# SonicWall® SonicOS 6.5.1.1

## Release Notes

### April 2018

These release notes provide information about the SonicWall® SonicOS 6.5.1.1 release.

Topics:



# About SonicOS 6.5.1.1

SonicOS 6.5.1.1 introduces a number of new features, fixes many known issues found in previous releases, and supports three new SonicWall network security platforms. See the New Features and Supported Platforms sections for more information.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.5. For more information, see the previous release notes, available on MySonicWall.

# Supported Platforms

SonicOS 6.5.1.1 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- NSA 5650
- NSA 4650
- NSA 3650
- NSA 2650
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

The New Platform Information table provides information about the three new SonicWall NSA appliances.

**New Platform Information**

| Hardware Component | NSA 3650 | NSA 4650 | NSA 5650 |
|---|---|---|---|
| 10 / 5 / 2.5 / 1G (SFP+) ports | 2 | 2 | 2 |
| 10 / 5 / 2.5 / 1G (copper) ports | N/A | N/A | 2 |
| 2.5 / 1G (SFP) ports | 8 | 4 | 4 |
| 2.5 / 1GbE (copper) ports | 4 | 4 | 4 |
| 1 GbE (copper) ports | 12 | 16 | 16 |
| 1 GbE MGMT port | 1 | 1 | 1 |
| Console RJ45 port | 1 | 1 | 1 |
| USB 3.0 ports | 2 | 2 | 2 |
| Fan | 2 | 2 removable | 2 removable |
| Power Supply | Removable 120W adapter (up to 2) | Redundant 350W (up to 2) | Redundant 350W (up to 2) |
| Built-In Storage (M0) | 32 GB | 32 GB | 64 GB |

# New Features

This section describes the new features introduced in SonicOS 6.5.1.1.

Topics:

- SonicOS API
- AWS Integration with SonicOS
- Next Gen Anti-Virus and DPI-SSL Enforcement
- CFS Blocking of Individual Videos
- Capture ATP Friendly Filename Display
- DHCPv6 Relay
- DPI-SSH Blocking of SSH Port Forwarding
- FQDN Address Objects for NAT
- FQDN Over TCP DNS
- Access Rule Enhancements
- CFS Custom Header Insertion for HTTP Requests
- Enhanced HTTP/HTTPS Redirection with DP Offload
- LLDP Support
- Per User Client Side UI Preferences Storage
- Refactored SonicOS Web Interface Layout
- Capture Threat Assessment Client Enhancements
- Increased SPI/DPI Connection Capacity
- DPI vs DPI-SSL Dynamic Connection Sizing
- DPI-SSL Scalability Through Extended Memory
- Active/Active Clustering on NSA Platforms

- SonicOS Global Search
- Source MAC Override for NAT
- UUID for Rules and Objects
- UX/UI Improvements for Content Pages
- WAN DDOS Protection Performance Enhancement

# SonicOS API

SonicOS APIs provide an alternative method to the SonicOS Command Line Interface (CLI) for configuring selected functions. For detailed information, see the *SonicOS API Reference*, available on the Support portal at https://www.sonicwall.com/en-us/support/technical-documentation.

**Topics:**

- Supported Methods and MIME Types
- HTTP Status Codes
- Status & Error Representation
- Enabling SonicOS API
- Client Authentication
- Example - Commit Pending Configuration
- Example - Address Object API Calls

## Supported Methods and MIME Types

SonicOS API utilizes four of the methods defined in the HTTP protocol (RFC 7231 & 5789) to create, read, update and delete resources. The table below describes the HTTP methods currently supported by SonicOS API.

**Supported HTTP Request Methods**

| HTTP Method | Description |
|---|---|
| GET | Retrieves the specified resource or collection of resources. GET is a read-only operation that does not alter appliance state or configuration. A GET operation should not contain a request-body. |
| POST | Submits data to be processed by the specified resource or collection of resources. In most cases, the POST verb is used by SonicOS APIs to create and add a resource to a collection of resources (for example, add a new MAC address-object to collection of objects). |
| PUT | Updates the specified resource. The data included in the PUT request-body replaces the previous configuration. |
| DELETE | Deletes the specified resource or collection of resources. |

SonicOS API uses standard HTTP status codes to report success or failure when servicing a request.

SonicOS APIs currently supports the following MIME types:

- Text/plain

  Example:

  ```
  GET /api/sonicos/address-objects/mac
  Accept: text/plain
  ```

- Application/JSON

Example:

```
POST /api/sonicos/address-objects/mac
Content-type: application/json
Accept: application/json
{
   "address_object": {
      "mac": {
       "name": "001122334455"
      ,"address": "001122334455"
      ,"multi_homed": true
      ,"zone": "LAN"
       }
   }
}
```

The **Content-type** HTTP header is used to specify the format (MIME type) of the request body (input). The **Accept** HTTP header is used to specify the format of the response body (output).

# HTTP Status Codes

SonicOS API uses standard HTTP status codes to report success or failure when servicing a request.

**HTTP Status Codes**

| Code | Status Text | Description |
|---|---|---|
| 200 | OK | The request succeeded. |
| 400 | Bad Request | An invalid request was submitted. Verify that the request URI is correct and that the request body is as expected. |
| 401 | Not Authorized | The user is unauthenticated or lacks the required privileges for the operation requested. |
| 403 | Forbidden | The request was understood by the server but denied. The response body will note the reason why the request was denied. |
| 404 | Not Found | The resource specified was not found. |
| 405 | Method Not Allowed | The HTTP verb specified is not allowed or supported by the resource specified. |
| 406 | Not Acceptable | The MIME type specified in the HTTP 'Content-type' and/or 'Accept' header is not supported. |
| 413 | Request body too large | Maximum size of the request body was exceeded. |
| 414 | Request URL too long | The request URL exceeded the maximum size allowed or contains extra/unknown parameters (directories). |
| 500 | Internal Server Error | The request failed due to an internal server error. The response body should note the reason why the request failed. |

# Status & Error Representation

All plain text output from the last CLI command executed is captured and returned back to the client. If the command executed was not a **show** command, and the requested operation succeeded, then the response body is empty. This is consistent with the CLI when executing a command via SSH or the serial console in that status is only rendered to the console upon error.

A JSON status object is guaranteed to be returned in the response body when performing a POST, PUT, DELETE operation or upon error(s) encountered when processing a request.

## Schema Structure

```
{
   "status": {
      "success": {boolean}
      ,"cli": {
         "depth": {number}
         ,"mode": "{string}"
         ,"command": "{string}"
         ,"configuring": {boolean}
         ,"pending_config": {boolean}
         ,"restart_required": "{string}"
      }
      ,"info": [
         { "level": "{string}", "code": "{string}", "message": "{string}" }
         ...
      ]
   }
}
```

## Schema Attributes

### Schema Attributes

| Attribute | Type | Description |
|---|---|---|
| status | object | Status object. |
| status.success | boolean (true\|false) | Boolean success flag. Refer to the status.info array for more detailed info as to what caused the error if the success flag is false. |
| status.cli | object | CLI status. Note, this attribute will only be included when an API sent one or more commands to the CLI backend. |
| status.cli.depth | number (uint8) | Current mode depth of the CLI. 0 = top-level mode, >= 1 config mode. |
| status.cli.mode | string | Name of the current mode. |
| status.cli.command | string | Command last executed. Note, this attribute will only be included upon command error(s). |
| status.cli.configuring | boolean (true\|false) | Boolean configuring flag. Should always be true upon one or more consecutive POST, PUT or DELETE API calls that modify configuration. |
| status.cli.pending_ config | boolean (true\|false) | Boolean pending-config flag. Should always be true upon one or more consecutive POST, PUT or DELETE API calls that modify configuration. This flag should be cleared once any/all pending changes are committed (saved). |
| status.cli.restart_ required | string | Appliance restart status. Some configuration changes require an appliance restart in order to take effect. The following values indicate the type of restart needed:<br>• NONE<br>• APPLIANCE<br>• CHASSIS<br>• CHASSIS_SHUTDOWN<br>• ALL_BLADES |
| status.info | array | Informational message(s). |
| status.info.level | string | Status level. One of the following types: info, warning, error. |
| status.info.code | string | Status code. If success, E_OK is returned, else E_{*XXX*} where *XXX* = error code. |
| status.info.message | string | Status message. |

# Enabling SonicOS API

SonicOS API is disabled by default in SonicOS. Any attempts to access SonicOS API while disabled will result in an HTTP 403 *Forbidden* error.

SonicOS API can be enabled by one of the following methods:

- In the SonicOS web management interface, navigate to **MANAGE | System Setup | Appliance > Base Settings** and select the **Enable SonicOS API** checkbox.
- In the CLI, starting at the `config#` prompt:

```
config(<serial number>)# administration
(config-administration)# sonicos-api
(config-administration)# commit
```

# Client Authentication

SonicOS API currently offers two mechanisms for client authentication:

- HTTP Basic Authentication (RFC 2617)
- Challenge-Handshake Authentication (CHAP)

Regardless of the authentication mechanism used:

- Only a single administrator can manage (modify configuration) at any given time. This remains true regardless of where an admin is logged in from (web management UI, CLI, GMS or SonicOS API).
- Only users with full admin privileges are allowed to access SonicOS API.
- Only a single SonicOS API session is currently allowed.

HTTP Basic Authentication is the simplest method for client authentication as it does not require cookies, session identifiers, etc. HTTP Basic Authentication uses the standard **Authentication** HTTP header to pass user credentials between the client and server. Because HTTP Basic Authentication provides no means for protecting the confidentiality of a user's credentials, SonicOS API requires user credentials to be transmitted over HTTPS.

For SonicOS API HTTP Basic Authentication, use the Linux command-line **curl** command with the **-u** option:

- Login:

```
curl -k -i -u admin:password -X POST https://a.b.c.d/api/sonicos/auth
```

- Logout:

```
curl -k -i -X DELETE https://a.b.c.d/api/sonicos/auth
```

# Example - Commit Pending Configuration

All SonicOS APIs that modify configuration (POST, PUT, DELETE) do not take effect immediately. Rather, configuration is staged and is not pushed to run-time config and saved to flash/permanent storage until API clients explicitly execute a POST request to `/api/sonicos/config/pending`. This is the same behavior as in the SonicOS CLI and equivalent to invoking the **commit** command from the top-level config mode.

