Cisco Protects Internal Infrastructure from Web-Based Threats

BUSINESS BENEFITS

- Protected Cisco infrastructure from zero-day threats
- Supported policy of allowing employees to use unmanaged devices for work
- Blocked twice as many malicious objects as malware scanning alone
- Did not add significant IT overhead

"The IronPort WSAs blocked one percent of all web transactions, or 30 million in just the first three months. These could have been commands to or from botnets, retrieval or leaking of user passwords and other personal information, and malware downloads."

Jeff Bollinger, Senior Information Security Investigator

IronPort Web Security Appliance blocked 30 million malicious objects in first three months of production.

The web is becoming the predominant exploit vector. Just browsing, without even clicking a link, is enough to get compromised. Black lists and white lists fail to block a significant portion of malicious websites, because 77 percent of websites with malicious code are legitimate sites that have been compromised.[1]

Cisco IT uses multiple technologies to combat web-based threats. NetFlow provides a statistical analysis of all network traffic. Cisco® Intrusion Prevention System (IPS) and the host-based Cisco Security Agent identify anomalous behavior that can signal malware infections. Antivirus software routinely stops known treats. But Cisco also needed protection against zero-day threats, when the signature is not yet known.

Recent changes in Cisco IT's client strategy increased the urgency of a solution. For example, employees can now use any device for work, including unmanaged personal devices that might not be protected. Employees visit social networking sites more frequently, and links on these sites are notorious for delivering malware. Smartphone operating systems are also becoming a target for hackers.

Cisco IronPort™ S670 Web Security Appliances (WSAs) protect against web-based threats without changing the user experience. The IronPort WSA is a web proxy that inspects and then either forwards or drops web traffic based on reputation filters or the outcome of inline file scanning. The cloud-based reputation service is Senderbase.org.

For the first three months of production for Research Triangle Park, North Carolina and the East Coast, the IronPort WSA S670s blocked just under one percent of traffic, or 30 million transactions. Blocked transactions could have been commands to or from botnets, retrieval or leaking of user passwords and other personal information, and malware downloads.

Fifty-two percent of all objects blocked were the result of a low reputation score. Malware scanning alone would not have detected and blocked these threats.

[1] Websense Security Labs, "State of Internet Security, Q3 - Q4, 2008."

Management overhead is very low. The IronPort WSAs automatically update themselves every few minutes from the central Senderbase database.

FOR MORE INFORMATION

To read the entire case study or additional Cisco IT case studies on 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.**