

The Future Of The Firewall

Jeff Wilson

Security functions are finding new homes in appliances, switches and routers.

Jeff Wilson is principal analyst, VPNs and security with Infonetics Research (www.infonetics.com), specializing in firewalls, IDS/IPS, VPNs, integrated security appliances and application security. He can be reached at jeff@infonetics.com.

“What is a firewall?” My mom asked me that question the other day, demonstrating the fact that Internet security is no longer the domain of reclusive super-nerds. Honestly, that can be a tough question to answer when the person asking still doesn’t know how to make “folders” and put “files” in them.

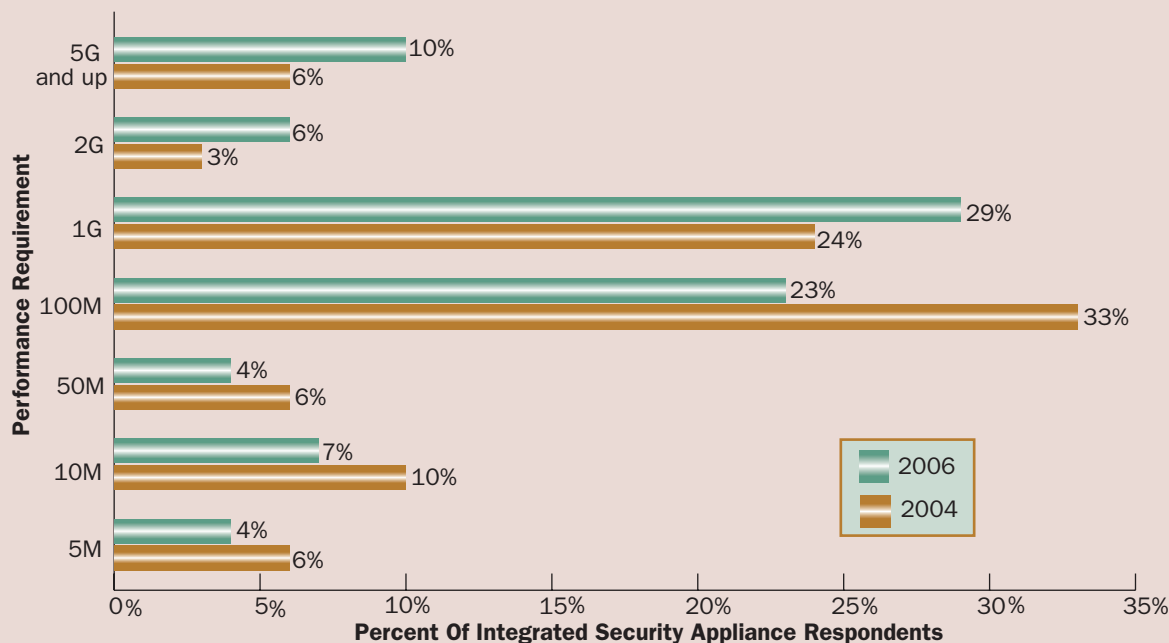
I told Mom that firewalls keep the bad guys from getting on to your network, server or personal computer; the answer satisfied her. It’s a simple and accurate answer, and it’s not going to change. What will change is how firewalls, and other devices, will perform firewall functions.

A Brief History Of Firewalls

The term firewall has other uses besides referring to Internet security; homes and cars have fire containment barriers, also called firewalls. In the late 1980s, routers used packet filtering to separate network segments so problems in one segment didn’t affect other segments. In the early 1990s, members of the then-small Internet community noticed increasingly frequent attacks, acknowledged that their private community wasn’t really private any more, and a multi-billion-dollar market was born.

In the early-mid 1990s, companies like DEC, TIS, ANS and Raptor built specialized (and complicated) firewall products and offered development toolkits to help companies protect their Internet-connected networks. In 1994, Check Point launched Firewall-1, the first packaged firewall product that attempted to be user-friendly. From the beginning, many firewalls have used packet filtering (static, dynamic or stateful),

FIGURE 1 Customer Performance Requirements For Firewall Appliances



Source: Infonetics Research study: User plans for Security Products and Services, North America 2004

circuit gateway information, and/or application-layer information/proxies to perform the important job of keeping bad guys out. Even as far back as the early 1990s, some firewalls have used more than one technology to accomplish this goal (the DEC SEAL used packet filtering and application proxies).