Pending configuration can be canceled (deleted) at any time by executing a DELETE request to `/api/sonicos/config/pending`. Any/all pending configuration is canceled upon client session termination, whether due to idle-timeout or explicit logout. In this case, all unsaved changes are lost. It is the client's responsibility to either commit pending configuration after each POST/PUT/DELETE API call or maintain pending changes on the client side to be restored in a later session.

**Endpoint**

| **Endpoint** | **HTTP Method & Body** | | | |
|---|---|---|---|---|
| URI: */api/sonicos/config/pending* | GET | POST | PUT | DELETE |
| Schema: *N/A* | Empty | Empty | - | Empty |

## Schema Structure

A schema is not really applicable here as POST, PUT and DELETE HTTP body is expected to be empty. However, GET will return any/all pending (unsaved) configuration.

## Schema Attributes

Not applicable.

## Examples:

# GET Pending Changes (unchanged)

Request:

```
GET /api/sonicos/config/pending
Accept: application/json
```

Response:

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
}
```

# GET Pending Changes

Request:

```
GET /api/sonicos/config/pending
Accept: application/json
```

Response:

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
   "address_objects": [
      {
         "pending": "ADD"
         ,"ipv4": {
            "name": "B"
            ,"host": {
               "ip": "2.2.2.2"
            }
            ,"zone": "WAN"
         }
      }
   ]
}
```

# POST Pending Changes

Request:

```
POST /api/sonicos/config/pending
Accept: application/json
```

Response:

```
HTTP/1.0 200 OK
Server: SonicWALL
Content-type: application/json; charset=UTF-8
{
   "status": {
```

```
        "success": true
        ,"cli": {
           "depth": 1
           ,"mode": "config_mode"
           ,"configuring": true
           ,"pending_config": false
           ,"restart_required": "NONE"
        }
        ,"info": [
           { "level": "info", "code": "E_OK", "message": "Success." }
        ]
     }
  }
```

## Example - Address Object API Calls

# Create a new IPv4 Address Object named ***Web Server***

```
POST /api/sonicos/address-objects/ipv4
Content-type: application/json
```

```
{
   "address_object": {
      "ipv4": {
         "name": "Web Server",
         "zone": "DMZ",
         "host": {
            "ip": "192.168.168.168"
         }
      }
   }
}
```

# Modify the ***Web Server*** Address Object host IP

```
PUT /api/sonicos/address-objects/ipv4/name/Web%20Server
Content-type: application/json
```

```
{
   "address_object": {
      "ipv4": {
         "host": {
            "ip": "192.168.168.1"
         }
      }
   }
}
```

# Delete the ***Web Server*** Address Object

```
DELETE /api/sonicos/address-objects/ipv4/name/Web%20Server
```

# AWS Integration with SonicOS

The SonicOS integration with Amazon Web Services (AWS) enables logs to be sent to AWS CloudWatch Logs, Address Objects and Groups to be mapped to EC2 Instances, and creation of VPNs to allow connections to Virtual Private Clouds (VPCs). SonicOS communicates with the various Application Programming Interfaces (APIs) of AWS.

**Topics:**



# Creating an AWS Identity

IAM Identities, including Users and Groups, can be created and managed from the IAM page in the AWS Management Console.

Assuming that the AWS Account is already created and that an Administrator with either Root access or widespread privileges is logged into that account, it is then necessary to create an *IAM User*, if one does not already exist, that will be used by the firewall to access the various AWS APIs for the services supported by the firewall.

The user needs certain permissions to access the different services. These permissions can either be granted directly to the user or included in a security access policy assigned to an IAM Group and then the user added to that group.

The security policy used, either for a group to which the user belongs or attached to the user directly, must include the following permissions:

- AmazonEC2FullAccess – For **AWS Objects** and **AWS VPN**
- CloudWatchLogsFullAccess – For **AWS Logs**

The IAM user can be created specifically for use by the firewall alone. However, if the same user is going to access the AWS Management Console, the **Programmatic access** checkbox must be selected.

The second step of the Add User wizard determines which permissions the user will have assigned, either through adding the user to a group or attaching the permission policies directly.

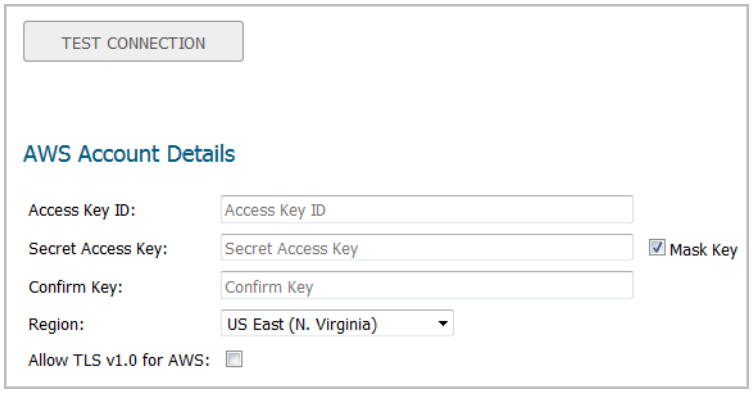
After reviewing the details of the user to be created and pressing the **Create User** button, there is a final and critical stage.

–DO NOT LEAVE THE ADD USER WIZARD–

You must retrieve the **Secret Access Key** that has been created for the user. The Secret Access Key together with the Access Key will be used in the configuration of the firewall. It will be needed for all API access to AWS. You should either copy it to a safe location or download the CSV file and keep that in a safe, secure location.

# AWS Access Configuration in SonicOS

You can configure SonicOS with the AWS Security Credentials on the **MANAGE | System Setup | Network > AWS Configuration** page.




The settings include an AWS Identity and Access Management (IAM) User's Access Key (**Access Key ID**), the corresponding **Secret Access Key** and a default region. The default region is used by the **AWS Logs** page, and for initialization of the **AWS Objects** and **AWS VPN** pages (though different regions can be selected on those two pages).

# AWS Logs Configuration

Logged events generated on the firewall can be sent to the AWS CloudWatch Logs service. From there, the data can be used by AWS hosted analysis tools such as ElasticSearch and Kibana.

The SonicOS **AWS Logs** page allows configuration of the AWS endpoint to which the logs are sent along with settings affecting the frequency with which the data is posted.

In order to send the logs from SonicOS to Amazon CloudWatch Logs, you must first create a Log Group and a Log Stream in AWS. Assuming that you have an Identity Access Management (IAM) user account with the appropriate permissions to access CloudWatch Logs from the AWS Console, navigate to the CloudWatch section and select the Logs item in the left hand navigation menu. Ensure that you have selected the appropriate AWS Region for the logs to be stored. As with many AWS services, CloudWatch Logs is region specific. First create the Log Group and then the Log Stream.

***To enable AWS logs in SonicOS:***

1. Navigate to the **MANAGE | Logs & Reporting | Log Settings > AWS Logs** page.
2. Select **Enable Logging**.
3. Ensure that the selected AWS **Region** is the one in which the Log Group and Log Stream were created. You can change the region used by the firewall either on this page or on the AWS Configuration page.
4. Enter the names of the **Log Group** and **Log Stream** that you created earlier and which will hold the logs sent to AWS CloudWatch Logs.
5. The logs will be sent at the specified **Synchronization Interval**. Change the Interval to suit your needs.
6. Click **ACCEPT**.

# AWS Objects Configuration

The **AWS Objects** page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with Address Objects (AOs) and Groups (AGs) configured on the firewall.

New AOs are created for Instance IP addresses, AGs for all addresses of an Instance and those Instance AGs can be added to existing Address Groups. Those objects, as with any other AOs and AGs, can then be used in firewall policies for networking, access control and to shape the interaction with EC2 Instances running on AWS.

In AWS, tag the EC2 Instance to then be able to use that tag when defining Address Object Mappings in SonicOS. With the Instance selected, click on the **Actions** button to launch the popup menu, and then choose **Instance Settings > Add/Edit Tags**.

***To create a new Address Object Mapping:***

1. Navigate to the **MANAGE | Policies | Objects > AWS Objects** page in SonicOS.
2. Click **New Mapping**.
3. Click the **New Condition** button to choose from the whole range of allowable properties.
4. For example, select *Custom Tag* for **Property**, then enter the key and value used in your EC2 Instance tag and click **OK**.
5. Optionally add a second mapping condition by clicking **New Condition** again.
6. When ready, click **OK**.
7. Click **ACCEPT** to save the mapping.

