EXHIBIT 9

Security

Dell™ SonicWALL™ SonicOS 6.2.6.0

Release Notes

August 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 6.2.6.0 release.

Topics:

About SonicOS 6.2.6.0

SonicOS 6.2.6.0 includes two important new features:

- Capture Advanced Threat Protection
- Content Filtering Service 4.0

See the New features section for more information.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.2. For more information, see the previous release notes, available on MySonicWALL or on the Support Portal at: https://support.software.dell.com/release-notes-product-select.

TZ Series / SOHO Wireless feature support

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.6.0 support most of the features available for other platforms. Only the following features are ***not*** supported on the TZ series or SOHO Wireless appliances:

- Active/Active Clustering
- Advanced Switching
- Capture ATP (supported on TZ500/500W and TZ600)
- Jumbo Frames
- Link Aggregation

- Port Redundancy
- Wire Mode

Supported platforms

SonicOS 6.2.6.0 is supported on the following Dell SonicWALL network security appliances:

- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless
- TZ400 and TZ400 Wireless
- TZ300 and TZ300 Wireless
- SOHO Wireless

New features

This section provides information about the new features in SonicOS 6.2.6.

Topics:

- About Capture ATP
- About CFS 4.0

About Capture ATP

Capture Advanced Threat Protection (ATP) is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV). Capture ATP helps a firewall identify whether a file contains a zero-day virus by transmitting a suspicious file to the Cloud where the Capture ATP service analyzes the file to determine if it contains a virus. Capture ATP then sends the results to the firewall. This is done in real time while the file is being processed by the firewall.

The **Capture ATP** > **Status** page displays a graph chart that shows the percentages of benign and malicious files discovered, as well as the total number of files analyzed. It also displays a log table that shows the results of individual files submitted for analysis.

Capture ATP must be configured on each firewall individually. Once the Capture ATP service license is activated, you can enable Capture ATP on the **Capture ATP** > **Settings** page.

Capture ATP can also analyze files that you upload for analysis from the **Capture ATP** > **Status** page. After the files are analyzed they are listed in the table on the **Status** page. You can click on any file in the log table on the **Status** page and see the results from the detailed analysis of that file.

Note that Capture ATP is only supported on the following appliances. The smaller TZ appliances and the SOHO wireless appliance do not support Capture ATP.

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless

For more information about using Capture ATP, refer to the *SonicOS 6.2.6 Capture ATP Feature Guide*.

About CFS 4.0

Content Filtering Service (CFS) 4.0 has been redesigned to improve performance and ease of use. The workflow was redesigned and more accurate filtering options have been provided. Refer to *SonicOS 6.2.6 Content Filtering Service (CFS) 4.0 Feature Guide* for more details. For information about upgrading from an older version of CFS, see the *SonicOS 6.2.6 CFS 4.0 Upgrade Guide*.

Topics:

CFS workflow

When processing packets, CFS follows this workflow:

1. A packet arrives and is examined by CFS.
2. CFS checks it against the configured exclusion addresses, and allows it through if a match if found.
3. CFS checks its policies and finds the first policy which matches the following conditions in the packet:
   - Source Zone
   - Destination Zone
   - Address Object
   - Users/Group
   - Schedule
   - Enabled state
4. CFS uses the CFS Profile defined in the matching policy to do the filtering, and returns the corresponding operation for this packet.
5. CFS performs the action defined in the CFS Action Object of the matching policy.
6. If no CFS Policy is matched, the packet is passed through without any action by CFS.

CFS settings

The following global settings are used in CFS 4.0:

- Global settings
  - **Max URI Caches (entries)** – Defines the maximum number of cached URI entries. Cached URI entries save the URI rating results, so that SonicOS does not need to ask the backend server for the rating of a known URI. In CFS 3.0, the cache size had a maximum; in CFS 4.0 the maximum is changed to the entry count.
  - **Enable Content Filtering Service** – This option can be cleared to bypass CFS for all packets. By default, it is selected.
  - **Enable HTTPS content filtering** – When enabled, CFS first attempts to get the ServerName from the client "hello". If that fails, CFS attempts to get the CommonName from the SSL certificate and then get the rating. If both attempts fail to get the ServerName/CommonName, CFS uses the IP address for the rating.
  - **Blocked if CFS Server is Unavailable** – If the CFS server cannot provide the rating request within the specified duration (5 seconds by default), this option defines whether to allow or deny the request.
- **CFS Exclusions**
  - **Exclude Administrator** – When enabled, content filtering is bypassed for all requests from an account with administrator privileges.
  - **Excluded address** – Content filtering is bypassed for all requests from address objects selected in the **Excluded address** list.
- **Custom Category**
  - **Enable CFS Custom Category** – Allows the administrator to customize the ratings for specific URIs. When CFS checks the ratings for a URI, it first checks the user ratings and then checks the CFS backend server for the ratings.
- **Advanced Settings**
  - **Enable Smart Filtering for Embedded URL** – When enabled, detects the embedded URL inside Google Translate (Https://translate.google.com) and filters the embedded URL too. Requires that client DPI-SSL be enabled also.
  - **Enable Safe Search Enforcement** – Enforces Safe Search when searching on any of the following web sites:
    - www.yahoo.com
    - www.ask.com
    - www.dogpile.com
    - www.lycos.com

    Requires that client DPI-SSL be enabled also.
  - **Enable Google Force Safe Search** – When enabled. overrides the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action. Note that typically Safe Search happens automatically and is powered by Good, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.
  - **Enable YouTube Restrict Mode** – When enabled, accesses YouTube in Safety mode. YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals.
  - **Enable Bing Force Safe Search** – When enabled overrides the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.