So that's what firewalls have been, so far—but what will they be? If my mom were to ask me this question, I'd have another simple answer: In the future, firewalls will continue to protect systems and networks from bad guys, but they'll come in a package that fits any situation, and they'll do an even better job securing things.

More Form Factors, Plus Higher Performance

Every network-connected system on earth faces threats that could be mitigated with a firewall, but many still are not protected by firewalls. Why is this? The simple answer is cost, and cost's constant companion, ease-of-use. Firewalls come in a variety of form factors—software that installs on the host, software for network servers, standalone hardware appliances, network-integrated firewalls (built into modems, routers and switches)—available at a range of prices, but we aren't yet to the point where everyone can afford to buy one and anyone can figure out how to use one.

Home users can get built-in firewalls with their \$69 broadband routers and wireless access points, and sometimes they even turn these on, but the products typically lack many features of enter-

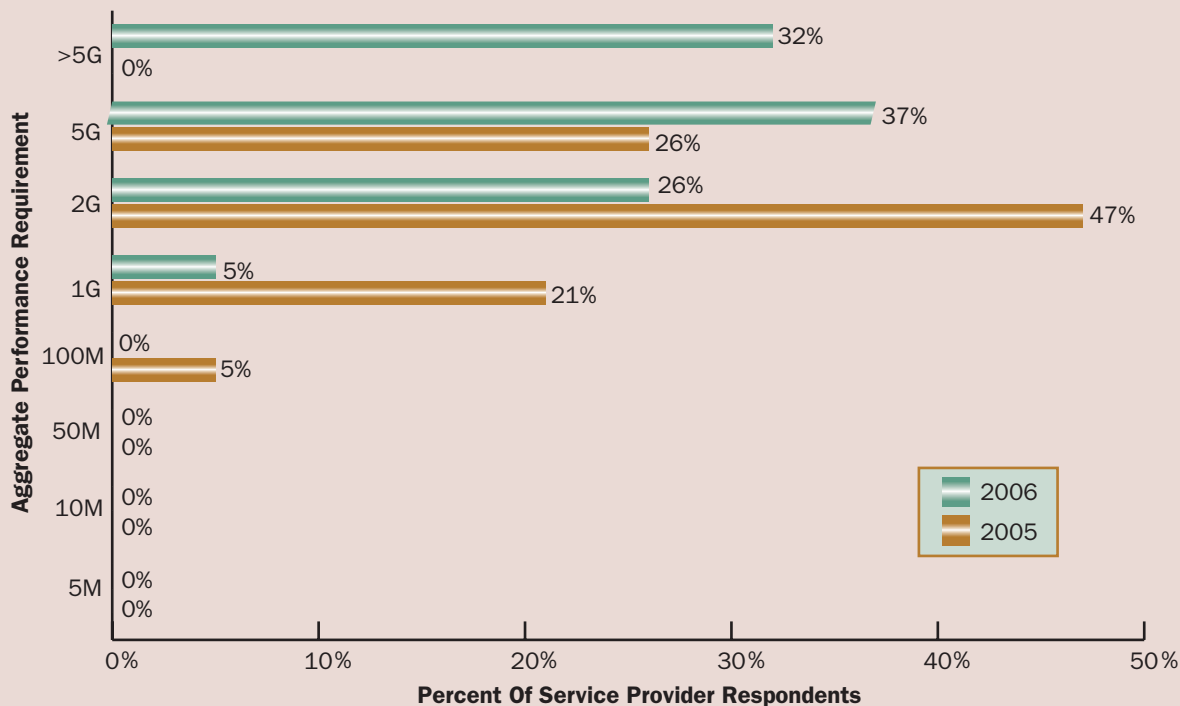
prise-class firewalls. Advanced features like virus scanning, spam filtering and intrusion protection are gradually being commoditized and will likely trickle down in the next year or two to home users.

Many small and medium organizations are in a situation similar to the home users, in that the products they can afford or are willing to spend money on aren't necessarily capable of protecting them from today's sophisticated attacks. Enterprise-class firewalls start at about \$300, and that price will come down, but many small and medium organizations don't know how to find the right products, nor do they know how to install and manage them. For these customers, the coming generations of routers may be the easiest way to get good protection, as they will have built-in enterprise-class security technology.

