



BEYOND THE FIREWALL: The next level of network security

Prepared by:

Ian Poynter
Information Security consultant

Brad Doctor, CISSP
Principal Security Architect
Latis Networks, Inc.

January 2003

White paper

Table of Contents

Introduction	2
Where your firewall and anti-virus fall short	2
Technologies beyond the firewall	4
Intrusion detection/intrusion prevention systems (IDSs/IPSs) ...	4
Vulnerability assessment (VA) tools	5
StillSecure solutions	6
StillSecure Border Guard IPS products: protection, automation, and control	6
StillSecure VAM: assessment and management that continuously ensures network security	7
Conclusion	8

About the authors

Ian Poynter is an information security consultant based in Cambridge, MA. He was formerly the President of Jerboa Inc., a strategic information security consultancy. He has been active for more than 15 years in the technology industry, focusing on networking and human-computer interfaces. He works with a wide range of industries to implement solutions for corporate network and Internet security. Mr. Poynter has delivered Internet security training to key corporate information systems personnel around the country and has appeared as an expert speaker at a variety of professional meetings including the Computer Security Institute (CSI) 2002 Conference, The BlackHat Briefings, The Internet Security Conference (TISC), WebSec, USENIX Security, and Network+Interop.

Brad Doctor is Latis Networks' principal security architect. He has been involved in IT security for more than 10 years. Prior to Latis Networks, Mr. Doctor consulted for such companies as Apple Computer, Phoenix Technologies, and The Monster Board fulfilling network and host-based security needs. In addition to traditional IT security, Mr. Doctor also worked with Quova, Inc. as the Director of Research where he led the development of Quova's proprietary IP Geolocation technology, which is presently used by Visa International to detect credit card fraud.



Latis Networks, Inc.
361 Centennial Parkway
Suite 270
Louisville, CO 80027

P: [303] 381 - 3800
F: [303] 381 - 3880
www.stillsecure.com

INTRODUCTION

The myth that a firewall alone is sufficient to protect a network has been proven false time after time in recent years, yet many still hold firmly to the belief. The sensational news stories of crippling viruses and stolen credit card numbers fail to mention that almost all of the victims of these attacks had network security – in the form of a firewall – in place. In fact, it's estimated that 80% of network attacks get through or around the firewall (Computer Security Institute).

Network security is a means to a simple goal: managing risk and liability. Your network is a conduit to information vital to your success. If this information — such as intellectual property, financial records, customer data, or perhaps patient and medical records — were compromised, the consequences could be catastrophic. In the wake of a network security breach, you could be subject to regulatory fines and penalties, lose customers, face liability claims, and irretrievably damage your reputation. With so much at stake, you must look beyond the firewall for adequate protection.

This white paper discusses a number of advanced network security technologies that can help you defend against today's sophisticated attacks. We tell you why your firewall and anti-virus alone are no longer sufficient to protect your network. Within a layered-security framework (see sidebar), we then describe advanced technologies, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and vulnerability assessment (VA) tools, that can dramatically improve your security posture. We also discuss how the **StillSecure** line of IPS and VA products can provide the bedrock on which a secure network is built. You'll learn why it is imperative to strengthen your security profile to defend against today's sophisticated and increasingly frequent network attacks.

WHERE YOUR FIREWALL AND ANTI-VIRUS FALL SHORT

A firewall and anti-virus software are the bare necessities for securing your network. While these measures play a crucial role in network security, they are incapable of defending against many of today's advanced threats and vulnerabilities. A quick review of basic firewall functionality demonstrates why this is so.

Operating on level 1 of the layered security framework, a firewall acts like a traffic cop. It permits network traffic to pass through based on a number of specific metrics. For example, a request destined for your email server is allowed through; a request addressed to your corporate accounting system is denied (see *Figure 1*). Usually, traffic destined for your Web server (port 80) or email server (port 25) is granted access. Unless you specify otherwise, a firewall typically blocks all traffic addressed to other locations (i.e., servers, databases, or application servers) on your network, thus protecting those hosts against unauthorized, external access.

It is important to keep in mind that most firewalls do not analyze the contents of the data packets that make up network traffic. The firewall simply allows or prohibits access, in whole, based on the external data packet characteristics – specifically, destination and source IP addresses and ports.

THE LAYERED-SECURITY FRAMEWORK

Network engineers discuss network security in terms of layers or levels. This provides a convenient framework for understanding the various types of threats and vulnerabilities and how they can impact your organization. By implementing security measures at each level, you create a comprehensive, robust security profile.

