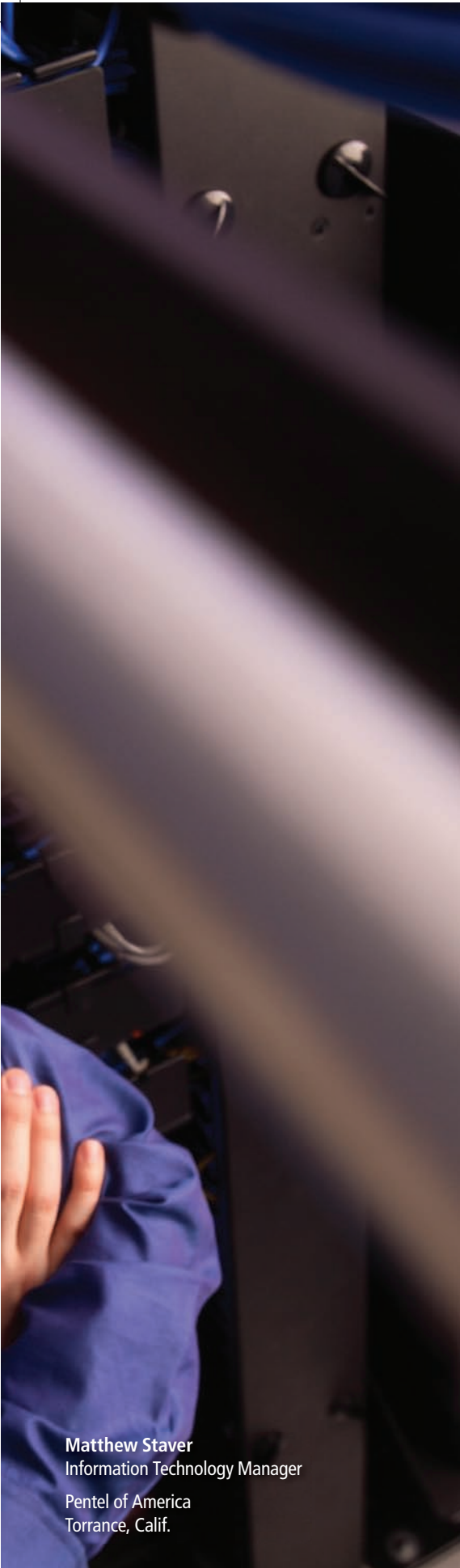




Battling Bad Guys at the Gateway

A solid layer of defense safeguarding your gateway can ensure that threats never make it past the network front door.



Having a traditional static firewall at your network gateway may have offered enough security at one time. However, times — and threats — have changed.

Today, companies of all sizes have to defend themselves against the growing range and volume of network risks — everything from viruses, worms and bots to rootkits, Trojans and other malware.

IT managers want as many of these threats as possible blocked before they reach desktop or notebook systems. The idea is to minimize staff time spent reacting to threats and to avoid the danger of users not making the right response to client-level security prompts.

Ensuring that URL requests and HTTP (Hypertext Transfer Protocol) Web traffic is filtered not only for threats but also for productivity and bandwidth-wasters is also important. And IT wants to check for activity or content that might violate compliance or other regulations.

Even when the network appears to be running smoothly, IT managers need gateway security that watches for “information leakage.” This includes outbound traffic containing sensitive information, viruses, spam or other signs that there’s spyware or some other problem in the network.

What’s more, this security has to be done in a way that, once installed, requires minimal administrative time, particularly in sub-enterprise-size companies. It also needs to let IT be able to demonstrate compliance to any relevant government or industry security mandates.

Pentel’s Gateway Solution

One company that has updated its gateway security solution to address today’s network threats and related IT concerns is Pentel of America (www.pentel.com), headquartered in Torrance, Calif.

Pentel manufactures and sells high-quality writing and drawing instruments and related products including automatic pencils, leads, erasers, nonrefillable rollerball pens, refillable ballpoint pens, markers and correction fluids.

While the company is in the business of making writing instruments, it relies on network infrastructure and the Web to keep operations rolling smoothly. This includes its sales within the business-to-business and retail channels like office-supply superstores, supermarkets and other retail outlets.

“We’ve got three sites in the United States, plus one in Mexico, connected by T1 lines to our Torrance facility,” says Matthew Staver, information technology manager for Pentel’s U.S. locations.

“We have several dozen servers, running Microsoft Exchange, Oracle’s E-Business Suite, intranet Web server and applications for vendor-managed inventory [VMI] along with electronic data interchange [EDI],” Staver says.