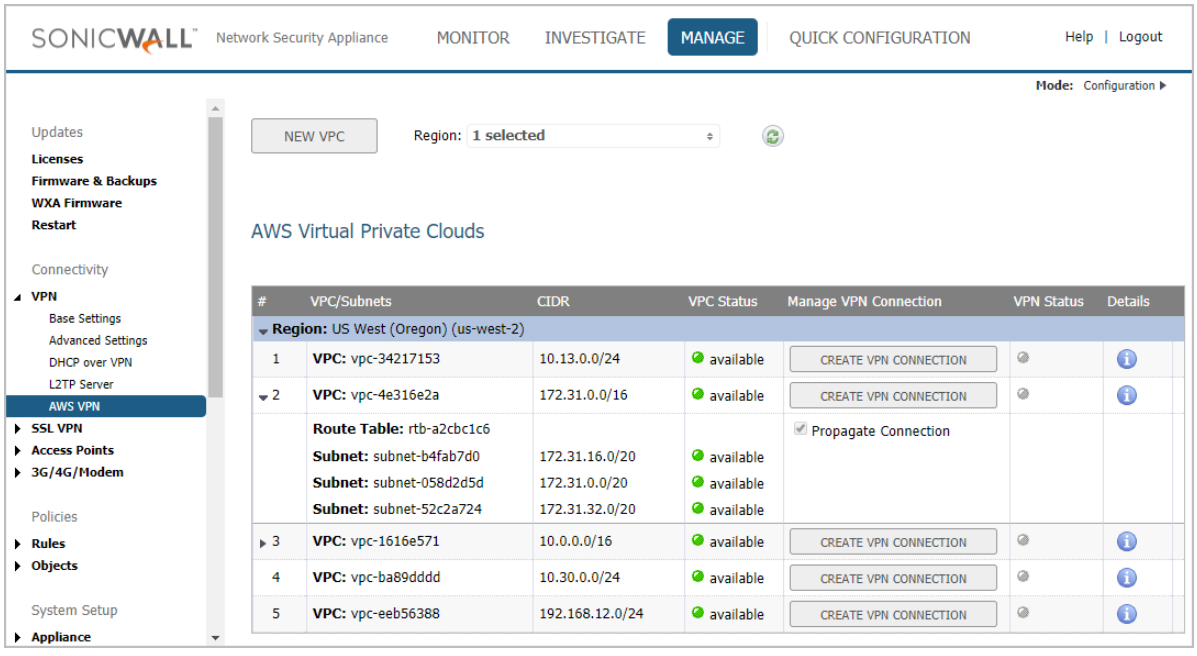
   Address Objects are then created for the IP addresses of each EC2 Instance that matches the mapping.
8. Select **Enable Mapping**.
9. Click **ACCEPT** to make the Address Object Mappings take effect.

With mappings in place, a **Synchronization Interval** set, **Regions to Monitor** specified, and **Enable Mapping** selected, you will see Address Objects and Groups representing the matched EC2 Instances and their IP addresses start to appear.

On the **AWS Objects** page, the Address Group and the Mapped Address Groups are shown in the AWS EC2 Instances table. Expanding the relevant row reveals the Address Objects corresponding to an Instance's public and private IP addresses. You can see those same host Address Objects on the **Objects > Address Objects** page in SonicOS.

# AWS VPN Configuration

Establishing and managing the connections between the computers on the local area network (LAN) and those in the Virtual Private Clouds (VPCs) on AWS is achieved by using the **MANAGE | Connectivity | VPN > AWS VPN** page in SonicOS.



The VPC table on the SonicOS **AWS VPN** page reflects the VPC information that is available on the AWS Console under the VPC Dashboard.

The administrator can browse VPCs from one or more AWS Regions and create VPNs between the firewall and the subnets on each of those VPCs. The creation of firewall VPN and Route Policies, VPN Tunnels and associated Address Objects along with the necessary gateways and propagating the connections on AWS are all done automatically when the administrator clicks the button to establish a connection.

***To create a new VPN connection:***

1. Navigate to the **MANAGE | Connectivity | VPN > AWS VPN** page in SonicOS.
2. Click the **Create VPN Connection** button in the row for the VPC you wish to connect to the firewall.
3. In the **New VPN Connection** dialog, verify that the **IP Address** field contains the public IP address of the firewall, or change it as needed.

   If the firewall is behind a router or some other proxy, NAT rules should be put in place to ensure VPN traffic initiated from the AWS side is able to be routed back to the firewall.
4. If the firewall detects that route propagation is disabled for one or more route tables within a VPC, the dialog will include the **Propagate connection to all existing subnets in the VPC** option. Select it unless you prefer to propagate the connection only to specific subnets (see Step 6).
5. Click **OK**.

   A series of processes on both the firewall and AWS configure the VPN connection between them. You can click the *Information* 'i' button in the table row for details about the VPN connection. Use the *Refresh* button on the **AWS VPN** page to reload the data in the table and on the associated dialogs.
6. After the VPN Connection is established, expand the row on the **AWS VPN** page to display all of the subnets in that VPC, organized by route table. Select **Propagate Connection** for each route table (unless you chose to enable propagation for all route tables in Step 4) and the associated subnets.

***To delete a VPN connection:***

1. On the **MANAGE | Connectivity | VPN > AWS VPN** page, click **Delete VPN Connection** in the related table row.
2. Click **YES** in the confirmation dialog.

   Deletion removes the associated VPN and Route Policies, and the Tunnel interfaces on the firewall. On AWS, it removes the Customer Gateway only if it is not being used elsewhere (perhaps on other VPN Connections from the same firewall, but to other VPCs). It does not delete the VPN Gateway or change the Route Propagation settings.

# Next Gen Anti-Virus and DPI-SSL Enforcement

SonicOS firewalls, version 6.5.1.1 or higher, are designed to support the enforcement service for Next-Gen AV (NGAV).

NGAV is the natural evolution of traditional AV that protects computers from the full spectrum of modern cyber attacks, delivering the best endpoint protection with the least amount of work. NGAV has a different technical approach in the way malicious activity is detected and blocked by taking a system-centric view of endpoint security, examining every process on every endpoint to algorithmically detect and block the malicious tools, tactics, techniques and procedures (TTPs) on which attackers rely.

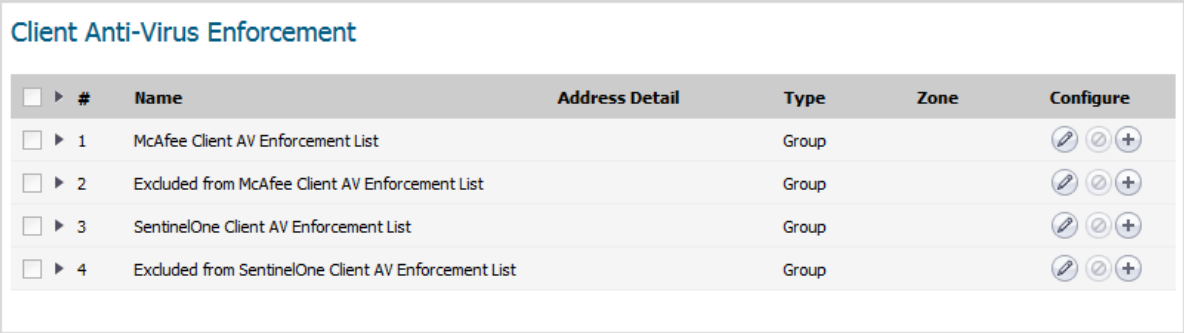
NGAV does four critical things to protect businesses:

- Prevents commodity malware better than traditional AV
- Prevents unknown malware and sophisticated attacks by evaluating the context of an entire attack resulting in better prevention (traditional AV does not).

- Provides visibility and context to get to the root cause of a cyber attack and provide further attack context and insight (traditional AV does not)
- Remediates attacks (traditional AV simply stops mass malware)

Additionally, NGAV is easy to deploy and easy to administer from the cloud. Currently, SonicWall firewalls are designed to support NGAV enforcements such as DPI-SSL Enforcement and SentinelOne AV enforcement.

This new feature is configured in the **Client Anti-Virus Enforcement** section of the **MANAGE | Security Configuration > Security Services > Client AV Enforcement**:




# CFS Blocking of Individual Videos

Starting in SonicOS 6.5.1.1, SonicWall Content Filtering Service (CFS) can filter and block individual YouTube videos. Previously, CFS could only allow or block *all* YouTube videos.

CFS inspects the site domain for each HTTP connection, and if the domain matches `youtube.com`, it extracts the video information from the query string, then reconstructs a new URI and sends a rating request for it to the CFS server. The reconstructed URI looks like this: `www.youtube.com/watch/v=-uWymC73jOY`.

This feature is supported when using the SonicWall public CFS server, but not when using a local CFS server. This is due to a conflict with the blacklist/whitelist feature in the local CFS server.

This feature only works if the SonicWall CFS server already has a rating for the specific video identified in the "`v=`" parameter of the URI.

No SonicOS configuration is required.

# Capture ATP Friendly Filename Display

In SonicOS 6.5.1.1, SonicWall Capture Advanced Threat Protection logs the friendly filename of scanned files for the following non-HTTP protocols:

- SMTP
- IMAP
- POP3
- NetBIOS
- FTP

With this feature, system administrators can easily identify the files being scanned by Capture ATP and their status. Previously, *(unknown)* was displayed for filenames of these protocol types in the Capture > Status table, and log messages referred to *a file*.

Limitations:

- Friendly filenames up to a maximum of 256 characters are supported.
- This feature cannot parse filename information for TCP protocol streams.

- This feature cannot parse a filename if it is not part of single network packet.

No SonicOS configuration is required.

# DHCPv6 Relay

SonicOS 6.5.1.1 supports DHCPv6 Relay. A DHCP relay agent is a node that acts as an intermediary to deliver DHCP messages between clients and servers, and is on the same link as the client. A *DHCPv6* relay agent is used to relay messages between the client and the server when they are not on the same IPv6 link.

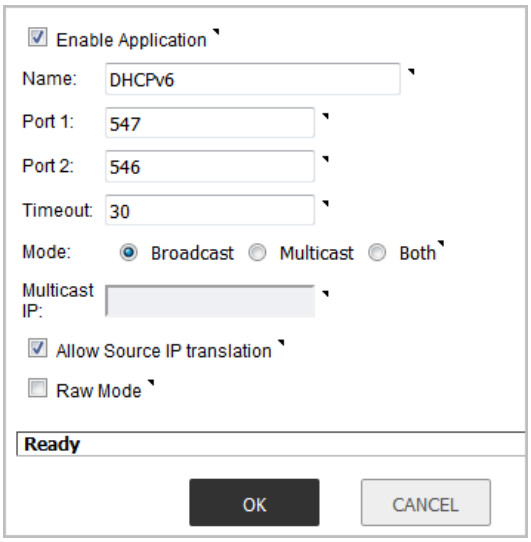
In SonicOS 6.5.1.1, supported destination addresses can be global addresses or link-local addresses, but not multicast addresses. DHCPv6 relay can be enabled on both physical and virtual interfaces. You can configure it from the **MANAGE | System Setup | Network > IP Helper** page.

