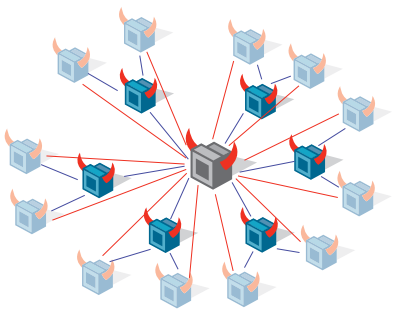
Cisco IronPort Web Reputation Filters

THE INDUSTRY'S FIRST WEB REPUTATION FILTERS PROVIDE A POWERFUL DEFENSE AGAINST MALWARE

Cisco® IronPort Web Reputation Filters are designed to combat the increasingly prevalent and dynamic nature of malware. Today's threats are no longer found as an email attachment. Instead, they are well orchestrated – utilizing social engineering techniques that mirror and target legitimate websites. According to the Cisco Threat Operations Center, exploited websites are responsible for more than 87 percent of all web-based threats today. Malware writers are now targeting well-known, trusted websites.



A single botnet can spawn thousands of malware-laden botsites in just a few hours.

One of the fastest growing vectors for distributing these web-based threats is through compromised hosts (known as botsites) that follow instructions from a command-and-control network (known as botnets). Spreading through recruiting emails and webpage spam, malicious botsites self-propagate through their own established peer-to-peer networks. These botnet/botsite systems represent an intelligent malware distribution platform that is reusable and self-defending.

As the first line of malware defense, Cisco IronPort Web Reputation Filters analyze more than 5 billion web transactions daily – blocking up to 70 percent of malware at the connection level, prior to signature scanning. By utilizing a global footprint of URL traffic data, this unique web reputation system is able to offer an industry-leading 60 percent higher malware catch rate than traditional signature scanners.

Cisco IronPort Web Reputation Filters leverage Cisco Security Intelligence Operations (SIO), an advanced security infrastructure that provides threat detection, correlation and mitigation to continuously facilitate the highest level of security for Cisco customers. Using a combination of threat telemetry, a team of global research engineers and sophisticated security modeling, Cisco SIO enables fast and accurate protection – allowing customers to securely collaborate and embrace new technologies.

OVERVIEW (CONTINUED)

Cisco IronPort Web Reputation Filters examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains. This gives Cisco IronPort technology a powerful advantage over solutions that reduce web reputation to a simple URL filtering category. Cisco IronPort Web Reputation Filters are the industry's only reputation system to include exploit filtering, botsite defense and URL outbreak detection – protecting users from known and unknown exploits (including adware, Trojans, system monitors, keyloggers, malicious/tracking cookies, browser hijackers, browser helper objects and phishing attacks) delivered through cross-site scripting (XSS), cross-site request forgery, SQL injections or invisible iFrames.

As the industry's first and best web reputation filtering system, Cisco IronPort Web Reputation Filters provide a powerful outer layer of malware defense at the network perimeter.

THE CISCO IRONPORT DIFFERENCE

Cisco IronPort email and web security products are high-performance, easy-to-use and technically-innovative solutions, designed to secure organizations of all sizes. Purpose built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

Leveraging the Cisco Security Intelligence Operations center and global threat correlation makes the Cisco IronPort line of appliances smarter and faster. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

FEATURES

Cisco IronPort Web Reputation Filters intelligently apply web security policies based on a requested URL's reputation. This prevents malicious web traffic from even entering the network, while allowing legitimate web requests to flow unobstructed.

Accurate Reputation Scores

The Cisco IronPort SenderBase® Network is the world's first and largest web and email traffic monitoring system. SenderBase collects data from more than 100,000 networks around the world, ten times more than competing reputation monitoring systems. By tracking a broad set of over 150 web- and email-related parameters, the Cisco IronPort SenderBase Network supports very accurate conclusions about any given URL or IP address. Parameters examined to determine URL reputation include: domain registration information, use of dynamic IPs, traffic volumes, patterns in the URL being requested, as well as the use of behavior-based scanners. Cisco IronPort web reputation technology leverages real-time cloud scanning, powered by SenderBase, to find and block access to compromised websites before malware can become operational. The breadth of data available to Cisco through the SenderBase Network allows virtually every active URL and IP address on the Internet to receive a web reputation score. By comparison, even the best URL filtering technologies from other vendors have scored only 15 percent of webpages.

