SONICWALL®

SonicWall® SonicOS 6.5.4.6

Release Notes

May 2020

These release notes provide information about the SonicWall® SonicOS 6.5.4.6 release.

Topics:

- About SonicOS 6.5.4.6
- Supported Platforms
- New Features
- Resolved Issues
- Known Issues
- System Compatibility
- Product Licensing
- Upgrading Information
- SonicWall Support

About SonicOS 6.5.4.6

SonicWall SonicOS 6.5.4.6 provides several new features and fixes a number of issues found in previous releases. For more information, see the New Features and Resolved Issues sections.

This release supports all the features and contains all the resolved issues found in previous SonicOS 6.5 releases. For more information, see the previous release notes, available on MySonicWall at: https://mysonicwall.com.

Supported Platforms

SonicOS 6.5.4.6 is supported on the following SonicWall appliances:

- NS*a* 9650
- NS*a* 9450
- NS*a* 9250
- NS*a* 6650
- NS*a* 5650
- NS*a* 4650
- NS*a* 3650
- NS*a* 2650
- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600 / TZ600P
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ350 / TZ350 Wireless
- TZ300 / TZ300P / TZ300 Wireless
- SOHO 250 / SOHO 250 Wireless
- SOHO Wireless

New Features

This section describes the new features in this release.

Topics:

- SonicWall Switch Support
- Enhancements for DPI-SSL with CFS
- SD-WAN Scalability
- Wireless Access Points RF Enhancements
- Capture Threat Assessment (CTA) v2.0
- SFR Updates for Simple Reporting

SonicWall Switch Support

SonicOS 6.5.4.6 introduces support for all models of the SonicWall Switch. Switch models are available in different form factors and some act as Power Sourcing Equipment (PSE) to provide Power Over Ethernet (PoE) to connected devices.

- Desktop form factor Switches with external power supplies:
    - SWS12-8 – Eight 1Gb Ethernet ports and two 1Gb SFP ports
    - SWS12-8POE – PoE capable ports: eight 1Gb Ethernet ports and two 1Gb SFP ports
- Small form factor Switch with internal power supply:
    - SWS12-10FPOE – PoE capable ports: ten 1Gb Ethernet ports and two 1Gb SFP ports
- Rack mountable 1U form factor Switches with internal power supplies:
    - SWS14-24 – 24 1Gb Ethernet ports and four 1Gb/10Gb SFP+ ports
    - SWS14-24FPOE – PoE capable ports: 24 1Gb Ethernet ports and four 1Gb/10Gb SFP+ ports
    - SWS14-48 – 48 1Gb Ethernet ports and four 1Gb/10Gb SFP+ ports
    - SWS14-48FPOE – PoE capable ports: 48 1Gb Ethernet ports and four 1Gb/10Gb SFP+ ports

The SonicWall Switches are designed to connect SonicWall firewalls with wireless access points, IP surveillance cameras, VoIP phones and other PoE-capable devices, as well as other Ethernet-based networking equipment or computers. The Switch provides simple, yet powerful PoE manageability with features such as: IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, port mirroring, voice VLAN, QoS, static routing, 802.1x authentication, and access point management.

The SWS12-8POE switch supports only 802.3af PoE to connected devices, while the other PoE capable switches support both 802.3af and 802.3at standards.

For more information about SonicWall Switches, refer to the *Switch Quick Start Guide* and *Switch Getting Started Guide* at https://www.sonicwall.com/support/technical-documentation/?category=Switch.

For information about managing and configuring a SonicWall Switch from the SonicOS web management interface, see the *Switch Controller* chapter of the *SonicOS 6.5 System Setup* administration guide at https://www.sonicwall.com/support/technical-documentation/?category=Firewalls.

Enhancements for DPI-SSL with CFS

SonicOS 6.5.4.6 provides performance improvements that reduce latency when accessing HTTPS sites with both DPI-SSL and CFS enabled. This is achieved by optimizing the handling of situations when, for example, a user browses to HTTPS sites that are not trusted by CFS, such as Facebook.

SonicOS provides a new flow that better coordinates the TCP packet acknowledgments, DPI-SSL decryption and state machine, packet inspection by other security services (GAV, IPS, etc), buffering of TLS records, CFS rating response from the cloud server, and the CFS policy actions (Allow/Modify/Block).

SD-WAN Scalability

This release enhances SD-WAN to support scalable tunnel interfaces for distributed enterprises. This increases the supported number of remote sites from 100 in previous versions to up to 1000 sites in SonicOS 6.5.4.6.

Configuration maximums are increased for a number of SD-WAN settings.

