



Simply better network security.™

C O N T E N T S

Overview

Network security threats—
viruses are just the beginning

The components of basic network
security: a picture of complexity

The power of simplicity:
strengthening network security
through integration

The eSoft Enterprise Solution:
simplified network security

For more information



Why Your Network May Not Be As Secure As It Should Be
How Simplifying Can Make Your Network More Secure

Overview

Integrating the Internet into business environments has allowed many companies to extend their market reach, improve efficiencies and speed time to market. But the same Internet technologies that enable these opportunities also expose enterprise networks to considerable risks, including intrusions, malicious service interruptions, loss of data and loss of time as a result of responding to attacks. According to Internet Week, network security breaches cost businesses on average 5.57 percent of annual gross revenue.¹

Until recently, most corporate IT departments had the business opportunity vs. vulnerability risk equation well in hand, using a combination of best practices, such as eliminating unnecessary services, strengthening and enforcing passwords, performing system updates regularly, and the use of hardware and software components that guard entry to the network such as firewalls, gateways and routers.

Now, however, the rapidly evolving variety of threats—and the exponentially increasing amount of damage they can cause—is causing anxiety in corporate boardrooms. Cyber attacks are increasing both in frequency and intensity. In 2001, the CERT® coordination center reported a total of 52,658 reported security incidents, but in just the first two quarters of 2002, that number was already 43,136.² In the last four months of 2001, InfoWorld reported a 79 percent rise in the intensity of cyber attacks.³ At the same time, IT has become more and more critical to enabling overall corporate e-business objectives, and corporate boards are holding IT departments accountable for aligning business objectives and strategy. The mounting volume of threats and the increased pressure from the boardroom are forcing IT departments back to the drawing board to strengthen and redefine their IT security perimeter.

The bewildering variety of security solutions available today, however, typically address just one or a few security issues, leaving most businesses with a very fragmented approach to network security that is both costly and very difficult to manage and grow with the business.

This paper provides an overview of network security threats and how they are typically managed, and proposes an improved, simplified approach that can be achieved through the integration of security technologies.

¹ Marcia Savage, Internetweek.com, 2/12/01, "Network Breaches Hit the Bottom Line." <http://www.internetweek.com/story/INW20010212S0005>

² http://www.cert.org/stats/cert_stats.html#incidents.

³ InfoWorld, 3/8/02, "Big plans to secure the future." <http://www1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/ct/xml/02/03/11/020311ctpulse.xml&dctag=security>.

Network security threats—viruses are just the beginning

So how much at risk is your network? Looking at it from a hacker's point of view can tell you a great deal. Threats range from being open to hackers looking for vulnerabilities they can exploit, to direct, active attacks, to unauthorized network use that can pave the way for more malicious attacks.

- **Network scanning**—searching networks for potential victims. This includes determining what a network looks like and how it might be exploited.
- **Data capture**—capturing data that is sent over the Internet, including data theft and username/password theft
- **Unwanted network use**—while this threat primarily causes loss of productivity and increases corporate liability, it can also provide an avenue for indirect attacks
- **Active attacks**—this includes direct attacks on vulnerable servers, as well as indirect attacks, such as viruses and Trojan Horses.
- **Blended threats**—an increasingly primary concern for corporate IT, blended threats combine the methods of viruses, worms and Trojan horses.

Network Scanning

With network scanning, an attacker's first step is to determine what vulnerabilities can be exploited. To do this, attackers may use automated tools to scan networks and identify potential targets. These automated tools can sweep through the Internet address space and use DNS lookups to further refine their search. Fingerprinting tools allow attackers to determine the operating system or type of device that owns each address. Port scans can then identify what services are available at each address. These services can then be checked for known vulnerabilities.

Data Capture

Hackers can steal data without even breaking into your network. Most Internet traffic travels over the public network unencrypted, in plain view, allowing anyone in the data path to view it. Most Web, e-mail and file transfer data is not only sent unencrypted, but users' account names and passwords are also not protected. Not only is there the risk that traffic can be captured, but also that users' account information can be compromised, allowing the attacker to retrieve other data that those users have access to.

Unwanted Network Use

Networks are often used in ways that were not intended or condoned by the organization running the network. Employees can misuse network resources by surfing non-business related Web sites, sending and receiving personal e-mail, using personal chat and instant messaging applications, and sharing personal files over the network. Non-employees can also misuse network resources by sending unsolicited spam e-mail to network users. These misuses can waste valuable bandwidth and disk space, as well as reduce employee productivity and increase company liability.

Active Attacks

There are a variety of types of active attacks with different goals. Some attacks are meant only to disrupt service for other users. These attacks, known as Denial of Service (DoS) attacks, are not used for stealing information, but rather for preventing others from using a particular service. This can range from crashing a Web site, to flooding an Internet link with bogus packets so that there is no bandwidth available for legitimate use. While no data is compromised, the consequences can be quite serious, as many e-commerce sites rely on service availability for their revenue.

