



Press Release

Media Contact:

Atchison Frazer
Fortinet, Inc.
+1 408 235 7700 x318
afrazer@fortinet.com

Fortinet Achieves Network Intrusion Detection System (NIDS) Certification from ICSA; Becomes First “Quadruple-Certified” Product

SANTA CLARA, Calif., Aug 27, 2003 — Fortinet – the only provider of ASIC-powered, network-based antivirus firewall systems for real-time network protection – today announced that the FortiGate™ Antivirus Firewall product line has achieved the T1-level network intrusion detection systems (NIDS) certification from ICSA Labs®, an independent division of TruSecure® Corporation. FortiGate Antivirus Firewalls are now the only systems in the world with four ICSA certifications for a single product.

To achieve certification, Fortinet’s NIDS functionality was required to identify 100 percent of the exploits launched against the test network via a 10 megabits/second Internet connection. The FortiGate platform becomes the only security system to achieve combined ICSA certification in four areas – NIDS, antivirus, IPSec and firewall

"Given the complexity and fast-moving nature of today’s network security environment, customers increasingly rely on independent testing and certifications for assurance that their security products actually deliver," said Richard Kagan, vice president of marketing at Fortinet. "ICSA Labs is trusted by companies worldwide and so we’re extremely proud of this latest certification for our NIDS functionality. Our customers can now be confident that the FortiGate Systems’ NIDS will provide them with accurate, timely alerts and minimal false positives."

To achieve certification, Fortinet's NIDS capability was tested against a suite of attacks, and was also tested for its ability to ignore "noise" and minimize false positives. A false positive is defined as an alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. The false positive criteria allow a minimum number of unique alerts during a 24-hour period of 100 percent live traffic and include reporting on any incorrectly identified, defined or classified alerts. Fortinet is the only company that produced zero false-positives in the NIDS certification testing.

"The recent flurry of new threats highlights the need for continuous, accurate and speedy recognition of attacks on Internet-connected systems," said Scott Markle, technology program manager at ICSA Labs. "ICSA Labs congratulates Fortinet for becoming the first vendor to achieve four ICSA certifications on a single platform."

The ICSA Labs NIDS Certification program is an independent and comprehensive process that rigorously tests, assesses and validates NIDS in multiple network environments on an ongoing basis. The test methodology includes new exploits and more stringent false positive criteria as well as an increase in the network traffic.

Current methodology, criteria and full ICSA Lab reports can be found at:

<http://www.icsalabs.com/html/communities/ids/certification.shtml>

Also available is a white paper titled "False Positives: A Users Guide to Making Sense of IDS Alarms" by Marcus Ranum available at:

<http://www.icsalabs.com/html/communities/ids/whitepaper/FalsePositives.pdf>

About ICSA Labs (www.icsalabs.com)

ICSA Labs, an independent division of TruSecure Corporation, offers vendor-agnostic testing and certification of security products. Hundreds of the world's top security vendors submit their products for testing and certification at ICSA Labs. The end-users of security technologies rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, cryptography, PKI, IPSec, VPN, firewall, PC firewall, intrusion detection, content security, and Wireless LAN.

About Fortinet (www.fortinet.com)

Fortinet's award-winning FortiGate™ series of ASIC-accelerated antivirus firewalls, winner of the 2003 Networking Industry Awards Firewall Product of the Year, are the new generation of real-time network protection systems. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time – without degrading network performance. The FortiGate systems deliver a full range of network-level services – firewall, VPN, intrusion detection and traffic shaping – as well as application-level services such as antivirus and content filtering, in dedicated, easily managed platforms. Fortinet, named to the “Visionaries” category in the 2003 Gartner Enterprise Firewall Magic Quadrant, is privately held and based in Santa Clara, California.

#