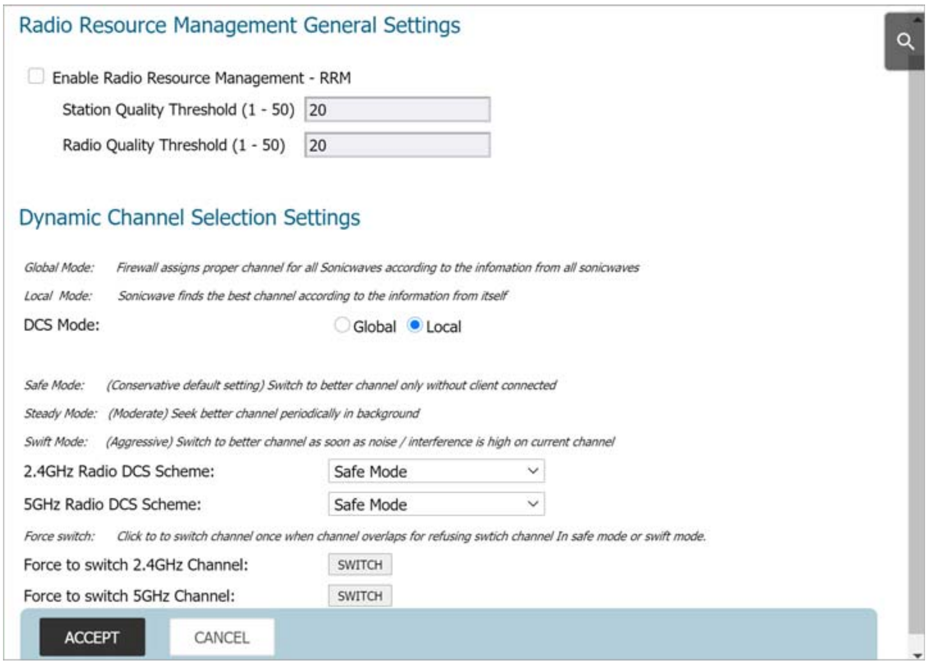
SD-WAN Maximums per Platform

Platform	Max SD-WAN Groups	Max SD-WAN Interfaces	Max SD-WAN Group Performance Probes	Max SD-WAN Child Performance Probes	Max SD-WAN Path Selection Profiles
NSA 2600	500	1000	500	1000	1000
NSA 3600	600	1200	600	1200	1200
NSA 4600	700	1400	700	1400	1400
NSA 5600	750	1500	750	1500	1500
NSA 6600	800	1600	800	1600	1600
SM 9200	1000	2000	1000	2000	2000
SM 9400	1000	2000	1000	2000	2000
SM 9600	1000	2000	1000	2000	2000
NSa 2650	500	1000	500	1000	1000
NSa 3650	600	1200	600	1200	1200
NSa 4650	700	1400	700	1400	1400
NSa 5650	750	1500	750	1500	1500
NSa 6650	800	1600	800	1600	1600
NSa 9250	1000	2000	1000	2000	2000
NSa 9450	1000	2000	1000	2000	2000
NSa 9650	1000	2000	1000	2000	2000

Wireless Access Points RF Enhancements

SonicOS 6.5.4.6 provides **Radio Resource Management** and **Dynamic Channel Selection** enhancements to **Access Points** settings.

> **NOTE:** Radio Resource Management is supported on SonicWall access points that have a dedicated scan radio, including SonicWave 231c, 231o, 432e, 432i, and 432o. The RRM feature is not supported on SonicWave 224w or on SonicPoints.



Radio Resource Management General Settings

☐ Enable Radio Resource Management - RRM

Station Quality Threshold (1 - 50) 20

Radio Quality Threshold (1 - 50) 20

Dynamic Channel Selection Settings

Global Mode: *Firewall assigns proper channel for all Sonicwaves according to the infomation from all sonicwaves*

Local Mode: *Sonicwave finds the best channel according to the information from itself*

DCS Mode: ○ Global ● Local

Safe Mode: *(Conservative default setting) Switch to better channel only without client connected*

Steady Mode: *(Moderate) Seek better channel periodically in background*

Swift Mode: *(Aggressive) Switch to better channel as soon as noise / interference is high on current channel*

2.4GHz Radio DCS Scheme: Safe Mode

5GHz Radio DCS Scheme: Safe Mode

Force switch: *Click to to switch channel once when channel overlaps for refusing swtich channel In safe mode or swift mode.*

Force to switch 2.4GHz Channel: SWITCH

Force to switch 5GHz Channel: SWITCH

Radio Resource Management and Dynamic Channel Selection Options and Values

Option Name	Description
Enable Radio Resource Management - RRM	Enable this option to activate the settings for **Station Quality Threshold** and **Radio Quality Threshold**. This option is disabled by default.
Station Quality Threshold (1-50)	Health index to track and assess the status of wireless client connections, from 1 to 50. A higher index value means the wireless station is connected with higher data rate and less packet drop. Wireless clients will be disconnected if station quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20
Radio Quality Threshold (1-50)	Health index to track and assess the status of radio band utilization, which varies between 1 and 50. A higher index value means radio band utilization is lower with less packet drop. The radio transmit power will be lowered if the radio quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20