Other attacks are meant to take over servers, so that data can be stolen or modified, or so the server can be used to launch other attacks. These attacks typically exploit operating systems or applications that are misconfigured or have vulnerabilities caused by software bugs. Common targets are Web servers, mail servers and DNS servers, because they provide the critical infrastructure for the Internet and are often not protected by firewalls or other security products.

There are also indirect attacks that rely on innocent or ill-informed user behavior to be successful. These include viruses and Trojan horses and they are typically spread via e-mail or file downloads. Users unknowingly open a file or run an application without realizing that it has been infected and can spread to other files or network resources. Some attacks, such as worms, can propagate even without assistance from a user by automatically copying themselves through e-mail or other network services.

Blended Threats

A new breed of attack, heralded by Code Red and Nimda worms last year, combine the methods of viruses, worms and Trojan horses, exploiting weaknesses in operating systems and applications, and using multiple attack methods to get past network defenses, such as e-mail, Web sites, IRC, ICQ, Instant messenger and network protocols. Dubbed blended threats, these attacks spread very quickly because they employ so many vectors. Once a blended threat has infected a computer, it can destroy or manipulate files, leave back doors, Trojan horses or zombies, all of which can be used to automate hacking and spread the attack even more rapidly. At the height of its spread, the Code Red worm infected more than 359,000 computers in less than 14 hours, with about 2,000 new infections each minute.⁴ While simply updating virus signatures could stop previous worms, blended threats can continue to spread via IIS servers, Web browsing, and file sharing. This makes the attacks much more difficult to detect, stop and analyze.

And blended threats are increasingly devastating to the bottom line. Not only does an attack require an immediate cleanup, it also requires a review of all non-affected systems to assess their vulnerability and it results in a measurable loss of productivity, sometimes even taking a business offline completely. Wired.com reports that Code Red alone is estimated to have cost businesses up to \$2.6 billion in clean-up and lost productivity.⁵

⁴ George V. Julme, InformationWeek, 5/20/02, "One Step Ahead."
<http://www.informationweek.com/story/IWK20020516S0020>

⁵ Michelle Delio, Wired.com, 1/14/02, "Find the Cost of (Virus) Freedom."

The components of basic network security: a picture of complexity

Typically, preventing and combating this array of complex threats requires a variety of security solutions and best practices—including firewalls, virtual private networks (VPNs), content filtering, reporting, vulnerability assessments, intrusion detection and software maintenance—that together provide a secure perimeter for your enterprise network.

Firewalls

Firewalls provide an excellent foundation for perimeter security by only allowing certain network traffic to enter or leave the network, as defined by a set of policies. They can protect internal servers and workstations from direct attacks from the Internet, as well as hide internal resources so they can't be detected. Firewalls can also authenticate internal and external users, so their identity can be verified and logged before granting access to network resources. Additional firewall network interfaces can be used to further separate networks and apply different security policies to each. For example, a DMZ network can be created to host public servers, which are isolated from the LAN in case they are compromised.

Virtual Private Networks

VPNs provide private access to network resources over a public network. They're commonly used to provide remote access to outside users, such as those who travel or work from home. While the firewall keeps unwanted users out, a remote access VPN allows trusted users in. VPNs are also used to connect remote offices and business partners. In this case, a VPN provides a much more affordable option to dedicated leased lines. VPNs also enhance firewalls by providing strong authentication of users, so a would-be attacker cannot capture their accounts and passwords.

Content Filtering

Content filtering solutions come in a variety of forms, but all share the common trait that network traffic is inspected beyond the packet headers, and decisions are made based on the payload content about whether to allow or deny the traffic. A common example is Web site filtering, where HTTP requests are inspected to determine the type of content, and a decision is made about whether that content is allowed to enter the network. Another example is anti-virus scanning, where messages are scanned for known viruses, and any infected attachment can be removed before delivering the message. Content can also be filtered based on the type of application that generates it, such as peer-to-peer file sharing and instant messaging. This extends beyond firewall filtering, because the content of the packet is inspected, rather than relying on the protocol and port number, which may not be known. Unwanted e-mail, such as spam, can also be filtered out at a network gateway, based on analysis of message headers and body.

Logging and Reporting

Network requests that violate the pre-defined security policy should always be logged because they may provide evidence of an attempted attack. Because there can be many such requests, reporting tools are important for summarizing log data so that trends can be recognized and analyzed. There are also reasons to log valid requests. This allows network usage to be analyzed for potential misuse. For example, Web requests and e-mail messages may be logged so reporting tools can summarize network usage per user.

Vulnerability Assessment

It's important to be able to see your network from a potential hacker's point of view, so you can understand where your risks are and take appropriate actions to minimize those risks. Vulnerability assessments provide this kind of view of your network, and can show your potential vulnerabilities and suggest corrective actions. Shrink-wrapped products provide all the necessary information, but are often difficult to implement because of the need to view the network from the outside. Services that provide the ability to scan your network from the Internet are the easiest to implement.

Intrusion Detection and Prevention

Intrusion detection systems (IDS) can recognize potential network attacks and either alert administrators or automatically respond to thwart the attack. This complements the post-mortem analysis provided by logging and reporting tools. There are two common techniques for implementing IDS. One approach is to monitor the network for known attack signatures, similar to the way anti-virus technology works. The other approach, known as anomaly detection, is to learn what traffic is normal for a given network and then recognize abnormal behavior. While this technology is still young, it holds great promise for automating responses to network security incidents.

