

## A Strong Foundation is Fortinet's Forte

The company believes in product design from the ground up, resulting in faster and more functional products.

Fortinet's Fortigate series of ASIC accelerated antivirus firewalls recently won the 2003 Networking Industry Awards Firewall Product of the Year. They are a new generation of products that detect and eliminate the most damaging, content-based threats from e-mail and Web traffic in real-time.

Fortinet claims to be the only provider of ASIC-powered, network-based antivirus firewall systems for real-time network protection. FortiGate systems, the only ICSA quadruple-certified security products (antivirus, firewall, IPSec, and NIDS), also deliver a full range of network-level services including firewall, VPN, traffic shaping, and application-level services on an integrated, manageable platform.

Fortinet was founded in 2000 by Ken Xie, the co-founder and former president and CEO of NetScreen. The company is privately held and headquartered in Santa Clara, California, with offices

in Australia, Canada, China, France, Germany, Hong Kong, Japan, Korea, Singapore, Taiwan and the UK.

A graduate of Tsinghua University in Beijing and Stanford University in the US, Xie founded Fortinet about a year after he left NetScreen. Xie's interest still lies in addressing the issue of protection against viruses encountered in the networking infrastructure.

### NCA: Why did you leave NetScreen?

**Ken Xie:** I left NetScreen because I became interested in pursuing other areas beyond layer 3 and layer 4 firewall technology.

### NCA: With NetScreen's acquisition of Neoteris, how does that impact your deal with Neoteris?

**Xie:** We partnered Neoteris based on their request, as they had to fill a gap in their technology (i.e. content-based

threats on remote PCs can easily pass through SSL tunnels and enter corporate networks).

The partnership was terminated after the acquisition by NetScreen. We don't have any plans to licence technology from any SSL VPN vendors. We have had requests for partnerships from other SSL vendors and may do so in the future if they can provide access to additional channel partners.

### NCA: What is the difference between Fortinet and NetScreen's products?

**Xie:** Fortinet is focussed on complete, real-time network protection. We call our technology Complete Content Protection and are able to detect and defeat content-based threats (viruses, worms, Trojans, inappropriate Web content, e-mail spam, etc.), as well as lower level network layer threats and simple intrusions.

Fortinet's technology provides ASIC acceleration for virus scanning and content filtering as well as intrusion prevention, intrusion detection, firewall, VPN and other network layer functions. Our products are the world's fastest for real-time screening of network traffic for viruses, worms, Trojans, etc.

More importantly, we provide a dynamic, real-time update capability from our FortiResponse Infrastructure, and can automatically deliver new protections to our systems to stop new threats in a matter of minutes.

From the perspective of today's products, the only meaningful comparisons between NetScreen and Fortinet products are in the firewall and IPSec VPN area. The NetScreen architecture is designed to provide high performance for network layer threats, but does not accelerate the processing of content-based threats. The newly introduced NetScreen Deep Packet Inspection technology deals with only a limited number of attacks (approximately 200) whereas our antivirus and IDS/IDP technology deals with over 2000 attacks.



Ken Xie (third from left) says that Fortinet has had requests for partnerships from other SSL vendors, which it may consider if these partners can provide access to more channel partners.

We do have both detection and prevention, and we believe we have the best product in the space that covers both. One good example is the ICSA intrusion detection prevention certificate—only three companies in the world have been certified: Fortinet, Cisco and Sourcefire. NetScreen has tried to get certified for the last two years, but they did not pass. Their new release started with a figure of 200 for intrusions, but to get certification you have to cover close to 1500. That's quite a gap.

The performance of NetScreen's current products decreases by approximately 75% when the deep inspection (IDP) capabilities are enabled. In addition, NetScreen does not maintain a dynamic update infrastructure—the IDP signatures for ScreenOS 5 must be updated manually by system administrators. NetScreen's products are most effective at providing traditional, layer 3 and layer 4 firewall and VPN services.

**NCA: When you say the ASIC-accelerated antivirus firewalls are**

**the new generation of real-time network protection systems, how far do you go into IDP as against IDS?**

**Xie:** Currently our IDS database includes approximately 1500 attacks, and we can update these dynamically (as with antivirus signatures) from our Forti-Response Network. Our current Intrusion Prevention System detects and prevents 34 classes of attacks, such as port scans and SYN floods.

We can respond to attacks by dropping packets, closing firewall ports, resetting connections, and proxying connections. In FortiOS 2.8, we no longer distinguish between intrusion detection and intrusion prevention—every attack signature can include a prevention response, and the complete attack database is automatically updated from the FortiResponse Network. Combined with ASIC acceleration for the content processing, our Dynamic Attack Prevention system provides an effective protection against attacks.

With FortiOS 2.8, ours is the only system that can provide a multi-layered response to all phases of an attack, i.e. in response to a worm like Blaster or Slammer

we can update the IDP dynamically to stop the initial (probe) phase of the attack, detect and block the download phase, and also use the AV system to detect and stop the main executable.

We believe that this type of dynamic response, plus real-time performance, are essential for meeting today's and tomorrow's needs.

**NCA: What is so different about Fortinet's products?**

**Xie:** In making a product, we try to leverage all the new technologies. Fortinet does its design architecture from the ground up. We design the chip first, then the system board and the operating system, then the antivirus, firewall and the infrastructure to support it.

It is a huge engineering effort, but the end product is a faster and much better functional piece. It took us almost two years to come up with a product, whereas most software companies can produce something in several months.

But we want to build a strong foundation. Once the foundation is solid you can build much higher. \*

— Tony Henderson