Release Notes for Cisco Security Packet Analyzer 6.2(2)

September 22, 2016

This document provides general information about Cisco Security Packet Analyzer software release 6.2(2) software.

This document includes the following sections:

Introduction

Cisco Security Packet Analyzer can accelerate security incident response time and reduce or avoid any potential damage by capturing, querying, and analyzing the relevant packets. This can help to quickly identify the source of malware command and control, or the loss of sensitive company data. Cisco Security Packet Analyzer is an integral part of network security solutions such as Cisco Stealthwatch. Here are its key functions:

- A large rolling buffer on disk to store packet data related to security incidents, and avoid missing the most recent data due to storage space limitation.
- Ability to control the capture by pre-filtering to store only interesting network traffic and make efficient use of the storage resources.

Cisco Systems, Inc.
www.cisco.com

- Intelligent queries can be constructed to extract only the packets that are relevant to security incidents. Queries may be performed through a built-in user interface, or remotely through an API.
- Able to queue multiple simultaneous query requests.
- Able to view the last 100 queries and their results.
- A local packet decoder and analyzer is available to handle large capture files and avoid large file transfers.
- Secure SMB and SFTP file server support for moving critical data to long term storage for compliance and archives.
- High speed SAS port for attaching large external disk storage.
- Real time and in-depth network traffic analysis is performed while capturing the interesting packets to the rolling disk buffer.

System Requirements

For details about Cisco Cisco Security Packet Analyzer system requirements, see your respective installation documentation on Cisco.com.

Supported Device and Feature Information

This release supports Cisco Security Packet Analyzer 2400. It supports three data interface options: two 10G (2x10G) data ports, Four 1G (4x1G) Ethernet (RJ45) ports and Four 1G (4x1G) optical (SFP) ports. You need to choose one and only one interface option according to your requirement.

Supported Browsers

Packet Analyzer supports the following browsers:

- Mozilla Firefox ESR 38
- Microsoft Internet Explorer 11

Restrictions and Limitations

- The packet query function applies only to capture to disk file sessions. To query packet from capture to memory sessions and an individual capture file, use the filters in packet decode function.
- Capture query will not be applicable to the captured files which have been modified. For example, in **Capture > Packet Capture/Decode > Files** page, if you change the captured file name by renaming or merging, then that capture session associated capture files can no longer be used for query.

- Capture query does not query packets from any file that is being written to. That means, if your query time window stretches to or beyond the current time, you may not see these packets in your query result if they are still in the file that is being written to.
- **Capture > Packet Capture/Decode > Query** page can show only the last 100 queries in the History table.

Known Issues in Release 6.2(2)

For a complete list of known and resolved bugs and enhancements for this release, use the Cisco Bug Search tool.

Cisco Bug Search

Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve our customers' effectiveness in network risk management and device troubleshooting.

BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The service has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To use the BST to search for a specific bug or to search for all bugs in a release:

Step 1 Go to https://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at https://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press Return.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter Cisco Security Packet Analyzer 6.2(2) and press Return. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Tip To export the results to a spreadsheet, click the Export All to Spreadsheet link.

Please see Bug Search Tools & Resources on Cisco.com. For more details on the tool overview and functionalities, check out the help page, located at http://www.cisco.com/web/applicat/cbsshelp/help.html

Accessibility Features in Packet Analyzer Release 6.2(2)

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Documentation

You can access the following additional Packet Analyzer guides on Cisco.com. For other documentation related to Packet Analyzer, see Related Documentation, page 4.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

- *Cisco Security Packet Analyzer 2400 Installation and Configuration Guide*
- *Cisco Security Packet Analyzer User Guide*
- *Release Notes for Cisco Security Packet Analyzer 6.2(2) (this document)*

Related Documentation

For platform-related software and hardware documentation, see the Related Documentation section in your Packet Analyzer installation guides.

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at the following URL:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.