A Guide to Evaluating E-Mail Security Solutions

New e-mail protections are now available to ensure the safety, privacy and security of corporate networks, data and personnel. The increased sophistication, versatility and effectiveness of e-mail security solutions have been paired with improved ease-of-use, providing a transparent, simply managed barrier against spam, phishing and other *inbound e-mail-based attacks as well as* ***outbound compliance.***

CONTENTS

SONICWALL

Abstract

E-mail security requires full-blown coverage and the very latest advances in technology to stay ahead of serious e-mail attacks. E-mail threats evolve daily, and today's e-mail security solutions have the power and flexibility to keep up with, and in many cases stay ahead of, the attacker community. From inbound attacks such as spam and phishing to outbound threats such as the theft of corporate data or the inadvertent transfer of personal information or malicious content outside the organization, protection can be provided with minimum impact on personnel, computer systems, and the pace of everyday business.

Comprehensive e-mail security can also fit comfortably into corporate budgets. Solutions have matured to the point where full protection is accessible to companies ranging from small businesses with a limited array of key systems to international corporations maintaining dozens of massive, vulnerable installations. By joining a dynamic, end-to-end e-mail security methodology with a consolidated, high-performance architecture and simplified administrative capabilities, companies of any size can protect their valuable resources easily and with confidence.

Challenges of E-mail Security Implementation

Although many vendors are now providing a range of high-performance e-mail security solutions at various enterprise levels, the increasing complexity of these solutions has created its own set of new problems. The threat itself is so broad in scope and is evolving so quickly that current solutions are having trouble keeping up with the challenge while remaining cost-effective and easy to manage.

Fortunately, technology is available than can deliver the predictive capabilities and quick response techniques necessary to guard effectively against e-mail-based attacks, with full support for corporate security policies and regulatory compliance. Not all e-mail security products provide this range of functionality, however. When selecting an e-mail security solution, it is essential to assess carefully the depth, versatility, and scalability of the technology, along with its ability to handle new threat variants. In addition, e-mail security solutions must optimize corporate resources to provide an affordable, easily maintained system that does its job efficiently and transparently.

The specific issues raised by today's e-mail security threats range from highly technical demands to purely practical administrative considerations.

Technical Demands

1. Global vulnerability

The line between inbound and outbound threats has grown increasingly thin. Once malicious code is embedded in a corporate system, it can launch destructive actions within the corporate network or travel with dangerous intention to customers' and partners' systems. Furthermore, e-mail is a fundamentally complex process, typically involving the sending servers, the e-mail content, various types of attachments, embedded URLs or other contact points, the Web sites to which the embedded URLs link, the recipients, and the effect on both internal and external e-mail communities. E-mail security solutions must address explicitly the requirements of today's highly integrated and universal e-mail environment by monitoring at all levels, and in all directions.

2. Expanding threat variations

Not only are there numerous types of potential e-mail attacks - spam, viruses, phishing, Directory Harvest Attacks (DHA), etc. - but within each category attackers use many different strategies and develop new techniques constantly. Security technology must be able to recognize, predict, and respond to all types of attacks, and even be robust enough to learn new tricks as they appear. Products must also be able to clearly differentiate one type of attack from another and apply appropriate measures to each.

3. Malicious content

As attackers become more sophisticated, e-mail security solutions must apply effective filters that can locate problematic content in increasingly greater detail. Altered spam words are a notorious case in point. The word “Viagra,” for example, has 600,426,974,379,824,381,952 variations, depending on the use of spaces, extra characters and so on.(1) E-mail security must be alert to all spammer tricks.

Virus threats, phishing, and other types of e-mail-based attacks also require specially targeted content analysis. For example, the components of a phishing e-mail differ from spam and must be approached with targeted methodology in order to achieve accurate results. Furthermore, analytical methods should extend to the contact information contained not only in the header, but also in the body of e-mails, in order to uncover inconsistencies that indicate trouble.

4. Blended threats

E-mail attacks are commonly a mixture of various methods, applied either simultaneously or in sequence. For example, spam and phishing e-mails that target individuals can contain viruses posing a danger to the entire corporate network. E-mail security solutions must take an integrated approach to detecting and blocking various types of e-mail-based threats.

5. Authentication complexities

Server authentication plays a major role in blocking e-mail attacks, but can be a complex procedure in today’s diversified Internet environment. For example, a good incoming e-mail could fail authentication after being forwarded by a third party or originating from a source that didn’t set its DNS records to support authentication. In addition, a sending server’s “reputation” (determined by outside Web services that monitor junk mail traffic) can sometimes be unclear. A combined approach utilizing both authentication and reputation techniques helps ensure a more accurate assessment of a sending server’s actual status, and also reduces “false positives” that can disrupt business by wrongly filtering out innocent e-mail traffic.

6. Response time demands

An ideal e-mail security solution would respond instantaneously to any type of threat, leaving no time for damage to occur. In the real world, the only way to achieve near-perfect response time is to provide predictive methodologies that can deduce the likelihood of an attack or a breach in corporate policy early in the threat lifecycle. Predictive techniques can pinpoint dangers ranging from inbound e-mails with suspicious attachments to anomalies in a company’s outbound e-mail traffic.

