Cisco IT Refreshes IPS Sensor Platform Network Wide

Cisco IPS 4500 and 4300 Series Sensors deliver greater throughput, faster traffic flow processing, and smaller form factor.

Organizations face a relentless battle to protect their intellectual property and other valuable corporate assets and data from a vast and varied army of security threats. Like most enterprises, protecting data centers and all areas of the corporate network is a top priority for Cisco. To augment its security detection and prevention measures, in 2013 Cisco IT began refreshing the Intrusion Protection System (IPS) Sensor models throughout Cisco's global network.

An integral component of Cisco's overall security landscape, the sensors have both intrusion prevention (active blocking) and intrusion detection (passive monitoring) operational modes. Cisco IT deploys sensors where the most critical corporate assets reside, including near data center gateways, the DMZ core, extranet partner gateways, VPN headends, and colocations.

The network refresh includes IPS 4510 and 4520 models, the first Cisco® IPS Sensors to support direct 10-Gbps connectivity. The IPS 4500 Series Sensors protect individual components within the data center, such as web servers, databases, and enterprise-class applications. After refreshing areas of the network that have business-critical assets and 10-Gbps line rate requirements, Cisco IT will replace IPS 4260 Sensors with IPS 4360 Sensors, which protect servers and end hosts in edge, campus, and branch environments.

The upgraded IPS Sensors yield several performance improvements:

- As mentioned, the Cisco IPS 4500 Series has the ability to inspect traffic flows at 10 Gbps, with average inspection throughput of 3 Gbps to 10 Gbps
- IPS 4360 average inspection throughput of 1.25 Gbps
- Average latency <150 microseconds for both the IPS 4500 and 4300 Series

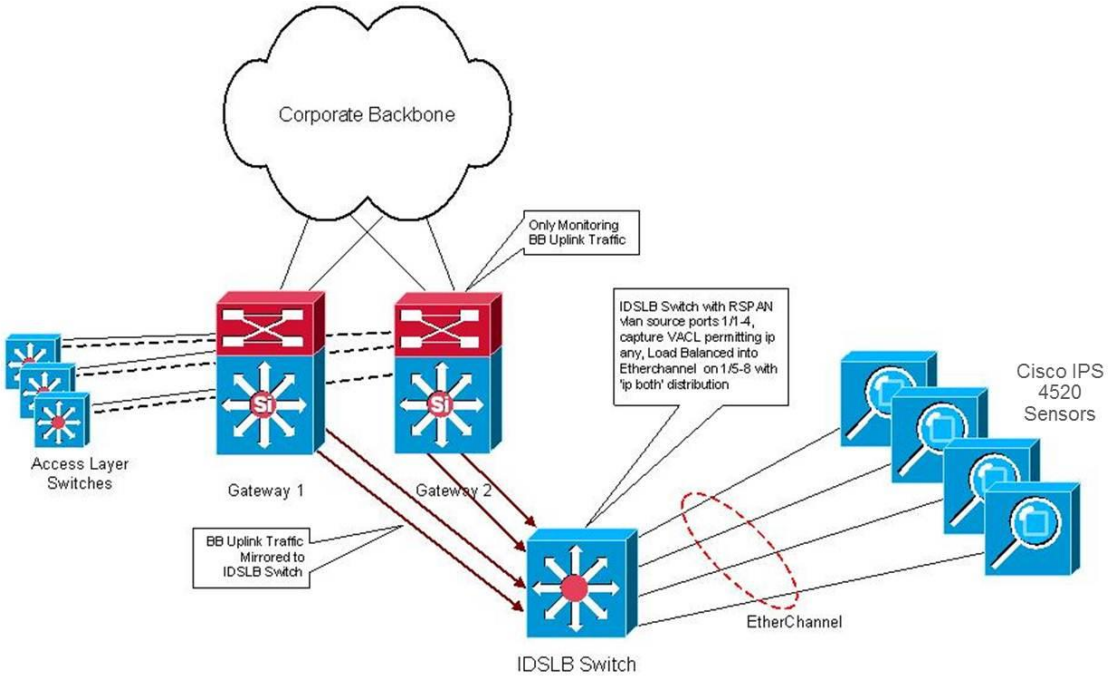
Additionally, the IPS 4360 Sensor is only one rack unit compared to the two-rack-unit 4260 Sensor.

"These smaller form factor boxes are a good fit for companies moving toward virtualization, and looking to decrease their physical hardware and use space more efficiently," says Kyle Bolton, engineer in Cisco's Computer Security Incident Response Team (CSIRT).

