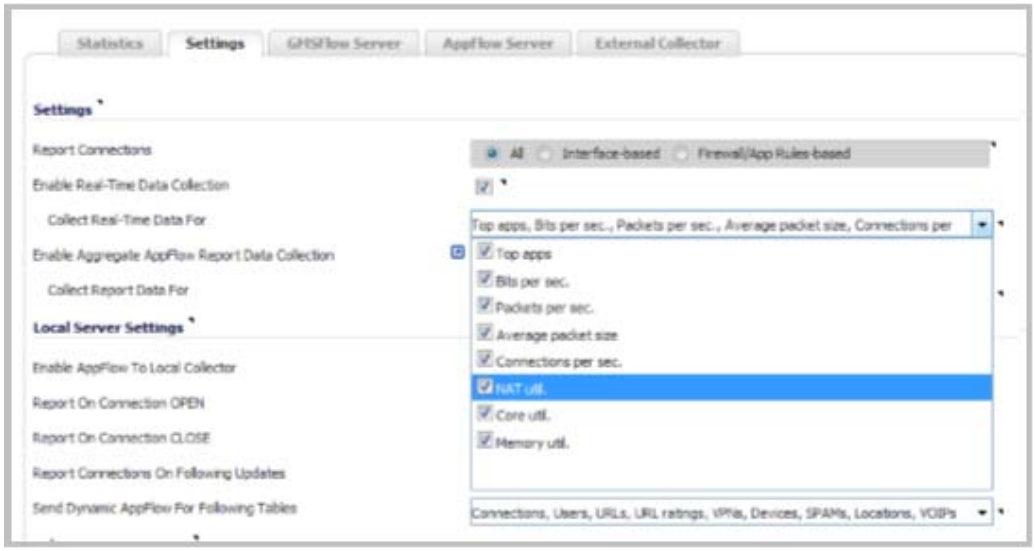
- **IP Flow Information Export (IPFIX)** exports NAT utilization stats to the License Manager Protocol (LMP), GMSFlow Server, AppFlow Server, and External Flow Collectors.



- **Syslog** receives reports on connections that meet NAT policy when translation occurs.



The collected statistics are aggregate usages of all NAT policies with translation, on all blades, and at a defined time.



NOTE: This feature only supports IPv4 addresses.

Resolved Issues

This section provides a list of resolved issues in this release.

Certificates

Resolved issue	Issue ID
Administrators without full permissions can download imported certificates. Occurs when administrators who are not in the SonicWall Administrators user group attempt to download imported certificates.	211749

Encryption

Resolved issue	Issue ID
The TLS Padding (Zombie POODLE and GOLDENDOODLE) and ROBOT attack vulnerabilities exist in SonicOS. Occurs when a connection to the appliance uses cipher block-chaining (CBC).	215940

Networking

Resolved issue	Issue ID
A misconfigured DHCP server on an external router causes the firewall to reboot. Occurs when the DHCP server does not have a subnet mask configured for the IP address range provided to the WAN interface of the SonicWall firewall.	219488
Under certain conditions, a vulnerability allows a user to access a limited section of the SonicOS command line interface (CLI).	210581

Known Issues

This section provides a list of known issues in this release.

AppFlow

Known issue	Issue ID
New filter does not save. Occurs when saving a new filter in AppFlow.	202988

Application Firewall

Known issue	Issue ID
Firewall application rule to limit bandwidth of HTTP downloads for ppt/txt files is not limiting bandwidth for incoming traffic (LAN-->WAN download).	202332

DPI-SSL

Known issue	Issue ID
When visiting certain websites, the browser displays a CA certificate error and the user must agree to the risk in order to continue to the website. Occurs when Client DPI-SSL presents a self-signed CA certificate generated using Go Daddy Class 2 Certification Authority to the client computer for certain websites. However, the Go Daddy Class 2 Certification Authority was removed from the list of Trusted CAs due to a weak signing algorithm.	220615
A secure FTP connection cannot be established. Occurs when DPI-SSL Client is enabled.	199229