***To configure DHCPv6 relay:***

1 Navigate to the **MANAGE | System Setup | Network > IP Helper** page.

2 In the **Relay Protocols** section, click **ADD**.

3 In the **Add IP Helper Application** dialog, configure the protocol **Name**, **Port 1**, **Port 2**, and **Timeout** fields.




4 For **Mode**, select **Broadcast**.

5 Select the **Enable Application** checkbox and **Allow Source IP translation** checkbox.

6 Click **OK**.

7 In the **Policies** section, click **ADD**.

8 In the **Add IP Helper Policy** dialog, select **DHCPv6** from the **Protocol** drop-down list.

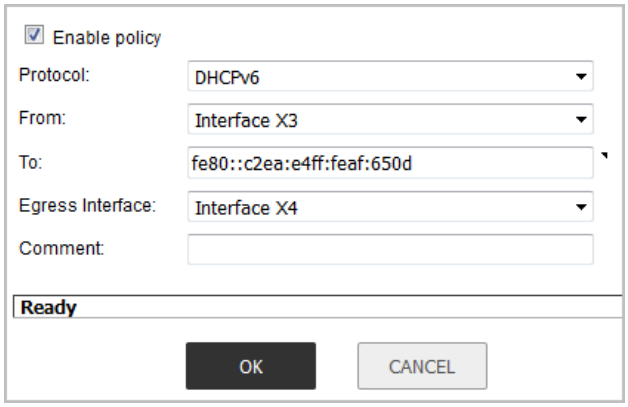
9 Select the desired interface from the **From** drop-down list.

10 In the **To** field, type in the destination IPv6 address.

11 In the **Egress Interface** drop-down, do one of the following:

- If the destination in the **To** field is a global address, there is no need to select an egress interface.

- If the destination in the **To** field is a link-local address, select an egress interface.




12 Click **OK**.

A new DHCP lease will appear in the **DHCPv6 Relay Leases** section of the page when the client gets a new IP address from the server.

# DPI-SSH Blocking of SSH Port Forwarding

SSH makes it possible to tunnel other applications through SSH by using port forwarding. Port forwarding allows local or remote computers (for example, computers on the internet) to connect to a specific computer or service within a private local-area network (LAN). Port forwarding translates the address and/or port number of a packet to a new destination address and forwards it to that destination according the routing rules. Since these packets have new destination and port numbers, they can bypass the firewall security policies.

To prevent circumvention of the application -based security policies on the SonicWall firewall, SonicOS 6.5.1.1 supports blocking of the port forwarding feature for Local and Remote port forwarding.

- Local port forwarding allows a computer on the local network to connect to another server, which might be an external server.

  *Dynamic* port forwarding allows you to configure one local port for tunneling data to all remote destinations. This can be considered as a special case of Local port forwarding.

- Remote port forwarding allows a remote host to connect to an internal server.

You can enable this feature by selecting the **Block Port Forwarding** checkbox and enabling either or both Local Port Forwarding and Remote Port Forwarding from the **MANAGE | Security Configuration | Decryption Services > DPI-SSH** page in SonicOS.

DPI-SSH must be enabled for blocking of SSH port forwarding to work. DPI-SSH decrypts incoming SSH packets and inspects the commands. If any local or remote port forwarding requests are made when the blocking feature is enabled, SonicOS will block those requests and reset the connection.

SSH is a secure channel that supports shell, file transfer, port forwarding, and other services. Specific clients and servers are supported.

DPI-SSH port forwarding supports the following clients:

- SSH client for Cygwin
- Putty
- SecureCRT
- SSH on Ubuntu
- SSH on CentOS

DPI-SSH port forwarding supports the following servers:

- SSH server on Fedora

- SSH server on Ubuntu

SSH port forwarding supports both:

- Route mode
- Wire mode – only supported in Secure Mode

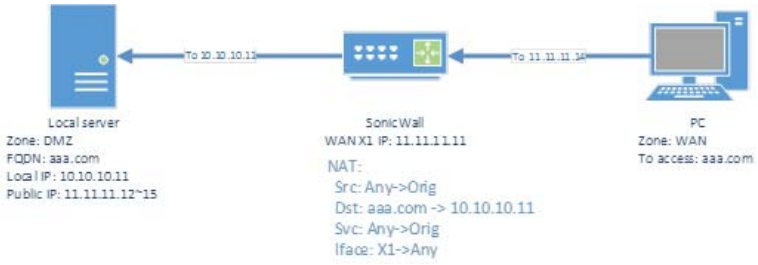
SSH port forwarding supports a maximum of 1000 connections, matching the maximum supported by DPI-SSH.

# FQDN Address Objects for NAT

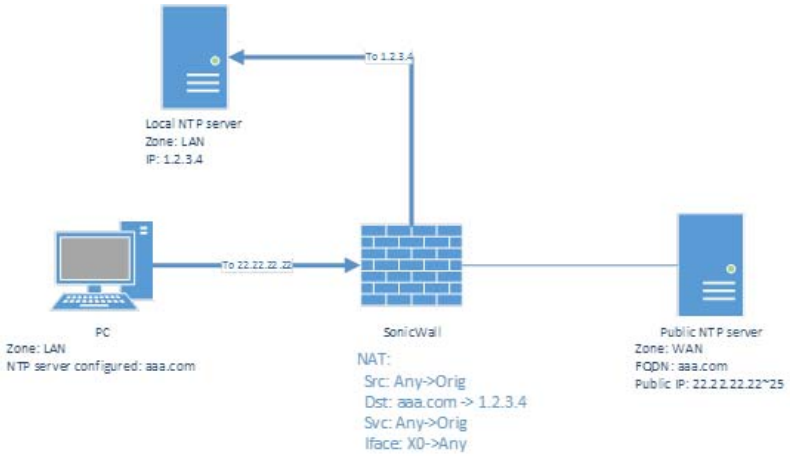
SonicOS 6.5.1.1 supports NAT policies using FQDN Address Objects for the original source/destination.

Use cases include:

- Specifying public IP addresses with FQDN to a local server




- Specifying a public server with FQDN for consistency across replacement with a server that has a known IP address




- Routing traffic from/to a FQDN to have a source IP address other than the outbound interface IP.


The following functionality is supported:

- The original source/destination can be a pure FQDN or an address group with FQDN(s) and other IPv4 or IPv6 addresses, depending on the IP version of the NAT policy. A new FQDN address object can be directly created from the **MANAGE | Policies | Rules > NAT Policies** page.

FQDN is not supported for the translated source/destination.

- IP Version options are provided for a NAT policy only if the version is ambiguous based on settings for original/translated source/destination fields. Either IPv4 or IPv6 must be selected.
- Mousing over an FQDN object of a NAT policy displays the IP addresses in the same IP version as the NAT policy.
- When NAT translation is performed, only the IP addresses in the NAT's IP version are considered.
- The Advanced page is disabled if FQDN is used in either or both the original source/destination fields.

  If probing is enabled and/or the NAT method is configured to a non-default value such as Sticky IP, neither of original source/destination address objects can be modified to contain an FQDN.
- FQDN based NAT policies are supported in High Availability configurations.

# FQDN Over TCP DNS

SonicOS 6.5.1.1 provides a new **Enable DNS host name lookup over TCP for FQDN** option on the **MANAGE | System Setup | Network > DNS** page.

By default, DNS queries are sent over UDP. The DNS response can include a Truncated flag if the response length exceeds the maximum allowed by UDP.

When the **Enable DNS host name lookup over TCP for FQDN** option is enabled and the Truncated flag is set in the DNS response, SonicOS sends an additional DNS query over TCP to determine the full DNS response for multiple IP addresses. When the option is disabled, DNS queries are sent over UDP and SonicOS only processes the IP addresses in the DNS response packet, although the Truncated flag is set in the response.

The DNS query times out after 1 second if no DNS response over TCP is received from the DNS server.

# Access Rule Enhancements

SonicOS 6.5.1.1 provides several feature enhancements to Access Rules:

- Rules with Any zone
- Priority Options
- Rule Hit Counters
- Timestamps

## Rules with Any zone

- Allows using *Any* for source and destination zones of an access rule during configurations.
- Maintains a single flat list for the configuration table.
- Adds source and destination zones as key dimensions to search in the lookup table.
- Prioritizes rules based on zones in the auto prioritize feature.
- No changes to how manual priority works.
- A single set of counters per unit for *save count*, *connection count* and similar counters.

## Priority Options

- New rules have the option of setting a priority for the rule in the table. The following three options are provided:
    - Auto Prioritize - SonicOS chooses the index according to an algorithm in which the most specific rules are given the highest priority.
    - Insert at the end - New policies are inserted at the end of the rule table.
    - Manual Priority - New policies are inserted at the index provided by the administrator.
- The SonicOS web management interface and CLI provide an option to choose the priority of the new rule.

## Rule Hit Counters

- Support per rule counters to keep track of rule hits.
- Counters are saved in the exported configuration settings to maintain persistence.
- Counters are displayed in the SonicOS web management interface and in the TSR.
- An option to clear counters is available in the SonicOS web management interface and CLI.

## Timestamps

- Support for the following timestamps per rule:
    - Creation Time – Time that the rule was created.
    - Last Updated – Time when the last edit was done.
    - Last Hit – Time when the most recent connection was classified by this rule.
- Timestamps are saved in the exported configuration settings to maintain persistence.
- Timestamps are displayed in the SonicOS web management interface and in the TSR.

# CFS Custom Header Insertion for HTTP Requests

In SonicOS 6.5.1.1, administrators can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

This feature requires the following:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.

***To configure a CFS custom header and enable custom header insertion:***

1. In the SonicOS web management interface, navigate to the **MANAGE | Policies | Objects > Content Filter Objects** page.
2. Click **CFS Profile Objects**.
3. Click the **Add** icon.
4. In the **Add/Edit CFS Profile Object** dialog, click **Custom Header** to display the Custom Header Insertion options.

