# Cisco Protects Internal Infrastructure from Web-Based Threats

> "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

## Background

Cisco is working to become a borderless enterprise, where authorized employees, partners, and customers can access any service, anywhere, from any device. Cisco IT's policy of allowing employees to use any device, including unregistered personal devices, requires an effective web security solution. For Cisco, this solution is the Cisco IronPort™ S670 Web Security Appliance (WSA), which combines signature-based malware detection with reputation filtering and inline file scanning. In just the first three months of production for Research Triangle Park, North Carolina and the East Coast, the Cisco® IronPort WSA S670s blocked more than 30 million malicious objects that signature-based detection alone would have missed. This case study describes web security requirements at Cisco, how Cisco uses the appliances, and initial results. Cisco customers can draw on Cisco IT's real-world experience to implement the Cisco IronPort WSA in their own environments.

## Challenge

The web is becoming the predominant exploit vector,[1] and since 2008, Cisco IT has noted a significant increase in attacks originating from the web. "Just browsing, without even clicking a link, is enough to get compromised," says Jeff Bollinger, senior information security investigator at Cisco.

Commonly used black lists and white lists fail to block a significant portion of malicious websites. According to Websense Security Labs, 77 percent of websites with malicious code are legitimate sites that have been compromised,[2] and legitimate sites do not appear on black lists. The same report states that, in the last half of 2008, 70 percent of the 100 most popular sites either hosted malicious content or contained a masked redirect to lure unsuspecting victims to malicious sites.

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.

[1] Symantec, Internet Security Threat Report, 2011.
[2] Websense Security Labs, "State of Internet Security, Q3 - Q4, 2008."

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

But Cisco also needed protection against zero-day threats, when the signature is not yet known. “Because the detection rate for zero-day exploits is near zero, antivirus software alone isn’t enough to protect a host against security threats,” says Bollinger.

Recent changes in Cisco IT’s client strategy increased the risk of web-based threats and the urgency of a implementing a solution:

- The company has adopted a policy of giving employees a choice of any device to use for work, including unmanaged personal devices. “We have to assume that our employees’ unmanaged personal devices have little protection,” Bollinger says. “Therefore, we need to build protection into the network.”
- Employees now visit social networking sites more frequently. Links on these sites are notorious for delivering malware.[3]
- More Cisco employees are using smartphones for browsing. Smartphone operating systems are becoming a target for hackers.[4]

Therefore, the Cisco Computer Security and Incident Response Team (CSIRT) and Cisco IT wanted a tool that would block malicious websites before they loaded on browsers. Solution criteria included:

- Increasing the level of security protections at the application layer of the network.
- Protecting unmanaged endpoints to support the Cisco commitment to allowing employees to work with any device.
- Gathering data on the types and volume of web-based threats and attacks.
- Maintaining the same browsing experience. In particular, Cisco IT did not want to require employees to change their browser settings.

## Solution

Cisco IT achieved the goal of protecting against zero-day threats without changing the user experience using the Cisco IronPort S670 Web Security Appliance (WSA). 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 IronPort WSA combines many technologies in one platform. Cisco initially is using two capabilities: Web-Based Reputation Filters (WBRS) and the Webroot and McAfee antimalware scanning engines.

Unlike many companies, Cisco is not using the IronPort WSA’s web-filtering capabilities to block entire website categories, such as gambling or shopping. The company’s policy is to trust employees to use their time productively. “Cisco has always had a permissive web-access policy because of its engineering and development focus,” Bollinger says.

**What Happens When an Employee Requests a Website**

When an employee clicks a link or enters a URL, behind the scenes, the request is sent by way of Web Cache Communication Protocol (WCCP) to a load-balanced pool of Cisco IronPort S670 WSAs. The WSA determines

[3] ITbusiness.ca, “Malware, Spam in 10 Percent of Facebook Links,” October 6, 2010.
[4] PCWorld, “Six Biggest Rising Threats from Cybercriminals,” May 19, 2011.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

whether to allow or reject the entire website, or individual objects on the website, based on a reputation score from the Senderbase.org cloud service. The service is the same one used by Cisco IronPort Email Security gateways.

