



An Advanced Reputation Management Approach to Stopping Emerging Email Threats

CONTENTS

| | |
|---|---|
| The Evolution of Reputation Management | 2 |
| Emerging Security Threats | 2 |
| Advanced Reputation Management (ARM) | 3 |
| How ARM Works | 4 |
| Extended Security Benefits | 4 |
| Extended Administrative Benefits | 5 |
| Integrating ARM into a Complete Email Security Solution | 5 |
| Conclusion | 6 |

Abstract:

More sophisticated and complex threats to email systems continue to emerge and require an advanced defensive approach. Traditional single-point defenses such as Sender IP Reputation are no longer a sufficient defense against these new threats. Such single-point defenses represent only an individual layer in a multi-layered Advanced Reputation Management defense that can identify and manage the reputations of not only an email's sender IP address, but also its structure, text, embedded URLs, images, attachments, phone numbers and email addresses.

The Evolution of Reputation Management

The original email reputation management system began with Real-time Blackhole List (RBL). The very first RBL was developed in 1997 by Paul Vixie for the Mail Abuse Prevention System (MAPS). Referring to a network link that drops rather than forwards incoming traffic, Vixie intended the "blackhole" in this case to drop email traffic from sites that directly sent or enabled spam. The original RBL consisted of a list of suspect sites transmitted to subscribing systems administrators over Border Gateway Protocol (BGP). Subscribers could then apply the list to block TCP/IP traffic from those sites.

While RBL reputations presented a significant step forward in managing spam, it also presented inherent challenges. MAPS meticulously worked to verify sites for accuracy before publishing them to the list. While this helped reduce false positives, it also significantly delayed subscribers' ability to respond to attacks quickly. Over time, MAPS developed RBL clients that integrated with email software to enable administrators to customize their own RBL to reject incoming mail on a per-server basis.

The MAPS RBL laid the groundwork for the development of the DNS-based Blackhole List (DNSBL) format. The Domain Name System (DNS) Internet service translates domain names/hostnames to IP addresses (forward DNS) and IP addresses to their associated domain names/hostnames (reverse DNS) with the help of a DNS server. Rather than being simply a discreet list, a DNSBL added multiple standards for dynamically listing and delisting IP addresses. DNSBL service providers could then distribute updated lists via the Internet Domain Name Service (IDNS) using a standardized format. Early developers of DNSBLs added such criteria as whether a sending mail server used potentially exploitable open relays or proxies, or whether a mail server sent spam to a "honey pot" system designed to attract and gather spam for identification and analysis.

Today, there are dozens of DNSBL services available and most email servers can query these services to verify the reputations of IP addresses. However, these services apply different standards for adding, removing, or retaining IP addresses on their lists. Subsequently, some service lists may not contain potentially dangerous IP addresses, or erroneously include valid ones.

Emerging Security Threats

As IP reputation systems have grown in popularity, spammers and hackers have increasingly focused significant resources towards undermining IP reputation systems. Their attacks have focused on compromising legitimate mail servers either at companies with good reputations, or cracking Web mail accounts at ISPs and ASP's, such as Yahoo® or Gmail®. This allows spammers to avoid or delay listing on traditional IP reputation systems by sending bad mail mixed with good email from the compromised servers of legitimate businesses.

Although, spammers do manipulate their IP addresses, they do not manipulate all aspects of a spam message uniformly. Like other profit-making entities, spammers cut overhead costs by reducing complexity. Spammers tend to reuse IP addresses, as well as content, layout, hyperlinks and images. This presents an opportunity: an additional defensive layer of reputation identification and management beyond IP addresses alone.

Email-borne threats continue to become increasingly more sophisticated because spammers are typically technically savvy and early adopters of innovative technology. For example, spammers created content-based tricks such as gibberish words and phrases, white-on-white text, tiny fonts, word salad, optical illusions, image spam, attachment spam and other advanced techniques in an attempt to deceive spam filters. Or, in the first half of the decade, when Sender Policy Framework (SPF) was first being defined and rolled out in attempt to identify legitimate email, spammers adopted the technology faster than legitimate companies.

Phishing scams pose another significant threat. Distinct from spam, phishing emails imitate legitimate emails, often copying actual corporate communication. Criminals send out billions of phishing emails every month which can lead to identity theft, security breaches, and financial loss and liability. Leveraging social engineering techniques to evade corporate security systems, criminals gain network access and steal confidential corporate data and financial assets. With the unwitting cooperation of an employee, network defenses such as firewalls, Intrusion Detection and Prevention systems and secure identification cards can become less effective. Because phishing emails are designed to look like legitimate business correspondence, they consistently elude standard spam filters, and email policies alone are an insufficient defense. Phishing defense requires specific analysis, identification and handling.