Radio Resource Management and Dynamic Channel Selection Options and Values

Option Name	Description
Dynamic Channel Selection Mode **DCS Mode**: **Global / Local**	**DCS Mode** supports two settings for automatic channel selection: • **Global Mode** – Firewall assigns proper channel for all SonicWaves according to information received from all SonicWaves. • **Local Mode** – SonicWave finds the best channel according to the information from itself.
Auto Channel Enable: **2.4GHz Radio DCS Scheme** **5GHz Radio DCS Scheme**	**2.4GHz** or **5GHz Radio DCS Scheme** options are: • **Safe Mode** (CGI value 0) SonicWaves switch to a better channel only without clients connected. This is conservative mode. • **Steady Mode** (CGI value 1) SonicWaves seek a better channel periodically in the background. This is moderate mode. • **Swift Mode** (CGI value 2) SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode. **Safe Mode** is the default.

Capture Threat Assessment (CTA) v2.0

SonicOS 6.5.4.6 introduces Capture Threat Assessment (CTA) v2.0. Capture Threat Assessment is a SonicWall service that provides network traffic and threat report generation in PDF format. The service is provided directly from the SonicOS web management interface. You can navigate to the **INVESTIGATE | Reports > Capture Threat Assessment** page to configure settings and generate the report. Previous reports are saved in the cloud and displayed as a table on the page.

CTA v2.0 provides a number of enhancements for the current Capture Threat Assessment cloud service and reporting on all SonicWall firewalls, as described below.

ⓘ **NOTE:** App Visualization licensing is recommended for complete report data.

Topics:

- New Report Template
- Meaningful Application Statistics
- Industry and Global Level Statistics Comparison
- Report Customization
- Key Findings Summarization
- Recommendations
- Generating the Report

New Report Template

A new report template design provides the latest SonicOS look and feel.

SONICWALL

Capture Threat Assessment Report

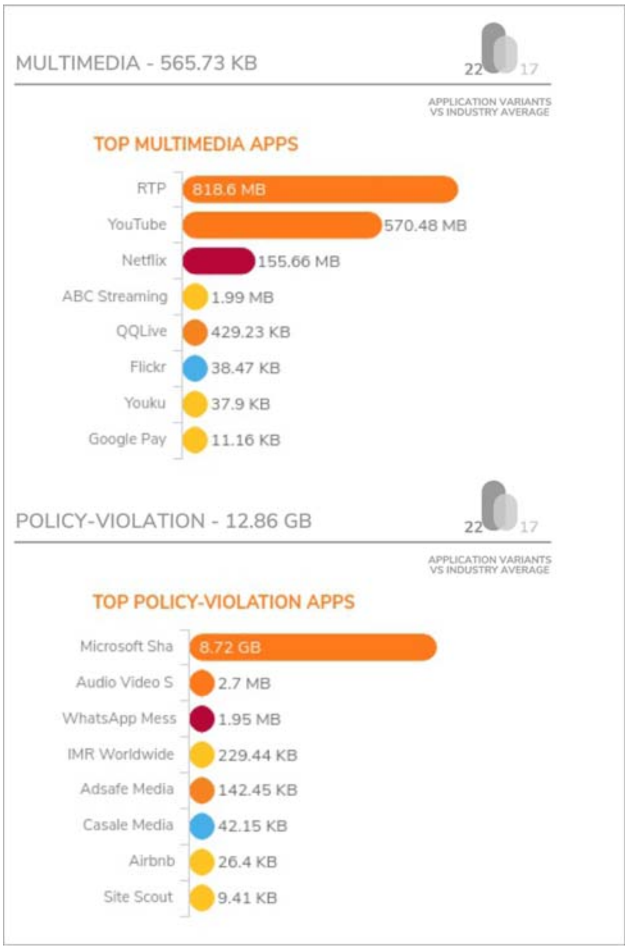
SonicWall
Jan 27 2020 10:07:54 +0530
Report Period: 6 Day(s)
Serial Number: C0EAE4FBAA7A

Prepared By:
SonicWall

SECURE MORE.
FEAR-LESS.

