Special Report

Reassessing security:

New tools and techniques

By Bob Violino, Network World
Tim Green, Network World

Sponsored By:

ZONE LABS

Aventail™

ForeScout

Produced By:

NetworkWorld
www.nwfusion.com

Reassessing security: New tools and techniques

While there is no such thing as perfect security, the technology is evolving quickly, enabling the fleet of foot to stay a step ahead of those with evil intent.

This Network World special report looks at the changing face of security and some of the new thinking and new tools that are emerging, including vulnerability-management offerings and SSL alternatives to traditional VPNs.

Table of Contents

Containing vulnerabilities

New-style vulnerability-management offerings point out which security flare-ups most threaten your network, and help you stomp them out quickly.

BY BOB VIOLINO
NETWORK WORLD, 10/21/02

Your vulnerability-assessment software is working great, churning out loads of information on your security soft spots. The problem is, it's working a little too well. You've got so much data from network scans that you can't figure out which security concerns are the most pressing, let alone how to address those quickly and effectively.

Enter the emerging field of vulnerability management. Vulnerability-assessment and other security vendors, such as Foundstone, Qualys, Symantec and Vigilinx, offer new products, feature upgrades or services that help you figure out what to do after the scan. These offerings typically identify which vulnerabilities can affect your network and which need immediate attention.

The ability to manage vulnerabilities, not just scan for them, comes none too soon. The number of vulnerabilities is skyrocketing, according to CERT. It reports the number of computer vulnerabilities for the first half of 2002 at 2,148 compared with 2,437 for all of 2001.

"Companies need to prioritize the application of security fixes based on the risk to the business," says Michael Rasmussen, a research director at Giga Information Group.

Services, software combo

State Employees Credit Union, a Lansing, Mich., provider of financial services, has found coupling an outsourced service with vulnerability-management software an effective way to manage increasing network threats. Because it has extended its network in recent years with wireless automated teller machines and Web-based home banking applications, the credit union has watched potential vulnerabilities rise.

Worried that conventional vulnerability-assessment tools couldn't keep up with new threats, and knowing that he couldn't afford to devote a staff member to full-time vulnerability scanning, Alan Darbe, vice president of IS at the credit union, says he decided to try Digital Defense's Frontline service and vulnerability-management tool. With Digital Defense's help, Darbe quickly evaluates reported vulnerabilities to determine the financial and operational risk to the firm. Then, using the vulnerability-management software, he and his team immediately address high-risk threats. The software also updates the fixes as needed.

A managed service and reporting tool is helping the network team at State Employees Credit Union keep vulnerabilities under control, Darbe says.

Previously, the credit union had "no formal way of assessing vulnerabilities" to stop attacks, Darbe says. "Now we're taking a more proactive approach."

For example, a Digital Defense scan showed that an intruder could get access to internal passwords. Needless to say, the credit union fixed that problem.

The credit union spends about $50,000 per year for the vulnerability-management service, which Darbe says has greatly eased and speeded up the process of tracking and fixing security soft spots.

The money on vulnerability management is well spent, he adds, because information security is a priority for the firm, which holds hundreds of millions of dollars of members' savings.

Making the impossible possible

If you're looking for a stand-alone vulnerability-management tool, expect to spend tens of thousands of dollars. Base prices range anywhere from $10,000 to $50,000, with additional charges per IP address, or device, to be scanned (see chart on next page).

The reporting capabilities are worth the investment in vulnerability-management tools, some users say. At Lancaster General Hospital in Pennsylvania, IS Security Manager Terry Grogan relies on PentaSafe Security Technologies' VigilEnt Security Manager vulnerability-management tool to guard against attacks to its mixed network of Unix and Windows NT servers.

The software continuously audits networks and systems for vulnerabilities, recommends corrective action and generates detailed reports nightly across computing platforms.

The hospital uses the product mostly for its reporting capabilities, Grogan says. "It lets me know user activity levels and alerts

me to any significant security events, weak passwords or other concerns. In the past I had to read 110 network logs a day to see if there was any suspicious activity. It was an impossible chore. I looked at only our most critical servers because I didn't have the time to look at anything else," she explains.

