Gateway Security: There’s No Silver Bullet

Securing the network requires understanding internal and external threats and implementing a multilayered approach.
According to the 2006 CSI/FBI Computer and Crime survey, even though 97 percent of the enterprises surveyed used antivirus software and 98 percent used a firewall, 65 percent had suffered a virus outbreak or incident.

That’s no surprise since Carnegie Mellon University’s Computer Emergency Response Team (CERT) reported that the total number of vulnerabilities found had increased significantly between the years 2000 and 2006 — from 1090 to 8064 vulnerabilities — and that the number of incidents reported has also increased exponentially.

No Single Solution
As a result, IT organizations are faced with multiple regulatory requirements and evolving threats. But there’s no silver bullet for securing a network. That highly sought after single solution simply doesn’t exist, says Jason Wright, product manager at TippingPoint (3Com).

“The people who are creating them are constantly evolving the threats to get around current security systems, so what you need to have is a multilayered defense approach, which includes a basic firewall, an intrusion prevention system (IPS) and an antivirus system,” he says.

In addition, policies and procedures that are considered best practices, such as changing passwords on a regular basis and patching systems, will help organizations develop multiple layers of defense.

Getting Proactive
“A recent FBI survey puts internal network threats at about a 50/50 ratio of probability with external threats. More attacks these days are coming from internal networks than they are from external sources,” says Jon Kuhn, director of product management, SonicWALL. “So a proactive strategy would be to protect the perimeter but also look at what’s happening with the internal systems.”

Steve Hargis, director of solutions marketing for Enterasys Networks, agrees. “It’s important to have a proactive posture when it comes to security. Generally, attacks target the larger deployed systems out there because there’s more opportunity to spread a malicious attack,” he says.

Hargis continues, “It’s important that the IT organization monitors this closely. The more you can be proactive in minimizing the opportunities for people to take advantage of these vulnerabilities, the more secure your environment is going to be.”

Integrated Collaboration
This type of comprehensive approach involves having collaborative systems that are integrated, says David Graziano, manager, regional sales, Federal AT security at Cisco. “Some customers have purchased point solutions to solve a particular problem. So they bought a firewall to make sure that they’re blocking their perimeter, and then they’ve put in an IPS to monitor that,” he says.

Graziano adds, “One of the challenges facing IT professionals today is that they’re overwhelmed by the amount of data they have. They need to create a self-defending network.” That’s a combination of integrating key security components such as a firewall, virtual private network (VPN), and network access control (NAC) with intrusion prevention.

Once you’ve done that, Graziano says, you can actually start to be more collaborative. “You can have them talk to one another, so that you can make more accurate decisions with less data.”

Don’t Forget Reactive Defense
While proactive systems are key to preventing known attacks, you also need to be able to react to things that are going to circumvent any proactive measures you have in place. “There are certain threats that are difficult to proactively protect against, such as zero-day attacks,” says Hargis.

A zero-day (or zero-hour) attack is a computer threat that exposes undisclosed or unpatched application vulnerabilities. They take advantage of computer security holes for which no solution is currently available. “Since there’s no knowledge of the attack historically, there are no valid signatures that can quickly recognize the attack and prevent it from propagating. So there’s no proactive measures to put in place to prevent that attack from causing harm,” says Hargis.

“Developing a proactive and reactive approach that’s integrated into a single architecture is the best methodology for an IT organization to adopt,” he adds.

TippingPoint’s Wright agrees. “It’s difficult to keep systems patched and updated in a timely manner. Sometimes there’s not even a patch available. At that point, you’re heavily reliant on an IPS to look out for malicious traffic and prevent it from reaching vulnerable systems.”

Detecting Bad Behavior
An IPS is an inline device that inspects all traffic in real time and compares it with existing threats. There are certain rules and assumptions about the way traffic is created and formed. IPSs use deep packet inspection, which offers organizations the opportunity to create a proactive strategy against ongoing threats to external and internal networks.

“We have to look at these threats on a detailed level, and deep packet inspection has become the de facto standard where you look at all the traffic that’s traversing over the network,” says SonicWALL’s Kuhn. “You need to take that traffic apart and ensure that there are no hidden threats lurking there.”

“There are rules about how traffic should always act. So if you violate these protocols you’re usually looking to do something outside the normal course of communications,” TippingPoint’s Wright says.

This is where behavior-anomaly detection systems come in, which let you monitor the network as it’s running in a normal, healthy state and understand when things are not running that way. Similar to an intrusion detection system (IDS) or IPS software-based appliance, it looks at application communication flows and different characteristics of the network. It uses different points of detection from different systems to zero-in on the core of the problem.

“It’s more of an intelligent detection system than the more traditional types of signature-based systems,” says Hargis. “Behavior anomaly systems are geared much more toward the unknown threat or the zero-day attack, where you don’t have a very specific, proactive approach available.”

Public Sector Concerns
Unlike enterprises, the public sector and education have particular security concerns that require a slightly different security strategy. While an enterprise can
simply lock down access to the Internet, for example, most federal, state and local government sites, as well as higher education sites, need to offer a more open computing platform.