Backscatter or NDR (non-deliverable-return) spam are messages that look like returned emails that could not be delivered to their intended sender. Spammers spoof such messages, attempting to bypass the email security system.

Directory Harvest Attacks (DHAs) are exhaustive "brute force" attacks. DHAs bombard mail servers with emails sent to variations of possible email addresses to check which ones bounce and which are legitimate. The extensive volume of a DHA strains email infrastructures. In addition, DHAs acquire information on email addresses for the company that criminals use in follow-up, targeted spam, virus and phishing attacks.

Denial of Service (DoS) attacks are malicious attempts to bring down email infrastructures. By sending an enormous volume of email traffic into an organization at a coordinated time, attackers attempt to overwhelm the network and email infrastructure, bringing email to a complete stop.

How to Combat these Threats: Advanced Reputation Management

Extending reputation management beyond mere Sender IP Reputation, Advanced Reputation Management (ARM), developed by SonicWALL®, not only includes current reputation information on Sender IP addresses, but also all significant components of the message, or "contact points", including message structure, content, embedded URLs, images, attachments, phone numbers, email addresses and other factors. In addition, ARM can apply Bounce Address Tag Validation (BATV) for NDR messages, as well as DHA protection, DoS protection and other quality of service defense techniques.

Further, ARM applies "cross-vector" threat-related information between security systems (i.e. firewall, content filtering, intrusion prevention, email security systems), to enable a more intelligently collaborative and comprehensive response. Most email security solutions group threats by vectors corresponding to particular ports by which suspect traffic might breach the network perimeter (e.g., the email vector would relate to traffic over Port 25, the Web vector to traffic over Port 80, etc.). With ARM, each component of a vector can receive independent analysis and filtering. For example, the reputation of a sending IP Address could be derived from the fact that the IP address hosted a Website that distributed malware, and that same IP address is now trying to send email.

How ARM Works

ARM updates its reputation data dynamically with threat protection information from the SonicWALL Global Responsive Intelligent Defense (GRID) Network™. The GRID Network collaboratively gathers, analyzes and vets cross-vector threat information from millions of business-oriented sources around the world in real time. The GRID Network then correlates this data to develop reputation scores known as GRIDprints, which dynamically update ARM securely, anonymously and in real time to improve its overall effectiveness.

Due to its distributed nature and its use of multiple different data sources, the GRID Network can vet the evaluation from one contributor against multiple other contributors, allowing the GRID Networks' collaborative filtering process to be highly accurate and fully self-correcting. Unlike competitive solutions that leave businesses vulnerable by taking an hour or longer to update with the latest attack information, ARM receives GRIDprint updates of reputation-based threat protection information from the GRID Network in near real time.

ARM does not rely on only one subset of reputation input, but rather on a collaboration of multiple cross-verified GRID Network sources. The GRID Network receives inputs from SonicWALL users, honeypots and industry lists. In addition, the GRID Network also monitors and extrapolates reputation information from top-tier independent DNSBLs and other vetted sources. SonicWALL intensively vets these contributing sources for credibility, reliability and accuracy on an ongoing basis. By consolidating collaborative input from verified sources, ARM eliminates the need for businesses to depend on multiple less-effective, slow-responding and error-prone DNSBL services.

Trend analysis on input from these cross-verified sources can also contribute to ARM receiving more accelerated reputation adjustments. Multiple-sourced acceleration is particularly effective against explosively virulent botnet attacks. The longer an email system is left waiting to receive a negative reputation update, the more likely it is to be exposed.

ARM is also unique in that it derives reputation information from business-focused sources, unlike other solutions that rely upon rented or purchased lists from consumer-focused ISPs. ARM provides SonicWALL Email Security (available as a hardware appliance, virtual appliance or software), SonicWALL Comprehensive Anti-Spam Service, and SonicWALL Anti-Spam Desktop solutions with dynamically up-to-date analysis of email component reputations. Building upon this successful foundation, SonicWALL has actively developed and expanded the breadth of the information shared over the GRID Network, and has integrated the entire range of SonicWALL solutions—including Unified Threat Management (UTM), anti-virus, anti-spyware, intrusion prevention, content filtering and application firewall defenses—that contribute to and take advantage of this global threat monitoring.

Extended Security Benefits

By expanding the concept of reputation management beyond Sender IP address, SonicWALL has engineered ARM to flexibly add new reputation criteria as new threats, and methods of defending against them, have emerged.