The figure below shows the five levels of network security and the various technologies that operate at each level. This paper is concerned with the security measures, highlighted in yellow, which function on the first two levels: the perimeter level (1) and the network level (2).

Security level	Applicable security measures
5. Data	<ul style="list-style-type: none"> • Encryption
4. Application	<ul style="list-style-type: none"> • Application shield • Access control/user authentication • Input validation
3. Host	<ul style="list-style-type: none"> • Host-IDS • Access control/user authentication
2. Network	<ul style="list-style-type: none"> • Intrusion detection/prevention systems (IDS/IPS) • Vulnerability assessment (VA) tools
1. Perimeter	<ul style="list-style-type: none"> • Firewall • Anti-virus • VPN encryption

Given this basic functionality, a firewall is powerless to defend against a number of today's sophisticated threats and vulnerabilities, including:

- **Attacks embedded in legitimate network traffic** — many network attacks are embedded in traffic that the firewall deems permissible. A number of well-known attack types, including Code Red, NIMDA, and the Klez virus gain access to and cripple networks by masquerading as legitimate Web server requests or email traffic.
- **Access gained through wireless network segments** — On most networks, wireless LAN (WLAN) segments connect inside the firewall, allowing a back door into the network. Wireless access points (WAPs) can be readily exploited by individuals with malicious intent. *Figure 2* shows a wireless access point on what many might consider to be a "secure" network (note the firewall monitoring the Internet connection). Without security installed on the wireless segment, such a network is extremely vulnerable. As indicated in *Figure 2*, a hacker who compromises the wireless segment gains free run of the entire network.
- **Attacks originating from behind the firewall** — A number of common technologies and poor business practices can give rise to attacks that

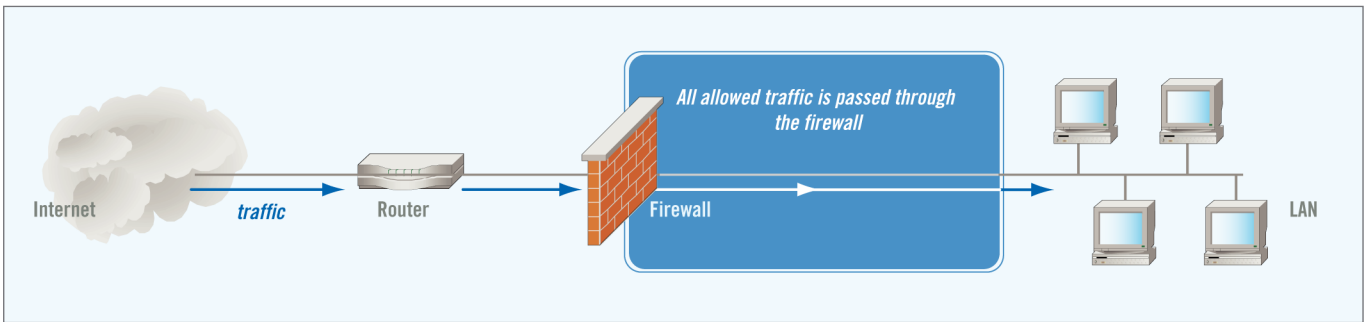


Figure 1. The firewall can permit or deny traffic based on the traffic's destination, among other options.

originate from behind the firewall. For example, mobile devices such as laptops can be removed from the trusted network segment and connected to untrusted networks, where viruses and vulnerabilities can be introduced. Upon reconnection, these vulnerabilities expose the trusted network to attack.

Other vehicles that can expose your network to attack from behind the firewall include peer-to-peer (P2P) connections, instant messaging transmissions, downloads, and dialup access. Many organizations, for example, still have modem pools, or they outsource the pools and have a T1 connection from the vendor directly to their internal network without security.

- **Poorly maintained device security profiles** — When devices are added to a network, they are typically configured with a security profile that specifies, for example, which ports are allowed to be open and what software is authorized for installation. Over time,

the maintenance of this security profile can lapse. Configuration changes occur or new software is installed that introduce vulnerabilities that can be readily exploited. Limited IT budgets and resources often prohibit the periodic device-by-device security audits that should occur.

- **Vulnerabilities introduced by third-party applications** — Ninety percent of external attacks leverage mis-configured services or pre-existing vulnerabilities on third-party software and applications (Computer Security Institute). For example, the infamous Code Red worm exploited an IIS Web server vulnerability. Other prevalent application vulnerabilities include unvalidated parameters, poorly enforced access control, and insufficiently protected account credentials and session tokens.