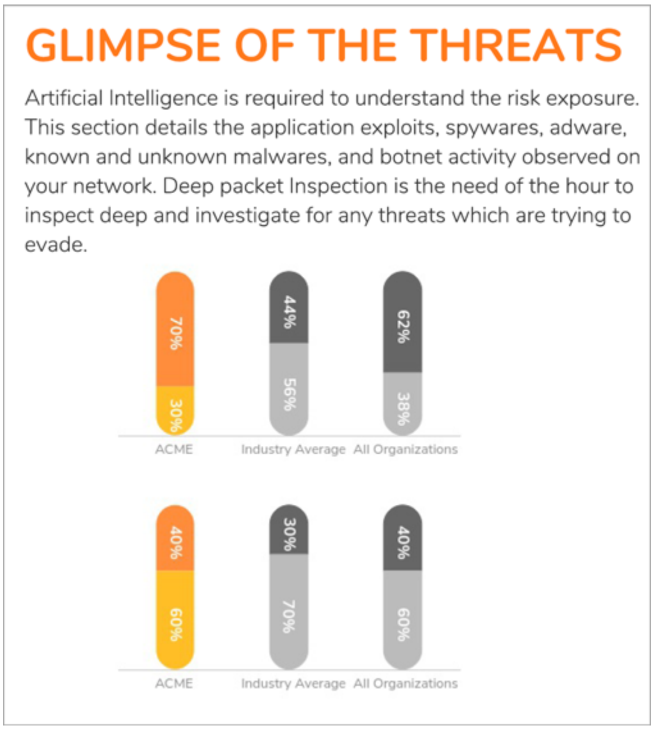
Meaningful Application Statistics

The new report template adds more meaningful application, threat, web and network data.



Industry and Global Level Statistics Comparison

A new report template provides you with the ability to compare your statistics alongside industry and global data.

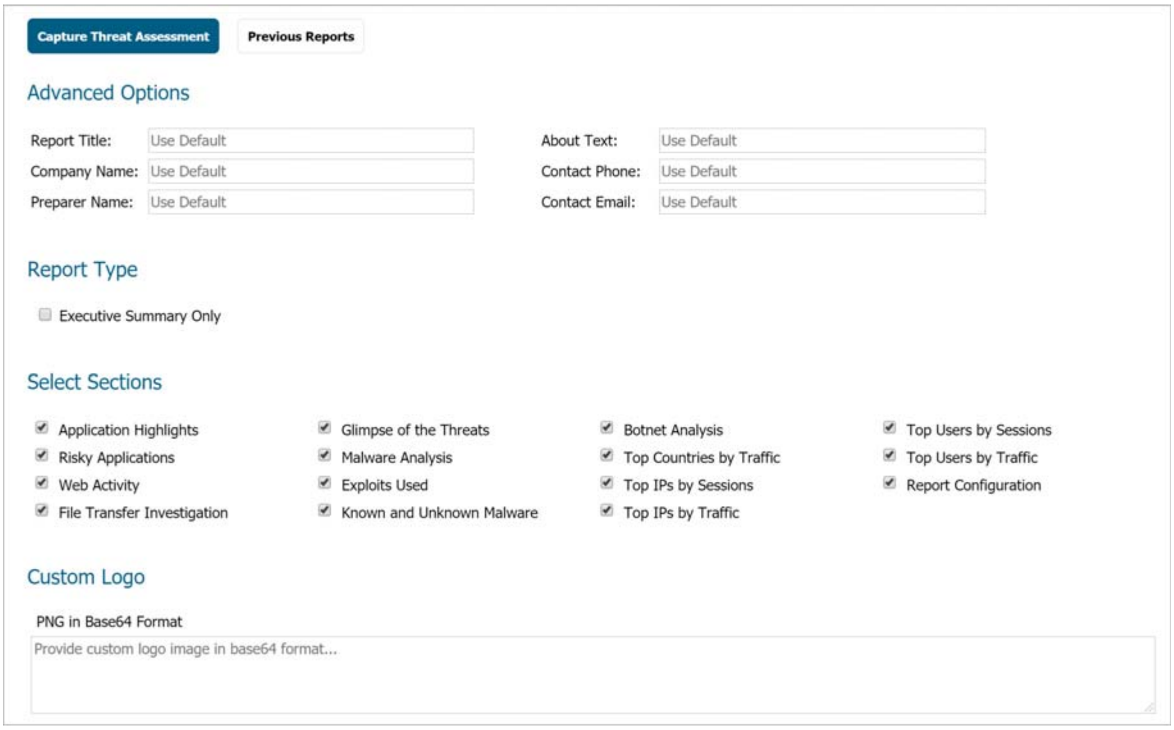


GLIMPSE OF THE THREATS

Artificial Intelligence is required to understand the risk exposure. This section details the application exploits, spywares, adware, known and unknown malwares, and botnet activity observed on your network. Deep packet Inspection is the need of the hour to inspect deep and investigate for any threats which are trying to evade.

Report Customization

Customizable settings on the **INVESTIGATE | Reports > Capture Threat Assessment** page provide a way to customize the report features, customer name, customer logo and custom templates so you can design the report according to your requirements.