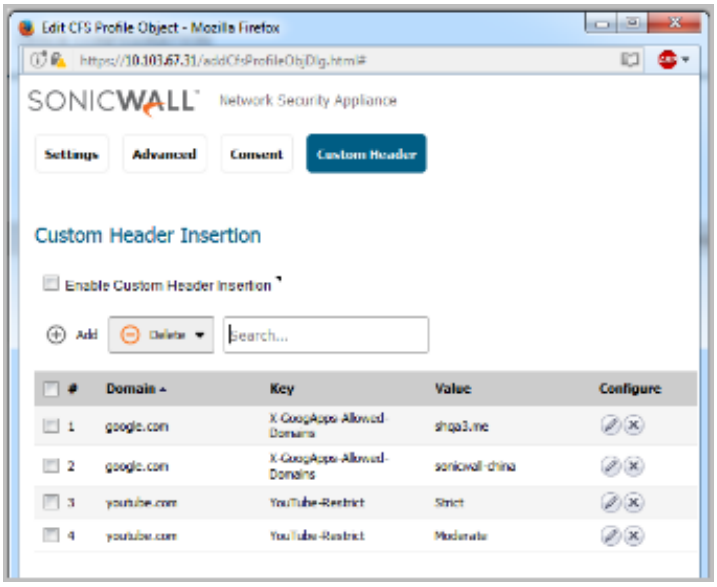
5 Select the **Enable Custom Header Insertion** option.

6 Click **Add** to configure the **Domain**, **Key**, and **Value** for the custom header entry.

**Domain** is used to check whether the host in an HTTP request is matched to an entry during packet handling. **Key** and **Value** are used to generate the right header for the entry when building runtime data for custom header insertion.

The **Domain** can contain:

- Each domain name can contain up to 16 tokens separated by periods (**.**).
- The domain name cannot start or end with separators.
- Each token can contain up to 128 printable ASCII characters.
- Tokens in a domain name can only contain the characters: **0-9a-zA-z$-_+!'(),.**
- IPv4/IPv6 addresses can be defined as a domain name, for example `[2001:2002:2003::2005:2006]`.




7 Click **OK**.

# Enhanced HTTP/HTTPS Redirection with DP Offload

In SonicOS 6.5.1.1, this feature improves handling of HTTP/HTTPS redirection requests that occur when user authentication is required for users to get access through the firewall. HTTP/HTTPS requests received from sources that are not authenticated users are redirected to the firewall's login page, which is served up by its built-in web server. This redirection happens if Single Sign-On (SSO) cannot identify the user, or if SSO is not in use.

If HTTP/HTTPS requests are received from sources from which users do not log in, and one or more such sources repeatedly try to open new connections, it can flood the firewall with connections that all need to be redirected. These could be non-user devices that are validly trying to get access, or it could be malicious code attempting a DOS attack. The effect that it has on the firewall is to cause high CPU load in the Control Plane (CP), which can impact web management access if it gets too high.

This feature improves efficiencies in both the web server and the HTTP/HTTPS redirection processes, and offloads most of the redirection processes to the Data Plane (DP) where the processing can be spread across multiple cores.

***To enable the HTTP/HTTPS redirection feature:***

1 In the SonicOS web management interface, select the **Add rule to enable redirect from HTTP to HTTPS** option.

   This option is found in the **Edit Interface** dialog when editing a physical interface from the **Network > Interfaces** page, depending on the **Mode/IP Assignment** setting. You can also set this option in the **Add Interface** dialog when adding a **Virtual Interface** or a **WLAN Tunnel Interface**.

   Enabling redirect from HTTP to HTTPS creates an access rule that also enables certain intermediate redirect pages to be fetched via HTTP even when the final page is served via HTTPS. This effectively allows redirection from HTTPS to HTTP for those intermediate tasks, but does not incur any security issues.

2 Click **OK**.

Elements of this feature can be controlled by *internal* User Authentication Settings options. This includes an option to globally enable/disable redirection processing in the DP, a flush option to clear the redirect files cache, and an option to specify the internal NAT port number used for the web server. Contact SonicWall Technical Support for information about internal settings.

# LLDP Support

SonicOS 6.5.1.1 supports Link Layer Discovery Protocol (LLDP) on the following platforms:

- NSA 3600 / 4600 / 5600 / 6600
- SuperMassive 9200 / 9400 / 9600

LLDP is also supported when High Availability is enabled.

LLDP is used to discover neighboring devices and their capabilities. LLDP operates at Layer 2 and exchanges LLDP Protocol Data Units (LLDPDUs) between the neighbors containing a sequence of variable length information elements that include type-length-values (TLV). The information is stored in the SNMP MIBs. LLDP makes troubleshooting easier, especially in cases where the peers are not detected by ping or traceroute.

Three LLDP modes are supported in SonicOS 6.5.1.1:

- LLDP-receive (already supported in previous versions of SonicOS 6.5)
- LLDP-transmit
- LLDP-transmit-receive

LLDP profiles can be created on individual interfaces to choose the modes.

LLDP is supported with the following interface types and modes:

- L2 Interface – if the physical port is configured in L2 Mode
- L3 Interface – if the physical port is configured in L3 Mode
- Wire-Mode Interface – supported only for the physical interface, but not for VLAN interfaces
- L2 Bridge Interface – supported for the physical interface, but not for VLAN interfaces
- VLAN Sub-Interface – not supported
- LAG/LACP – supported on the primary port of the LAG

Each LLDP frame starts with three mandatory TLVs: Chassis ID, Port ID and TTL. The mandatory TLVs are followed by any number of optional TLVs. The LLDP frame ends with a mandatory End-of-frame TLV.

The Mandatory TLVs table describes the mandatory LLDP TLVs supported for both transmit and receive.

### Mandatory TLVs

| TLV Name | TLV Type | Description | SonicOS Usage |
|---|---|---|---|
| Chassis ID TLV | 1 | Identifies the firewall chassis. Each firewall must have exactly one unique Chassis ID. | SonicOS sends the MAC address of the firewall in the Chassis ID field. The MAC address is same as the firewall serial number. |
| Port ID TLV | 2 | Identifies the port from which the LLDPDU is sent. The firewall uses the interface's ifname as the Port ID. For example, Port ID can be X1, X2, X3, … | The Port ID subtype 5 (interface name) is used to identify the transmitting port. |
| Time-to-live (TTL) TLV | 3 | Specifies how long (in seconds) LLDPDU information received from the peer is retained as valid in the local firewall (range is 0-65535). The value is a multiple of the LLDP Hold Time Multiplier. When the TTL value is 0, the information associated with the device is no longer valid and SonicOS removes that entry from the database. | Calculated internally |
| End of LLDPDU frame TLV | 0 | Indicates the end of the TLVs in the LLDP Ethernet frame. | |

The Optional TLVs table describes the optional LLDP TLVs supported for both transmit and receive.

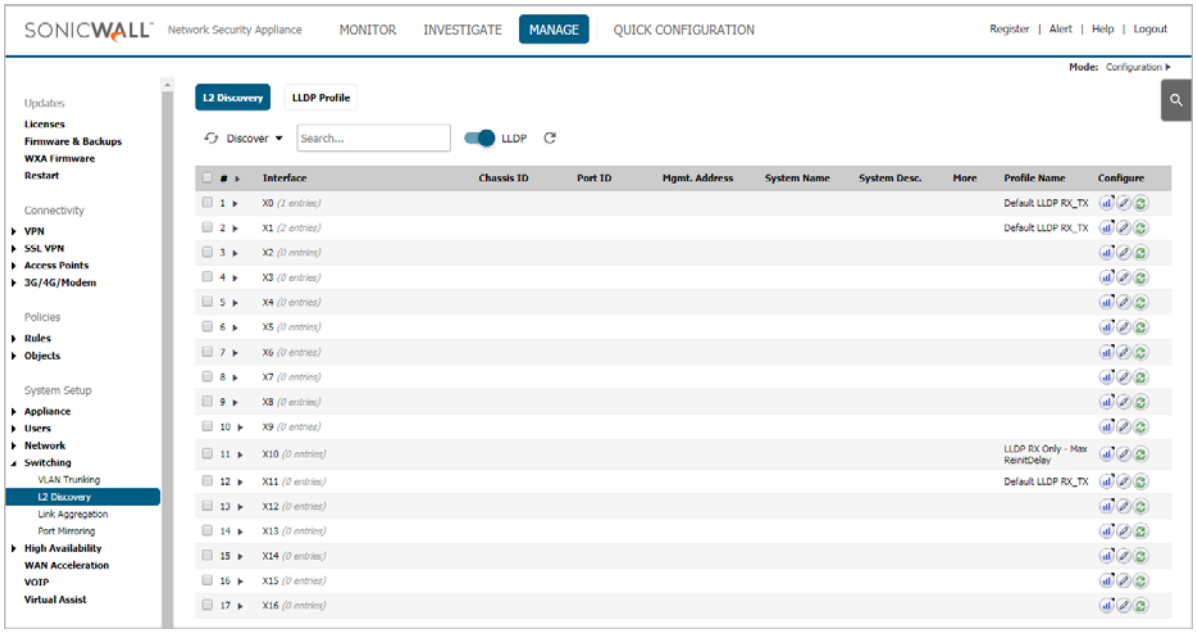
### Optional TLVs

| TLV Name | TLV Type | Description | SonicOS Usage |
|---|---|---|---|
| Port Description | 4 | The port description in alpha-numeric format. | Advertises the values/string added in the comment section of network interface field. |
| System Name | 5 | The firewall name in alpha-numeric format. | Advertises the Firewall Name configured on the System Administration page. |
| System Description | 6 | The full name and version identification of the system's hardware type, software operating system, and networking software in alpha-numeric format. | Advertised as “Firewall” in this field. |

