



February 11, 2011 • Vol.33 Issue 3

The Next Generation Of Firewall Technology

Palo Alto Networks Knows The Ins & Outs Of Protecting Your Networks

According to Nir Zuk, founder and CTO of Palo Alto Networks (www.paloaltonetworks.com), his company's products are the best on the market--a bold statement, to be sure. Spend some time listening to Zuk's reasoning, however, and you might have to admit that he makes some very valid points. Dive into your own research on Palo Alto's enterprise firewall technology, along with some due diligence on the state of the competition, and you could find yourself becoming the company's latest convert.



Changing Technologies

For one thing, Zuk says, SPI (stateful packet inspection) is dead. This might be easy to dismiss as mere hyperbole, except for the fact that Zuk was one of the original developers of SPI technology at Check Point Software Technologies.

The problem with stateful inspection, Zuk says, is that it focuses on ports and IP addresses. Ports are like main circuit breakers: too big and clumsy to use as filtering criteria when what matters is the activity, good or bad, flowing through them. IP addresses are also not tied to users, who can circumvent policy just by using a different device.

Instead, Zuk says, the answer is to focus on the user, the apps he's using, and what he's doing with each app, especially now that app vulnerabilities have become a favorite exploit. A block/allow toggle on port 80 isn't granular enough by far. Even blocking or allowing Facebook doesn't dig deep enough. Instead, the firewall must support policies that allow the user--no matter what computer he's using--to do business-related activities with Facebook, but not things that may leak corporate data or give malware a toehold.



Nir Zuk, founder and CTO of Palo Alto Networks

And it's not just Facebook, or Twitter, or any other Web 2.0 app with corporate uses in addition to their admittedly time-wasting ones. There's SharePoint, WebEx, Dropbox, IM applications, P2P, and more.

■The Next Generation

So what makes a firewall a next-generation firewall? First of all, Zuk says, it has to be from Palo Alto Networks. He laughs, but he's not completely kidding.

Like Palo Alto's App-ID technology, a next-gen firewall should center on apps, users, and actions, not port/IP (SPI). "It takes what you do [to secure] the Web and email and applies it to all apps," he says. Next, it must have anti-malware technologies that are fully integrated into the firewall at a very low level to avoid the latency of isolated components redundantly scanning the same content. Integration is also necessary because of the complexity of today's threats, says Mike Rothman, an analyst at and president of security firm Securosis (www.securosis.com).

Latency avoidance is critical, as the firewall must be fast enough to allow all company network traffic to pass through it with no loss of performance. That centralized control ideally includes cloud and mobile traffic, too. (In contrast, Zuk says, a typical UTM [unified threat management] solution is too slow for enterprise use because it's not integrated well, although a good one would work fine for small to midsized companies.)

Each security component must be best-of-breed, Zuk says. In short, a collection of mediocrity does not a security solution make. A next-gen firewall must detect content running inside SSL encryption or using obfuscation techniques, and it must be built from the ground up on dedicated, specialized hardware.

It must also provide excellent visibility. Paraphrasing Zuk, you need to know what's happening on your network before you can set policies, and that's hard to do with most firewalls today. It must provide outstanding granularity, while at the same time offering high-level policy such as "no browser-based instant messaging on the network," Zuk says. Finally, it must be cost-effective with a low cost of ownership.

Zuk's overarching point is that firewalls need to evolve based on the threats networks face today.

Rothman agrees. Companies need to invest in technology that addresses what the bad guys are doing, he says, or they'll be disclosing breaches to their customers later on. ■

by Marty Sems