“For our employees, we have about 200 desktop computers. For warehouse management, we have Intermec handheld wireless computers for bar code scanning and bar code label printing.”

Over the past year or so, it became clear that Pentel’s original gateway security solution was no longer adequate.

“We were getting over 700,000 spam messages a month, plus viruses, spyware, phishing and other attacks,” recalls Staver. “The product we were using for URL filtering wasn’t working very well, and the renewal cost was expensive — especially for a single-task solution.”

Staver notes that it was time to renew or replace the primary software licenses. The firm’s hardware was getting old enough that he was seeing performance problems, as traffic levels continued to grow. ▶

Matthew Staver
Information Technology Manager

Pentel of America
Torrance, Calif.

The firm also had a server-based e-mail scanning gateway, which worked well, but handled only SMTP (Simple Mail Transfer Protocol) e-mail.

“We were looking for a converged solution that would give us more bang for the IT buck,” says Staver. “We needed to filter spam and other e-mail threats along with Web traffic — all while not taking up a lot of time being managed.

“We have a fairly small IT shop and our Oracle applications take up most of our time,” Staver adds. “So the more systems that run with little or no administration, the better. And we wanted a gateway-level solution to block unwanted content before it got to user inboxes on our mail servers, or to desktops or other servers.”

Pentel’s new gateway security solution, a Trend Micro InterScan Gateway Security Appliance (IGSA), is addressing IT goals including low administrative overhead and reduced facilities footprint. The IGSA offers an all-in-one gateway defense from multiple threats at the Internet level.

“Using the browser-based user interface, I had all our policies set up within twenty minutes,” Staver notes. “I haven’t really had to touch them since, except when I need to open up access to a Web site that’s in a category we block.”

The firm now has a converged gateway security solution that’s easy to manage and covers plenty of bases. “Even though we’re not a huge enterprise, we needed enterprise features,” Staver adds. “The Trend Micro gateway solution includes a robust feature set with all the capabilities you might find in a bigger solution.

“By having spam, viruses, phishing and blended attacks blocked at the gateway, we’re improving productivity,” says Staver. As an added benefit, “We’ve gone down from 6U of rack space plus a tower for our old inbound, outbound and URL filters, to a single rack unit device with 66 percent less power and cooling requirements.”

Stopping Threats at the Gateway

“Every company needs gateway-level protection,” says Paul Stamp, principal analyst for security at Forrester Research Inc.

Part of the challenge, according to Stamp, is that “security budgets are flat or declining, while requirements to support compliance, mobility and collaboration are increasing.”

The good news, says Stamp, is that vendors are making gateway security solutions “easier, less expensive and available to companies that previously had access to only some security features.

“For example, intrusion protection or content filtering used to be only the domain of large enterprises,” he says. “Now they’re commonplace in companies below that size.”

Today’s ramped-up gateway security starts with more intelligent firewalls that go beyond the traditional static inspection and VPN (Virtual Private Network) access. They are now taking closer-than-ever looks at packets.

“Stateful packet inspection [SPI] is a necessity,” says Paul Kaspian, product marketing manager, Check Point Software Technologies Inc. “The firewall understands ‘state,’ based on the last three packets. It has a sense of what transactions and

connections are being attempted, or that it saw the same type of transaction 10,000 times in the last few seconds.”

Today’s gateways can also do Network Address Translation (NAT), allowing the computers on your company networks to share a single public IP address. This provides another layer of security from Internet malefactors trying to break through your network.

Gateway Security “Beef-Up”

“Companies are beefing up their gateway security in general,” reports Brian Krause, security specialist at CDW. “There’s a lot of demand for Web filtering — the ability to block access to inappropriate or counterfeit URLs, and to be able to filter and block malicious code from getting to users’ computers.

“Web filtering is also useful for compliance, to save network bandwidth and promote user productivity,” Krause adds. “Management wants to know what sites users are going to or trying to go to when they shouldn’t be.”

Additionally, “We’re seeing huge interest from both enterprises and SMBs [small- and medium-sized businesses] in getting gateway-level intrusion-protection systems [IPS],” he adds. “A lot of SMBs are getting UTM [Unified Threat Management]-type firewalls, which do several security tasks. So adding IPS functions to them isn’t a much bigger investment.”

CA’s Secure Content Manager, for example, provides antivirus, antispyware and e-mail content filtering, along with URL (Web content) filtering. Juniper Networks also offers high-end firewall and intrusion detection/prevention products.