### Optional TLVs

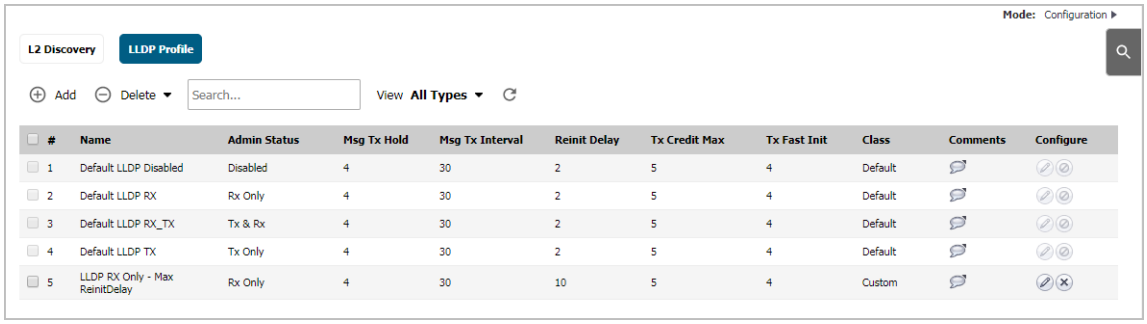
| TLV Name | TLV Type | Description | SonicOS Usage |
|---|---|---|---|
| System Capabilities | 7 | This field contains a bit-map of the capabilities that define primary functions of the system. Describes the deployment mode of the interface, as follows:<br>• An L3 interface is advertised with router (bit 6) capability and the “other” bit (bit 1).<br>• An L2 interface is advertised with MAC Bridge (bit 3) capability and the “other” bit (bit 1).<br>• A virtual wire interface is advertised with Repeater (bit 2) capability and the “other” bit (bit 1). | Advertises the features supported by the firewall and the enabled features. |
| Management Address | 8 | One or more IP addresses used for the management of the device, as follows:<br>• IP address of the management (MGT) interface<br>• IPv4 and/or IPv6 address of the interfaceLoopback address<br>• User-defined address entered in the management address field; If no management IP address is provided, the default is the MAC address of the transmitting interface. The interface number of the specified management address is included. Also included is the OID of the hardware interface with the specified management address (if applicable). If more than one management address is specified, they are sent in the order they are specified, starting at the top of the list. A maximum of four Management Addresses are supported.<br>This is an optional parameter and can be left disabled. | Advertises the management IP address of an interface if it is configured. |

The LLDP options are configured on the **MANAGE | System Setup | Switching > L2 Discovery** page.

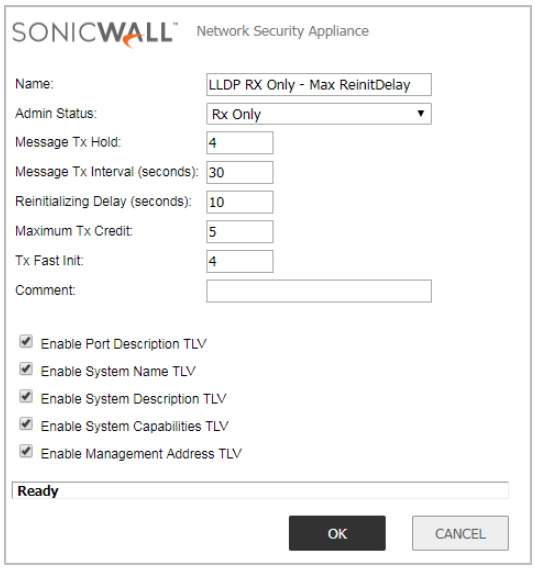



By default LLDP is globally enabled. You can toggle the **LLDP** switch to enable or disable LLDP transmit and receive globally.

LLDP profiles are created on the **LLDP Profile** screen of this page. SonicOS 6.5.1.1 supports a maximum of 20 LLDP Profiles.




You can add an LLDP Profile by clicking **Add**, or edit one by clicking the **Configure** button in its row.



The fields of the LLDP Profile are described as follows:

- **Name** – Any string value given to the LLDP profile
- **Modes** – Disable, Receive-Only, Transmit-Only, Transmit-and-Receive
- **LLDP Protocol Parameters** – The following parameters are used for the LLDP transmit state-machine. Changing the values will affect the duration and the number of frames transmitted during each cycle.
    - **msgFastTx** – This variable defines the time interval in timer ticks between transmissions during fast transmission periods (that is, txFast is non-zero). The default value of msgFastTx is 1; this value can be changed by to a value in the range 1 through 3600.
    - **msgTxHold** – This variable is used, as a multiplier of msgTxInterval, to determine the value of txTTL that is carried in LLDP frames transmitted by the LLDP agent. The default value of msgTxHold is 4; this value can be changed any value in the range 1 through 100.
    - **msgTxInterval** – This variable defines the time interval in timer ticks between transmissions during normal transmission periods (i.e., txFast is zero). The default value for msgTxInterval is 30 seconds; this value can be changed to any value in the range 1 through 3600.
    - **txFastInit** – This variable is used as the initial value for the txFast variable. This value determines the number of LLDPDUs that are transmitted during a fast transmission period. The default value of txFastInit is 4; this value can be changed to any value in the range 1 through 8.

| Parameter | Min Value | Max Value | Default Value |
|---|---|---|---|
| msgFastTx | 1 | 3600 | 1 |
| msgTxHold | 1 | 100 | 4 |
| msgTxInterval | 1 | 3600 | 30 |
| txFastInit | 1 | 8 | 4 |

SonicOS provides four Default LLDP Profiles:

- **Mode Disabled** with all the default values of LLDP protocol parameters.
- **Mode Receive-Only** with all the default values of LLDP protocol parameters.
- **Mode Transmit-Only** with all the default values of LLDP protocol parameters.
- **Mode Transmit-and-Receive** with all the default values of LLDP protocol parameters.

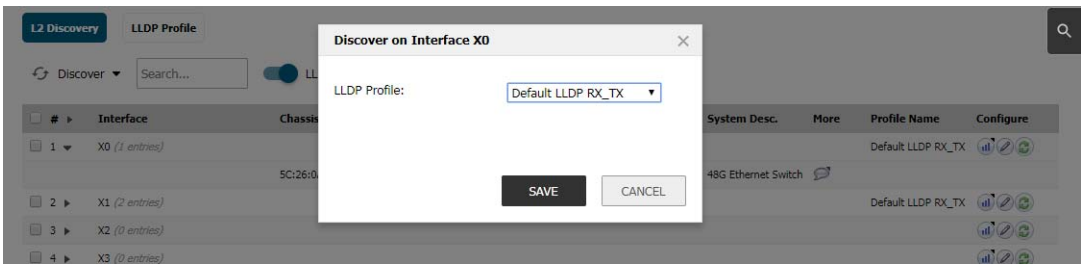
***To associate an LLDP Profile with an L2 Discovery interface:***

1 Navigate to the **MANAGE | System Setup | Switching > L2 Discovery** page.

2 Click the **Configure** button in the row with the desired interface.

3 In the popup dialog, select the **LLDP Profile**.

4 Click **SAVE**.




The following neighbor information is displayed per interface:

- **Interface** - Existing interface name
- **Chassis ID** - A string value mostly representing MAC address of the peer

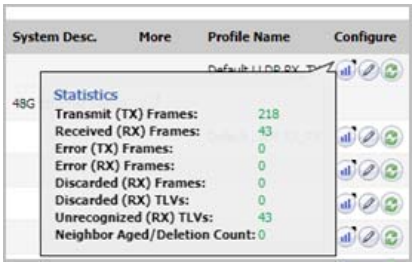
- **Port ID** - A string value mostly port name or number
- **Management Address** - Either IP or MAC address
- **System Name** - A string value representing the name of the peer device
- **System Description** - A string value representing description of peer device

Additional peer information is displayed in a popup by hovering your mouse pointer over the **More** icon for the interface:

- **MAC Address** - A string value
- **Vendor** - The vendor name from the main menu
- **Port Description** - A string value from the Comments field for the interface on SonicWall firewalls
- **System Capabilities** - A string value representing the list of capabilities supported by the peer device
- **Enabled Capabilities** - A string value representing the list of capabilities enabled by the peer device


LLDP interface statistics are displayed in a popup by hovering your mouse pointer over the *statistics* icon under **Configure** for the interface:

- Transmit (TX) Frames
- Received (RX) Frames
- Error (RX) Frames
- Error (TX) Frames
- Discard (RX) Frames
- Unrecognized (RX) Frames
- Neighbor Aged/Deletion Count




LLDP only functions when the interface link is up. When link goes down or the mode is changed to Receive-Only or Disabled, a final LLDP shutdown LLDPDU is sent with:

- Chassis ID TLV
- Port ID TLV
- TTL TLV
- End of LLDPDU TLV

The statistics counters are reset after the link goes down.

# Per User Client Side UI Preferences Storage

SonicOS 6.5.1.1 provides the ability to separate the client-side UI preferences for each admin user, so each admin user can have their own UI settings consistent through every login. It maintains the settings for each admin even when other admin users log in through the same browser. This feature also offers options to store/retrieve client-side data shared across users or pages.

One common use case of this feature is restoring the last visited page for different logged-in admins.

Another common user case is restoring display options of certain table pages. For instance, display options such as IP version, view type and From/To zone in the Access Rules page can be restored for different admin users respectively. Only certain table pages can benefit from this feature, including all Object list pages, Access Rules page, and Connection Log page.

No configuration is required for this feature.

# Refactored SonicOS Web Interface Layout

The main page of the SonicOS web management interface is updated to use a flexbox with embedded iframes, and other features of modern browsers. This provides the foundation for new features such as Global Search in the UI. APIs relying on window.frames are not impacted and will continue to work as in previous releases.

This feature is supported in modern browsers:

- Chrome: 45+
- Firefox: 38+
- IE: 10+
- Edge: All
- Safari: 9+
- Opera: 32+

# Capture Threat Assessment Client Enhancements

SonicOS 6.5.1.1 adds new functionality to the existing Capture Threat Assessment feature:

- Auto-Email the SFR File
- On-Demand SFR File Push to Capture Threat Assessment Server
- SFR File Data Content Additions
- New Capture Threat Assessment Page Location

**NOTE:** On the SOHO-W, bandwidth data information might not be available in the SFR file due to certain limitations in Flow Reporting on that platform.

