Snort IPS for the Cisco 4000 Series Integrated Services Routers

General

Q. What is Snort® IPS for the Cisco® 4000 Series Integrated Services Routers (ISR)?

A. It's an open-source network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Based on industry-recognized Snort technology, Cisco Snort IPS has two major components: a detection engine (Snort Engine) and a flexible rule language (Snort Rules) to describe traffic to be collected. The Snort Engine runs in the service container of the Cisco 4000 Series ISR. It provides lightweight threat defense for compliance with Payment Card Industry Data Security Standards (PCI DSS) and other regulatory compliance mandates.

Q. Why would I want it or need it on my router?

A. You can address PCI DSS and other regulatory compliance in branch sites with no need to deploy special security appliances.

Q. How does Snort for the 4000 Series differ from the open-source version of Snort?

A. While Snort technology is open source, Cisco has fully integrated it into the Cisco IOS® XE Software code base to take advantage of the additional compute power offered by the 4000 Series service container. It is configurable only through the router command-line interface (CLI), and Cisco Prime can be used for centralized deployment and management. Snort rules can be downloaded only from Cisco.com so as to provide for additional validation and the quality and assurance of the Cisco brand.

Snort Rule Sets and Configuration

Q. Can I download Snort rule set updates from snort.org?

A. No, the router will reject Snort rule set updates that are not downloaded from Cisco.com.

Q. What types of Snort rule sets are available for the 4000 Series routers?

A. There are two types available as a term subscription. The Subscriber Rule Set offers the best protection against known threats and is fully supported by Cisco. The Cisco Talos Security Intelligence and Research Group provides proactive security research and instant updates upon the discovery of a new threat. The second rule set, the Community Rule Set, offers entry-level protection against known threats and does not provide any coverage ahead of exploits. It includes a far smaller number of signatures. It's released 30 days after the inclusion of a new threat signature and does not include support from Cisco.

Q. What Snort rule set package should I use?

A. Cisco recommends using the Subscriber Rule Set for the best lightweight threat protection.

Q. How can I customize Snort IPS?

A. You can choose between intrusion detection system (IDS) mode and intrusion prevention system (IPS) mode, and you can decide where to send logs generated by Snort. You can decide whether to automatically point your router to Cisco.com for Snort rule set updates. You can also choose to manually download the Snort rule set updates from Cisco.com, store them on a local server, and point your router to it. You can customize the Snort rule set package by whitelisting (disabling) certain signatures.

Q. What is signature whitelisting?

A. You can eliminate false positives in your network by disabling (whitelisting) certain signature IDs. Doing this will prevent those signatures from firing.

Q. How do I keep my Snort IPS up to date?

A. Cisco recommends that you download Snort rule set updates as soon as they become available or automatically point your router to check for their availability. Moreover, you should update your Snort IPS engine OVA file within 90 days of your last Snort rule set update.

Platform Support

Q. What routers support Snort IDS/IPS?

A. All routers in the 4000 Series:

- 4321
- 4331
- 4351
- 4431
- 4451

Q. Do I need any memory or flash upgrade to be able to run Snort IPS?

A. Yes. You need a minimum of 8 GB of memory and 8 GB of flash. Please check out the system requirements table at http://www.cisco.com/c/en/us/products/collateral/security/router-security/datasheet-c78-736114.html

Q. Are there any hardware and software dependencies?

A. Yes. Download the Snort IPS OVA that is compatible with your Cisco IOS XE Software release. Also, when ordering the Snort rule set updates, make sure to select the product ID specific to the 4000 Series router model that you have.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-736113-00 11/15