Firmware GUI

Known issue	Issue ID
The error message “Failed to initiate import” is displayed. Occurs when opening the “import user” dialog on the LDAP configuration page.	200745

Log

Known issue	Issue ID
Every change/add/delete in the Network Monitor is logged 'N' Times, where 'N' equals the number of blades. Occurs when changes are made in the Network Monitor.	198941

Networking

Known issue	Issue ID
Enabled RIP/OSPF is disabled. Occurs when restarting the firewall.	203636

SSL VPN

Known issue	Issue ID
SSL VPN user information is not synchronized between high availability units. Occurs when SSL VPN is enabled and user logs in from a NetExtender client.	200283

VoIP

Known issue	Issue ID
VoIP service is disabled. Occurs when the firewall is configured in Network Address Translation (NAT) mode.	200078

VPN

Known issue	Issue ID
Traffic from Firewall protected subnet to client failed when the client connected to an IKEv2 VPN policy which gateway IP is specified, and IP Pool is used as remote network.	200078

System Compatibility

This section provides additional information about hardware and software compatibility with this release.

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.4.1.1 requires GMS 8.6 or higher for management of firewalls using the new features in SonicOS 6.4.1.1.

WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.4.1.1. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 9.0 and higher
- Safari 5.0 and higher running on non-Windows machines

NOTE: On Windows machines, Safari is not supported for SonicOS management.

NOTE: Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.

Upgrading Information

SonicOS 6.4.1.1 supports the upgrade of SonicOS 6.4.0.0 to SonicOS 6.4.1.1 on NS*sp* 12000 series appliances and on SuperMassive 9800 appliances.

SonicOS 6.4.1.1 supports the upgrade of SonicOS 6.2.7.8 to SonicOS 6.4.1.1 on SuperMassive 9800 appliances.

You can also import configuration settings to a SuperMassive 9800 running 6.4.1.1 from the following appliances running SonicOS 6.2.5.x, 6.2.6.x, and 6.2.7.x:

- SuperMassive 9200
- SuperMassive 9400
- SuperMassive 9600

It is not recommended to import settings from SonicOS 5.9 or from SonicOS 6.2.9 or higher.

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.2 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/en-us/support/technical-documentation.

IMPORTANT: You might need to update the ChassisOS and ChassisROM (FailSafe) versions prior to installing SonicOS 6.4.1.1 on your SuperMassive 9800, unless this was already completed. If this update has not been done, please contact SonicWall Technical Support before upgrading your appliance to 6.4.1.1.

On SuperMassive 9800, the minimum ChassisOS and ChassisROM (FailSafe) versions required for upgrading to SonicOS 6.4.1.1 are:

- ChassisOS 6.0.3.5
- ChassisROM (FailSafe) 6.2.1.7

On NS*sp* 12000 series, the minimum ChassisOS and ChassisROM (FailSafe) and BMC versions required for upgrading to SonicOS 6.4.1.1 are:

- ChassisOS 6.0.7.7
- ChassisROM (FailSafe) 6.2.4.3
- BMC 3.3

NOTE: The ChassisOS Apps version 6.0.7.5 is embedded in SonicOS 6.4.1.1 on NS*sp* 12000 series, and ***is not backward compatible*** to the previous versions of ChassisROM (FailSafe) and ChassisOS.

NOTE: The BMC version is not displayed in SonicOS. BMC stands for Baseboard Management Controller and is used to gather the following sensor values and control the hardware.