At Motorola, security managers had relied on sporadic reports from division-level operations staff for its vulnerability assessments. "In some cases, they did a really good job; in others they were not as diligent. So we had wide disparities in our degree of visibility," says Bill Boni, chief information security officer at the Schaumburg, Ill., company. Now Motorola uses Foundstone's FoundScan software to centralize vulnerability scanning on its global network, which operates in 47 countries and connects 200,000 devices, and to assess the risk of found vulnerabilities, he says.

Using the software, Motorola scans its internal network for vulnerabilities every month and its network perimeter every other week, Boni says. The Foundstone software identifies what threats are the biggest risks. Motorola used to scan the network only several times each year; it was prohibitively costly to scan more often because of the network's vast size, he notes.

With vulnerabilities identified and prioritized, you will also need firm procedures for applying needed fixes quickly (see story, "Practical patch management" http://www.nwfusion.com/supp/security2/patch.html). The team approach works for some. Cincinnati Children's Hospital in Ohio has a 10-person incident response team, with individuals specializing in areas such as virus protection, Internet security, intrusion detection, firewalls and various operating systems. Team members are notified whenever a vulnerability is found, and gather when an exploited vulnerability would have high impact on the company.

"Our policy is if there's any kind of vulnerability - whether it comes in from the help desk or anywhere else - it goes to the [security] team," says Mike Belmont, associate director of IS security at the hospital.

No doubt, as the number of security threats rises, vulnerability management will become a standard part of corporate security strategy.

Tips of the trade:

What to do when vulnerabilities flare up

- Keep an up-to-date inventory of hardware, operating systems and applications, so you can identify which specific vulnerabilities could affect your company.
- Prioritize vulnerabilities based on the potential risk to the business, and address those with the highest level of risk first.
- Develop procedures for quickly applying fixes to particular vulnerabilities.
- Keep track of who is responsible for specific vulnerabilities and whether the correct fixes were successfully applied.

Getting a fix on vulnerabilities

This sample of tools and services fall into the emerging vulnerability- management field.

Vendor	Product	Pricing	Description
BindView	bv-Control	Pricing not available.	Uses vulnerability assessment to find security holes and configuration management to close security holes, enforce security policies and configure systems to best practices. It helps managers audit critical systems, report vulnerabilities, enforce policies and establish security standards.
Configuresoft	Enterprise Configuration Manager 4.0 software	Starts at $995 per server and $30 per workstation.	Provides an enterprise view of security settings for every Windows NT or higher server and desktop in a network; lets administrators assess systems for vulnerabilities and compliance with security policies; can centrally change configurations on any machine or group of machines to correct problems discovered by vulnerability scanners.
Digital Defense	DDI Frontline 2.0 service and software	Based on the number of IP addresses assessed and network size and complexity	Provides recurring external and internal vulnerability scanning and penetration testing; lets managers track the resolution of vulnerabilities.
Foundstone	FoundScan software and service	Starts at about $30,000, based on the number of scanned devices and IP addresses. It is also available as a managed service.	Software measures and resolves security vulnerability risks in traditional networks, wireless access points and Web applications; provides network mapping, integrated remediation management, a continually updated vulnerability database, short- and long-term trend analysis and Web-based reports.
nCircle Network Security	IP360 Network Exposure Management System	Pricing not available.	Provides network monitoring, alerts, reporting and vulnerability responses. One feature automatically blocks traffic to network devices with newly discovered security flaws.
Mazu Networks	Mazu Enforcer software	Starts at $32,000, based on configuration options.	Lets companies monitor network traffic for vulnerabilities; includes reporting tools.
PentaSafe Security Technologies	VigilEnt Security Manager 3.1 software	$10,000 base; agents are priced per platform ($1,100 for a Windows NT agent, for example).	Continuously audits networks and systems for security vulnerabilities; lets managers identify vulnerabilities, take corrective action, and generate detailed reports across multiple platforms.
Predictive Systems	Information Sharing and Analysis Centers (ISAC) services	Starts at $50,000 per year for 25 users.	Based on ISACs, a shared database of security threats, vulnerabilities, incidents and solutions. "Vulnerability matching module" lets managers know if a particular vulnerability matches a piece of equipment, operating system or application within their company, and determine how critical the threat is.
Qualys	QualysGuard	Ranges from $995 for one IP address to $59,995 for 256 IP addresses.	Identifies and eliminates network vulnerabilities through a Web-based architecture; sends IT managers fixes and patches based on the severity of vulnerabilities.
Symantec	Enterprise Security Manager 5.5 host-based application	Pricing not available.	Host-based application provides security policy compliance management, including the discovery of policy deviations and vulnerabilities. It identifies systems that are vulnerable to a specific threat, and helps managers prioritize fixes.
Vigilinx	IntelliShield service	$40,000 to $100,000 yearly fee, depending on number of users.	Continually monitors a database of threats and vulnerabilities; lets managers track vulnerabilities on more than 5,500 IT products.