Advanced Options

Report Title:	Use Default	About Text:	Use Default
Company Name:	Use Default	Contact Phone:	Use Default
Preparer Name:	Use Default	Contact Email:	Use Default

Report Type

☐ Executive Summary Only

Select Sections

☑ Application Highlights
☑ Risky Applications
☑ Web Activity
☑ File Transfer Investigation
☑ Glimpse of the Threats
☑ Malware Analysis
☑ Exploits Used
☑ Known and Unknown Malware
☑ Botnet Analysis
☑ Top Countries by Traffic
☑ Top IPs by Sessions
☑ Top IPs by Traffic
☑ Top Users by Sessions
☑ Top Users by Traffic
☑ Report Configuration

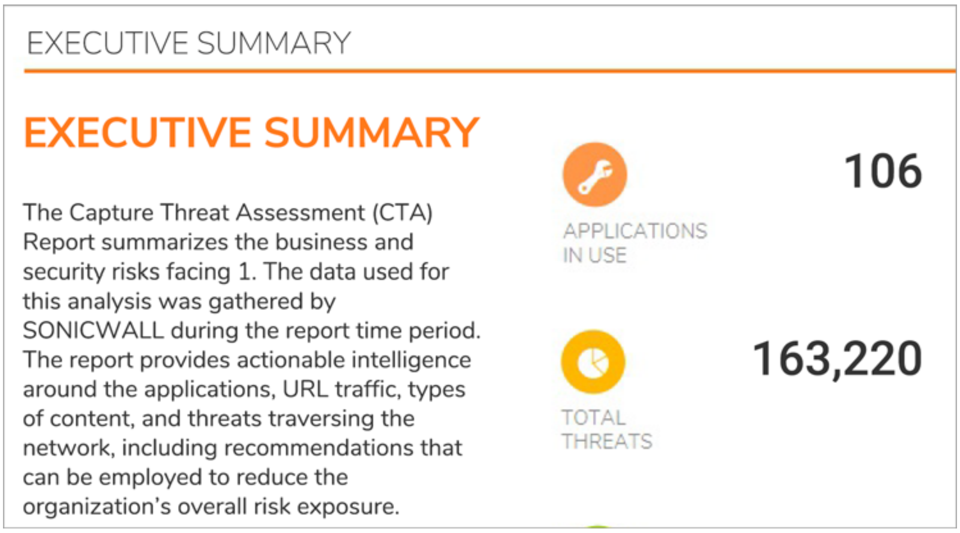
Custom Logo

PNG in Base64 Format

Provide custom logo image in base64 format...

Key Findings Summarization

The new report template provides a key findings page that summarizes the overall pages into a single page for quick reference by executives.



EXECUTIVE SUMMARY

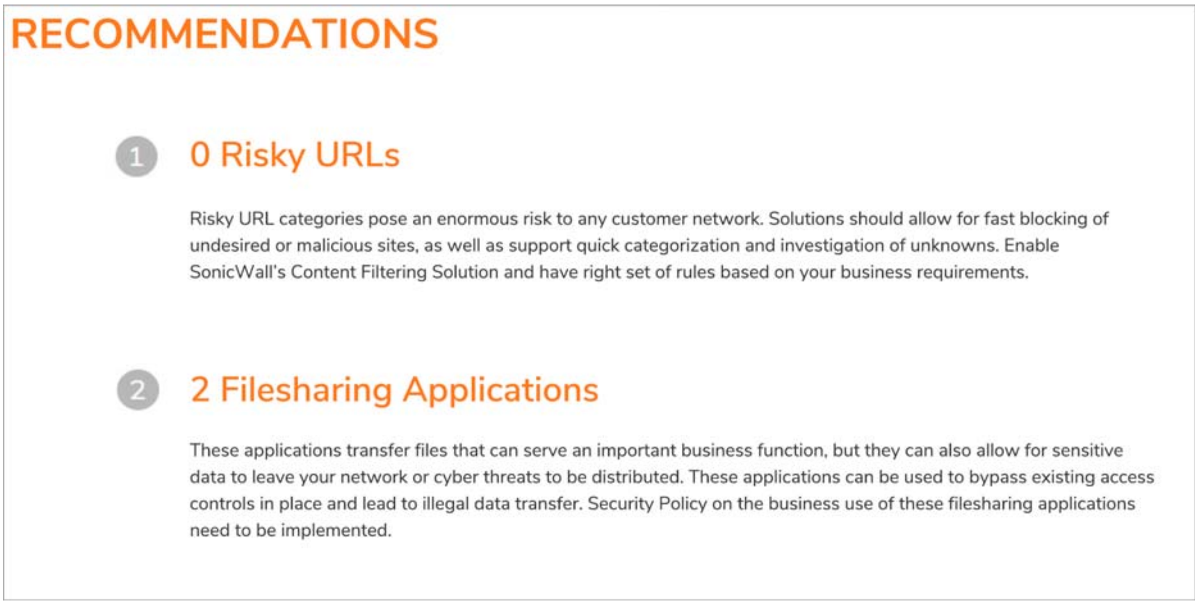
EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing 1. The data used for this analysis was gathered by SONICWALL during the report time period. The report provides actionable intelligence around the applications, URL traffic, types of content, and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

APPLICATIONS IN USE	106
TOTAL THREATS	163,220

Recommendations

The new report template provides a recommendation page with a summary of steps you can take to fix the issues found during the reporting period.