Large organizations with knowledgeable IT staff have a growing range of good choices, including security appliances and firewall blades for LAN switches. Over the next two years, vendors of networking equipment who do not already offer built-in or optional firewalls will include them. Throughput capacities (performance) will also improve, as network and appliance vendors respond to the many large organizations that are anticipating increased firewall deployments on internal wireless LANs and between their wireless and wired LANs. As Figure 1 shows, customers are moving from appliances that secure 100-Mbps LAN links to those with 1-Gbps capacity, and beyond.

Firewalls still aren't as easy to configure or as inexpensive as they could be

FIGURE 2 Service Provider Performance Requirements For Network-based Products



Source: Infonetics Research study: Service Provider Plans for VPNs and Security: North America, Europe and Asia Pacific 2005

It would take four or more devices to secure each boundary

Service providers, too, are looking to increase their firewall deployments, typically for network-based products in four different applications: managed CPE services, network-based services, data-center use and protecting their own internal networks. Providers have strong requirements for remote management, virtualization (the ability to create virtual domains within a given hardware device, enabling one device to serve many customers) and most importantly, performance.

In our study, “Service Provider Plans for VPNs and Security: North America, Europe and Asia Pacific 2005,” we asked service providers the same question we asked enterprises about performance requirements for firewalls. Most providers currently look for network-based products in the 1-Gbps to 5-Gbps range, but they expect to shift to 2-Gbps to >5-Gbps in 2006 (Figure 2).