Because a firewall is strictly a boundary device, it is powerless to defend against these threats and vulnerabilities. It is not designed

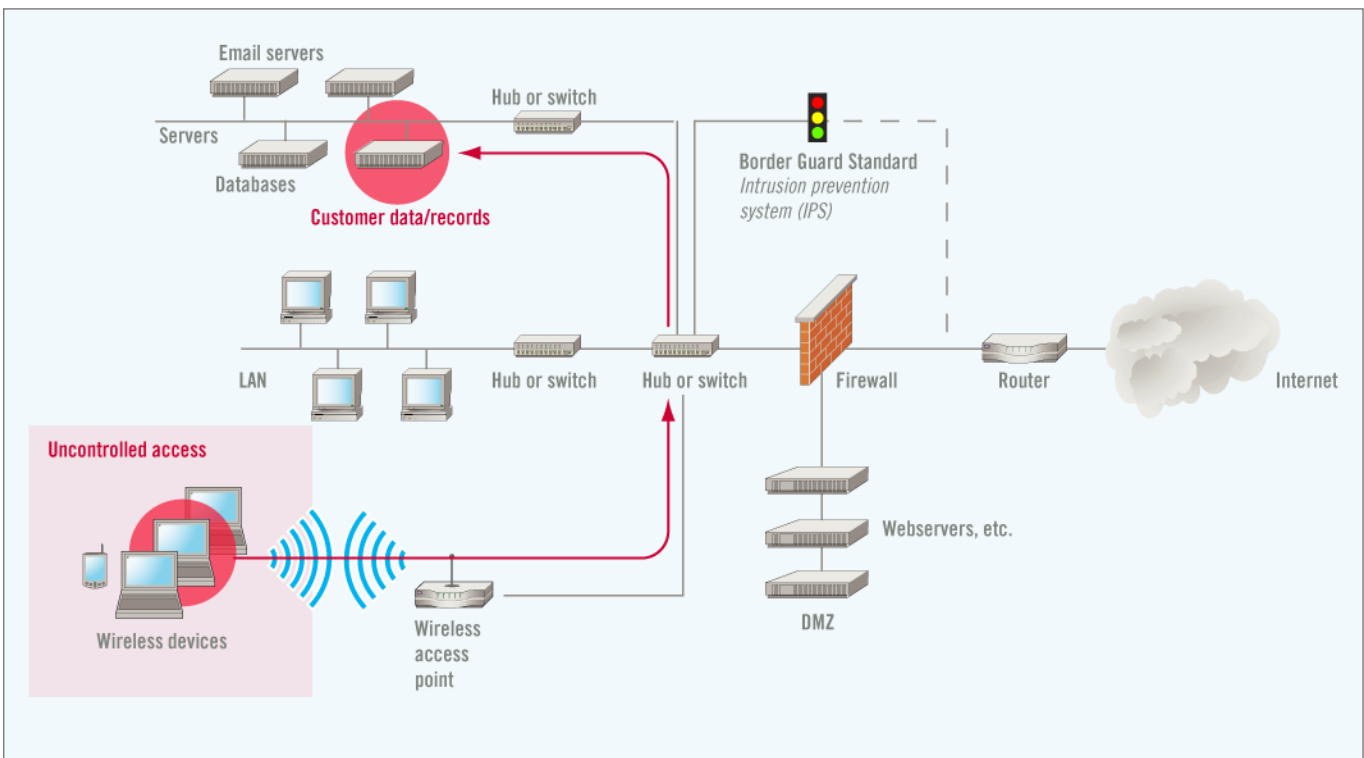


Figure 2. Most wireless segments have minimal or easily compromised security in place and provide hackers direct access to your digital assets.

to protect you from threats originating inside the network. As hackers and hacking tools become increasingly sophisticated, and as the number of attack attempts continues to grow, many organizations are implementing additional, advanced levels of security to meet today's threats.

TECHNOLOGIES BEYOND THE FIREWALL

Although a firewall is incapable of providing comprehensive network security, it is an important component of your perimeter — or level 1 — defense. Beyond the firewall, at the network level (level 2), reside advanced technologies such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and vulnerability assessment (VA) tools. These technologies perform sophisticated analyses on network threats and vulnerabilities.

Before adopting these advanced technologies, you should have a clear understanding of their capabilities and what you hope to achieve by deploying them. Having a detailed security policy with specific goals establishes a baseline from which you can objectively evaluate competing technologies and products. As every network is unique, you need to examine your network configuration, the amount of traffic it handles, and your business processes to determine the ideal blend of security technologies.

