

White Paper

Network Security Options

Trends in protection against network intrusion, attack, and resource hijacking

SecureWorks
Third Quarter, 2000

INTRODUCTION

Economics had at one time reserved high-speed, always-on Internet connections for only the largest of businesses. Recent developments in digital subscriber line (DSL) and similar services now place these connections within the grasp of virtually all organizations, at all locations.

This upward trend in connectivity represents a dramatic increase in information accessibility and exchange—and it also means significant vulnerability for individual and networked systems alike. While attackers can gain access to networks and systems through *any* connection to the outside world, always-on connections are continuously available and therefore especially susceptible to attack.

Any facility with an always-on Internet connection is potentially at risk of Denial of Service (DoS) attacks, resource hijacking, e-mail viruses, and other Internet-borne threats that have substantially negative effects on systems and networks. These security threats are always present and always changing, making them challenging to track and counter.

In meeting that challenge, there are many Internet security tools to choose from that, with adequate expertise, can be combined to provide multiple levels of security. For locations with 250 or fewer network users, however, the right path to secure network operation is made difficult by a number of factors.

First, many smaller installations lack the expertise to accurately identify and address security problems. This is especially true if an IT department does not exist or lacks sufficient breadth. Even when security equipment and services are installed, many traditional solutions require in-house talent to configure and monitor operation on an ongoing basis. Lastly, budgetary constraints, in terms of both trained personnel and equipment, typically represent a significant hurdle for these locations.

Traditional security solutions have shortcomings in all of these areas. What's needed is an affordable and tailored solution capable of overcoming these obstacles, one that doesn't require highly paid on-staff security experts, active end user-provided monitoring and response, or expensive equipment.

This paper takes a look at approaches to network security, including the use of firewalls, intrusion detection systems, and virtual private networking (VPN). Special emphasis is given to a new service offering from SecureWorks with capabilities that extend beyond those of traditional firewall and intrusion detection products by providing real time monitoring and human response.

TRADITIONAL APPROACHES TO NETWORK SECURITY

FIREWALLS

Firewalls provide a kind of boundary defense by creating a level of separation between an internal network and the outside world. A firewall can be software- and/or hardware-based and is used primarily to prevent unauthorized outside access to intranets or LANs. All inbound traffic encounters the firewall first, and any data that does not meet specified security criteria is rejected. Outbound traffic is typically also checked, and specific types of traffic can be limited or completely disallowed.

Firewalls examine data traffic by means of a packet filter, a set of rules that determine which traffic passes and which is rejected. Packet filtering is a good first line of defense but is susceptible to attack and circumvention.

To help counteract these attacks, better firewalls implement *stateful* packet filtering. Plain packet filtering examines individual packet content against specific rules, without any correlation across packets. Stateful filtering keeps better tabs on traffic through a broader approach that enables the firewall to track process-level (not just packet-level) activity. Stateful filtering provides better traffic authentication and minimizes some threats.

Even then, a firewall alone does not offer sufficient network and system protection. The best firewalls remain prone to many attacks, including tunneling and application-based attacks. Tunneling allows traffic that should be screened to pass through by encapsulation within packets corresponding to other network protocols. Application-based attacks take advantage of existing applications by directly exploiting their vulnerabilities.

Finally, firewalls demand significant upkeep to be effective. Tracking and installing firewall software updates takes time, and a significant amount of network and security expertise is required to effectively configure a firewall to be useful against an ever changing and ever growing array of intrusions and attacks.

INTRUSION DETECTION SYSTEMS (IDS)

Intrusion detection systems monitor network traffic for suspicious activity or data patterns. The action taken by the IDS upon detection of an intrusion varies but usually consists of issuing alerts when potentially hostile traffic is detected.

Intrusion detection is a logical complement to a firewall and extends the capabilities of the network manager to identify and respond to a variety of threats. An IDS looks for signs of intrusion (unauthorized users trying to gain access) or misuse (authorized users overstepping their bounds) by comparing the data that passes through it against a data base of attack signatures, which are data sequences that uniquely identify intrusions.

As network security systems, IDSs are relatively passive. They detect problems, issue notices about them, and then continue monitoring. And rather than monitoring live traffic, some IDSs analyze the audit trails created by servers and other networked systems. This latter approach introduces delays in system managers' response time against intrusions and allows attackers more time to exploit network vulnerabilities.

Other than issuing attack alerts, IDSs do not respond to attacks. Whether installed standalone or in tandem with a firewall, intervention by a skilled network manager is always required to

analyze the alerts, assess the situation, and determine the appropriate response. IDS alone cannot distinguish between real and apparent threats and can thus generate a high number of false positives, events that approximate attack signatures but happen to be legitimate data. In this case, too, a system administrator has to make a determination as to the appropriate action.