Administrative Considerations

1. Rising Costs

Security costs have skyrocketed over the past decade, and show no signs of peaking. E-mail security solutions that can enhance system protection while limiting the cost of implementation and maintenance are greatly in demand. The easiest way to start putting a cap on costs is to select an all-in-one solution that utilizes a single e-mail security infrastructure to manage the entire e-mail security system. System consolidation is also an issue - i.e., a minimum number of reliable, high-performance servers that provide total coverage as well as high availability and sufficient scalability and redundancy.

2. Complicated e-mail security systems

E-mail security systems are necessarily complex, which can sometimes translate into complicated software applications requiring time and extensive knowledge to operate and monitor. The most efficient solutions offer a simplified administrative interface that is effective, easy-to-use, and requires very little hands-on attention. Specific features that can aid in streamlining system maintenance include:

- Quick configuration options
- Easy customization
- The ability to choose between uniform and split architecture arrangements
- Automatic updates
- Integration with standard directory systems (e.g., LDAP, Microsoft Active Directory, etc.)
- Centralized management
- Web-based interface
- Robust, full-featured reporting

3. Compliance requirements

Government security regulations are growing more widespread (e.g., SOX, GLBA, HIPAA, etc.), and companies are rapidly expanding internal security measures that protect business data and networks, as well as the privacy of corporate personnel. As a result, the burden on the IT team to deliver appropriate functionality and reporting has become much more intense. E-mail security solutions can make the job easier by providing features specifically keyed to legislative requirements, and flexible enough to accommodate evolving corporate policies. Essential capabilities include encryption, digital signature, content filtering, and anti-attack processes targeted specifically to spam, phishing, viruses, and other advanced e-mail-based threats.

Total Solutions for a Secure E-mail Environment

E-mail security systems must provide a broad canvas, yet probe deeply into the specifics of particular types of attacks. Comprehensive solutions also combine functional complexity with simple interfaces, flexible configuration, and easily accessed reports.

Global Coverage

Complete lifecycle monitoring

Without an true end-to-end e-mail monitoring system, gaps in a corporate e-mail security solution could be fatal. Effective e-mail security covers all the bases by using advanced statistical methodologies throughout the corporate e-mail environment. Properly armed against attack, this type of full-featured system thoroughly evaluates message content; closely examines e-mail attachments; accurately tracks the reputation of e-mail servers; and continually analyzes the impact of threats and attacks on the entire corporate community. Information breaches are covered as well; for example, sophisticated detection technology can monitor e-mail traffic for inconsistencies that typically indicate an attempt to transfer corporate data without authorization.

Technologies such as SonicWALL Email Security also apply a collaborative review, in this case through SonicWALL Self Monitoring Active Response Team (SMART) Network (tm), a real-time network of over one million global users whose responses help identify and react to new e-mail dangers.

Protection against all types of threats

Spam and phishing attacks are among the most widely-known e-mail threats. Many e-mail security systems have devised effective techniques to combat these problems. The question is whether or not these solutions probe deeply and broadly enough to catch all of today's very clever intruders.

Spam

Spam "scoring," the most common way to block junk mail, requires continual adjusting because new variants appear regularly. It can also interfere with good e-mail when a particular e-mail instance fails to fit into existing programmed parameters. A more accurate, less time-consuming approach utilizes a combination of analytical techniques that enable the e-mail security system to securely and confidently quarantine suspect e-mail while accurately determining which e-mail can be sent safely on to recipients. SonicWALL Email Security is a case in point, achieving 98 percent effectiveness at blocking spam, In addition to accessing the industry's largest proprietary database for server authentication, this advanced solution employs a highly granular form of e-mail content examination based on 200,000 different analytical methods.

Phishing

Phishing e-mails imitate legitimate businesses in an attempt to defraud recipients of personal or corporate information ranging from social security numbers to corporate payroll data. Research indicates that phishing caused more than $44 billion in damages worldwide in 2004.(2) Phishing requires its own particular form of protection, geared to the specific nature of the threat. SonicWALL, for example, applies specially targeted analytical methods to detect e-mails with phishing-specific content. It can also determine the reputation of contact points included in suspect e-mails, uncover inconsistencies in e-mail links, and identify attempts to leverage browser or operating system vulnerabilities.

Viruses

In most instances, users rely on "signatures" (specially developed code) to combat viruses as soon as possible after "time zero" (outbreak time). Certain products have taken the next step by providing predictive capabilities that go beyond the foundation task of searching for newly identified and long-standing strains, catching malicious code before it can cause even the slightest damage. SonicWALL Time Zero Virus Technology, for example, provides predictive anomaly detection methods, which are enhanced by dual-engine signature technology (through SonicWALL partners McAfee and Kaspersky) that improves response time and helps ensure full protection. In SonicWALL's case, these advanced anti-virus techniques can be applied easily to both inbound and outbound virus threats.

In addition, a large network of real-world e-mail users can improve anti-virus response capabilities by providing quick, statistically accurate feedback about new virus threats. On November 13, 2004, time zero for virus “Sober.J,” SonicWALL’s predictive techniques immediately stopped 4 out of 5 of the virus variants. SonicWALL SMART Network input then put a stop to the fifth variant. All of this occurred before the arrival of the signature.

