Cisco IPS 4500 Series Sensors

Q. What is the Cisco IPS 4500 Series Sensor?

A. The Cisco® Intrusion Protection System (IPS) 4500 Series is a high-throughput, dedicated sensor. The 4500 Series sensors are built on the Cisco ASA 5585-X Adaptive Security Appliance chassis. At first customer shipment (FCS), the 4500 Series operates as a single Security Services Processor (SSP) blade in the bottom slot (slot 0). The Cisco IPS 4500 Series do not require a Cisco ASA blade to operate.

Q. Which customers are most likely to need the Cisco IPS 4500 Series?

A. Organizations that require high throughput and separation of security controls are optimal customers for the 4500 Series. Dedicated security staff at large organizations may require complete control of their IPS systems and thus prefer dedicated appliances. The Cisco IPS 4500 Series is attractive to customers who do not want to pay for both a high-end firewall offering and a high-end IPS and are seeking a solution based on price for performance.

Q. Where should customers deploy the Cisco IPS 4500 Series?

A. The data center and high traffic network junctions are optimal deployment sites for the 4500 series. Customer data centers require data and access security, and an invisible, in-line IPS is well suited for this setting. Internal network edges such as those found between campuses and subnet cores can also benefit from security segmentation. Organizations with Internet connections greater than 2 Gbps also benefit from the 4500 Series.

Q. What is the difference between the Cisco IPS 4500 Series and the Cisco ASA 5585-X Series-based IPS?

A. While the physical differences are minimal, there are multiple operational differences. These are the same systematic differences found between Cisco's firewall IPS solutions and dedicated IPS platforms.

- Dedicated IPS platforms are invisible on the wire and default to a fail-open operation to ensure network continuity.
- The dedicated IPS controls all packet processing and its own I/O.
- The evasion detection and normalization process is fully under the IPS's control, and its outputs are visible to the threat-detection process.
- The firewall defaults to a closed condition in a failure and is detectable on the network.
- When IPS is coupled with the firewall, there are additional packet routing and inspections on the firewall that offload some IPS processing.
- The Cisco ASA can provide identity context to determine flows for inspection by specific IPS policies.

Q. What is the difference between the Cisco IPS 4500 Series and the Cisco IPS 4200 or 4300 Series?

A. There are no IPS software differences: the Cisco IPS 4200, 4300, and 4500 Series run the same software version. All three series operate with the same signatures offering the same protections.

The primary difference is performance: the 4500 Series offers significantly improved throughput and latency. The maximum connections and connection-per-second rates for the 4500 Series are significantly higher as

well. Much of the performance gain is made through the use of hardware- accelerated regular expression processors that the 4200 Series do not have.

Physical differences are significant because the Cisco IPS 4500 Series is based on the Cisco ASA 5585-X appliance platform. The 4500 Series has an open slot (slot 1) for future expandability. The 4200 Series does have more I/O flexibility. What's more, the Cisco IPS 4260 and 4270 Series can be ordered with a hardware bypass network interface card (NIC).

Q. What are the performance characteristics of the Cisco IPS 4500 Series?

A. Cisco has redefined IPS performance measurement in a format that is customer and field-service friendly. We have moved away from a pure HTTP performance metric to an average of five deployment-focused tests. Using a third-party testing tool and their test suite, we test for performance that is typical of:

- A remote office or small to medium-sized business
- An enterprise application suite
- An enterprise data center
- An educational institution at the Internet edge
- A service provider environment

We then average the five tests to get a system performance value. Data sheets then present this value and a performance range to show the breadth of potential performance the customer will experience. Cisco sales engineers will be trained on the test-specific values.

Q. What are the management options for the Cisco IPS 4500 Series?

A. At FCS July 2012, Cisco IPS Device Manager (IDM) Version 7.1.4 and Cisco IPS Manager Express (IME) Version 7.2.3 support the Cisco IPS 4500 Series natively. Cisco Security Manager Version 4.3 also supports the 4500 Series.

Q. Have the Cisco IPS 4260 and 4270 Series now reached end-of-life?

A. At this time there are no end-of-life activities in place for the Cisco IPS 4200 Series. The same software version runs on Cisco IPS 4200, 4300, and 4500 Series, offering investment protection for existing customers who are looking to augment their existing Cisco IPS deployments, or replace older units with better throughput and performance.

Q. Why would a customer select the 4500 Series over the 5585-X ASA/IPS combination?

A. As discussed in the "differences" question above, there are operational differences between the two. These operation differences will create preferences within different buying groups. Team focused purely on security, with needs for stricter security access controls and security visibility, will prefer dedicated IPS appliances. In addition, at a future point, the Cisco 4500 Series may become even higher performing by accepting a module in the second (currently empty) slot. As always, it is important to gather needs and understand the buying and operational dynamics of the teams involved.

Q. Why would a customer select the 5585-X ASA/IPS combination over the Cisco IPS 4500 Series?

A. The converse of the question still comes down to the buying and operating groups. The operational differences between the two solutions create preferences within different buying groups. Network operations teams or those with common operators/managers of firewalls and IPS solutions will likely prefer a firewall/IPS combination. As always, it is important to gather needs and understand the buying and operational dynamics of the teams involved.

Q. What are the physical differences between the 4500 Series and the Cisco ASA 5585-X Series- based SSPs?

A. The products are physically identical except for the silk screened identifier at the front.

Q. Can I simply upgrade my existing 5585-X Series-based SSPs into a 4500 Series equivalent?

A. No, the software will only install on hardware that is uniquely identified as applicable. While the Cisco IPS Device Manager (IDM) Version 7.1 code base is common, the packages specific to the 5585-X SSPs and the 4500 Series have some operational differences, given the absence of the Cisco ASA appliance.

Q. What version of IPS software will run on the 4500 Series?

A. The initial release will be Version 7.1.4.

Q. Will the Industrial Control Security signatures operate on the Cisco IPS 4500 Series?

A. Yes, any IPS that can use the IDM Version 7.1 code base can operate these signatures. Data center and high traffic network segments are less likely to see industrial control network, so from a topology perspective, buyers may be less likely to pursue them. From an aggregation perspective, it may be valuable to detect such traffic's leakage into the standard IT network using a Cisco IPS 4500 Series Sensor.

Q. Will the Global Correlation and Reputation Filter operate on the Cisco IPS 4500 Series?

A. Yes, any IPS that can use Version 7.1 software base, such as the 4500 Series, can operate with the SIO provided Global Correlation and Reputation Filter. Note that Global Correlation is beneficial largely at the Internet edge.

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 C67-711991-00 07/12