For example, email follows statistically consistent distribution patterns. As part of ARM reputation criteria, the GRID Network considers an email's geographic source location and time zone to identify unusual or suspicious distribution trends. Moreover, if the GRID Network has identified a global spam attack as originating from or targeting a particular geographic locale, email falling into either category would have its spam likelihood rating escalated.

Frequency of reporting can also accelerate a change in an email's reputation. For example, if the GRID Network receives a bad rating on a particular embedded URL at 10:00 a.m. PST, and then rapidly receives

additional bad ratings from multiple different systems by 10:01, the GRID Network identifies an escalating trend and accelerates a bad reputation on ARM for emails containing that URL.

Moreover, unlike other reputation management solutions that do not examine the entire data stream or simply reject files over a certain size out-of-hand, ARM does not limit the size of files it is able to scan. This is particularly important in defending against streaming media, graphics and other excessively large files common in today's Web 2.0 environments, which are often prone to malware infestation.

Extended Administrative Benefits

ARM also provides granular controls without complexity. For example, certain IP Reputation solutions might expect administrators to discern a difference somehow between a 14.1 and 14.2 level of aggressiveness on a scale of 20. In contrast, administrators can use SonicWALL's easy interface to adjust defense aggressiveness on an intuitive 1-5 scale, with 1 representing a low, 3 an average, and 5 a high aggressiveness across multiple different filtering mechanisms. The consequences of changing a setting are discernable yet granular enough to provide control. ARM's aggressiveness level is fully customizable, so the administrator retains complete control.

Unlike many alternative reputation systems, ARM automatically logs all email transactions, including both accepts and rejects. By automatically logging transactions, ARM provides administrators with greater confidence and flexibility by enabling them to confirm potential false positives. Other IP Reputation products reject without any record to verify what was rejected.

Furthermore, Administrators can initiate centralized management and reporting across multiple systems to reduce the chance of email-borne threats entering the network.

Integrating ARM into a Complete Email Security Solution

SonicWALL ARM is just one component of the comprehensive SonicWALL Email Security solution. ARM can eliminate up to 98% of spam at the connection level, before it enters the network. SonicWALL's Advanced Content Management (ACM) then analyzes and filters any remaining email, resulting in up to 99.93% overall effectiveness. ACM uses more than a dozen comprehensive layered techniques including comprehensive Adversarial Bayesian™ analysis, which includes advanced text and image parsing engines; lexicographical distancing; image analysis (white-on-white, tiny fonts, etc.); gibberish detection; and corporate or user allow/block lists. ACM scans content in every significant email component (body, subject, attachments, etc.) to assure compliance with corporate policy, and can block or re-route non-compliant emails to appropriate LDAP-based groups or individuals. These technologies deliver the most effective defense available against the latest emerging email threats.

Beyond ARM and ACM, SonicWALL Email Security solutions also integrate an array of additional multi-layered defenses for inbound and outbound traffic, including SonicWALL GRID Anti-virus, Anti-Phishing, Policy Management, Compliance Defense Management and Outbound Threat Management:

SonicWALL GRID Anti-virus uses the dynamically updated GRID Network and its extensive list of malware signatures to block the most common threats automatically, as well as prevents Time Zero attacks.

SonicWALL Anti-Phishing leverages SonicWALL's expertise and success with Adversarial Bayesian for anti-spam, anti-phishing incorporates a unique and patented Bayesian Fraud™ analysis into its content analysis.

SonicWALL Policy Management intelligently identifies emails that violate policies, providing monitoring and reporting and applying multiple enforcement actions.

SonicWALL Compliance Defense Management delivers a powerful framework for driving both external / regulatory (e.g., PCI, SOX, HIPAA) and internal / corporate (e.g., intellectual property policy) compliance initiatives, and includes routing for email data leakage prevention, encryption and archiving.

SonicWALL Outbound Threat Management provides robust anti-zombie defense by identifying and blocking zombie-generated email and alerting the administrator to potentially infected machines.

Conclusions

Advanced Reputation Management delivers the most effective defense against the latest emerging email threats. ARM greatly expands the concept and functionality of reputation management beyond identification and classification listing of Sender IP addresses alone. Defending against the onset of increasingly sophisticated threats, Advanced Reputation Management forms the cornerstone of an integrated multi-layered approach to protect organizations from inbound spam, phishing and email-borne malware, as well as from outbound data leaks and botnet transmissions.



SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124 T +1 408.745.9600 F +1 408.745.9300 www.sonicwall.com

©2011 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.