Implementation of an IDS alone doesn't provide sufficient protection. But even when coupled with a firewall system a network can remain vulnerable. For sites that have few or no network administrators, keeping track of an IDS is impractical. Traditional IDSs also have significant system footprints, deployment complexity, and high cost in common, making them impractical for sites that have little or no network management staff.

In addition, due to their proprietary design, most commercial IDSs are slow to incorporate new attack recognition signatures. In many cases, the IDS updates that detect newly identified attacks lag by as much as 45 days after the identification of an attack signature by such authoritative bodies as the CERT[®] Coordination Center¹.

VIRTUAL PRIVATE NETWORKING (VPN)

Before use of the Internet became commonplace, organizations installed dedicated circuits or networks to interconnect campuses and branch offices. Now that Internet access is widely available, its use for the same purpose through VPN technology is generally far more economical, and many companies prefer this alternative.

By definition, private networks offered a high degree of security because they were dedicated point-to-point links. But any communication over the public Internet is susceptible to monitoring and even hijacking. To be useful, virtual private networking must approximate the same level of security afforded by private networking in a public environment. To do this, VPN employs encryption and other security mechanisms to ensure that only authorized users gain access to data and networks.

VPN represents tremendous convenience for employees, partners, and even clients who might need to remotely log onto their networks. But the same support also creates vulnerabilities that are only waiting to be exploited.

Although VPN protects data while it is in transit, the endpoints are typically not secured. When a partner is given VPN access to a network, for example, vulnerabilities present on the partner's network transfer upon connection. This is especially true if the computer used for VPN is connected to an unprotected LAN. In this scenario, the user's files are vulnerable, and the connection could allow hackers to use the user's VPN client to gain authenticated access to corporate intranets and sensitive documents.

¹ The CERT/CC is a major reporting center for Internet security problems. For more information, see www.cert.org.

ACTIVE MONITORING: THE BETTER APPROACH

No standalone security method can offer complete protection against the range of attacks networks can suffer. Even when combined, traditional solutions can leave holes, have known exploitable flaws, and usually require significant management expertise to be effective. Conventional systems are designed only for prevention. Effective security is more than just prevention—it's real time monitoring and response.

THE SECUREWORKS MODEL

The best approach to reliable network security is one that blends the best features of traditional approaches with active monitoring, skilled human confirmation, and effective countermeasures. SecureWorks delivers just such an approach.

SecureWorks' service can be compared to a home alarm service, in which detectors are placed at entry points and monitored around the clock at a remote center. But a home alarm service can't actually prevent a determined intruder from climbing in a window; it can only send notice that something bad may have happened. SecureWorks does much more—literally stopping network intruders and even providing the tools and human expertise to follow their trail.

ACTIVE MONITORING

Active monitoring is facilitated by SecureWorks' iSensor, the Internet security appliance located at the customer premises. The iSensor installs between the customer's local area network (LAN) and the Internet connection to provide intelligent network activity monitoring. This allows securists at the SecureWorks Internet Monitored Security Center (IMSC) to examine, stop and report security threats.

STATEFUL PACKET FIREWALL

iSensor's built-in firewall implements stateful packet filtering to provide the highest possible level of protection. Standard packet filtering works with individual packets only, but the iSensor's stateful packet filtering also tracks state information across multiple packets. This approach puts information into context and differentiates between real threats and data that coincidentally matches a known attack type.

INTEGRATED INTRUSION DETECTION SYSTEM

The iSensor's integrated intrusion detection system (IDS) enables it to continually check traffic for a variety of potential and legitimate intrusions, including port scans, viruses, and denial of service (DoS) attacks. IDS monitors for telltale signs of security violations by checking against known "attack signatures," data sequences that can be matched against a data base of known attack types. Several hundred attack signatures are stored in the iSensor's internal data base, and the list is automatically updated as new signatures are discovered.

COMPLEMENTARY SECURITY FOR VPN

Standard VPN protects data transmission but can leave the connection's endpoints vulnerable to attack. SecureWorks complements traditional VPN infrastructure by protecting the endpoints of a connection and enabling true end-to-end security.

REMOTE CONFIGURATION MANAGEMENT SYSTEM (RCMS)

A unique SecureWorks feature, the RCMS uses patent-pending encryption to ensure secure communications between installed iSensors and the IMSC. The RCMS provides three critical

functions: periodic iSensor and network traffic status (the EKG, or “heartbeat” of the system), remote attack signature and software updating by the IMSC, and immediate alerts upon attack detection.