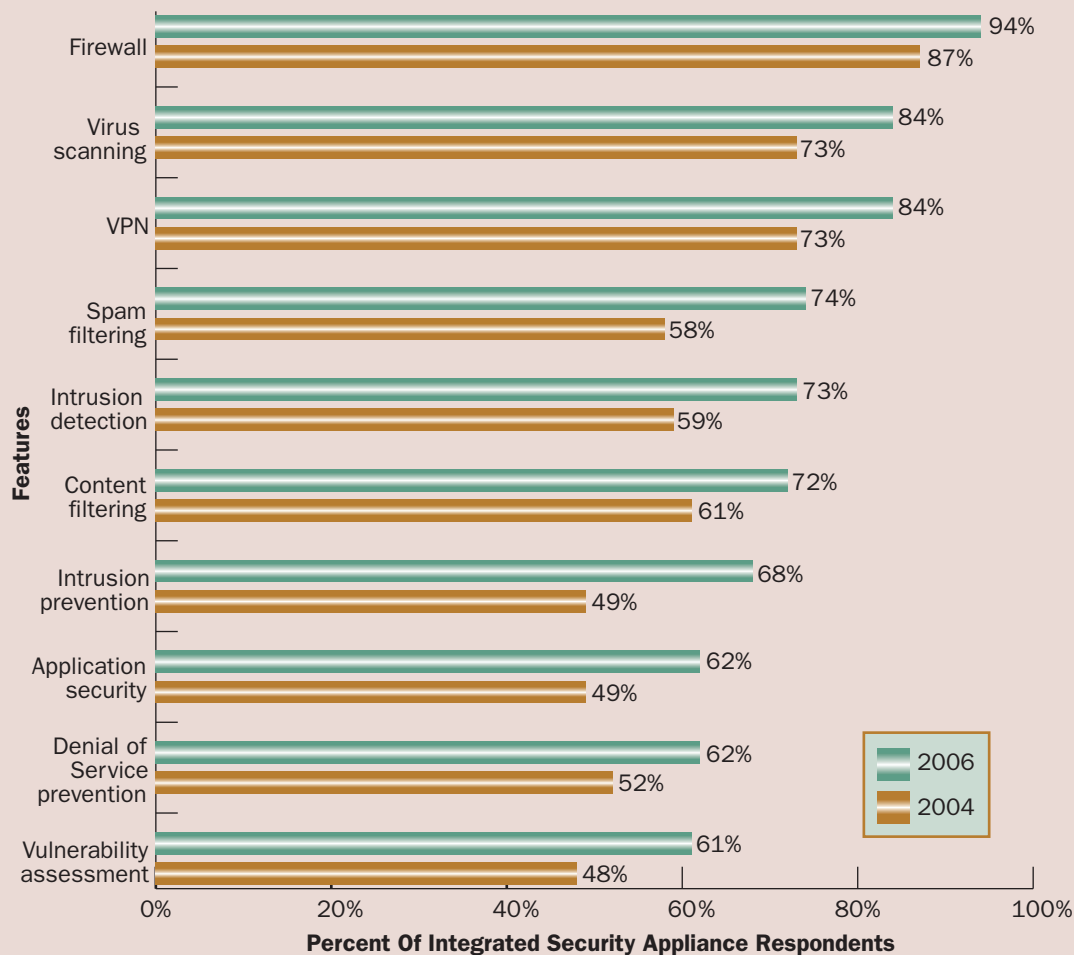
Firewall Functions Will Improve, Too

Security devices, like the attacks they must thwart, improve over time. Unlike basic network trans-

mission speeds, which are constrained by physics of the media, firewall functions are only limited by the hackers’ imaginations. New attacks lead to new firewall features, which lead to new attacks in an endless cycle of development. In the mid-to-late 1990s—the first boom in the firewall market—most firewalls focused on the network and stopping network attacks, and that worked well for a time. In 2005 and beyond, firewalls have to do much more.

Most firewalls already have integrated virtual private network (VPN) functionality, and most firewall vendors are now integrating gateway virus scanning, intrusion detection/prevention, and Web/application security. There are stand-alone products that individually offer each of these functions, but mainstream network managers probably won’t buy, deploy and manage four or more devices at every boundary, which is what’s currently required to provide adequate security. The market needs one device, and that device will be called a firewall.

FIGURE 3 Desired Features For Next-Gen Firewalls



Source: Infonetics Research study: User plans for Security products and services, North America 2004

Don't let the semantics confuse you. If you define a firewall only in terms of packet filtering (even stateful packet inspection), you may think that many of today's enterprise-class firewalls aren't really firewalls. I think it's more appropriate to default to that simple definition that I gave my mom—the firewall is a bad-guy stopper—and I think most customers care more about stopping the bad guys than about the specific technologies integrated into the firewall so that it can do a better job. So let's keep it simple and just keep calling them firewalls.

In 2004, enterprise customers told us that, when considering future firewalls, they are thinking of devices with a whole host of features beyond packet filtering and stateful inspection, as shown in Figure 3. Anticipating this demand, firewall and LAN switch/router vendors are retooling their products; specifically, these companies are adding more security functions (like intrusion prevention), building partnerships with antivirus (AV) vendors to integrate gateway AV, and looking at Web/application security technology. In truth though, as things stand today, most enterprise customers are still chugging along, satisfied with their current-generation products that mostly use stateful inspection and packet filtering.

Wireless LAN Drivers

A major firewall hardware trend is being driven by wireless LAN adoption, because early WLAN security was bad or non-existent. Consequently, customers began moving VPN and firewall products that were designed for the network edge inward to the WLAN, or to where the WLAN joins the wired infrastructure.