The Senderbase cloud service assigns each website a reputation ranging from -10 to 10. Websites with scores from -6 to -10 are automatically blocked, without scanning. Websites with scores from 6 to10 are allowed, also without scanning.

“Most sites have a reputation in the +6 to -6 range, meaning insufficient data is available to know whether the site is bad or good,” says Bollinger. When a Cisco employee requests a webpage with a reputation score in this range, the antimalware services in the IronPort WSA scan the files and web objects before they are loaded into the browser. The scan looks for strings or references matching a malware signature in the Webroot or McAfee databases. If banners or links on a page are compromised, those objects do not load, but the others do.

If the entire site is compromised or malicious, Cisco employees are redirected to an internal page, stating that the website they were attempting to visit is unsafe. The page explains that the website was blocked because it is unsafe, and provides an email link for support.

**Global Deployment**

Cisco deployed the Cisco IronPort S670 WSA in three phases:

- **Proof of Concept (POC):** Cisco CSIRT led a 300-user POC, conducted over six months in one building of the Cisco campus in Research Triangle Park (RTP), North Carolina. The appliances inspected all web-bound traffic, as well as the return traffic from the web to Cisco users’ devices. Cisco CSIRT enabled WCCP on each desktop VLAN to redirect traffic with destination port 80/TCP to the IronPort WSAs. WCCP enables the IronPort WSA to inspect a user’s web traffic, making it unnecessary for Cisco IT or employees themselves to configure the web browser to use the IronPort proxy. Not requiring a specific browser configuration supports Cisco IT’s any-device strategy. “During the POC, we validated that reputation filtering blocked malicious traffic that malware filtering missed,” Bollinger says. No outages occurred during the POC.
- **Pilot:** Next, from early 2009 to early 2011, Cisco CSIRT extended the solution to all 3000 employees on the RTP campus. Every web request initiated over a wired or wireless network was redirected to one of four Cisco IronPort WSAs. During the pilot, the IronPort appliances blocked one percent of all web traffic, representing four million objects that otherwise might have infected the network or led to information leakage.
- **Enterprise deployment:** Cisco IT has been begun deploying the Cisco IronPort WSAs in other large campus sites, beginning with offices whose Internet traffic is routed through RTP. “Scaling from 3000 to 30,000 users only requires changing an access list, enabling WCCP on the routers, and pointing the routers to the IronPort WSAs,” says Bollinger. IronPort WSAs are also currently in production on the San Jose, California and Bangalore campuses. Users do not notice any change when their web requests are sent through the proxy server.

## Design and Location Decisions

For the POC, Cisco CSIRT deployed the Cisco IronPort WSAs at the building’s desktop gateway switches. Two appliances provided more than sufficient processor capacity for the 300 users in the POC. “Capacity requirements depend on the number of applications enabled on the WSA, such as reputation, antimalware, authentication, and

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

so on, as well as the number of users," says Bollinger.

For the pilot, Cisco IT gave careful thought to device placement. Tradeoffs are available between implementing the solution in all Internet points of presence (POPs) and minimizing the number of appliances to manage.

Cisco IT decided to deploy IronPort WSAs at each Internet POP. Just four to six devices at each POP can support all 130,000 users in the Cisco enterprise. This design gives Cisco IT the flexibility to deploy where web traffic is most concentrated, while excluding certain networks from the proxy as necessary.

To make sure that the IronPort WSAs did not interfere with Cisco Wide Area Application Services (WAAS), which also uses WCCP, Cisco IT deployed the appliances upstream from Cisco WAAS. "We inspect traffic only after WAAS has finished compressing and accelerating its traffic," Bollinger says.