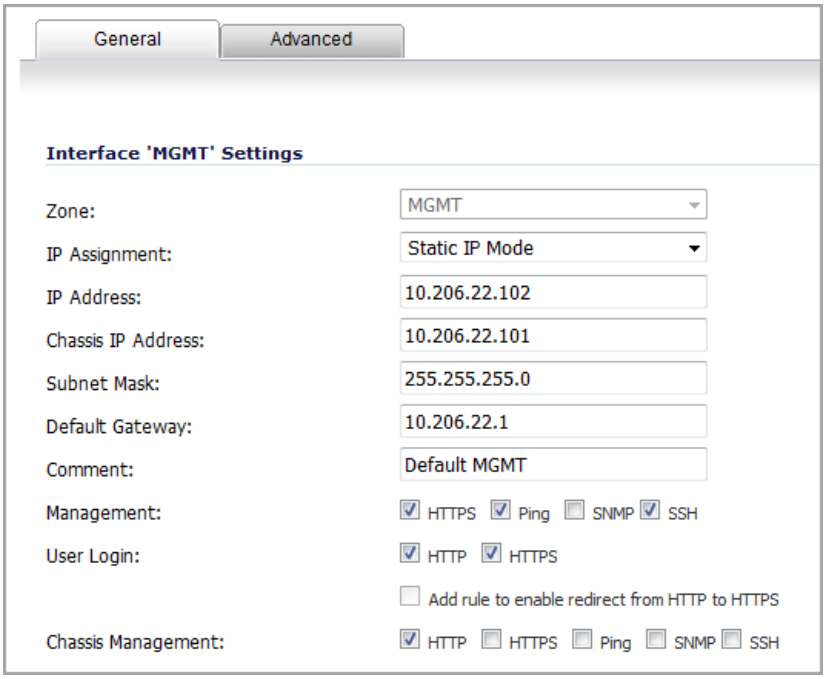
- Temperature
- Fan
- Power up and down chassis
- Power up and down blades

These sensor values are displayed in SonicOS.

The ChassisOS and ChassisROM (FailSafe) and ChassisOS Apps versions are displayed in the SonicOS SafeMode page.

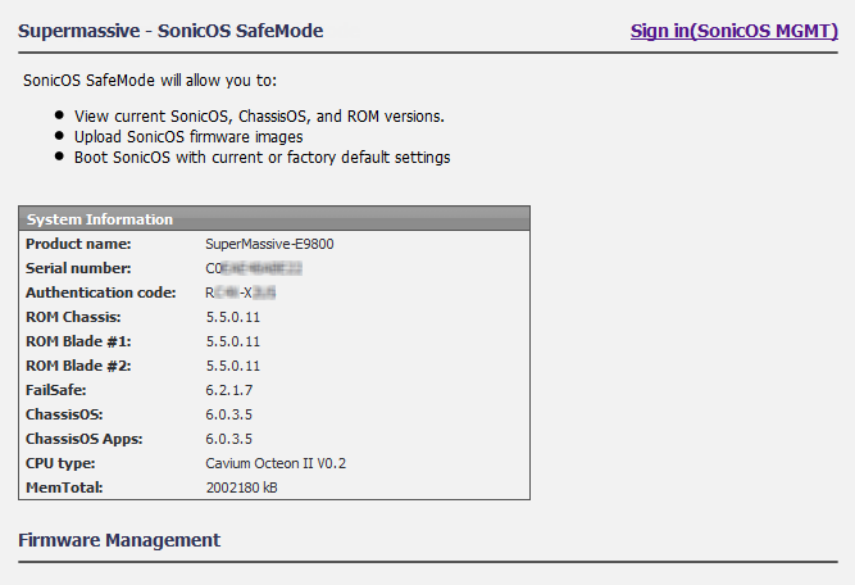
To view the SafeMode page:

1 Log into the appliance and navigate to the **Network > Interfaces** page. This page displays the **Chassis IP Address** and **Chassis Management** settings.



2 For **Chassis Management**, select the **HTTP** check box and then click **OK**.

3 Point your browser to the chassis IP address using HTTP, such as `http://10.206.22.101` in our example (use the chassis IP address for the primary unit in an HA pair). The SonicOS SafeMode page displays.



The ChassisROM (**FailSafe**) and **ChassisOS** and **ChassisOS Apps** versions are displayed.

4 After checking the versions, boot SonicOS to a firmware version displayed under **Firmware Management**.

5 Log into SonicOS and navigate to the **Network > Interfaces** page.

6 For **Chassis Management**, clear the **HTTP** check box and then click **OK**. This disables the SafeMode feature and protects your appliance from unauthorized access.

SonicWall Support

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

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 video tutorials
- Access MySonicWall
- 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.

Legend

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

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

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 7/25/19

232-004966-00 Rev A