RECOMMENDATIONS

1 0 Risky URLs

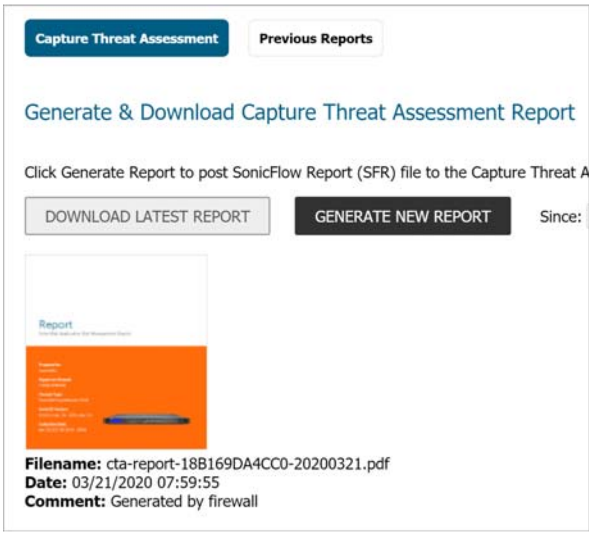
Risky URL categories pose an enormous risk to any customer network. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unknowns. Enable SonicWall's Content Filtering Solution and have right set of rules based on your business requirements.

2 2 Filesharing Applications

These applications transfer files that can serve an important business function, but they can also allow for sensitive data to leave your network or cyber threats to be distributed. These applications can be used to bypass existing access controls in place and lead to illegal data transfer. Security Policy on the business use of these filesharing applications need to be implemented.

Generating the Report

Navigate to the **INVESTIGATE | Reports > Capture Threat Assessment** page in SonicOS. Then click **GENERATE NEW REPORT**.



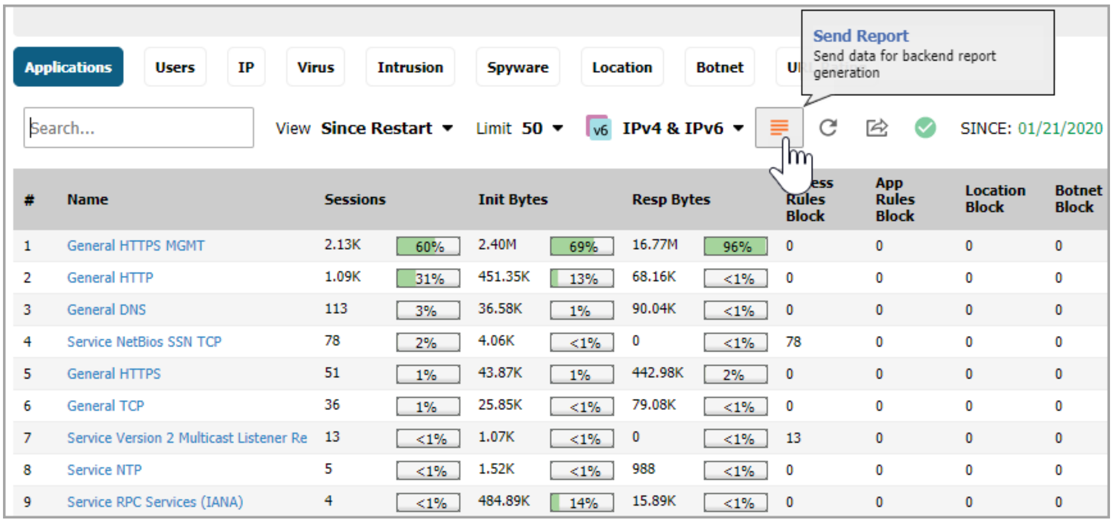
Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat A

Filename: cta-report-18B169DA4CC0-20200321.pdf
Date: 03/21/2020 07:59:55
Comment: Generated by firewall

SFR Updates for Simple Reporting

This feature provides improvements to the SonicFlow Report file (SFR) for CTA and 7/30/365 Simple Reporting. The SFR file can be downloaded from the **Investigate | Reports | AppFlow Reports** page in the SonicOS web management interface. Click on the **Send Report** button.



