



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

IronPort Web Reputation Filters

OVERVIEW

IronPort Web Reputation Filters™ provide a strong outer layer of protection for a corporate network. As the first line of defense on *IronPort S-Series*™ appliances, *Web Reputation Filters* immediately scan and allow or deny Web requests — passing only a small fraction of the requests on for further analysis. This yields the highest level of security, while maintaining the end-user experience.

IronPort Web Reputation Filters perform a threat assessment of requested websites, based on their likelihood to host malware. This assessment returns a reputation score that allows the appliance to apply Web security policies, as specified by the administrator. *IronPort Web Reputation Filters* stop the broadest range of threats. The solution

quickly and accurately blocks known and emerging threats, including adware, Trojans, system monitors, keyloggers, malicious/tracking cookies, browser hijackers, browser helper objects and phishing.

IronPort® applies a defense-in-depth approach that significantly improves the performance of *IronPort S-Series* Web security. With *IronPort Web Reputation Filters*, URLs with a high reputation score are passed through the system without further scanning. URLs with a low reputation score are immediately denied, protecting the corporate network. Websites with reputation scores that fall within an administrator-set “suspicious zone” undergo more intensive analysis. This unique technology significantly increases the anti-malware catch rate of the *IronPort S-Series*.

FEATURES

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

IronPort's SenderBase® Network is the world's first and largest email and Web 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 40 Web-related parameters, *SenderBase* supports very accurate conclusions about any given URL. Parameters examined to determine URL reputation include: the volume of traffic measured, the URL's presence on various whitelists and blacklists, presence of downloadable code, age of domain, use of dynamic IPs, number of domains being hosted and rate of domain hosting change.

Sophisticated security modeling analyzes *SenderBase* data to determine a score from -10 (worst) to +10 (best). For example, a



FEATURES (CONTINUED)

webpage that is hosted by a dynamic IP address, has been active for a short period of time and has executable code will quickly receive a low score. Whereas a site that is registered by a Fortune 500 firm, has little volume change and no downloadable content will receive a high score.

The breadth of *SenderBase* data allows virtually every active URL on the Internet to receive a Web reputation score. By comparison, even the best URL filtering technologies have scored only 15 percent of webpages.

DYNAMIC PROTECTION

Proactive scoring decisions are made using *SenderBase* to collect data in real time. This results in constantly updating the scores of virtually every active URL on the Internet. If a site becomes compromised, and suddenly starts distributing spyware, this behavior is measured and the reputation will fall — causing the site to now receive scanning by the *IronPort Anti-Malware System™*.

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 further”.

Automatic updates are pushed to each *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*. Real-time updates occur every five minutes. This eliminates the need for any ongoing management of *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.

A sophisticated alert engine allows administrators to set up individual alert subscriptions, based on severity levels. Anti-malware alerts are calibrated in three categories: informational, warning and critical. This provides administrators with clear visibility into the application and enables them to take appropriate and timely action, if required.

BENEFITS

Substantially reduced risk of infection IronPort’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 *IronPort Web Reputation Filters* to stop both known and emerging threats. This results in a malware catch-rate significantly greater than stand-alone, signature-based Web security solutions.

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



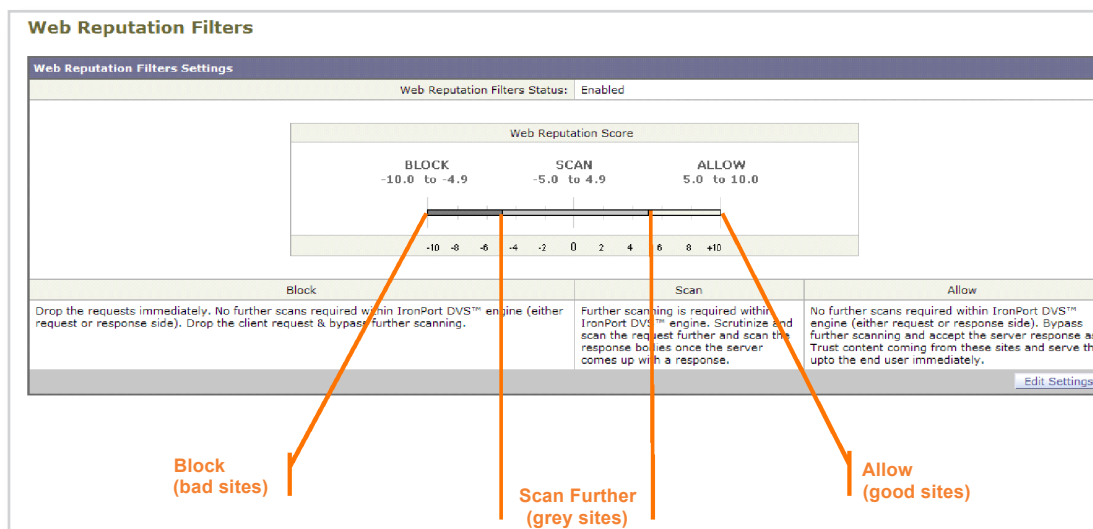
BENEFITS
(CONTINUED)

Complete administrative control *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. Extensive reporting supports additional analysis for policy maintenance as well as meeting management requests for trends and progress.

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

FIGURE 1.

IronPort Web Reputation Filters' graphical user interface makes it simple to manage security policies and settings. Administrators control the aggressiveness of the system by adjusting the thresholds for "block", "allow" and "scan further".



SUMMARY

IronPort® first introduced the concept of reputation filtering for email over three years ago. IronPort is using a similar approach for another dramatic shift in Web security. *IronPort Web Reputation Filters* analyze the traffic patterns and behavior of a Web server, to make a determination about its trustworthiness. The approach is powerfully simple – malware does not typically come from reputable Web servers, it comes from untrusted Web servers that have unusual traffic patterns and network behavior. With extremely high accuracy and near-zero latency for customers, *IronPort Web Reputation Filters* provide a powerful defense against malware.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

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



IronPort Systems, Inc.

950 Elm Avenue, San Bruno, CA 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

Copyright © 2006 IronPort Systems, Inc. All rights reserved. IronPort and SenderBase are registered trademarks of IronPort Systems, Inc. All other trademarks are the property of IronPort Systems, Inc. or their respective owners. Specifications are subject to change without notice. P/N 435-0218-1 9/06