INTRUSION DETECTION/INTRUSION PREVENTION SYSTEMS (IDSs/IPSS)

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSS) have a number of functional characteristics in common. In fact, most IPSS have an IDS at their core. The key difference between the technologies is implied by their names: IDS products only *detect* malicious traffic, while IPS products *prevent* such traffic from entering your network. The following sections describe each of these technologies in more detail.

IDS technology

An IDS analyzes network traffic looking for indications of attacks and malicious intent. As *Figure 3* shows, a typical IDS installation straddles your firewall and monitors traffic in a promiscuous (undetectable) mode.

An IDS maintains a database of known attack profiles, which are commonly referred to as 'rules'. It compares each incoming data packet to this library of rules. When suspicious traffic is detected,

that is, when an incoming packet matches a rule, the IDS sounds the alarm, sending notifications that an attack has occurred.

Because an IDS analyzes each data packet, attacks embedded in seemingly harmless traffic are readily identified — and that's the core value of the technology. The key benefit of an IDS is its ability to provide notification of an attack in progress, which allows your IT staff to later review attacks and determine what configuration changes should be made to the network to avert similar attacks in the future. The IDS provides 24/7/365 monitoring of virtually all the traffic on the network that moves by it.

These IDS features give your IT staff a tremendous amount of information about network traffic. With sufficient resources, you can examine every suspicious or potentially damaging request.

The features that make IDSs so powerful can also make the technology extremely difficult to use. IDSs have a tendency to inundate you with alerts and notifications and produce numerous false alarms, also referred to as false-positives. While an IDS will likely detect and alert you to an attack in progress, such information could be buried under a mountain of false-positive or trivial data. IDS administrators can quickly become desensitized to the sheer volume of data produced by the system, which can have a detrimental effect on their ability to respond to legitimate threats.

To be effective, an IDS must be closely monitored and continually fine-tuned to the usage patterns and vulnerabilities discovered in your environment. Such maintenance typically consumes a fair amount of administrative resources. In fact, the Giga Information Group reports that 75% of IDS implementations fail due to the complexity of their operation. Keep this statistic in mind when evaluating an IDS vendor, and be sure to choose a product that can be maintained with your existing IT resources.

IPS technology

As the name implies, intrusion prevention systems (IPSS) don't simply detect attacks as do IDSs; they actually prevent attacks from taking place or automatically block them upon detection. They enable an organization to take proactive, highly automated steps to guard against intrusions.

Most IPS technologies are installed at the network perimeter and afford protection for all devices behind the point of deployment.

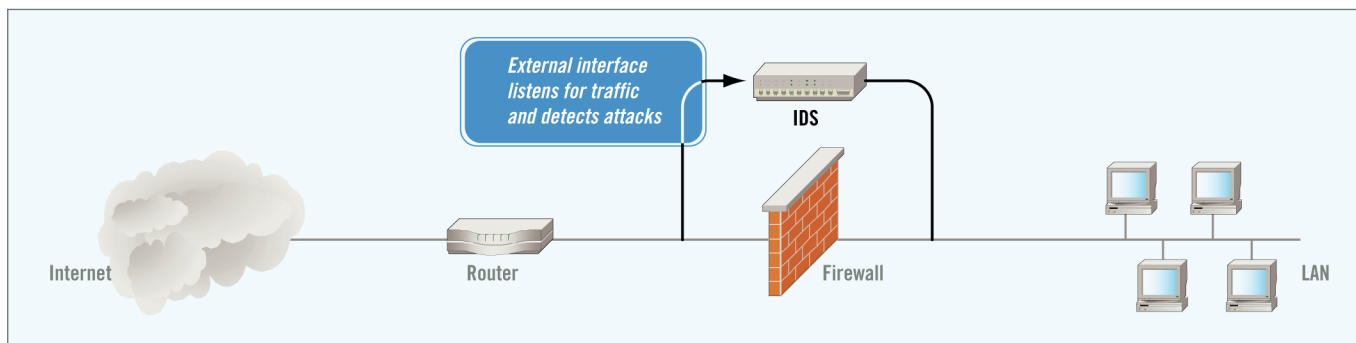


Figure 3. A typical IDS installation.

Two general types of IPS deployments are available: out-of-band IPS and in-line IPS. These are shown in *Figures 4 and 5*.