This feature is only available when the device is registered and has an App Visualization license.

## Auto-Email the SFR File

This allows scheduled emailing of the SonicFlow Report File (SFR file) to an email user account. The SFR file is attached to the email. You can then use this to upload to MySonicWall and use the offline Capture Threat Assessment tool to generate a report. This option is configured on the **SFR Mailing** screen on the **MANAGE | Logs & Reporting > AppFlow Settings** page.

The following email server settings are configured on this screen:

- **Send Report by E-mail** - enable/disable sending of SFR email

- **SMTP Server Host Name** - host name or IP address of SMTP server to use
- **E-mail To** - email account to receive the SFR file
- **From E-mail** - email name to denote the sender
- **SMTP Port** - TCP port use by the SMTP server
- **Connection Security Method** - specifies whether to use secure (select protocol) or non-secure email
- **Enable SMTP Authentication** - specifies whether SMTP server requires authentication
- **SMTP User Name** - user name to use for SMTP authentication
- **SMTP User Password** - password to use for SMTP authentication
- **Enable POP Before SMTP** - specifies if POP authorization is needed for sending email
- **POP Server Address** - IP address of POP server
- **POP User Name** - user name to use for POP authorization
- **POP User Password** - password to use for POP authorization

At any point even if the above parameters are not yet saved, you can test the email by clicking on **TEST EMAIL**. An alert message pops up for either a successful or failed email transaction.

To schedule the email to be sent, click **EDIT SCHEDULE**. A dialog is displayed to edit the App Visualization Report Hours schedule object. Like any other schedule object, you can edit this to be one-time, recurring or mixed scheduling. However, this is a system created object so you cannot delete it.

## On-Demand SFR File Push to Capture Threat Assessment Server

This provides a one click operation to send the SFR file to the Capture Threat Assessment backend site for report generation. There is a report table that lists all the generated reports stored in the backend. You can click to download or to delete the report file.

## SFR File Data Content Additions

Two new sections are added to the SFR file report format:

- **Real-Time Monitor History Data** for applications, bandwidth, packets, connections, core usage that is useful to generate graphs and charts in the Capture Threat Assessment report
- **DPI-SSL Visibility Monitor Statistics** monitors mode statistics.

There are no configuration options for this.

## New Capture Threat Assessment Page Location

The **Capture Threat Assessment** page is moved from **AppFlow Settings > Flow Reporting** to a new page of its own under **Investigate | Reports | Capture Threat Assessment**.

# Increased SPI/DPI Connection Capacity

SonicOS 6.5.1.1 increases the maximum number of Stateful Packet Inspection (SPI) and Deep Packet Inspection (DPI) connections supported on NSA 2600-6600 and SuperMassive 9200-9600 platforms. You can enable SPI or DPI connections on the **MANAGE | Security Configuration > Firewall Settings > Advanced** page in SonicOS.

The SPI Previous vs New Maximum Connections table shows the previous maximums and new target maximums for the number of connections supported on each platform with SPI enabled.

**SPI Previous vs New Maximum Connections**

| Platform | Previous Maximum Connections | New Maximum Connections |
|---|---|---|
| NSA 2600 | 225,000 | 500,000 |
| NSA 3600 | 325,000 | 750,000 |
| NSA 4600 | 400,000 | 1,000,000 |
| NSA 5600 | 750,000 | 1,500,000 |
| NSA 6600 | 750,000 | 1,500,000 |
| SM 9200 | 1,250,000 | 5,000,000 |
| SM 9400 | 1,250,000 | 7,500,000 |
| SM 9600 | 1,500,000 | 10,000,000 |

For appliances with DPI enabled, the DPI Previous vs New Maximum Connections table shows the previous maximums and new target maximums for the number of connections supported on each platform.

**DPI Previous vs New Maximum Connections**

| Platform | Previous Maximum Connections | New Maximum Connections |
|---|---|---|
| NSA 2600 | 125,000 | 250,000 |
| NSA 3600 | 175,000 | 375,000 |
| NSA 4600 | 200,000 | 500,000 |
| NSA 5600 | 500,000 | 1,000,000 |
| NSA 6600 | 500,000 | 1,000,000 |
| SM 9200 | 1,000,000 | 1,500,000 |
| SM 9400 | 1,000,000 | 1,500,000 |
| SM 9600 | 1,250,000 | 2,000,000 |

The maximum connection counts for the new hardware platforms (including NSA 2650) in the SonicOS 6.5.1.1 release are shown in the New Hardware Connection Counts table.

**New Hardware Connection Counts**

| Platform | Max SPI Connections | Max DPI Connections |
|---|---|---|
| NSA 2650 | 1,000,000 | 500,000 |
| NSA 3650 | 2,000,000 | 750,000 |
| NSA 4650 | 3,000,000 | 1,000,000 |
| NSA 5650 | 4,000,000 | 1,500,000 |

***To select the connection mode (SPI or DPI) for the firewall:***

1. Navigate to the **MANAGE | Security Configuration | Firewall Settings > Advanced Settings** page.
2. In the **Connections** section, select one of the following radio buttons:
   - **Maximum SPI Connections (DPI services disabled)** — Enables Stateful Packet Inspection. This option allows the most simultaneous connections, but does not provide as much security as Deep Packet Inspection.
   - **Maximum DPI Connections (DPI services enabled)** — Enables Deep Packet Inspection. This is the default and recommended setting for most SonicWall network security appliance deployments.

- **DPI Connections (DPI services enabled with additional performance optimizations)** — Enables Deep Packet Inspection with increased firewall DPI inspection throughput and fewer overall DPI connections. This option is intended for performance critical deployments.

3 Click **Accept**.

4 Restart the firewall. Any change to the Connection settings requires a restart for the changes to take effect.

# DPI vs DPI-SSL Dynamic Connection Sizing

For the products that support more than 250,000 DPI connections (NSA 2650 and higher), there is an option to adjust the number of desired DPI vs DPI-SSL connections. For every 125,000 DPI connections reduced, the number of available DPI-SSL connections increases by 750. For example:

- A reduction of 250,000 DPI connections results in an increase of 1,500 additional DPI-SSL connections.
- A reduction of 500,000 DPI connections results in an increase of 3,000 additional DPI-SSL connections.

***To configure a reduction in DPI connections:***

1 Navigate to the **MANAGE | Security Configuration | Firewall Settings > Advanced** page.

2 On NSA and SuperMassive platforms, the **Dynamic Connection Sizing** section is displayed below **Connections**.

**NOTE:** This setting is only available when one the following options is selected under **Connections**:
- **Maximum DPI Connections (DPI services enabled)**
- **DPI Connections (DPI services enabled with additional performance optimizations)**

3 Using the **DPI Connections** drop-down list, adjust the desired number of DPI connections.

For every 125,000 DPI connections reduced, the maximum number of DPI-SSL connections increases by 750.

4 Alternatively, adjust the desired number of DPI-SSL connections with the **DPI-SSL Connections** drop-down list.

5 Click **Accept**.

# DPI-SSL Scalability Through Extended Memory

An extended memory architecture in recent releases of SonicOS makes it possible for SonicOS to use memory beyond 4GB. In SonicOS 6.5.1.1, DPI-SSL data, including OpenSSL data, can reside in extended memory. This allows the number of DPI-SSL connections to scale significantly.

No configuration is required for this feature.

# Active/Active Clustering on NSA Platforms

SonicOS 6.5.1.1 extends support for Active/Active Clustering to the following platforms:

- NSA 3600
- NSA 3650
- NSA 4600
- NSA 4650
- NSA 5650

In this mode, multiple firewalls 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:** As with NSA 5600 and 6600, Active/Active Clustering is supported on the newly added platforms only with the purchase of a SonicOS Expanded License.

# SonicOS Global Search

SonicOS 6.5.1.1 provides a new global search button. Global search makes it easy for administrators to navigate to a desired feature. Results contain links to main pages which are part of menu items in the left-hand navigation pane.

Only static data can be searched. Dynamic data (such as object names and policy details) are out of scope for this revision.

The SonicOS management interface displays the search icon in the upper right corner of the page. When the search icon is clicked, a slider text box opens. You can enter your search queries in the field. The slider can be closed by pressing the **ESC** key or by clicking the **>** button or by clicking in the area outside the slider.

The search results are shown by pressing the up-arrow key or by clicking in the area below the search field. The results are sorted by relevance. By default, only the top 10 results are displayed. If there are more results you can click **Show more results** to view them.

The following types of queries are supported:

- Single word queries, for example ***ARP***
- Multi word queries, for example ***Network Interface***
- Queries with wildcards, for example ***Network Inter****

A maximum of 50 characters are allowed in the search query string. Alphanumeric (A-Z a-z 0-9) and special character set (. -_ / *) are allowed.

The search feature is not available on the classic/legacy management interface.

# Source MAC Override for NAT

Starting in SonicOS 6.5.1, an internal option is added that allows you to replace the source MAC address of an outbound or port-forwarded packet with the MAC address specified in a NAT policy. By default without this option, the MAC address of the output interface is used as the source MAC address of the packet.

This feature is disabled by default, and can be enabled using an internal setting. Contact SonicWall Technical Support for information about internal settings.

# UUID for Rules and Objects

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is widely used by many network devices providers for multiple purposes.

In SonicOS 6.5.1.1, UUID is implemented to uniquely identify some entities on SonicWall Network Security Appliances. In this release, SonicOS UUIDs are automatically generated and bound to the following SonicOS entities:

- Address Object
- Service Object

- User Object
- Zone Object
- Schedule Object
- Access Rule
- NAT Policy
- Routing Policy

The SonicOS UUID is a system-generated, read-only internal value that cannot be modified by the administrator. It is automatically generated when an entity is created. UUID takes more memory than an ID and might not be available in all SonicWall firewall products. The availability of SonicOS UUID feature depends on the product matrix.