Source: Network World

Fortifying the firewall

Today's world of open network access means rethinking the role of the firewall.

BY BOB VIOLINO
NETWORK WORLD, 07/29/02

Obviously, the firewall can no longer stand alone against all nasty intrusions. The chances that a virus or other ill-intended probe will penetrate a company's firewall rises almost daily, especially when ports are opened to give people outside the physical perimeter access.

Not that most network executives can even define the perimeter any longer. The distinction between what's inside and outside the corporate realm has vanished. In its stead has come modified perimeter architectures, built using more advanced firewalls that follow tenets of a security model for today's realities (see story, "Time for new security model").

When network managers began deploying firewalls as security tools a decade ago, they could easily define the network perimeter. Most people who had access to corporate networks worked on desktop computers in the main office; external links to business partners were virtually nonexistent. A simple firewall-based demilitarized zone between the private and public network made sense. But today's practice of allowing access to corporate data to anyone who might need it - mobile workers, telecommuters, business partners, suppliers - from wherever they are over wired or wireless links turns that sensible decision into a foolish one.

To provide a high level of access, companies punch holes through the firewall barrier and hide data from the firewall's view by using technologies such as VPNs and encryption.

This cripples firewalls - as they were originally designed - and keeps them from protecting companies against attacks, high-tech vandalism, theft of data or other security breaches.

Mirrored firewalls provide some comfort to Don Hoffman, who watches over extended enterprise network as director of IT security for The Mony Group, an insurance and financial services firm in New York.

On the attack

Data from the Computer Security Institute (CSI) shows the number of security breaches, already high, has grown in the past year. CSI's 2002 Computer Crime and Security Survey, released in April, indicates that 90% of the 503 participating U.S. organizations detected computer security breaches within the previous 12 months, up from 85% in the previous year. Eighty percent of the organizations said they suffered financial losses because of computer breaches, up from 64% the year before.

About 75% of survey respondents said their Internet connection was a frequent point of attack, compared with 33% who cited their internal systems as such. Forty percent detected system penetration from the outside, 85% detected computer viruses and 70% of those attacked reported vandalism.

"Companies need to provide a lot of access to their partners, customers and employees today, and they're using technologies like Web services and extranets more frequently. All of this points to the fact that perimeter security by itself is no longer adequate," says Laura Koetzle, security analyst with Forrester Research.

"Businesses need to have firewalls, but there must be various layers of firewalls as well as clear policies that determine how these firewalls interact," Koetzle says. "Having nothing protecting the middle of the enterprise is a sure way to let someone come in and do maximum damage."

In a survey of 50 IT managers conducted by Forrester earlier this year, "openness of our network" was the second most common response given (after viruses) when managers were asked to name their biggest IT security concern.

On the defense

Firewall vendors such as Check Point Software, CyberGuard, Network Associates, Secure Computing and Symantec are trying to address the needs of increasingly open networks by bolstering firewall capabilities. For example, they are developing directory-based firewalls that issue access rights after a user has logged in and logical firewalls that separate groups within an organization. Other initiatives include:

- Designing firewalls to work more easily with intrusion-detection systems and antivirus software, or embedding those capabilities in firewalls.
- Offering firewall protection for equipment such as home office computers and wireless handheld devices.
- Providing firewalls that are embedded in components such as network cards, so individual devices on a network can be protected against internal and external threats.
- Offering filtering levels so firewalls can better determine the threat of specific messages or applications being sent.