Real-Time Updates

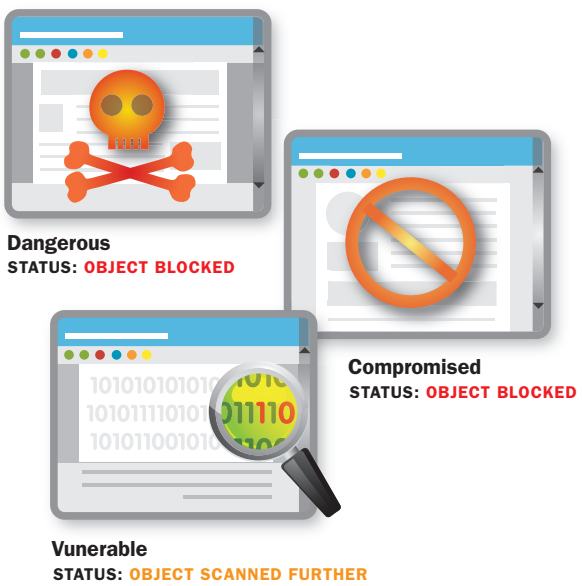
Advanced protection, powered by Cisco Security Intelligence Operations (SIO), delivers current and complete security information to Cisco customers and devices. Threat mitigation data is provided through:

- Dynamic rule updates for Cisco products, such as firewall, web, IPS, or email devices
- IntelliShield vulnerability aggregation and alert services
- Security best-practice recommendations and community outreach services

When a new threat is detected (based on processing data in Cisco SensorBase), it is extracted and correlated, rules and signatures are generated, and systems are dynamically updated. Updates are then immediately sent to Cisco security devices – enabling customers to stay ahead of the latest threats.

FEATURES (CONTINUED)

Exploit Filtering



With the addition of Exploit Filtering, Cisco offers uncompromised protection against one of the biggest invisible threats on the web: the transparent passing of malware through legitimate websites.

Dynamic Protection

Exploit Filtering zeros in on the latest network security threat: trusted websites that have been compromised to deliver Trojans or phishing attacks through techniques such as cross-site scripting (XSS), SQL injections and invisible iFrames. Cisco IronPort Exploit Filtering technology groups these websites into three risk levels:

- Dangerous – These sites are actively serving malware or have malicious scripts injected into the site and are immediately blocked.
- Compromised – These sites have malicious scripts present, but they have not been activated by the bot network's command and control servers. These sites, too, are blocked by default.
- Vulnerable – These sites are at put on a "risk watch" and actively monitored by Cisco's Threat Operations Center because they are susceptible to attack or have been linked to malware distribution in the past.

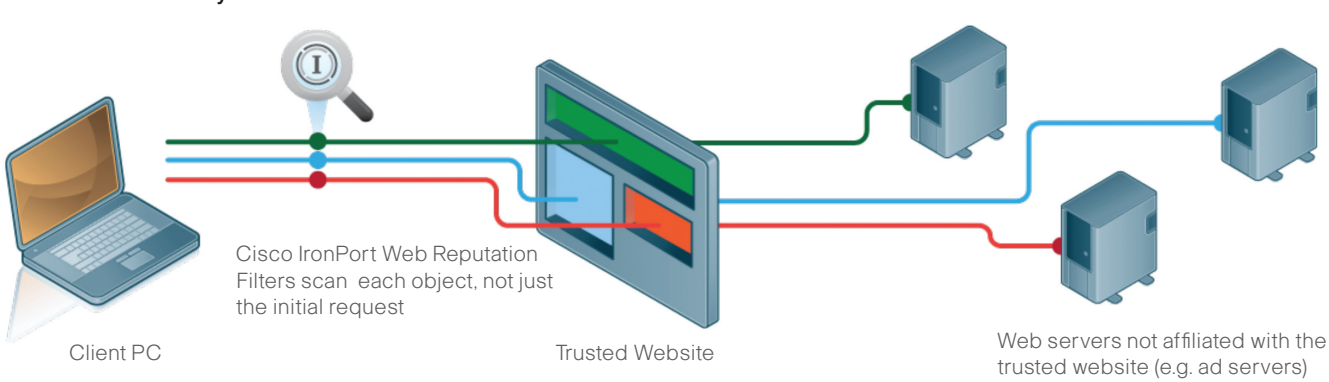
Botsite Defense utilizes next-generation threat assessment techniques on all content fetched by the browser – giving Cisco IronPort Web Reputation Filters the ability to detect and block botsites based on certain characteristics they exhibit. Looking at the content's origin, Cisco IronPort Botsite Defense leverages security-modeling techniques to provide dynamic protection against threats that target legitimate websites.