The UUID relies upon a combination of components to ensure uniqueness. SonicOS UUID contains:

- Global ID (aka, GID) per object type
- Network MAC address of the Network Security Appliances
- Object Type
- Version

UUID is bound to an entity and allows you to identify and track the history of an entity, for example, to see the referenced entities based on UUID.

- You can search for a partial or entire UUID from the SonicOS web management interface.
- If an object with UUID is referenced by another entity with a UUID, a clickable link allows you to jump to the referring entity.

  For example, when an address object is referenced by another entity, hovering your mouse pointer over the **Comment** icon displays a popup with details and a link to the referenced entity.
- You can add a configuration option on the SonicOS web management interface to show UUID column and policy name. For user-friendly notation, a user-friendly **Name** field is added for access rule and NAT policies configured by an administrator. This name is optional, but must be unique if configured.

When importing configuration settings from one appliance to another, GID remains the same as in the imported preference file to retain the same configuration state. However, when viewing the UUID, the MAC address from the imported settings is replaced with the MAC address of the current running network appliance.

# UX/UI Improvements for Content Pages

Two pages in the SonicOS 6.5.1.1 web management interface are updated for an improved user experience.

- The **CFS Policies** screen on the **MANAGE | Security Services | Content Filter** page in SonicOS 6.5.0.x is moved to its own page in SonicOS 6.5.1.1, located at **MANAGE | Policies | Rules > Content Filter Policies**.
- The **MANAGE | Logs & Reporting | RF Monitor** page in SonicOS 6.5.0.x is moved in SonicOS 6.5.1.1 to **MONITOR | Appliance Health | RF Monitor**.

# WAN DDOS Protection Performance Enhancement

SonicOS 6.5.1.1 improves WAN DDOS Protection performance and makes more efficient use of the Allow List. The Allow List was previously populated with the destination IP of any packet ingressing a LAN/DMZ interface, but is now populated only when a packet from a non-WAN source zone egresses a WAN interface.

A new **Always allow VPN Negotiation traffic** checkbox is added, which is disabled by default. When enabled, a VPN can be negotiated even when the appliance is under a non-TCP DDOS attack.

WAN DDOS Protection provides protection against non-TCP DDOS attacks and so should be used in combination with SYN-Flood Protection if TCP SYN-flood attacks are a concern. This feature is not intended to protect a well-known server of non-TCP services on the internet (such as a central DNS server), but is intended to protect LAN and DMZ networks for which the majority of non-TCP traffic is initiated from LAN/DMZ side, possibly in combination with limited WAN initiated traffic.

WAN DDOS Protection is configured on the **MANAGE | Security Configuration | Firewall Settings > Flood Protection** page.

# Resolved Issues

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

### Content Filtering Service

| Resolved issue | Issue ID |
|---|---|
| In some cases Sonicwall doesn't boot up completely, the console shows the message, `Starting CFS`.<br>Occurs upon a reboot due to the CFS running into an error condition when restoring the persistent cache data. | 198800 |

### DPI SSL

| Resolved issue | Issue ID |
|---|---|
| PC scan fails for CVE-2016-2183 SWEET32 attack on TSL 1.0 64-bit ciphers.<br>Occurs when weak ciphers, such as TSL 1.0, are allowed. | 197127 |

### Log

| Resolved issue | Issue ID |
|---|---|
| Log Monitor does not filter logs.<br>Occurs when the filter string (entered in the search field) contains a uppercase letter. | 198930 |

### Networking

| Resolved issue | Issue ID |
|---|---|
| Kernel route missing from NSM database.<br>This issue appears to occur due to a VPN redistribution issue if the source NAT is enabled. | 190839 |

### SSL VPN

| Resolved issue | Issue ID |
|---|---|
| Configured WINS Servers are not displayed in NetExtender on the DNS tab.<br>Occurs when NetExtender is used on Windows 10 clients. The WINS Servers are displayed in NetExtender on Windows 7 clients. | 197032 |
| The "access-request" message AVP Type 24 is truncated to 34 bytes, which causes the server to reject the connection and send an incorrect username/password to NetExtender.<br>Occurs when an internal server sends an OTP to the user connecting using NetExtender with the RADIUS state message (AVP type 24) using a message 42 bytes long. | 192916 |

### Switching

| Resolved issue | Issue ID |
|---|---|
| IPv6 SSL VPN fails to connect to the interface IP in LACP group; connection fails with console message, `dp_stack_output:1259: Need to free this WQE!!!`<br>Occurs when trying to connect from a PC on the WAN side, using IPv6 SSL VPN to the WAN interface of LACP, or with LAN/DMZ side LACP. | 194566 |
| Only one 10G interface is listed under the VLAN trunk port list on an appliance with multiple 10G interfaces, and a 1G port and 10G port can be configured as a Link Aggregation Group (LAG).<br>Occurs on a NSA 6600, on which X16, X17, X18 and X19 are all 10G interfaces, when configuring a LAG, and when a 1G interface like X2 is configured as a trunk port and the same VLAN ID is enabled for both X2 and X17. | 194004 |

### System

| Resolved issue | Issue ID |
|---|---|
| In some isolated cases, the SonicWall management interface ceases to respond or reboots due to the REAL_tDataPlane task suspension.<br>Occurs due to a pointer initialization error. | 198865 |
| Login fails with the error message, `Incorrect name/password`.<br>Occurs when the username contains the special characters @, /, or \. Any part of the username after the special character is discarded. | 196858 |
| Sonicwall exhibits a reboot issue.<br>Occurs at random and in some cases due to a task malfunction when the SonicWall is acquired by Cloud GMS. | 196399 |

### Users

| Resolved issue | Issue ID |
|---|---|
| LDAP option to filter users by location when importing from LDAP is missing.<br>Occurs when importing users from LDAP on the **MANAGE \| Users > Local Users & Groups > Local Users** page and clicking the **Users at/at or under** option in the import dialog. The option should be followed by a field with LDAP locations, but the field is missing. | 195781 |

### Vulnerability

| Resolved issue | Issue ID |
|---|---|
| Vulnerability to CVE-2018-5280 and CVE-2018-5281.<br>Occurs when LDAP configuration is vulnerable to Cross-Site Scripting. | 199274 |

### Wireless

| Resolved issue | Issue ID |
|---|---|
| Configure policy page without user authentication, redirection fails to post auth URL upon clicking **Accept**.<br>Occurs when the policy page is configured without user authentication for wireless users. | 197404 |

# Known Issues

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

### API

| Known issue | Issue ID |
|---|---|
| Unable to configure using API with Sonicwall Administrator.<br>Occurs when trying to enter Config mode using API with SonicWall Administrator. The mode does not change to Config mode and displays `Unauthorized` when trying to configure. | 201747 |
| Unable to use the preempt feature.<br>Occurs when attempting to preempt an existing admin user. The preempting user remains in non-config mode, and any attempt at configuration displays the message, `An administrator is already logged in for configuration`. | 200271 |

### DPI-SSH

| Known issue | Issue ID |
|---|---|
| Incorrect value has been sent in prefs file for user Object Group:Exclude field in DPI SSH.<br>Occurs when the value for the Excluded Object Group in the SonicOS management interface is NONE, but the GMS perfs file has the value of the Excluded Object Group as ALL. | 201616 |

### DPI-SSL

| Known issue | Issue ID |
|---|---|
| Block of attachment and append message actions do not work with SMTP over SSL.<br>Occurs when **SSL Client Inspection** is enabled and the **Application Firewall** option is selected on the **DPI-SSL/TLS Client** page and an App Rule policy exists to block attachments and add text, and then an email message matching the policy is sent. | 198590 |
| **Skip CFS Category-based Exclusion** does not work correctly.<br>Occurs when a common name like *bankofamerica.com* is added on the **DPI-SSL/TLS Client** page with the **Skip CFS Category-based Exclusion** option selected, category “20. Online Banking” is excluded, and then a LAN side PC attempts to access bankofamerica.com and it is excluded from inspection. | 198185 |
| CFS Category-based Inclusions/Exclusions does not exclude correctly.<br>Occurs when **Enable SSL Client Inspection** is selected on the **DPI-SSL/TLS Client** page and category *29 Search Engines and Portals* is excluded on the **CFS Category-based Exclusions/Inclusions** screen, and then a LAN side PC accesses `https://www.baidu.com` and DPI-SSL still occurs. | 196892 |

### SSL VPN

| Known issue | Issue ID |
|---|---|
| Fails to download the Virtual Assist from the user portal.<br>Occurs when attempting to download Virtual Assist by clicking the **Virtual Assist** icon. The message, `An add-on for this website failed to run`, displays. | 193798 |

### Users

| Known issue | Issue ID |
|---|---|
| The default partition policy changes, causing the partition feature to not work.<br>Occurs when adding a remote-user partition policy from CLI. | 197455 |

### VOIP

| Resolved issue | Issue ID |
|---|---|
| First series of short TCP-calls over VPN is running OK, but second series of calls to the same destination - not running; the second firewall has some issues.<br>Occurs when sending a second series of SIP/TVCP/VPN calls to the same destination with TCP transformation checked. | 202700 |

### X-series switch

| Known issue | Issue ID |
|---|---|
| Port Shield configuration for X1052 has errors.<br>Occurs when a Dell X1052 switch is connected to an NSA 3600. The X1052 switch has 10G, 1G FDX, and 1G copper-only slots, but the NSA 3600 treats all ports on the X1052 as 10G. | 200619 |

# System Compatibility

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

## Wireless 3G/4G Broadband Devices

SonicOS 6.5 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:
https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240

## GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.1.1 requires GMS 8.5 for management of firewalls using the new features in SonicOS 6.5.1.1. SonicWall GMS 8.4 supports management of all features in earlier SonicOS 6.5 releases.

## WAN Acceleration / 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 6.5. 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 45 and higher
- Firefox 38 and higher
- IE 10 and higher
- Edge (all versions)
- Opera 32 and higher
- Safari 10 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

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 6.5 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/support/technical-documentation.

# 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: 4/16/18

232-004293-00 Rev A