Out-of-band IPS (OOB IPS) systems straddle the firewall much like an IDS. As mentioned previously, an IPS contains built-in IDS technology that monitors and analyzes network traffic. As such, an IPS can readily detect attacks embedded in legitimate traffic. An IPS, though, takes the next step. Based on the IDS traffic analysis, an OOB IPS can manage the firewall, instructing it to terminate the suspicious activity. This functionality is indicated in *Figure 4*, where the management interface is in direct communication with the firewall.

In-line IPS products perform similarly. The key difference is that in-line IPSs have traffic-blocking functionality built in. This allows the IPS to terminate harmful traffic even more quickly than an OOB IPS.

In addition to protecting the network perimeter, in-line IPSs are well suited to guard against threats that originate behind the firewall. For example, in-line IPSs can secure private connections, such as those you might put in place for partners and suppliers, where firewalls are not traditionally installed, yet that are vulnerable to attack. Also, when installed between a wireless access point and your wired LAN, an in-line IPS eliminates the vulnerabilities that make wireless (or Wi-Fi) networks so easy to hack into.

The level of automation within an IPS can vary significantly among products. Many must be configured and managed to reflect the traffic patterns characteristic of the network on which they are installed. Possible side-effects of non-optimized performance include terminating legitimate user requests and locking out valid network resources. These side-effects can be minimized with fine-tuning controls available in some IPS systems. Overall, IPSs offer significant

value by automatically blocking network intruders and saving significant staff time reviewing mountains of firewall and IDS logs.

VULNERABILITY ASSESSMENT (VA) TOOLS

Vulnerability assessment (VA) tools are software that scan devices on a network for security flaws and vulnerabilities (see sidebar, p.6) that could be exploited by hackers or harmful traffic. Operating on level 2 (i.e., the network level) of the layered-security framework, VA tools typically maintain a database of rules that identify known vulnerabilities for a range of network devices and applications. During a network scan, the VA tool tests each device/application by applying the appropriate rules. The process outputs a list of discovered vulnerabilities, which can then be acted upon by IT staff.

VA scans should be run on a regular schedule. It's important to keep in mind that a network is not a static entity. As discussed previously, devices and applications are installed, modified, and removed on an ongoing basis, and each change can introduce — or re-introduce — vulnerabilities. A network with few or no vulnerabilities today could have dozens of new vulnerabilities next week — or even tomorrow. Today's high-end VA tools automate the selective scanning of your network. It would be advisable, for example, to scan your mission-critical devices, such as your Web server or inventory database, frequently — perhaps daily or even hourly. Employee workstations, on the other hand, would likely require less-frequent scanning — perhaps daily or weekly. By automating selective scanning, today's advanced VA tools adequately protect your network without imposing an undue burden on your network resources.

It is also crucial to keep the vulnerability rule database up to date. More advanced VA tools automate the update process, checking for and adding new rules as they become available.

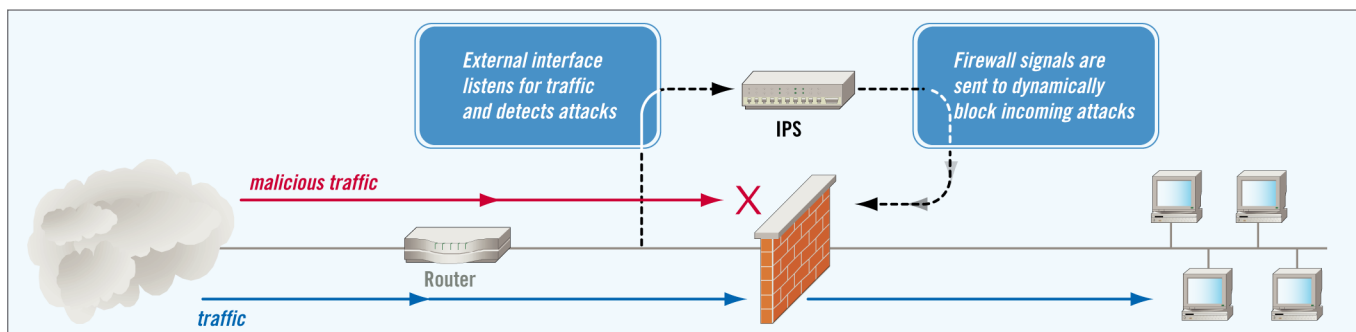


Figure 4. Out-of-band IPS installation.