Network executives taking advantage of new ways to design firewall-based perimeters are experiencing good results. The Mony Group has installed mirrored firewalls to protect its perimeter. If one firewall fails, another stands in the way and ensures protection, says Don Hoffman, director of IT security.

"This makes us less vulnerable if we're attacked," Hoffman says. "It used to be there was a single point of failure." Still, Hoffman pressures firewall vendors to do a better job of getting fixes out when weaknesses in firewalls are exploited or when new threats emerge such as logic bombs or spam. "That's an underlying issue with security. We know a vulnerability exists, but we have to wait for the patches or upgrades," he says, adding, however, that vendors are improving. "They used to be a week behind the problems, and now they're two or three days behind." Despite growing sophistication, firewalls aren't enough, Hoffman says. Mony also uses VPN, IDS, authentication and other technologies to secure its corporate network. Plus, Mony is exploring whether internal firewalls would be useful in protecting particular departments and even individual devices.

Of course new firewall technology is only a partial solution. Policies must also be created. OSG Tap & Die, a tools manufacturer in Glendale Heights, Ill., uses Secure Computing's Sidwinder firewall with a built-in VPN to connect via the Internet with its parent company in Japan and offices in Europe, and to selectively provide data access to workers in the field.

"When a salesman working in a hotel room needs to get access, he can come in through the firewall using the client VPN and I [can verify] he's actually the salesman through authentication," says Mike McKenna, IS manager at OSG. However, McKenna is cautious about granting employee requests to transfer data to and from Web sites blocked by the firewall. "The Swiss cheese effect comes into play where you're creating holes in the firewall," he says. "We can't just make random changes in the firewall to accommodate all the requests."

New policies really come down to common sense, says Tom Warfield, systems administrator in charge of networking at government contractor AST in Lawton, Okla.

"We have a simple rule, if you're not using something, shut it off," he says. It might sound obvious, but "people tend to leave everything - desktop computers, laptops or other systems - turned on," and that invites trouble that the firewall can't always block.

Firewalls and then some

With firewalls no longer able to be a solitary guardian against all potential threats, network executives "need to look at different ways to take the load off the firewall," says The Mony Group's Hoffman.

Hoffman says Mony is using technology such as intrusion-detection systems at the front and back ends of its firewall to help control access to internal networks and data. He says most firewall vendors will soon begin building intrusion-detection capabilities into their products, if they're not already (see story, "The promise of all-in-one security" http://www.nwfusion.com/supp/security2002/allinone.html).

firewall vendors must work with other security product developers to integrate their products, says Tom Warfield, a systems administrator who's in charge of networking at government contractor AST in Lawton, Okla. Warfield likes that his firewall supplier, Check Point, does so. "Check Point has allowed other vendors to integrate their products into the firewall, and it ensures that these products meet industry standards and certification," Warfield says. He cites one such partnership, which integrates Symantec's Norton AntiVirus products with Check Point's Firewall-1.

"The Norton software works well with our firewall," Warfield says. "In the past we had a lot of problems with people downloading viruses that spread through the company." The firewall/antivirus combination has been an effective solution, he says.

Making way for the new VPN

Secure Sockets Layer's arrival on the VPN scene has IP Security-based VPN vendors rethinking their product portfolios.

BY BOB VIOLINO
NETWORK WORLD, 12/23/02

VPNs based on the IP Security protocol have held a grip on the market, but an alternative using Secure Sockets Layer is steadily gaining ground.

Few people familiar with network security consider SSL a wholesale replacement for IPSec as a VPN protocol. But SSL proponents say that protocol is less expensive and easier to deploy when workers need remote access to Web applications such as e-mail and corporate intranets. And now, traditional IPSec VPN vendors are scrambling to add SSL to their product mixes to meet demand.

Browser-based SSL VPN products differ from IPSec VPN wares in that they do not require companies to install VPN client software on remote devices. Users who can authenticate to a company's network can make a secure connection from any laptop or desktop PC with a browser. That's because SSL firewall ports generally are kept open, so firewalls need not be reconfigured to provide access.

With IPSec VPNs, each remote device must run client software, which must be updated as necessary. Also, firewalls and the IPSec devices must be configured in tandem to allow network access.