View **Since Restart** Limit **50** **IPv4 & IPv6** SINCE: 01/21/2020

#	Name	Sessions		Init Bytes		Resp Bytes		ess Rules Block	App Rules Block	Location Block	Botnet Block
1	General HTTPS MGMT	2.13K	60%	2.40M	69%	16.77M	96%	0	0	0	0
2	General HTTP	1.09K	31%	451.35K	13%	68.16K	<1%	0	0	0	0
3	General DNS	113	3%	36.58K	1%	90.04K	<1%	0	0	0	0
4	Service NetBios SSN TCP	78	2%	4.06K	<1%	0	<1%	78	0	0	0
5	General HTTPS	51	1%	43.87K	1%	442.98K	2%	0	0	0	0
6	General TCP	36	1%	25.85K	<1%	79.08K	<1%	0	0	0	0
7	Service Version 2 Multicast Listener Re	13	<1%	1.07K	<1%	0	<1%	13	0	0	0
8	Service NTP	5	<1%	1.52K	<1%	988	<1%	0	0	0	0
9	Service RPC Services (IANA)	4	<1%	484.89K	14%	15.89K	<1%	0	0	0	0

The SFR is a compressed, encrypted, gzip file.

The following updates to the SFR are provided in this release:

- App Category ID and Risk Level columns are added in the Aggregate Application tables in the SFR.

  For reference, a decrypted snippet of this file is displayed here to show the new **CatID** and **Risk** fields:

  ```
  -- start Aggregate Application (IPv4) Report ver=3 mode=0 --

  #ID,Sessions,Rate,Initiator-Bytes,Responder-Bytes,ACL-Block-
  Count,DPI-Block-Count,GEOIP-Block-Count,BOTNET-Block-Count,Virus-
  Count,Intrusion-Count,Spyware-Count,Name,CatID,Risk

  0xc011,10,83,6492,6189,0,0,0,0,0,0,0,General DNS,101,0
  ```

```
0xc019,11,7506,338117,2075219,0,0,0,0,0,0,0,General HTTPS,101,0

0xc01a,887,16317,1093356,10069438,0,0,0,0,0,0,0,General HTTPS
MGMT,101,0

0xc031,1,7,1038,2553,0,0,0,0,0,0,0,General TCP,101,0

0xc059,2,57,304,228,0,0,0,0,0,0,0,Service NTP,102,0


-- end Aggregate Application (IPv4) Report --


-- start Aggregate Application (IPv6) Report ver=3 mode=0 --

#ID,Sessions,Rate,Initiator-Bytes,Responder-Bytes,ACL-Block-
Count,DPI-Block-Count,GEOIP-Block-Count,BOTNET-Block-Count,Virus-
Count,Intrusion-Count,Spyware-Count,Name,CatID,Risk


-- end Aggregate Application (IPv6) Report --
```

- The Top Domains by Bytes table is removed.

  Removing the Top Domains by Bytes table prevents excessive impact on CP core cycles. In previous versions of SonicOS, the snippets below appeared before and after this table:

  ```
  -- start top_domains_by_bytes ver=1 --


  -- end top_domains_by_bytes --
  ```

  These will no longer appear in the SFR.

- The SFR report version is changed to version 13, as shown in the following snippet:

  ```
  -- start fw_info --

  serial_num=C0EAE48582A0

  prod_code=10005

  fw_vers=6.5.4.5-45n--bugfix_6_5_4_5-0n

  rom_vers=5.4.1.2

  time=11/29/2019 10:07:28

  report_vers=13

  begin_report_time=11/29/2019 09:59:19

  ...

  -- end fw_info --
  ```

- The App Table version is changed to version 3. For example:

  ```
  -- start Aggregate Application (IPv4) Report ver=3 mode=0 --
  ```

Resolved Issues

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

Access Points

Resolved issue	Issue ID
Latency issue occurs in some environments when both the 2.4GHz and 5GHz radios are enabled on the SonicWave.	ACP-123
Station Status incorrectly shows 0% signal strength and 0 Tx/Rx bytes even if the client is connected and passing traffic.	GEN6-1019
Wireless clients lose connectivity when the SonicWave 432i experiences interference on the channel and cannot use dynamic channel selection.	GEN6-1022
The client can connect to different VLANs using the same SSID, leading to client roaming and connectivity issues. Occurs when the same SSID name is configured on different Virtual Access Points and the SSID converts to open authentication after being enabled.	GEN6-1036

Application Firewall

Resolved issue	Issue ID
SSL Control prevents traffic to HTTPS TLS v.1.2 sites, possibly due to a false positive.	GEN6-1021

DPI-SSL

Resolved issue	Issue ID
HTTPS file download speed drops dramatically when Client DPI-SSL is enabled.	GEN6-942

High Availability

Resolved issue	Issue ID
Unable to enable encryption for High Availability using the Command Line Interface (CLI).	GEN6-1027

Networking

Resolved issue	Issue ID
DNS-related memory corruption occurs during DNS resolution of GMS or syslog server names.	GEN6-467
Incorrect memory resource handling when recording Wire Mode information in the Tech Support Report (TSR) file.	GEN6-1001
Attempting to connect to the firewall SSL VPN feature on port 443 causes SonicOS to respond with a TLS 1.1 server "hello" even when TLS 1.1 is disabled. This causes a compliance test to fail.	GEN6-1207

