



The SonicWALL GRID Network: Collaborative Cross-vector Protection for Email Security

Leveraging a collaborative network of millions of business users to gather, analyze, and respond to cross-vector threats in real time.

CONTENTS

The Origins of the SonicWALL Grid Network	2
Cross-vector Protection	2
Collaborative Filtering	3
- Hashing thumbprints	
- Building reputations	
- Reputation-based filtering	
Self-correcting Data Base	5
- Business-focused criteria	
Anti-virus Protection	5
The Future	5
Conclusion	6

Abstract

The SonicWALL GRID Network collaboratively gathers, analyzes and vets cross-vector threat information from millions of business oriented sources around the world. Reputation-based threat protection information is then distributed securely, anonymously and in real time to improve the overall effectiveness of SonicWALL security solutions. Due to the distributed nature of this network and the use of multiple different data sources, the evaluation from one contributor can be vetted against multiple other contributors, allowing the GRID's collaborative filtering process to be highly accurate and fully self-correcting.

The SonicWALL GRID Network is unique to the enterprise security market in that it applies information from only business-focused sources, unlike other networks, which rely upon rented or purchased lists from Internet Service Providers (ISPs). The SonicWALL GRID Network's principal focus is to provide SonicWALL Email Security and SonicWALL Anti-Spam Desktop solutions with dynamically up-to-date e-mail component reputation analysis. Building upon this successful foundation, SonicWALL is actively developing and expanding the breadth of the information shared over the GRID Network, as well as integrating the range of SonicWALL solutions that contribute to and take advantage of this global threat monitoring information, in order to provide businesses with more comprehensive and responsive security solutions.

The Origins of the SonicWALL GRID Network

The SonicWALL Global Response Intelligent Defense (GRID) Network initially began in 2002 as an extension of the pioneering client-based anti-spam technology of MailFrontier (acquired by SonicWALL), which allowed users to designate e-mail in their inbox as "junk." If junked, the e-mail's sender was added to a "block" list, the e-mail was deleted from the inbox, and the e-mail was placed in a junk folder. If a user discovered that an e-mail was erroneously placed in the junk folder, then it could be marked "unjunk," and the process would be reversed. Subsequently, each identified junk or unjunk e-mail was disassembled into its elemental components: the sender, the content, the e-mails links, etc. MailFrontier then encoded these disassembled components in an anonymous and non-reversible manner and sent them back in a secure format to a central data center to be used for collaborative filtering, and created a network for this purpose.

When MailFrontier was acquired by SonicWALL, the data center was enlarged to enhance response times, processes were streamlined, and additional sources were formalized. Subsequently, the network was expanded to collect input from millions of contributors from around the world in real time. While this required significant speed and scalability to support, it greatly enhanced the recognition of—and response to—evolving threats as they developed in the world. This underlying technology evolved into the SonicWALL GRID Network.

Cross-vector Protection

Historically, security solutions have often grouped threats by vectors corresponding to particular ports by which suspect traffic might breach the network perimeter (e.g., the e-mail vector would relate to traffic over Port 25, the Web vector to traffic over Port 80, etc.).

The goal of the GRID Network is to collect, analyze and distribute "cross-vector" threat-related information between security systems, to enable a more intelligently collaborative and comprehensive response. For instance, an e-mail message might contain a URL that has been defined as suspect. Using a cross-vector approach, the GRID Network can block browser access to the URL over Port 80 on the Web vector, as well as blocking access to the message over Port 25 on the e-mail vector.

Each component of a vector can receive independent analysis and filtering. For example, a single e-mail message could be broken down into the components of sending IP address, text content, e-mail structure, URL links, file attachments, embedded images, etc. Individually, any of these components might be a recognized as a threat, and considered to have a "good" or "bad" reputation.

Collaborative Filtering

The GRID Network creates reputation scores for vector components through collaborative filtering. Collaborative filtering is the process by which a community made up of multiple business-focused sources shares information on identified threats, in order to collaboratively define suspect vector components that should be blocked or filtered.