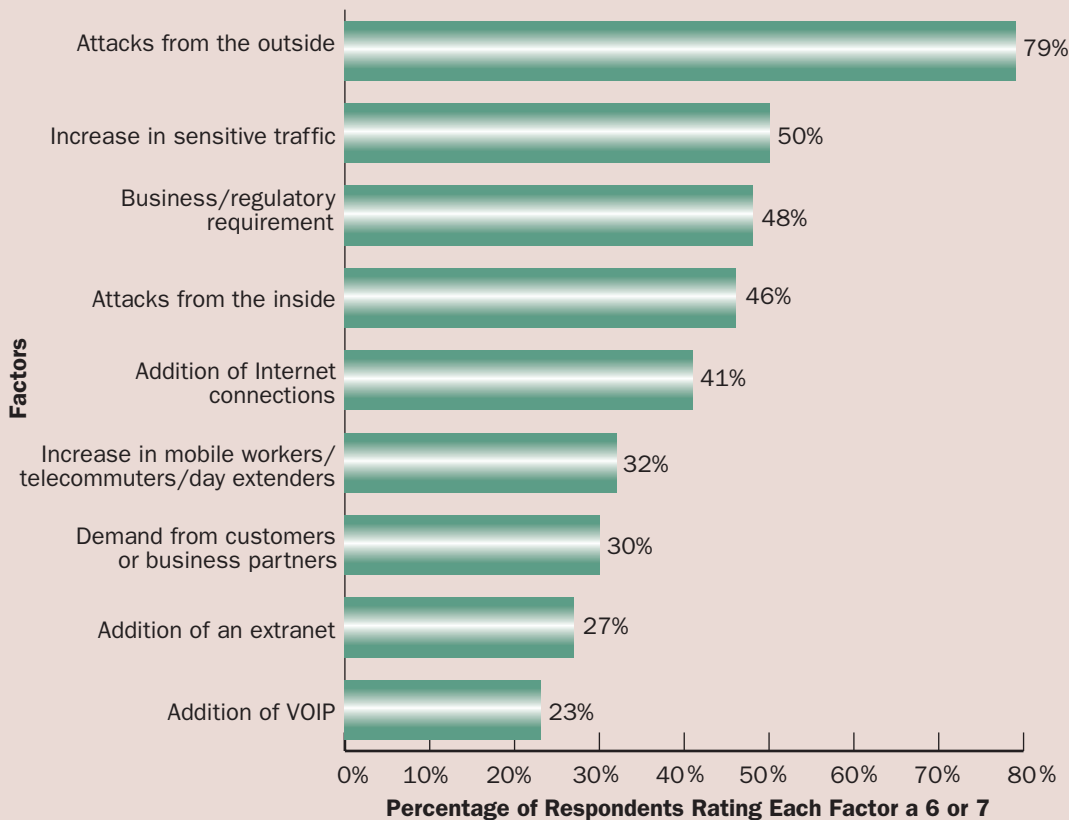
Vendors responded by developing high-performance, multiport VPN and firewall appliances, and, although these products began shipping in 2002, their real impact on VPN/firewall appliance revenue was not seen until 2004. That was the year in which many organizations began to realize they would need to build security into their LANs by adopting new switches and routers; by changing the way their networks are segmented; and by developing security policies for the internal network. This growing focus on internal security is driving some vendors to build firewall appliances with many Ethernet ports, and others to integrate security into their switch products.

Widespread deployment of wireless LANs and the consequent spike in interest in wireless LAN security is not only driving firewall purchases—it's also pushing development of wireless-specific features for firewalls. Many enterprises will




Most customers use only stateful inspection and packet filtering

FIGURE 4 Security Deployment Drivers



Source: Infonetics Research study: User Plans for Security and Services, North American 2004



**Future firewalls
will be faster,
more functional
and more
complicated**

deploy firewalls to protect WLAN segments, and will use VPN clients to encrypt WLAN sessions and authenticate WLAN users.

Initially, this looked like a short-term solution to the problem, as the wireless community was at work developing standard approaches to wireless security (e.g., 802.11i), but most companies continue to invest in VPNs and firewalls. Some firewall vendors have gone as far as building firewall appliances with integrated wireless access points, and more will join that trend.

Conclusion

We've discussed throughput, or performance, as a general requirement for high-end enterprise and service provider customers. If customers and service providers are already considering multi-Gigabit performance, it's not unreasonable to expect there to be applications for 10-Gbps and up in the next several years. This won't be as hard to meet for basic packet filtering and stateful inspection as it will for intrusion prevention, or for any content inspection that requires packet payload inspections. Advances in ASICs, network processors, software and system architecture will all be required to push tomorrow's firewalls up to and beyond the 10-Gbps performance mark.

So is the future of firewalls simple or complicated? I guess it depends on where you're sitting.

For the people building them, it's complicated to integrate scores of disparate functions and technologies into one platform that runs at 5 Gbps and up, and that always stops all the bad traffic and always lets the good traffic in—oh, and that costs less than \$100. Throw in the fact that hackers never go on vacation: As soon as you have a problem licked there is a new one ready to take its place. That's certainly a challenging position for any product manufacturer.

Firewall customers, however, will demand that the future be simple: No more worms, no more viruses, no more hacks, no more trojans, no more denial-of-service attacks and no more security headaches. End users, based on our research, have one primary concern when it comes to security: they don't want to be attacked from the outside (Figure 4).

And that's what a firewall does—keeps the flames off your network and off your devices, right? The firewall of the future may not look much like the firewall of today, and the historical bread and butter of firewalls—that is, packet filtering—won't even scratch the surface of what the firewall of the future will do. Eventually we may find it more appropriate to call it *an intrusion prevention system* or *integrated threat protection system*. But it seems more likely that we'll still call it a firewall □