IPS Data Center Deployment

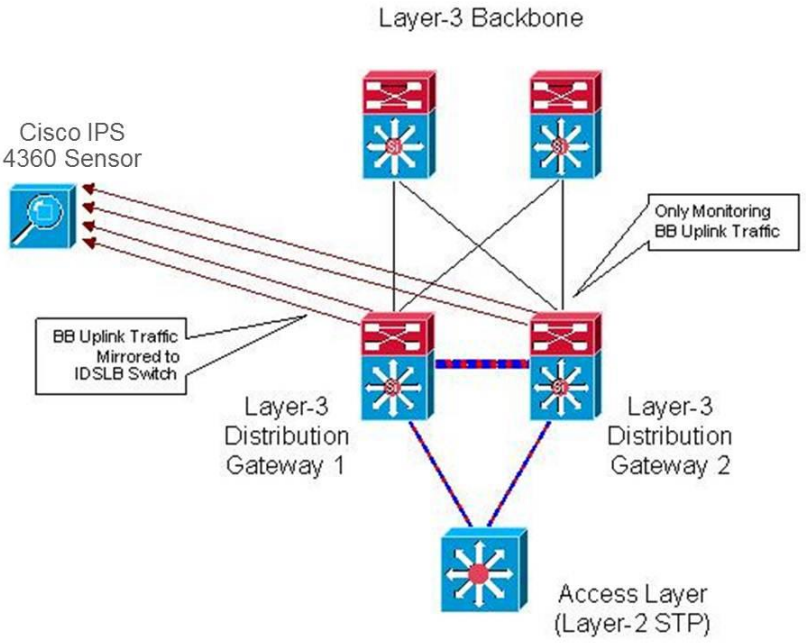
Cisco IT developed designs for deploying the IPS in large and small data center environments. Large data centers have a Cisco Catalyst® 6500 Series Switch, which uses EtherChannel load balancing to spread traffic among the Cisco IPS 4360 Sensors. The IPS 4500 Series Sensors are typically deployed in clusters of three or four to provide the required bandwidth coverage and redundancy (Figure 1).

Figure 1. Large Data Center Design



Other Cisco environments, such as small data centers, engineering server rooms, and offshore development centers, use a single Cisco IPS 4360 Sensor (Figure 2). Centralized CSIRT personnel manage the sensors remotely using out-of-band access on the IPS 4360 Sensor.

Figure 2. Small Data Center Design



To help ensure that the IPS implementation does not interfere with data center production activities, both the large and small data center designs are based on passive monitoring, which does not impact network performance, rather than inline monitoring. The switches receive a copy of network traffic that is duplicated into a Remote Span (RSPAN) VLAN and filtered by a VLAN access control list (VACL). The VACL filters out encrypted traffic, which is not inspected. All other traffic is load balanced using EtherChannel to the Cisco IPS Sensors.

CSIRT and Intrusion Detection

According to Verizon's 2013 Data Breach Investigations Report, companies need to put more focus on detection and remediation efforts, in addition to their intrusion prevention measures. The report, which analyzed data from 19 global organizations covering more than 47,000 reported security incidents and 620 data breaches, recommends that organizations focus on better and faster detection through a blend of people, processes, and technology. Sixty-nine percent of the data breaches cited in the report were detected by an external party, not IT.

Cisco CSIRT works hard to shatter statistics like this. The group focuses on detecting, investigating, and remediating security threats and vulnerabilities, with teams in engineering (design, implement, and operate all the security gear in Cisco's network), event analysis (scour logs to identify infections and remediate with the host and application owners), and investigations (research security postures globally and actively investigate detected issues).

The IPS Sensors are integral to CSIRT's detection and remediation efforts. The team relies on the intrusion detection, or passive monitoring, mode to help detect security threats and vulnerabilities before they can wreak havoc. Additionally, CSIRT regularly works with Cisco's Security Technology Business Unit to evaluate and beta test products such as the IPS Sensors, along with major releases of the service pack code and signature packs.

The IPS Sensors also help the team tailor its defenses proactively. For example, an IPS Sensor detects a malware outbreak. Hosts are being infected and talking to a command-and-control server. CSIRT receives an alert about the detected vulnerability and temporarily applies a Border Gateway Protocol (BGP) blackhole, blocking network connections to the affected server until the issue can be remediated.

Malware is increasing, says Bolton, and web malware occurs everywhere people visit on the Internet, including legitimate websites they visit frequently for business purposes. Data from the 2013 Cisco Annual Security Report confirms that the web is the most formidable malware delivery mechanism seen to date, outpacing even the most prolific worm or virus in its ability to infect a mass audience silently and effectively.

General malware infections alone cost time and money to repair. Cisco has a reimage policy for infected laptops, and reimaging and rebuilding one laptop requires, on average, six hours of downtime.

Distributed denial of service (DDoS) attacks are also on the rise. Cisco.com web servers are CSIRT's biggest concern. One way the CSIRT team helps minimize the impact of detected DDoS threats is by configuring the IPS Sensor to send automatic alerts when known DDoS triggers are detected (known triggers are matched using Cisco standard or custom signatures). Once alerted, the team can implement DDoS protection on other equipment.

"The IPS intrusion detection mode allows us to detect events directly on the network," says Bolton. "The IPS is one of our main front-line defenses when it comes to detection."

For More Information

Cisco IPS: http://www.cisco.com/en/US/partner/products/ps5729/Products_Sub_Category_Home.html

To read additional Cisco IT articles and case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**