SSL VPN

Resolved issue	Issue ID
NetExtender Client admin users see the message, "Your management session has ended" while trying to log into SonicOS for management on the X0 IP address.	GEN6-989
Users are unable to access the SSL VPN portal page and the error, "Access denied! For more information, contact your administrator!" is displayed.	GEN6-997

System

Resolved issue	Issue ID
SonicOS sometimes restarts when handling high volumes of SSL VPN traffic.	GEN6-44
SonicOS sometimes restarts when handling Exclusion and Inclusion address lists for multiple modules such as CFS, App Control, GAV, DPI-SSH, DPI-SSL.	GEN6-936
Users can experience slowness and timeouts while browsing with both DPI-SSL and CFS enabled.	GEN6-943
SCEP Client: CSR sonicwall Enroll fails when enrolling the firewall in the SCEP infrastructure when challenge password is enabled.	GEN6-992
Unhandled exceptions can occur on both CP and DP when the internal SonicOS DPI-SSL cache does not handle certain timing and corner case scenarios.	GEN6-993
The firewall sometimes restarts unexpectedly when waiting due to Network Object manager locks when there are a lot of FQDN address objects.	GEN6-1002
Both appliances in an HA pair reboot and SSL VPN sessions are dropped even though Stateful Sync is enabled.	GEN6-1011
DPI-SSL functionality degrades over time when connections and state information are not removed promptly on connection close.	GEN6-1023
The secondary unit in an HA pair keeps rebooting due to DP side: Core 8: Unhandled Exception. Occurs when the HA pair is being managed by SonicWall GMS and the GMS host setting uses an FQDN Address Object instead of an IP address.	GEN6-1033
The firewall goes down unexpectedly due to a stability issue associated with a data structure representing DPI-SSL caching.	GEN6-1182
The firewall goes down unexpectedly in a scenario where multiple SSH sessions are active simultaneously.	GEN6-1190
The firewall reboots after changing DHCP scope settings during handling of UC APL (DoDIN APL) configuration auditing of changes to DHCP Server configuration.	GEN6-1206

Users

Resolved issue	Issue ID
Unable to delete the users imported from LDAP with the error, “Network object not found”.	GEN6-1171

Vulnerability

Resolved issue	Issue ID
Update the Jquery version used in Virtual Office to 3.4.1 in response to CVE-2015-9251 and CVE-2019-11358 cross-site scripting vulnerabilities. SonicOS was not vulnerable to either of these CVEs.	GEN6-1020

Wireless

Resolved issue	Issue ID
After changing interface settings, the bound-to DHCP server lease scope is deleted.	GEN6-1000

Known Issues

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

Content Filter Service (CFS)

Known issue	Issue ID
The CFS policy is still applied to an administrator level user account even when the **Exclude Administrator** option is enabled in CFS.	GEN6-916

DPI-SSL

Known issue	Issue ID
The WAN side SMTPS client often cannot successfully send mail to the LAN side SMTP server when cleartext is enabled in the DPI-SSL server. **Workaround**: Disable the cleartext option.	GEN6-853
HTTPS websites fail to load when using a Route All Policy Based VPN and Client DPI-SSL is enabled on the remote site. **Workaround**: Disable DPI-SSL inspection on the VPN remote site. If the DPI-SSL service is still needed, enable DPI-SSL inspection on the VPN central site.	GEN6-1160

High Availability

Known issue	Issue ID
In a High Availability pair, the standby firewall cannot be managed using its monitoring IP address. Occurs after restarting the standby firewall.	GEN6-281

User Interface

Known issue	Issue ID
Firmware backup cannot be created when managing the firewall with the Edge browser. **Workaround**: Manage the firewall with Firefox, Chrome or Internet Explorer.	GEN6-554
Under Cloud Backup, clicking the **Delete all configurations** button for a selected firmware version can cause an error. **Workaround**: Manually delete all the cloud backup configuration files under the selected firmware version to be deleted.	GEN6-1189

Users

Known issue	Issue ID
User session time is not updating for any users in the Users > Status session table and user status is not updated after user sign-out. Occurs when Single Sign-On via Capture Client is enabled.	GEN6-312

VPN

Known issue	Issue ID
The Global VPN Client (GVC) cannot connect to the firewall when the WAN Group VPN policy is configured to use the certificate authentication method and the **OCSP checking** option is enabled. **Workaround**: Disable the **OCSP checking** option.	GEN6-768

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 6.5.4 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/support/knowledge-base/what-wireless-cards-and-broadband-devices-are-supported-on-sonicwall-firewalls-and-access-points/170505473051240/

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 8.7 SP1 or GMS 9.2 for management of firewalls using the features in SonicOS 6.5.4.

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 6.5.4. 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, Edge or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- Edge 81.0 and higher
- IE 10.0 and higher
- Safari 10.0 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

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.

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- View video tutorials
- Access 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.

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

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

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa.

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: 5/28/20

232-005208-00 Rev A