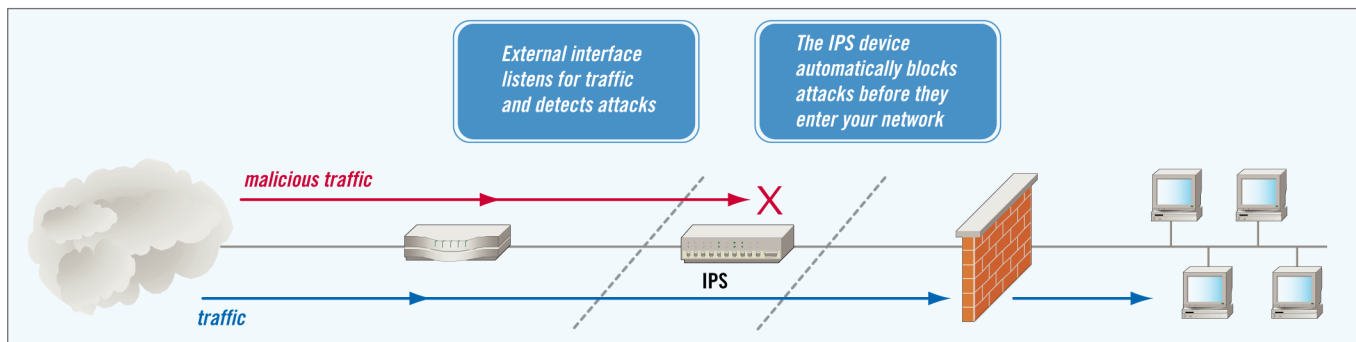


Figure 5. In-line IPS installation.

An important differentiator among VA tools is their ability to effectively manage the vulnerability repair process. Determining that a vulnerability exists is only the first step, and is of little practical value without the follow-on steps of repairing the vulnerability and then confirming that the fix was effective. Many of the VA tools currently on the market — and many third-party security consulting firms — simply provide a lengthy report on the vulnerabilities discovered. They leave it up to your IT staff to analyze the results, prioritize and implement repairs, verify that repairs are effective, as well as manage the entire process.

Today's advanced VA tools include a workflow management component that rectifies these important deficiencies. Full-featured VA tools can prioritize and track a vulnerability from discovery through confirmed repair. Without workflow management, VA tools generate data without assigning any responsibility for ensuring the needed fixes will occur. An effective VA product should also initiate follow-up scans to verify the effectiveness of the repairs made. With these additional workflow capabilities, VA management products help IT organizations enforce and bring accountability to security policies. All scanning, repair, and verification activities are now traceable for every vulnerability encountered on the network. This also satisfies many security and regulatory auditing processes.

EXAMPLE: A real-world vulnerability — OpenSSH CRC32 Buffer Overflow — illustrates why the VA process is a critical component of a secure network. SSH (Secure Shell) is an encrypted means of communicating with remote devices. SSH listens on a network port for all connection requests. When a new request is received, SSH asks the connecting computer for a user name and password. If both the user name and password are correct, a secure connection is created between the two devices.

The OpenSSH vulnerability allows an attacker to exploit the user name and password request by injecting certain malicious code. This code causes the SSH server to either crash or immediately grant a system-level session (root access). Without a VA tool running regularly scheduled scans, you might never know this vulnerability exists on your network. A thorough VA scan would identify where SSH software on your network is susceptible to this attack, and you could then take the appropriate steps to fix the problem.

STILLSECURE SOLUTIONS

STILLSECURE BORDER GUARD IPS PRODUCTS: PROTECTION, AUTOMATION, AND CONTROL

Latis Networks developed the StillSecure Border Guard family of IPS products to protect networks from attack and, through a high level of automation, reduce the IT resources required to operate a secure network. The Border Guard family can protect a variety of network architectures and includes:

- **Border Guard Standard** — An *out-of-band* IPS, Border Guard standard works in concert with your existing firewall to block attacks.
- **Border Guard Gateway** — An *in-line* IPS, Border Guard Gateway is ideal for perimeter defense and for securing traffic behind the firewall, such as extranet connections to satellite offices and suppliers.

WHAT IS A VULNERABILITY?

Vulnerabilities are security holes in computer operating systems, system software, and application software. Hackers exploit vulnerabilities to gain control of, damage, or bring down a device on your network. How do vulnerabilities occur? Vulnerabilities are present in network devices for the following reasons:

- **Software is not implemented or adequately tested to minimize security breaches.**
As once-private LANs and networks are connected to the Internet, their network devices and software applications are exposed and are wide open to attack.
- **Devices, such as servers, routers, or desktops, are not configured to prevent security breaches.** *For example, a port might be unintentionally open on a device that is not configured securely. Security knowledge, planning, and testing skills are required to properly configure devices and protect them from attack.*
- **Hackers create new types of attacks that take advantage of previously unknown weaknesses in software.**

- **Border Guard Wireless** — An *in-line* IPS designed specifically for wireless networks. It prevents intruders from compromising your network through notoriously insecure wireless access points.