### Configuring the IronPort WSAs

Cisco IT uses the following configuration options:

- **Redirection method:** Cisco CSIRT configured the Cisco IronPort WSA as a transparent proxy deployment, meaning that a router redirects web-browsing traffic to the appliance. Cisco users browse the web exactly as they would ordinarily, and do not have to change their browser settings when working from home or another location outside of Cisco. The other option would have been an explicit proxy deployment, which requires either pointing to a file on the network that directs the browser to a web proxy server, or else manually configuring each browser. "Explicit mode works well with managed endpoints, but Cisco is committed to letting employees use any device, including smartphones," Bollinger says. Explicit mode would have also required employees to change their proxy settings when browsing from outside of Cisco.

- **Fail Open:** Should an appliance fail, Cisco employees can continue to browse, without protection. Employees cannot tell the difference. "The fail-open capability of the Cisco IronPort WSA is very important to us," Bollinger says. The IronPort WSA can also operate as a fail-closed system for organizations that prefer this option.

### Support

The Cisco IT networking team deploys, configures, and patches the Cisco IronPort WSAs. The Cisco CSIRT team, in turn, controls security policy, including exceptions. For example, if a Cisco security researcher wants to visit a blocked site, CSIRT can open access for that individual only.

If an employee disputes the decision to block a webpage, Senderbase's email support team promptly reviews the reputation ranking.

## Results

Cisco is now experiencing its highest ever level of protection from web-based threats. During the pilot, the IronPort WSA blocked numerous Trojans and viruses as well as tens of thousands of commercial tracking cookies from reaching Cisco employees' devices. The logs were a revelation for CSIRT, according to Bollinger. "The logs showed that the biggest threats today are not underground hacking sites, but everyday websites such as blogs, forums, and wikis," he says. "Typically your system gets compromised simply by visiting a site, and you have no

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

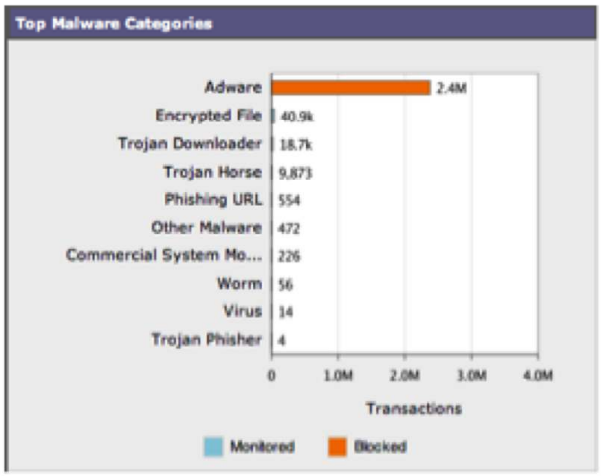
idea. The bulk of the web is really dangerous."

The Cisco IronPort WSA also protects users from zero-day exploits against business applications that have vulnerabilities. During the pilot, for example, a malicious .JPG file attempted to take advantage of an ActiveX vulnerability that did not have a patch at the time. If employees using a particular browser visited a website that included the .JPG, the browser loaded malware onto the client. Log data shows that the IronPort WSA blocked the image because of its low reputation score: -9. The logs also confirm that, in Cisco locations not participating in the pilot, simply loading an image on a webpage was enough to infect vulnerable devices.

### More Than 30 Million Objects Blocked During One Quarter

For the first three months of production for RTP and the East Coast, the four Cisco IronPort WSA S670s inspected more than three billion HTTP transactions. "The IronPort WSAs blocked one percent of all web transactions, or 30 million in just the first three months of production," says Bollinger. "These could have been commands to or from botnets, retrieval or leaking of user passwords and other personal information, and malware downloads. The IronPort WSAs effectively prevented this malware from entering the Cisco network." Figure 2 shows an IronPort WSA report on the malware types blocked.