URL Outbreak Detection is designed to identify and defend against URLs that have no reputation or signature, which are typically hosted on a botsite and controlled by a botnet. Utilizing the Cisco IronPort SenderBase Network, URL Outbreak Detection is able to identify virus outbreaks on average 13 hours before traditional anti-virus solutions – providing Cisco IronPort Web Reputation Filters with "always on" detection when tracking the infrastructure behind malware attacks, then adjusting to rapidly block them. URL Outbreak Detection closes the window of vulnerability on zero-day threats.

Comprehensive Management

Web-based administration makes it simple to manage web security policies. Administrators easily update and adjust-policies to meet the varied needs of the global enterprise. Administrators also control the aggressiveness of the system by adjusting the thresholds for "block", "allow" and "scan".

Protection For a Dynamic Web 2.0 World



Cisco IronPort Web Reputation Filters provide visibility far beyond the initial threat.

FEATURES (CONTINUED)

Comprehensive Management (Continued)

Automatic updates are pushed to each Cisco IronPort S-Series appliance on a regular basis. Once the appliance is configured, scores are dynamically updated based on the latest threat data from SenderBase. This eliminates the need for any ongoing management of Cisco IronPort Web Reputation Filters.

Comprehensive reporting and alerts deliver complete real-time visibility into trouble spots in a network's HTTP traffic requests. Reports provide actionable information (such as a list of top clients infected) as well as historical trends.

BENEFITS

Superior Protection Against Web-Based Malware Cisco's multi-layer, defense-in-depth solution provides a significantly higher malware catch-rate over existing, single layer solutions. The breadth and depth of SenderBase data allows Cisco IronPort Web Reputation Filters to stop both known and emerging threats. This results in a malware catch-rate significantly greater than traditional URL filters, which are not effective in identifying these threats because they rely on manual classification techniques andenable infected sites to hide behind generic classifications, such as shopping, finance, entertainment or news.

Lower Costs Cisco IronPort Web Reputation Filters are the only web security solution to categorize both high reputation and low reputation webpages. Most web traffic is to malware-free websites, allowing Cisco IronPort Web Reputation Filters to quickly offload this traffic from the scanning engine – saving system resources and lowering ownership costs.

Complete Administrative Control Cisco IronPort Web Reputation Filters give administrators significant control and flexibility. This unique solution allows different security policies to be implemented, based on different web reputation scoring ranges.

No Administrator Maintenance Required Managing policies can be time-consuming, frustrating for both administrators and users, and difficult to do accurately. Cisco IronPort Web Reputation Filters adjust scores automatically as SenderBase gathers new data. The administrator only needs to configure desired policies, and Cisco does the rest.

SUMMARY

As the first line of defense against malware, Cisco IronPort Web Reputation Filters provide customers with the critical security features necessary – exploit filtering, botsite defense and URL outbreak detection – to safeguard their networks from dynamic web-based attacks, without interrupting daily business communications. With extremely high accuracy and near-zero latency for customers, Cisco IronPort Web Reputation Filters on the Cisco IronPort S-Series web security appliance provide the most comprehensive solution available.

CONTACT US

Cisco sales representatives, channel partners and system engineers are ready to help you evaluate how Cisco IronPort products can make your infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from these industry-leading products, please call 650-989-6530 or visit us on the Web at www.ironport.com/leader

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**.

P/N 435-0218-3 4/09