THE SECUREWORKS ADVANTAGE

All enterprises, not just the largest, need network security. But for many organizations, having in-house network security specialists simply isn’t practical. With SecureWorks’ monitoring service, in-house expertise isn’t necessary, either. SecureWorks’ iSensor and IMSC staff watch network traffic around the clock, ready to act in case of intrusion.

UNOBTRUSIVE INSTALLATION

The SecureWorks service begins with the installation of an iSensor appliance. The iSensor is compatible with a variety of Internet connection methods, including those provided by cable modem, ISDN, DSL, and T1 services. It installs easily and transparently between the Internet service provider’s connection device (typically a router or a modem) and the LAN or LAN segments to be protected.

AFFORDABLE SERVICE

Many organizations can’t afford an in-house staff of network security specialists. SecureWorks’ patent-pending technology provides comprehensive Internet monitoring at a reasonable price, so it’s no longer necessary to sacrifice security and quality of service to control cost.

EXTENSIVE ATTACK SIGNATURE LIBRARY

As soon as it’s installed, the iSensor begins to protect against hundreds of known attack signatures. New attacks and variants of old ones are formulated all the time, and the iSensor’s data base can be updated soon after attack types are documented, usually within hours, not weeks.

REAL TIME RESPONSE AND COUNTERMEASURES

The countermeasures enabled by the iSensor’s attack signatures fall into three categories. Low level attacks are automatically detected, terminated, and logged. Mid-level attacks are often reported to IMSC specialists for further analysis, where a determination to shut down the attack is quickly made if the attack is found to be legitimate. Finally, high level attacks, such as distributed denial of service (DDoS) attacks, are immediately terminated.

ACCURATE THREAT IDENTIFICATION

Legitimate network traffic sometimes resembles mid-level attack signatures and can generate “false positives.” IMSC securists are able to differentiate between actual security threats and false positives, something conventional security can’t offer. In the event of a real attack, SecureWorks securists respond in real time and then notify the customer of the event and its resolution.

WEB-BASED CONFIGURATION INTERFACE

The iSensor is configured to operate with little to no end user attention. Default settings are appropriate for most installation, but the end user can modify certain operational aspects. To make things easy, the firewall settings can be modified to pre-defined low, medium, and high security settings. Users who want more granular control of the iSensor’s firewall settings can also edit specific firewall rules to meet their needs.

CONCLUSION

No Internet connection is immune to security problems. Security threats affect everyone connected to the Internet, not just Fortune 500 companies or high-profile services like Yahoo! and eBay. Moreover, attacks and intrusions on the rise. In a 1999 Information Security survey of 342 companies, 91 per cent said they had experienced a hacking incident in the previous year.² Other figures show that four times as many hacker attacks occur per day in North America today compared to just one year ago.³

Human intervention is a key component of any truly successful security system. Hardware and software can do some of the work, but accurate real time analysis can only come from a trained pair of eyes capable of discerning between real and apparent attacks. A recent eWeek article pointed this out, saying that, "IT managers are beginning to recognize that software alone cannot protect the network. A real time analysis is required to determine whether or not traffic violates specific [security] policies."⁴

Keeping basic IT functions running smoothly can be challenging, and staying on top of security issues as well can tax even the most organized groups. Many companies are therefore looking to outsource security. In a June 2000 report, IDC found that, "Companies are increasingly outsourcing their network security needs because the complexity of networked devices and systems is straining the ability of in-house IT resources to perform the needed security management tasks...."

Effective protection, however, has traditionally been found only in Fortune 500 corporate headquarters. Internet security has simply been too costly or unworkable for smaller businesses and branch offices. SecureWorks' advantage is its ability to monitor and respond to attacks in real time in a comprehensive, non-intrusive, and affordable manner.

With SecureWorks, businesses don't have to invest hundreds of hours and thousands of dollars in software, hardware and personnel to protect their networks. SecureWorks offers locations with 250 or fewer networked users an advanced, remotely managed Internet security monitoring and response service—at an affordable price.

ABOUT SECUREWORKS

SecureWorks delivers cost-effective, 24/7 Internet security monitoring and response services. The company is the first to offer Internet security that is comprehensive, non-intrusive, and affordable. SecureWorks' fast response capabilities are based on its patent-pending iSensor technology, working in tandem with securists at the company's Internet Monitored Security Center. For more information, please visit www.secureworks.net.

² Risk Management, July 2000

³ International Computer Security Association

⁴ eWeek Reader Pulse Poll, June 19, 2000