A FLEXIBLE RESPONSE TO SUSPICIOUS SENDERS KEEPS HOSTILE TRAFFIC OFF YOUR NETWORK.

IronPort Reputation Filters

OVERVIEW

IronPort Reputation Filters™ provide the outer layer of spam protection for your email infrastructure. As the first line of defense on the IronPort email security appliances, *Reputation Filters* dispose of up to 80% of incoming spam at the connection level—saving bandwidth, conserving system resources and yielding the highest levels of security for critical messaging systems.

The IronPort email security appliance receives inbound mail and performs a threat assessment of the sender. This assessment returns a reputation score that allows the appliance to apply mail flow policies as specified by the administrator. More suspicious senders are rate limited or eventually blocked. Recognized senders, such as customers or corporate partners, are allowed access and can bypass filters per the administrator's needs.

A proven preventive solution, *IronPort Reputation Filters* defend the largest ISP and enterprise networks, as well as small and medium-sized businesses, in production environments around the world.

FEATURES

IronPort Reputation Filters intelligently applies mail flow policies based on sender reputation—preventing malicious traffic from even entering your network, while allowing legitimate mail to flow unobstructed.

Over 100,000 organizations participate in the SenderBase Network, enabling the world's largest email traffic monitoring system.

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, 10 times more than competing reputation monitoring systems. By tracking a broad set of over 110 attributes, from an extremely large sample (more than 25% of the world's email), *SenderBase* supports very accurate conclusions about a given sender. Attributes tracked include global email volume, user complaints, controlling organization information, whether an IP address is an open proxy, URLs used in spam or virus attacks, fraction of invalid message recipients, correct DNS configuration, country of origin, a variety of blacklists and more.

FEATURES (CONTINUED)

Sophisticated security modeling leverages the breadth of SenderBase data to generate a granular reputation score ranging from -10 (for the worst senders) to +10 (for the very best). The data used includes both negative (such as whether or not an IP address is on one of the leading blacklists or open proxy lists) and positive attributes (such as whether or not an IP address generates few complaints or is controlled by a Fortune 1000 organization).

DYNAMIC PROTECTION

IronPort email security appliances automatically apply mail flow policies to senders based on their reputation score. As the appliance receives inbound mail, a threat assessment of the sender is performed. This assessment returns a granular reputation score, which is linked to mail flow policies specified by the administrator. So in the simplest terms, the more suspicious the sender appears, the slower their mail goes.

A full range of mail flow control policies can be defined to effectively cover all sender categories. Known bad senders are blocked. Suspicious senders are rate limited, preventing large traffic bursts from entering the network. Recognized senders are granted more generous policies such as bypassing spam filters, larger message sizes and TLS encryption. With *IronPort Reputation Filters*, administrators can make sure that "the punishment fits the crime."

"True" rate limiting based on sender reputation provides a unique and intelligent way of dealing with spammers that occupy the gray zone, where it's not clear if they are friend or foe. While most commercial systems available today offer some type of "throttling," they do so by limiting the number of connections from a given host. Spammers easily thwart this approach by sending multiple messages per connection and sending multiple recipients per message. The IronPort system can limit recipients per hour accepted. Since *Reputation Filters* respond to these gray zone mailers by this "true" rate limiting, but not actually blocking, the false positive rate is extremely low—less than 1 in 1 million.

COMPREHENSIVE MANAGEMENT

An integrated Web-based user interface makes it simple to manage sender groups and associated mail flow policies. Administrators easily create sender groups and configure policy parameters to meet their corporate-specific email security requirements.

Automatic updates ensure that once the IronPort email security appliance is configured; scores are dynamically updated based on the latest data from *SenderBase*. This eliminates the need for any ongoing management of *Reputation Filters*.

BENEFITS

Improved catch-rate *IronPort Reputation Filters* block up to 80% of incoming spam at the edge of your network, improving the overall efficacy of your anti-spam solution.

No Administrator Maintenance Required Managing local black- and whitelists can be time-consuming, frustrating for both administrators and users, and difficult to do accurately. *IronPort Reputation Filters* adjust scores automatically as *SenderBase* pulls in new data. The mail administrator only needs to configure their desired policies, and *Reputation Filters* does the rest.

BENEFITS (CONTINUED)

Reduced false-positives *IronPort Reputation Filters* intelligently combine many different metrics before determining a sender's reputation. Anomalies in a few parameters (such as appearing on a single blacklist) will not dominate the score, but confirmation of suspicious traffic patterns across many data types and sources will certainly result in a poor reputation. This unique ability to triangulate information across *SenderBase* makes *Reputation Filters* the undisputed leader in reputation accuracy.

Lower hardware costs and increased message throughput Eliminating spam and unwanted mail, before resource-intensive content filtering, will improve overall system performance and reduce the amount of supporting hardware required for the rest of the email infrastructure. Typical customer results show that downstream load is reduced by three to five times through use of *IronPort Reputation Filters*.

Reduced risk from denial of service or dictionary harvest attacks *IronPort Reputation Filters* score senders in real time and are adept at preventing damage from many types of distributed attacks. Attacks arising from zombie networks, which can bring content-based anti-spam systems to a grinding halt, can be gracefully managed with *Reputation Filters*.

SUMMARY

PREVENTIVE SECURITY—THE NEXT GENERATION OF SPAM CONTROL

Email threats are increasing rapidly in sophistication and continue to become more and more frequent. Traditional anti-spam solutions based on content filtering are only part of the solution. A truly effective anti-spam system needs a preventive, high performance outer layer of protection such as *IronPort Reputation Filters*.

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™

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 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, protecting, and growing mission-critical email systems.

REPUTATION FILTERS
10/05
DOC RELEASE