Extreme Security Threat Protection Release Notes

For Release 5.3.1

Published July 2015

9034880

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

1 Release Notes

Extreme Security Threat Protection firmware version 5.3.1 is available. These release notes address compatibility, installation, and other getting-started issues.

Description

Extreme Security Threat Protection firmware version 5.3.1 is a firmware update for the XGS IPS network protection platform. This release provides the following updates to Extreme Security Threat Protection firmware version 5.3:

- Serviceability and support enhancements:
  - Display system CPU, memory, storage information in the command line interface.
  - Restart the following system services in the command line interface: packet processing, packet capture, LMI, SiteProtector communication, and license and update services.
  - View and search system logs in command line interface.
  - Ability to retrieve support files via SFTP.
- Response enhancements:
  - Support of TCP for syslog forwarding.
  - Events (rsyslog) forwarded over TCP in LEEF or non-LEEF format show the same details as the content that is sent to the SiteProtector System.
- Network Access Policy enhancements:
  - Ability to determine the packet source and then control traffic by IP or by identity, based on the HTTP X-Forward-For header.
- IPS Policy enhancements:
  - Ability to derive a new IPS object from an existing IPS object.
  - Prompt warning message when enabling non-sequitur events and status type events in a non-default IPS object.
- Performance: Support FPL5 (25G bps) on XGS 7100
- Miscellaneous updates and implementation changes:
  - Disabled Top 10 URLs and Web Categories dashboard widget.
  - Customers who are pushing the boundaries of Connections per Second rates are likely affected by gathering Top Ten URL metrics for the dashboard.
  - Disabled mDNS responder due to a possible security issue.
  - Support for mutual certificate authentication for communication between the Network Security appliance and the SiteProtector System

NOTE

1 The Top 10 URLs and Web Categories dashboard widget is now disabled by default. You can enable this widget by changing the value of tuning parameter tune.url.topten.tracking to enabled and restarting the packet processing service.

2 The Outbound SSL Inspection feature currently has several known issues that will cause inspection to fail for some websites when the client is using the latest Firefox or Chrome browsers. These issues are under investigation, and will be addressed in a future fix pack.

Compatibility

The following web browsers are currently supported by the Extreme Security Threat Protection version 5.3.1 local management interface:

- Internet Explorer 10 or 11
- Firefox 28 or later
- Google Chrome 34 or later

If Extreme Security Threat Protection appliances use the SiteProtector System, the following database service packs must be applied:

- SiteProtector System 3.0 - Install all DBSPs up to and including SP3.0 DBSP 3.0.0.34
- SiteProtector System 3.1.1 - Install all DBSPs up to and including SP3.1.1 DBSP 3.1.1.16

Installation and Configuration

For step-by-step installation instructions, see the following topics in the IBM Knowledge Center:

- www.ibm.com/support/knowledgecenter/SSHLHV_5.3.1/com.ibm.alps.doc/concepts/alps_intro_page.htm
- www.ibm.com/support/knowledgecenter/SSHLHV_5.3.1/com.ibm.alps.doc/concepts/alps_getting_started_container.htm
- www.ibm.com/support/knowledgecenter/SSHLHV_5.3.1/com.ibm.alps.doc/tasks/alps_configuring_settings_lmi.htm

Known issues

You can find a list of known issues for IBM Security Network Protection 5.3.1 in Technote # 1715537: www.ibm.com/support/docview.wss?uid=swg21715537