Zombie, DHA, DoS Attacks

The broadest e-mail security solution also guards against newer - and potentially more dangerous - types of threats, including zombie machines, Directory Harvest Attacks (DHA) and Denial of Service (DoS) attacks. Zombie machines are computers on the corporate network that have been hijacked by malicious code in order to send out masses of e-mails that appear to have originated from the victimized system. DHAs are “brute force” attacks which bombard mail servers with randomized e-mail messages as a way to locate legitimate e-mail nodes for use at a later time. DoS is an attempt to crash an entire system infrastructure by overwhelming the network with a huge volume of incoming traffic at one point in time.

An effective e-mail security solution must include technical capabilities targeted to the specific nature of these varied threats. SonicWALL technology, for example, employs multiple specialized techniques to locate possible zombie machines and stop the transmission of outbound e-mail threats - in real time, and without any impact on e-mail services. SonicWALL technology also thwarts the fraudulent requests of a DHA at the perimeter, combining e-mail pattern analysis with data collected through synchronization with the corporate directory to prevent the theft of corporate directory information. DoS-style attacks are handled through unique e-mail pattern analysis and special threat detection tools to determine which mail servers are originating dangerous traffic.

Streamlined Administration

Ease of use

E-mail security systems require constant updates and monitoring throughout the entire inbound/outbound array of security services. The newest e-mail security technology can handle most of this processing internally, without requiring human intervention. Automatic updates, for example - as in SonicWALL Email Security solutions - ensure a more cost-efficient, easily managed e-mail security system. SonicWALL also provides a centralized, Web-based administrative interface that simplifies all management tasks. Figures show that a typical SonicWALL administrator spends only ten minutes a week on e-mail security system maintenance.

Flexible configuration is also important. Administrators need to be able to select uniform or split architectures, as well as centralized or decentralized configurations. Solutions such as SonicWALL respond to this need by offering a variety of configuration options, the simplest of which can be completed in under an hour. The most efficient solutions also permit a high degree of system consolidation, which maximizes hardware and software resources, and simplifies IT tasks.

E-mail security systems also need to offer flexible options for handling attack situations. For example, technology such as SonicWALL Email Security permits administrators to choose among different actions when responding to inbound threats, giving them the flexibility to send an alert or delete, quarantine, encrypt or bounce an offending e-mail as appropriate.

Simplified policy management and compliance

Today's security environments must comply with both legislative and internal corporate security policies, which in most cases involve highly specific system functionality and reporting requirements. Here, again, easy customization can minimize time and maximize results. As one example, SonicWALL Email Security provides an easy way for system administrators to create global or specialized group policies for inbound and outbound email using an identity-based architecture that is fully integrated with LDAP, Microsoft Active Directory and other standard directory systems. Administrators can also set up and revise access privileges very quickly, without any programming knowledge or high-level technical expertise.

Additional features that aid in compliance include sophisticated content analysis and support for compliance dictionaries - such as those used for legislative regulations - which detect harassing or derogatory language. Solutions such as SonicWALL Email Security also include robust reporting features, providing critical statistics about attack types, solution effectiveness, and system performance.

Cost-effective, high-performance architecture

To ensure effective, affordable functionality over the long term. e-mail security systems must be able to consolidate processing as much as possible, maintain high availability, scale as needed, and accommodate sufficient redundancy. The only systems that can meet these needs are those which, like SonicWALL Email Security, provide very high performance, and flexible configuration options.

Summary

E-mail security is unique in one major way, namely, the pace at which the security environment must change in order to keep up with diversified and evolving threats. Flexibility is key, as well as full coverage for the universe of threats that exist now or might present themselves in the near future. Companies require an easily managed, fully customizable e-mail security solution that performs at a very high level, without failures, and with a complete set of technical features geared specifically to particular types of e-mail-based attacks. Although varied e-mail security solutions are available, the only fully dependable ones are those that take an end-to-end approach to security challenges, with specially targeted analytical processes geared to specific threat types.

Integration with broader Web security solutions is also critical. SonicWALL technology, for example, provides a complete range of fully integrated Web and e-mail security solutions that take a global view of corporate networks, ensuring coverage from all angles. In particular, SonicWALL Content Security Manager adds essential protections against Web-based threats such as viruses, spyware, Trojans and worms while also successfully blocking wrongful access to inappropriate Web content.

The power and creativity of e-mail attackers has grown in recent years, but the power and functionality of Web and e-mail security solutions has evolved as well. Armed with proper knowledge, IT teams can easily select technology that will protect valuable systems while leaving personnel and resources free to handle everyday affairs and maintain business as usual.

(1) "There are 600,426,974,379,824,381,952 Ways to Spell Viagra." Cockeyed.com. 7 April 2004.
Retrieved from http://cockeyed.com/lessons/viagra/ viagra.html.

(2) "mi2g:Q3 2004: The Rise of Islamist Hacking and Criminal Syndicates." mi2g. 20 October 2004. Retrieved from http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/201004.php.