Border Guard products plug many of the security holes left open by your firewall. Each product:

- Automatically blocks incoming attacks, reducing IT man-hours spent on security and protecting your network 24 / 7 / 365.
- Includes automatic rule updates, ensuring protection and eliminating the need to manually research and integrate the latest attack profiles.
- Learns to gauge the response to suspicious traffic, greatly reducing the number of false positives.
- Provides detailed reporting to satisfy management and auditors.
- Employs an easy-to-use, entirely Web-based interface.

Border Guard products analyze all incoming data packets for embedded attacks. Employing exclusive *Dynamic Attack Suppression™* technology, Border Guard products identify and block the attacks and harmful traffic that would damage your network. Border Guard Wireless provides the full set of features that protect against the threats unique to wireless network segments, and Border Guard Gateway can be used to defend against attacks originating from behind the firewall.

With rule databases that can be updated as frequently as every hour, Border Guard products stop even the latest attacks. Through *Intelligent Attack Profiling™*, each Border Guard installation characterizes the traffic moving across the network and learns how to best respond to anomalous patterns — by terminating the traffic, sending alerts, or allowing access. As a result, false-positives are greatly reduced and the need for manual interaction is minimized. When interaction is required, Border Guard products can notify you via email or pager, send an SNMP trap or execute a custom script. This level of automation drastically reduces the administrative burden on your IT staff.

Each product includes a robust database that logs all network activity, and the built-in, drill-down reporting engine offers a wide range of customizable, actionable reports. The products' at-a-glance, Web-based interface is managed by the StillSecure Console, which lets you control all instances of Border Guard products installed on your network from a single user interface.

STILLSECURE VAM: ASSESSMENT AND MANAGEMENT THAT CONTINUOUSLY ENSURES NETWORK SECURITY

Latis Networks developed its VA tool, VAM (Vulnerability Assessment and Management), to not only identify all network vulnerabilities, but to manage and validate the vulnerability repair process as well. VAM comprises three integrated products:

- **Server VAM** — scans servers, routers, switches, and firewalls.
- **Desktop VAM** — scans for vulnerabilities specific to desktops, laptops, and printers.
- **Remote VAM** — scans Internet-visible servers, routers, switches, and firewalls.

Collectively, VAM products assess and manage vulnerabilities on all segments of your network. Figure 6 shows a typical VAM installation. Each VAM product includes:

- Exclusive *Intelliscan*™ technology, which automatically determines which scan rules are appropriate for each device.
- The built-in VAM *Workflow Management Engine*™.

- Automatic scan rule updates.
- Variable scanning frequency based on device importance.
- Detailed reporting to meet the needs of IT staff, management, and auditors.
- Easy-to-use, entirely Web-based interface.

VAM effectively addresses many of the threats that a firewall is incapable of detecting. Through its regularly scheduled and automated scanning process, VAM identifies any vulnerabilities introduced by mobile devices or through risky practices such as application downloads, instant messaging, and peer-to-peer connections. It also scans for vulnerabilities inherent in third-party applications, which hackers readily seek to exploit.

VAM's comprehensive vulnerability database, which can be updated automatically as often as every hour, enables the system's depth and flexibility of scanning. This library of scan rules includes research and advice to help you determine how to repair specific vulnerabilities.

VAM's built-in *Workflow Management Engine*™ makes remediation an integral part of the VA process. VAM tracks and assigns security vulnerabilities from identification to repair, ensuring accountability.

The OpenSSH vulnerability, discussed previously, illustrates the value of VAM's workflow management features. For example, once VAM discovers the OpenSSH vulnerability is present on a device, it automatically initiates the workflow process and assigns the vulnerability