SSL in the market

Market researchers predict that worldwide sales of SSL-based VPN gear will increase during the next several years. Infonetics Research expects market growth from about $56 million this year to an estimated $840 million by 2005. However, the firm says, IPSec products will continue to make up a huge share of the VPN market. Infonetics pegs sales of IPSec VPN and firewall hardware at $1.5 billion this year and $2.5 billion in 2005.

"SSL will address all those [remote workers] who don't really need access to many applications. It's a simple way to give them access to things like e-mail and benefits and payroll information. Those users who need access to a broad range of applications that are not all Web-based will require IPSec clients," says Jeff Wilson, executive director of Infonetics.

But the proliferation of Web-based applications - and the growing need for remote access - has turned SSL into a hot topic - a necessary development for traditional IPSec VPN vendors.

Check Point, which unveiled an SSL-based or "clientless" VPN in July, says SSL is ideal for companies that need to exchange data with business partners via extranets but don't want to install VPN clients. IPSec VPN vendors such as Nortel and SonicWall agree. Nortel introduced the Alteon SSL appliance in September; SonicWall began offering SSL products when it acquired Phobos two years ago. In the meantime, NetScreen Technologies says it's evaluating an SSL offering through possible partnerships.

Other IPSec VPN proponents, such as Symantec, still are evaluating how to fit SSL into their product lines. The holdup in part stems from these vendors having more or less viewed SSL as a competing technology. But as demand grows for clientless VPN connections, logic dictates that vendors add SSL-based products to their lineups.

Smaller vendors that have recognized the need for SSL VPN wares include Aspelle, Aventail, Neoteris and Whale Communications.

SSL by design

Some companies are finding they want both SSL and IPSec VPNs. Quad/Graphics, a Pewaukee, Wis., printing services company, provides connectivity for the limited number of employees who need access to production systems and other non-Web applications via an IPSec-based VPN from Cisco. But it has given the majority of employees remote intranet and e-mail access via an SSL-based VPN using Whale's e-Gap Remote Access Appliance.

Before Quad/Graphics installed the Whale SSL product four months ago, most employees didn't have a remote-access option at all. "With 10,000 employees potentially wanting to get access from home or on the road, we didn't want to have to install 10,000 [VPN] clients," says Damian Drewek, director of technical services at Quad/Graphics. "We knew it would be a maintenance nightmare."

Whale's SSL appliance runs on a server in the company data center. Using this clientless approach, the company can provide secure connections without having to rewrite applications on those thousands of end-user devices, Drewek says.

Deloitte Consulting in New York also uses a combination of SSL and IPSec VPNs. Most of the firm's employees access the corporate network while in the field via an SSL-based VPN from Aventail. Deloitte limits the use of IPSec VPNs, which it bought from Nortel, to those people who need to access applications running in the firm's four data centers.

Larry Quinlan, Deloitte CIO, likes SSL VPNs for their ability to traverse firewalls without the need for firewall reconfiguration. "That's important because the security department is not eager to reconfigure the firewall," he says.

On SSL's downside, Quinlan says, is the typical limitation to Web applications. But IPSec has its drawbacks, too - it doesn't easily traverse some firewalls, which can cause problems for mobile workers who need to get access from hotels or client offices, he adds.

SSL's limitation to Web applications has given some users pause. Divine, a professional services company in Chicago, mainly uses an IPSec VPN from NetScreen Technologies. Many of its remote workers are consultants who need broad application access, says Chuck Horvat, director of network services at Divine.

Divine hasn't found a need for SSL VPNs, Horvat says. Instead, the company relies on an application's Web front end and built-in SSL encryption. Microsoft Outlook is a case in point. Remote workers are authenticated with a user identification and password to access e-mail and the corporate directory.

"For us, it's best to have an IPSec VPN pipe because of the applications people need to access," Horvat says. "They can get to e-mail via SSL, but the majority of people still want to do things other than e-mail. Either solution is great, but each for very specific requirements."

SSL in the end

While many say SSL will replace IPSec for VPNs to Web applications, most industry watchers say the two types of VPNs will coexist, with plenty of room in the market for both.

Infonetics' Wilson sums it up: "They will work together to build a bigger remote access market."