The SonicWALL GRID Network community of information sources includes:

- SonicWALL Anti-Spam Desktop users
- SonicWALL honey pots (e-mail addresses and domains placed throughout the internet worldwide to collect spam, phishing and virus emails).
- Real-time blacklists (RBL) providers
- SonicWALL Web rating analysts (SonicLabs)
- Individually contributing industry professionals
- SonicWALL Email Security spam submissions
- SonicWALL Email Security probe accounts
- Other SonicWALL products or services

These sources collect, identify, define and transmit information on multiple vector components to the GRID Network for compilation and analysis, each applying unique processes and criteria.

Hashing thumbprints

In the case of Email Security, the reputation of components is determined through the compilation and weighting of junk and unjunk “votes.” When an e-mail is disassembled, each component is encrypted using a non-reversible hash process to create a “thumbprint” of that component. These thumbprints—not the original component data itself—are then sent to the data center with a corresponding reputation of good or bad, and tabulated in real time. Every transmission is encoded over HTTPS, using the DES/AES encryption of the browser.

Each user gets one vote per thumbprint per day. For example, if the same URL is determined to be bad by an Anti-Spam Desktop user in New York and another Anti-Spam Desktop user in Beijing, each user anonymously enters a single individual vote. This prohibits spammers from “gaming” the system and keeps inputs from any system from skewing the reputation results.

Building reputations

The Anti-Spam Desktop votes are tallied in a data sequencing process at the SonicWALL data center, where they are compiled and vetted against votes from all other sources. At any given time, there are over 20 million thumbprints in the GRID Network database. Currently there are over 2.0 million Anti-Spam Desktop contributors on the GRID Network, as well as over 8,500 active Email Security appliances whose administrators may directly contribute input.

The GRID Network also gathers and vets millions of e-mails per day from SonicWALL honey pots designed as bait e-mail addresses or domains for spam and phishing attacks. The GRID Network disassembles these collected honey pot e-mails into constituent thumbprints, and adds them as junk votes.

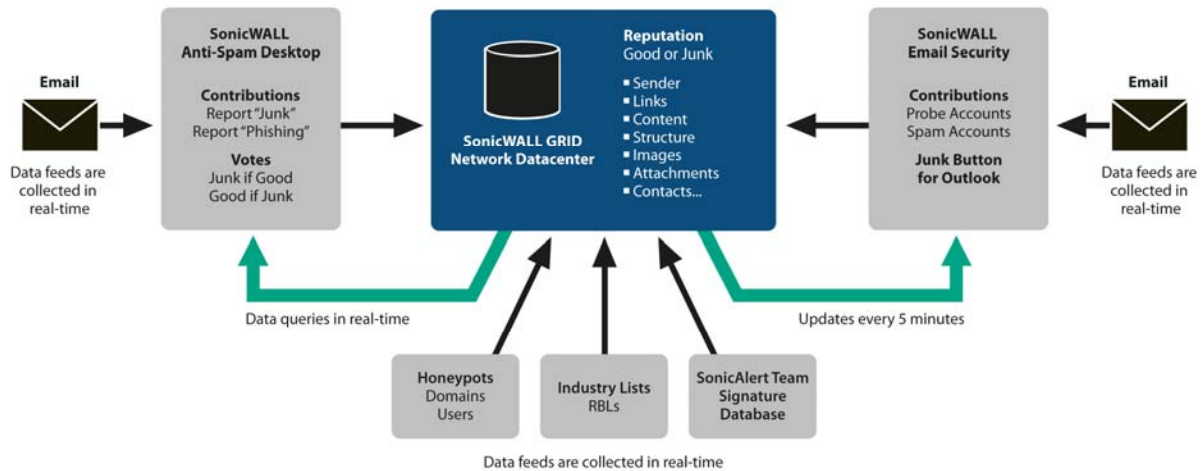
The SonicWALL GRID Network also uses information provided by real-time blacklist providers and individual industry professionals to contribute to the reputation vetting process. A team of over 50 specialized rating

analysts also review the sequencing results, vetting the data on multiple levels, and adding an additional layer of checks-and-balances.¹

Reputation-based filtering

When an e-mail is received by a SonicWALL Anti-Spam/Email Security system, one of the checks is to breakdown the e-mail into its component parts (thumbprints) and determine the reputation of each component from the SonicWALL GRID Network database. This database is part of every SonicWALL Anti-Spam/Email Security installation. If one or more components are flagged as junk, the e-mail is identified as having a reputation of junk.