“Government customers are under a great deal of pressure to provide security for the data they hold. Much of it is confidential, like social security numbers and tax and health care records. They need to maintain the integrity of the records,” says Haywood Talcove, vice president, public sector for Juniper Networks.

“The public sector is beginning to act like a service provider in how they are provisioning services to their customers, the public,” he comments. “They are requesting the same level of uptime as enterprises and other service providers, and requesting the same total cost of ownership experience.”

Time to Refresh the Network
According to Talcove, the public sector is going through a major refresh cycle since little of its IT infrastructure has been upgraded in the past seven years. “What’s unique about government is that they don’t have the opportunity to refresh products every 36 months. The stuff that they buy stays in for seven or eight years, so they look carefully at what meets their needs as they’re upgrading,” he says.

“Also, 40 percent of the federal workforce in the public sector is within five years of retirement — so the next generation of networks needs to be built so that they are much easier to operate.” As with most businesses, proactive planning is recommended. “You need a plan in place for how you’re going to protect information and mitigate risk,” notes Talcove.

The Smart Card
Cisco’s Graziano says that the public sector now needs to tie a lot of security components in with the common access card, which is an identification badge that the federal government is currently rolling out to civilian employees. (It’s already being used by the Department of Defense.) “It gives you access into a facility and it also gives you logical access onto a network,” he says. “What we’re seeing is the need to incorporate authentication capabilities within the cards, and that’s tied into NAC.”

The NAC appliance plugs into a Secure Sockets Layer virtual private network (SSL VPN) and an Internet Protocol Security virtual private network (IPSec VPN), and helps to enforce policy at endpoints. It scans the device to make sure things are up to date on the notebook. If it’s not up to date, it puts the notebook in a remediation Virtual Local Area Network (VLAN) and forces the user to update antivirus and any current patches, which helps protect against everyday issues on the network.

IPS in Education
In educational environments, where networks are designed to support the students, it’s important to maintain an open computing model. “In education they have this large group of students to provide network access to, but they don’t have as much control over what those students are doing on the network,” says TippingPoint’s Wright.

Wright adds, “Often you see students coming in with devices that aren’t protected. In primary and secondary education you often see students trying to access sites that shouldn’t be permitted on the network, so you have this issue of misuse inside the community that’s very difficult to lock down.”

For this reason an IPS is a great device because you can block traffic off the network and enforce policy to prevent instant messaging, Voice over Internet Protocol (VoIP) like Skype, file-sharing and downloading videos.

Education’s Unique Challenges
In K-12 the primary focus is on protecting the student from external threats. “It’s more about content filtering from externally available material. In fact, the higher education open computing model doesn’t fit in K-12,” says Enterasys’ Hargis. “They need to filter content in their environments.”

SonicWALL’s Kuhn agrees that education faces unique challenges, particularly on university campuses. Many universities require that students have notebooks when they matriculate. “The number one challenge with universities is that most have 2000 computers to begin with. But then you add 4000 students to that and the network grows by three or four times the normal amount,” says Kuhn.

Those uncontrolled PCs are in and out of the network, connecting at coffee shops or in dorm rooms. “The amount of threats found in universities today dwarfs the threats found in your typical business organization,” he says. “If you don’t have a complete security strategy for a university network where you’re segmenting out teachers and administrators from student networks, you’re going to have a huge problem on your hands.”
IPS Interior Protection
TippingPoint’s Wright suggests deploying an IPS with the firewall at the perimeter, and inside the core where the most traffic (fastest bandwidth) is routed, as the best form of defense. “You can prevent insiders from communicating those malicious attacks using an IPS coupled with NAC.”

“What most universities want is a network environment that can secure itself against attack,” says Hargis. “It needs key visibility of what’s going on in the network, so they can see when things are out of compliance. It’s about being able to enforce particular policies of network usage based on a broad context. That’s where an NAC strategy is key.”

Segmentation Strategy
For universities, segmentation of the user base is a solid strategy. “Bringing students and faculty in via SSL VPN is best,” says SonicWALL’s Kuhn. “Many universities are using NAC. So when a user comes onto the network and tries to access resources, they first have to download protection software that will block viruses and any other threats that are on that PC.”

This provides another layer of defense on the network so that if a virus does get on the network, it protects and blocks it from spreading.” An SSL VPN solution has traditionally been seen as an easy way to get users to use security resources on the network,” states Kuhn. “It can run a small ActiveX client, so when you log in, the traffic originating from that PC is encrypted over the Internet. The end user can use their full client applications over this secure channel.”

“It’s easy for them to use,” Kuhn continues. “They have a login and password, and when they log in, they’re given the choice of what applications they want to use. Or if they’re using applications on the notebook, they can download the ActiveX client that will encrypt all information from their PC into the organization.”

Remote Assessment Capability
“The technology has to involve not only an agent-based approach, but also a remote assessment capability,” says Hargis. “When a system comes online and attempts to access the network, you can check the health and the threat level of that system to determine whether it has an assessment agent installed or not.”

That integration is key to securing the gateway. “Once you have a collaborative and integrated environment where the devices can talk to one another, they can adapt proactively to threats in the environment,” adds Cisco’s Graziano.