Violino is a freelance writer covering business and technology. He can be reached at bviolino@optonline.net.

What's at stake?

Summary:
Traditional VPN vendors must figure out how to offer Secure Sockets Layer VPN products.

Opponents:
SSL VPN vendors include Aspelle, Aventail, Neoteris, Netsilica and Whale Communications. IPSec vendors include Cisco, NetScreen Technologies, Symantec and WatchGuard Technologies. Check Point, Nortel and SonicWall support both.

Outlook for resolution:
Each type of VPN serves a useful purpose.

User impact:
Secure remote access for Web and e-mail connectivity becomes more feasible with SSL VPNs.

SSL catching up to VPNs in popularity

Users adopt Secure Sockets Layer for remote access.

BY TIM GREENE
NETWORK WORLD, 02/18/02

A growing number of organizations looking for a fast, secure way to link remote users and business partners are turning away from traditional IP Security-based VPNs and toward products and services based on Secure Sockets Layer technology.

The reasons are many: Browser-based SSL alternatives require little or no software on remote PCs, and in most cases any PC with a browser can be used to make the secure connection, as long as the user can authenticate to a central server. And SSL firewall ports that the traffic uses are generally left open, so firewall reconfiguring is usually unnecessary. The idea is that SSL's simplicity translates into an easier installation and long-term cost savings because of simpler ongoing support.

Yo.net and Aventail are among the growing number of vendors delivering VPNs without using the collection of well-known IPSec protocols.

Conversely, Internet-based IPSec remote access VPNs require software on each remote PC that has to be installed, configured and updated for the VPN to work properly. Firewalls also must be configured in tandem with the IPSec devices to let IPSec traffic pass.

Early last year Toronto specialty clothing maker Accolade Group realized it needed a simple, secure Internet connection so employees in a sales office could reach servers in the main office. The company chose Yo.net because it could set up the link quickly.

Yo.net shipped a pair of servers, one for inside and one for outside Accolade's firewall, along with client software for the remote users' PCs, and Accolade was off and running. "This fits our needs, the price is right, we move on," says Harvey Ngo, Accolade's IT director.

When Rhode Island health consortium Lifespan needed to give hundreds of doctors access to patient files while complying with federal privacy rules, it chose service provider Aventail to set up its network.

"This is probably about as compliant as it's going to get right now," says David Hemendinger, CTO of Lifespan, about the privacy the service offers via SSL cryptography.

Simplicity was key at Alexander Randolph. The application hosting vendor needed to automate customer access to its human resources application, so it chose remote access equipment from Netilla because it required no modification of Alexander Randolph's customers' equipment.

"We can take people on and off this system very quickly. It's as easy as changing their name and password," says Walter Hill, a senior partner at Alexander Randolph.

While users seek these alternatives for the benefits they offer, they also do so to avoid the complexities of setting up and maintaining IPSec VPNs.

"[Aventail's Extranet service] gets me through most firewalls without requiring reconfiguration," says Ralph Rodriguez, CIO of eXcelon, a consultancy in Burlington, Mass. That's important because eXcelon's consultants work from their customers' sites and rely on their customers' networks to tap servers at eXcelon's headquarters.