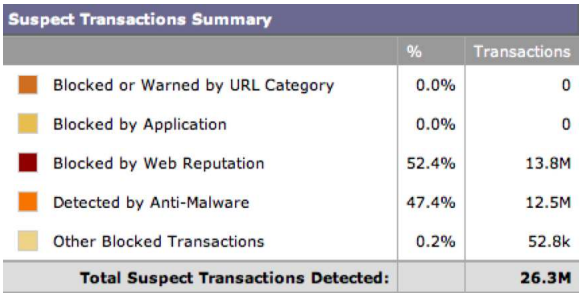
**Figure 1.** Blocked Malware Categories




Of the three billion objects that employees requested during the first quarter of production for the East Cost, 52 percent were blocked because of a low reputation score (Figure 3). "The IronPort WSA reports highlighted a few recently registered top-level domains as having especially poor reputations," Bollinger says. "All domains in the list were attempting to distribute and execute malware, and the IronPort WSA effectively prevented infections or data leakage on employees' devices."

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

**Figure 2.** More Than Half of Blocked Sites were Blocked Because of Poor Reputation



| Suspect Transactions Summary | | |
|---|---|---|
| | % | Transactions |
| Blocked or Warned by URL Category | 0.0% | 0 |
| Blocked by Application | 0.0% | 0 |
| Blocked by Web Reputation | 52.4% | 13.8M |
| Detected by Anti-Malware | 47.4% | 12.5M |
| Other Blocked Transactions | 0.2% | 52.8k |
| **Total Suspect Transactions Detected:** | | **26.3M** |

Many of the blocked objects were banner ads that distributed unwanted tracking cookies. Other blocked sites had very negative reputation scores, because they were previously or currently distributing malicious code or were part of spam campaigns.

### Low IT Overhead

Internally maintaining white lists and black lists is not a scalable solution. The Cisco IronPort WSA serves the same purpose by automatically updating itself from the central Senderbase database every few minutes. “We don’t have to schedule signature updates, because the appliances are constantly connecting to Senderbase,” Bollinger says. The only overhead is storing a log entry for every fetched object, whether the object is blocked or allowed. Cisco IT chooses to do this, although it is not required.

Cisco CSIRT uses the Cisco IronPort M-Series Security Management appliances for IronPort WSAs as well as IronPort Email Security Appliances.

## Lessons Learned

Based on their experiences, Cisco CSIRT and Cisco IT offer the following recommendations to other companies implementing Cisco IronPort WSAs:

- If you display a webpage explaining that the requested webpage has been blocked, make sure the explanation is easy to understand and tells how to get support if needed. Cisco includes an email link for support.
- If you need to restart the WCCP service, also restart the proxy services on the Cisco WSA. The restart synchronizes the WCCP cache on the router and the proxy. After Cisco IT introduced the Cisco WSA, some users reported slower performance. Cisco IT resolved the issue by restarting the proxy services.
- If you use an access control list (ACL) to redirect WCCP, be sure it includes all networks you want to redirect. You might need to include another ACL to bypass network segments that you do not want to redirect through the WSA.
- Deploy the IronPort WSA where it will intercept the most browsing traffic. At Cisco, this is the junction between the internal network and the Internet. To minimize the number of devices needed, Cisco configured WCCP redirection at the aggregation point for all outbound traffic. Be sure to include wireless gateways and remote access networks if you have a mobile workforce. Data center servers typically do not require protection from web-based threats, but protection may be advisable in some cases.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

## Next Steps

Cisco IT is considering using the ScanSafe cloud security service in conjunction with the Cisco AnyConnect VPN client. “ScanSafe provides the same level of web security, but from the cloud,” says Jawahar Sivasankaran, senior manager in the Cisco IT Customer Strategy and Success group. “The idea is to automatically route web requests from employees working in a Cisco office to the Cisco IronPort WSA, and requests from employees working anywhere else to the ScanSafe cloud. ScanSafe integration with Cisco ISR G2 routers is a core component of our future branch office and cloud computing strategy.”

## For More Information

To read more about Cisco IronPort Web Security Appliances, visit www.cisco.com/go/wsa.

To read 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.

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

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.

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.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.