To keep the SonicWALL Anti-Spam/Email Security current, updates from the SonicWALL GRID Network are received and automatically applied every 5 minutes. These updates allow SonicWALL Anti-Spam/Email Security to maximize the collaborative power of the GRID Network with absolutely no customer administration.



¹ Anti-Spam Desktop and Email Security each apply separate Bayesian engines used to analyze phraseology in order to identify both spam and phishing content. These contribute an additional layer of filtering protection, operating independently of the GRID Network reputation analysis.

Self-correcting Database

Collaborative filtering inherently provides a self-correcting human element. For example, the SonicWALL GRID Network might recognize that a particular IP address has transmitted a spam e-mail. However, the sender of the e-mail from that IP address is known to the contributor as legitimate, and having a good reputation. By vetting the evaluation from that one contributor against evaluations from multiple other contributors regarding this particular IP address and sender, a broader statistical sample is established, and a more accurate reputation score can be determined. This comprehensive vetting process is applied not only to IP addresses, but to all thumbprint types.

Business-focused criteria

Since the inception of the GRID Network, other vendors have attempted to create data centers to analyze vector information. To short-cut the process of building the network, these other vendors rely upon rented or purchased lists from consumer-based Internet Service Providers (ISPs). Such lists have limited value as consumer based opinions on spam are not equivalent to business-based opinions on spam. For example, an e-mail that would be considered acceptable content to a consumer using Yahoo!®, Gmail®, or MSN®, might certainly be marked as junk by millions of business users contributing to the GRID Network. The SonicWALL GRID Network was developed from the beginning to incorporate business oriented sources which is required to render proper reputation decisions for business users.

Anti-virus Protection

The SonicWALL GRID Network contains an active mechanism for tracking and responding to virus-related information. SonicWALL® GRID Anti-Virus™ leverages SonicWALL's anti-virus and anti-spyware technology to deliver anti-virus and anti-spyware protection in SonicWALL Email Security products. Using the dynamically-updated SonicWALL GRID Network and its extensive list of malware signatures, SonicWALL GRID Anti-Virus automatically blocks the most common threats. SonicWALL GRID Anti-Virus prevents users from downloading e-mail containing spyware and stops any existing spyware from being disseminated via e-mail systems.

SonicWALL GRID Anti-Virus can be further augmented by optional anti-virus subscriptions from our anti-virus partners McAfee® and Kaspersky Lab® for layered defense. SonicWALL receives continual signature updates from McAfee and Kaspersky Lab, and automatically distributes these, along with internally-defined SonicWALL GRID Anti-Virus signatures, with Email Security updates every five minutes. This layered approach to virus detection further enhances the protection provided by the SonicWALL Email Security system..

The Future

The collaborative filtering network pertaining to SonicWALL Anti-Spam Desktop and Email Security, however, is only one part of the SonicWALL GRID Network. The GRID Network encompasses all the information that flows through the SonicWALL data center. For instance, the SonicWALL Content Filtering Service, which tracks URLs of suspect Web sites, provides that information as a list to SonicWALL Content Security Management appliances, and also as a service to SonicWALL Unified Threat Management (UTM) network security solutions. One possible future opportunity would be to extend this information to Email Security as well.

Another future-use scenario might envision a SonicWALL UTM network security appliance that is conducting deep packet inspection (DPI) on a packet received from a particular IP address, and discovers that packet contained a virus. Potentially, that information could contribute to the reputation of that IP address across all other appliances on the GRID Network, such as a SonicWALL Aventail E-Class SSL VPN appliance that

might restrict remote access from or to that IP address. Likewise, the GRID Network might be useful in identifying suspect distribution patterns that could be used in tracking and blocking sophisticated, automated multi-prong attacks.

Conclusion

The SonicWALL GRID Network is a business-focused, collaboratively-filtered global network that provides users of SonicWALL products and services with the most up-to-date and comprehensive reputation profiles of vector component information in real time. Proven effective in the field for over five years, the GRID Network is now poised to form the foundation for cross-vector responsiveness across the entire network security spectrum.