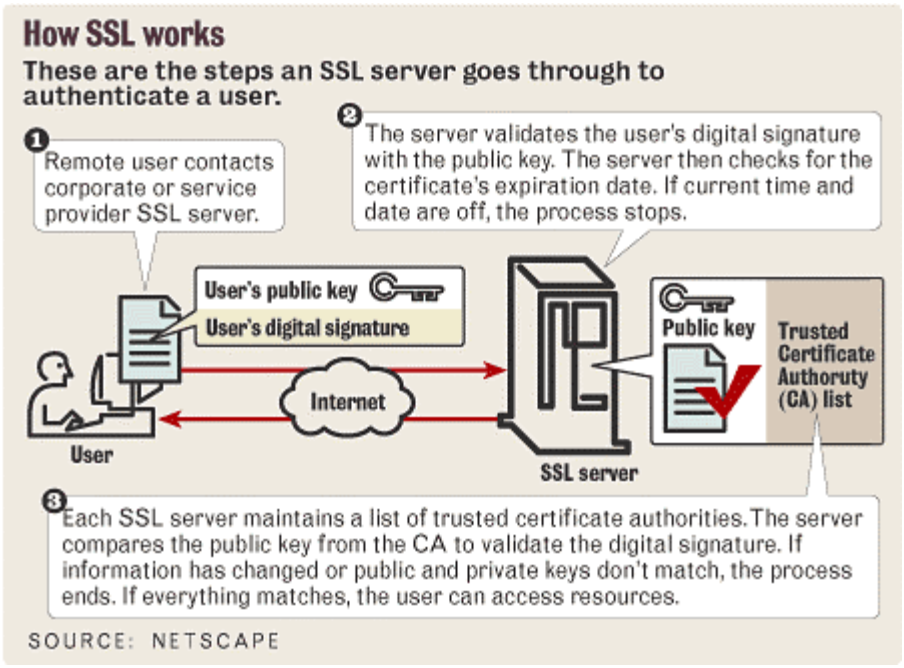
Despite the ease of configuring the technology, the security offered by these SSL-related VPNs can meet even stringent military standards. The Surgeon General's office for the Air Force uses such equipment from provider uRoam to enable remote-control access to PCs in its Virginia headquarters.

While the security is good, SSL-based remote connections don't fit all needs, says Kent Dallas, principal in Dalliesin, a VPN

consultancy in Alpharetta, Ga. "If you are just using e-mail and want to secure it, buy an SSL card for an Apache server," he says. But, for example, gear from vendor Neoteris won't support file-sharing applications, so an IPSec VPN might be the better way to go if you need to share files.

And SSL services don't work with applications that are not Web-enabled, hence the need for Lifespan to buy a second Aventail service based on IPSec. About 20% of Lifespan's users need the IPSec option for legacy applications, Hemendinger says.

Users should be wary of the authentication methods they use for granting access to these SSL VPN alternatives, Dallas says. "Most SSL requires a password only, so you need strong, nonguessable passwords. Most SSL implementations do not do client [digital] certificates. Most IPSec implementations use digital certificates," he says.



And because users don't control all the gear that runs the remote access network, they must be prepared for failures beyond their control, Dallas says. "If they have problems, would users still be able to connect? You need to look at what you do if the provider fails and how long it would take you to get back up, either with them or via some backup," he says.

These IPSec alternatives are not cheap. Yo.net equipment costs $3,500 per site plus $150 per client. Some VPN products cost less, but users say cost was not the major factor in their decision.

"We looked at it as a cost of doing business," Hill says. "We simply had to automate [our client interactions]."

"I really need developers in the field to access our intellectual property," Rodriguez says. "It would be worth it to use Aventail even if it did cost more [than an IPSec alternative]."

RELATED LINKS

Buyer's Guide: Vulnerability-assessment tools
Vulnerability-assessment tools edge toward usefulness in large networks.
Network World, 02/04/02
http://www.nwfusion.com/reviews/2002/0204bg.html

Network World Security Report: Practical advice for locking down the enterprise
A special report detailing tips and techniques for software patches, vulnerability warnings, password problems and security device management.
Network World, 10/21/02
http://www.nwfusion.com/supp/security2/

Network World Security Report: Defending the extended enterprise
Are firewalls enough? Should you invest in a bundled security product? What type of security planning should you undertake? We explore what it takes to secure your changing enterprise in this special report.
Network World, 07/29/02
http://www.nwfusion.com/supp/security2002/

Technology Insider: Network-based intrusion-detection systems
Network World, 6/24/02
http://www.nwfusion.com/techinsider/2002/0624security.html

VPN research center
The latest news, reviews, how-tos and more.
http://www.nwfusion.com/topics/vpns.html

VPN Buyer's Guide
Tasked with purchasing and implementing a VPN for your corporate network? We take a look at the big players and latest trends, from IPSec-based VPNs to SSL-based alternatives. We also have a 115 product guide to help you make an informed decision.
Network World, 10/28/02
http://www.nwfusion.com/reviews/2002/1028bg.html

Products rely on SSL rather than IPSec.
Network World, 01/21/02
http://www.nwfusion.com/news/2002/0121ssl.html

Request a reprint of this report.