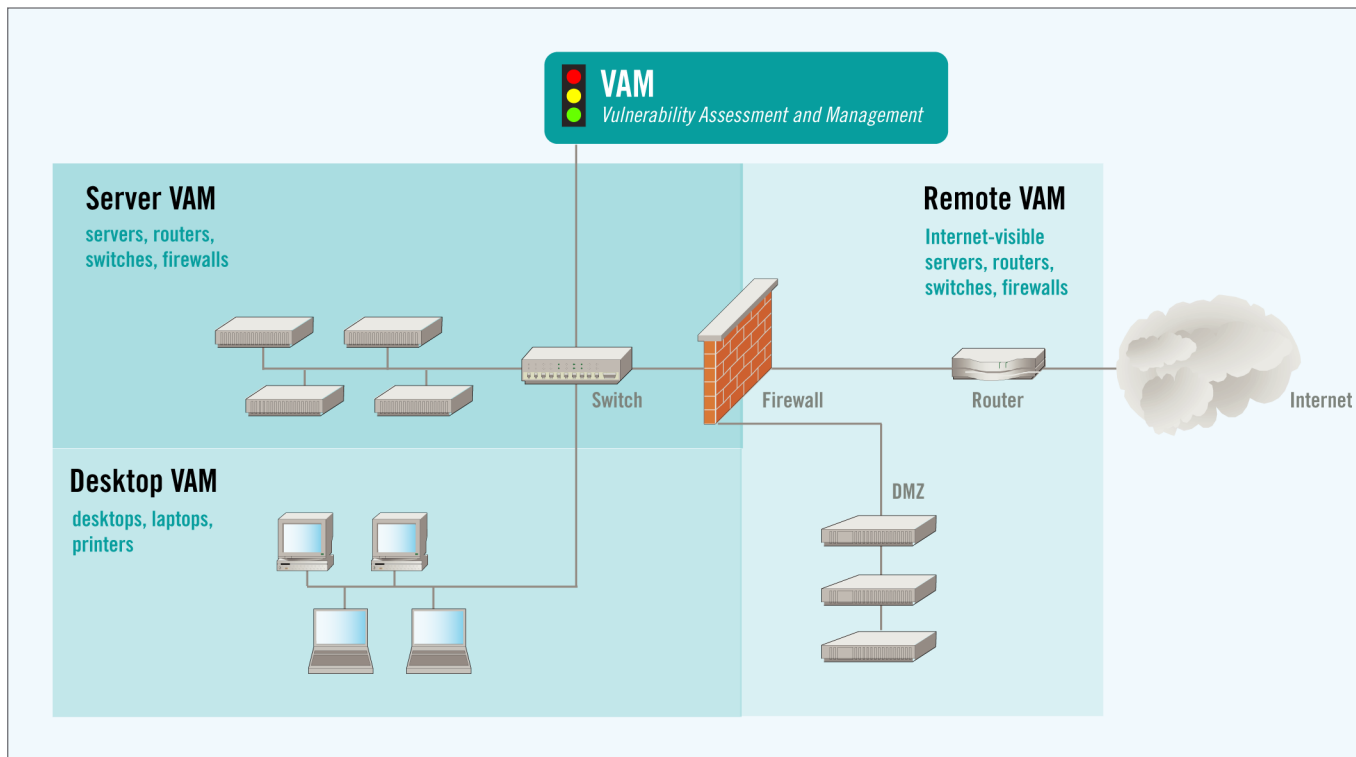


Figure 6. A typical StillSecure VAM installation. All three VAM products can be installed on a single host and managed from one user interface. The shading indicates the coverage each VAM product provides.

to the person designated as the device's primary repairer. The primary repairer is then responsible to ensure the SSH server is fixed within the allotted time as configured by the VAM administrator. Assuming the vulnerability is fixed within this time, the repairer then reports the issue as being fixed and VAM launches a verification scan to confirm the repair. If the vulnerability was properly corrected, VAM logs the resolution and it becomes a part of the permanent record VAM maintains for that host. If the vulnerability was not properly repaired, it is once again made active. Reactivation causes the workflow process to start anew. VAM will repeat this process until it confirms the repair.

As this example implies, VAM logs all scan and repair activities, and includes a comprehensive reporting engine that delivers customizable reports appropriate to specific audiences — board members, auditors or regulators, executives or fellow IT professionals.

VA tools have traditionally been seen as one-dimensional products used and understood only by network specialists. StillSecure VAM introduces much-needed management tools to VA technology, transforming VA from a solely technical process to a business process vital to an organization's success.

CONCLUSION

A firewall alone is no longer sufficient to protect the valuable assets stored on your network. Today, a properly configured and managed firewall represents only a single level in a multi-layered security strategy. A variety of technologies, such as intrusion detection and prevention systems (IDS/IPS) and vulnerability assessment (VA) tools provide the additional security needed to defend against today's sophisticated attacks. Latis Networks' StillSecure line of IPS and VA products provide the best-of-breed security tools designed specifically for security conscious mid-tier enterprises.