Software and Signature Updates

An important part of maintaining network security is maintaining up-to-date software and security signatures. This includes security software and associated data, such as URL databases and virus signatures. Unfortunately, many products rely on users to manually check for software and data updates, which results in this important task being frequently neglected. Solutions that automatically check for new software and data updates will allow you to keep current with minimal effort.

The power of simplicity: strengthening network security through integration

All these discrete security products are available today from a variety of vendors. However, as Lucy Bunker recently observed in VNUnet.com, this complex, piece-part approach is far from an ideal or cost-effective solution:

“Choosing a variety of solutions from a variety of vendors gives you multiple supplier contracts, multiple technical support services, and various different reporting tools and analysis... and you'll soon find that you've created a monster which requires additional resources to manage.”⁶

In addition, each component on its own has limitations. But if you can integrate the parts, you simplify the solution and gain strength and flexibility. Why?

With firewalls, some traffic must be allowed to pass through from the Internet to internal servers. For example, e-mail traffic is often allowed to pass through the firewall to an internal mail server. Without integrated content filtering, firewalls cannot determine whether the traffic is legitimate or safe. Without integrated VPNs, firewalls cannot provide secure remote access to internal resources.

If the VPN is inside the firewall, then the firewall is unable to inspect the encrypted VPN traffic. If the VPN is outside the firewall, then the firewall cannot be sure that traffic that it receives was protected by the VPN. However, a VPN that is integrated with the firewall provides greater flexibility because they work together to enforce a consistent security policy.

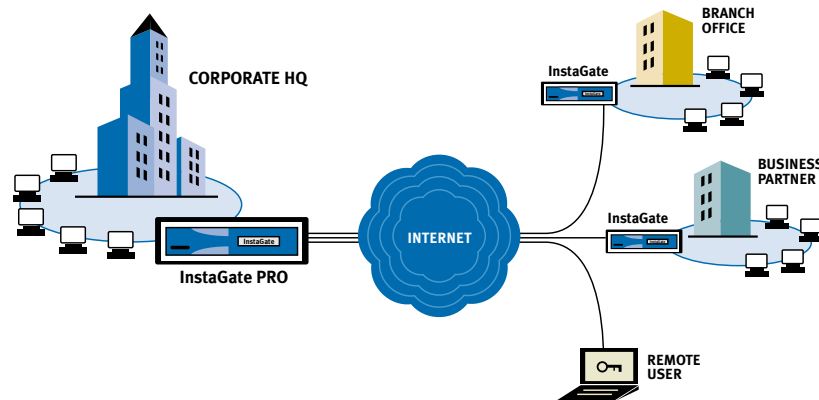
Content filtering solutions are also strengthened through integration with a firewall. The firewall is in an ideal position to see all traffic that enters or leaves the network, and should be responsible for redirecting that traffic to content filters as necessary. The administrator does not have to solve the problem of designing a network that ensures that network traffic passes through the content filter before entering or leaving the network. With an integrated product, the correct behavior is enforced at the gateway. In addition, firewall authentication information can be combined with filtering results, so the information can be easily correlated. For example, with web requests, it's useful to identify the source address, destination address, user name, URL and content category, all in the same log file or report.

Centralized logging and reporting provide a single location for analyzing network incidents and usage. Integrated products can provide logging and reporting, using shared storage and a common user interface, which makes reporting and analysis significantly easier.

Emerging blended threats, however, provide the strongest case for integrated security solutions. It's still unknown how blended threats will evolve, but their early success should tell us that these types of threats will become more sophisticated and will require a combination of technologies to prevent them. Integrated security solutions already provide the necessary components to stop these attacks and will evolve to improve communications between the components. Organizations that implement integrated security solutions will be the best positioned to protect their networks from these emerging blended threats.

The eSoft Enterprise Solution: simplified network security

eSoft network security solutions are designed to simplify the complexities of Internet security. The eSoft Enterprise Solution encompasses the SoftPak™ catalog, a comprehensive catalog of modular security extensions that are designed to work together on the InstaGate™ VPN firewall appliance. This unique, extensible architecture enables rapid, dynamic deployment and customization of a robust, reliable security solution that incorporates a stateful firewall, VPN capabilities, anti-virus protection, vulnerability scanning, Web site and content filtering, and a variety of optional security extensions that can be added as an organization's needs change.



The eSoft Enterprise solution combines a VPN firewall appliance with a comprehensive catalog of modular security applications that enable you to quickly create a secure network perimeter that is affordable and extensible.

With the eSoft Enterprise solution, everything needed to secure the IT perimeter runs on a single box that can be managed from a central, easy-to-use, Web-based tool that enables automatic updates and reduces software maintenance and support costs that contribute to a lower total cost of ownership.

For more information

To learn how the eSoft Enterprise Security Solution can help you simplify your network infrastructure security, visit us online at www.esoft.com or call us at **303.444.1600**.