Juniper’s SSG firewall gateways include WAN connectivity and routing, with models available in sizes appropriate to small branch office and small-business deployments up through medium- to large-sized branch offices and stand-alone medium-sized enterprises.

Integrated gateway security appliances from Check Point include the UTM-1, intended for 100- to 1,000-user, medium-sized businesses and branch offices with up to 100 users, and the VPN-1 UTM Edge, for 1- to 100-user remote and branch offices, according to Check Point’s Kaspian.

Both products include Check Point’s standard UTM feature set including firewall, intrusion prevention, VPN and antivirus. Check Point’s UTM-1 appliances are expandable with capabilities such as URL content filtering and SSL VPN (Secure Socket Layer Virtual Private Networking) preinstalled, and easily activated when the user purchases a license key.

“Having everything in one integrated appliance and being able to expand its capabilities by simply unlocking already-installed features avoids the worry of ‘What happens when I install something new?’” Kaspian points out.

Making Gateway Security Easier

Simplifying and streamlining the management of today’s gateway security is as important as the security itself. “Our IGSA handles all updates automatically,” states Bill Hansey, global product marketing manager, Trend Micro. “IT can schedule when they are to be done.”

Another growing requirement for gateway security, notes Check Point’s Kaspian, is management reporting. “I don’t

hear as many customers saying ‘I need to stop viruses at the gateway.’ Many of them have traditional security protection deployed, but are struggling with managing a complex security infrastructure.

“They have site-to-site VPNs and other features. They’re asking, ‘How do I bring new sites online, integrate them into my existing security and manage them? How do I update everything?’”

With Check Point’s centralized management infrastructure, says Kaspian, “A company can install a UTM-1 in a main site, and VPN-1 UTM Edge appliances in smaller ones, and create a policy for the entire organization which gets pushed to all sites. This lets them seamlessly update antivirus, intrusion prevention and antispam signatures from a single site.”

Guidelines and Policies

“Gateway security starts with guidelines, like ‘Employees will not access unauthorized Web sites or download/stream multimedia.’ Or ‘Incoming e-mail must be free of viruses,’” says Mark Albert, product manager for CA security products.

These guidelines are then used to select products which can implement them as policy rules, for example, to scan inbound and outbound e-mail for viruses, bad URLs or malware. “Businesses do want content-filtering guidelines,” notes CA’s Albert.

“Our best-practices advice is observe, create and implement,” he adds. “First, you have to observe your network activity, such as how many users are being blocked; are trying to access blocked Web sites; how much spam has been stopped in the past two hours; and so on.”

A lot of companies don’t want to enforce policies that restrict business; and too strict a policy can do that, Albert acknowledges.

“We advise businesses to put policies in place and see whether they’re too strict. Once you know your network, you’re in a better position to create policies that are appropriate,” he says. “For example, if there’s a site that everybody needs to go to, you don’t want to block access.

“Second, you have to create policies that mesh well with your business needs,” Albert adds. “Decide what you want to specify when, such as based on user-group and time of day. For example: ‘Everybody can Web-surf during lunch, and we know these groups usually have lunch at these times.’

“And third, implement those policies.”

In terms of spam filtering, he says, “IT administrators need to be able to block spam without creating too many false positives. And you want to let users check their spam, and self-manage their spam. We let them log into a Web-based quarantine manager and create their own allow/block list, which IT can override if need be.” ■

Let CDW assist with project-based consulting.

Talk with your account manager today.

Protecting the Gateway

Why businesses should care:

- Network and gateway security is still one of the best ways to protect the corporate network, according to Forrester Research security analyst David Friedlander. “It is the organization’s first line of defense to keep malicious code out of the network.”
- The gateway is a business’s first line of defense in a network and is the desired point of entry for hackers.
- Unrestricted browsing exposes corporate environments to common sources of malicious code attacks. Although virtually all companies run antivirus software, nearly 80 percent have nonetheless been attacked by viruses, worms and other malware, according to the FBI.

What businesses can do:

- Install a firewall appliance, configured with security policies and alert when new outbound action is attempted.
- Develop a comprehensive gateway hardware security solution that combines antivirus and antispam, authentication, intrusion detection and prevention, firewall and VPN services, and URL content filtering.
- At remote office/branch office locations, deploy integrated routing solutions that combine firewall, VPN, routing and switching functions in a single appliance, and support new services such as VoIP (Voice over Internet Protocol) and videoconferencing with high-strength security.

