One of the problems faced by high-volume transaction-processing systems is that security tools can cause significant bottlenecks in transmission. Firewalls, antivirus filters, virtual private network tools, and intrusion-detection systems can all cause significant slowdowns in throughput. Part of the problem is that despite massive increases in processing power, running security programs as ordinary software is not fast enough to keep up with the growing bandwidth of modern networks.

I had the pleasure of interviewing Rick Kagan, VP of Marketing of Fortinet <http://www.fortinet.com/> at the end of May 2004. Mr Kagan is an electrical engineer (BSEE University of Michigan; MSEE U Cal Berkeley) with 20 years in the industry working at ROLM, Bell Labs, Echelon Corp., NARUS and VPNet (now AVAYA).

Q: Tell us about your history.

A: We were founded by Ken Xie, former President and CEO of NetScreen, which was recently sold to Juniper (the big networking company that competes with CISCO) for ~$4B. The basic formula for NetScreen was to take a stateful inspection firewall and accelerate it in hardware, make it easier to deploy and more cost-effective. He applied similar logic in the founding of Fortinet, only this time he decided to tackle content-level threats in addition to network-level threats. We now have 440 employees and do business all over the world. The first thing that comes to mind about why Fortinet is different is that we make the world’s only ASIC-accelerated (ASIC = application-specific integrated circuit) antivirus system.

We have branded our platforms under the “FortiGate” name. They handle not only connection-based attacks as a firewall does but also content-based attacks such as spam, malicious software, and inappropriate Web content. Connection-based attacks include unauthorized access and denial of service. But most of the harmful attacks are content-based.

We have already shipped over 40,000 units since May 2002 and have won many awards including (two weeks ago), Security Product of the Year from Network Computing Magazine. The FortiGate series are also the only product line to have four separate certifications from TruSecure’s ICSA Labs: firewall, IPSec, antivirus, and IDS.

Our customers include many small-to-medium businesses, large enterprise organizations and increasingly ISPs & MSSPs (managed security service providers). We offer a value proposition for MSSPs that is unique: we integrate critical functions into a single system, providing easier management and lower management costs. It’s better for the customer too, they get better security than from a mixture of devices.

Q: What prompted you to integrating dedicated appliances into a single device?

A: Speed, lower costs and ease of management of an integrated platform are obvious answers,
but the more subtle issue is that the integration itself leads to better security. I would defy anyone to beat our system if they have to coordinate the parameters and responses of separate firewall, antivirus, antispam and content tools.

The nature of threats has evolved, with earlier systems focused on physical security, connection-based attacks focused on intrusions, and content-based attacks which are increasingly indiscriminate and which attack anyone connected to a public network. Spam and worms, for example, are the great levelers – they don’t seem to be focused on specific companies but rather impact everyone. The earlier defenses to connection-oriented attacks were network-based devices like firewalls and VPN gateways; in contrast, content-based defenses tend to be deployed as software (either on the server or on the clients) – like AV software for example. In our history, those solutions that have migrated to a network-centric installation have always won.

[More in the next and concluding article.]

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www2.norwich.edu/mkabay/www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay & Rick Kagan. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.