



Press Release

Fortinet Delivers Dynamic Threat Prevention Plus 50 Additional New Features/Enhancements to FortiGate™ Antivirus Firewall Platforms

FortiOS™ Release 2.8 Provides the Industry's Most Complete, Dynamic Protection Against Viruses, Worms and Intrusions

SUNNYVALE, Calif., Dec. 9, 2003 — Fortinet – the only provider of ASIC-powered, network-based antivirus firewall systems for real-time network protection – today announced a dynamic prevention technology aimed at responding in real time to blended threats, along with more than 50 new features and enhancements to the FortiGate™ Antivirus Firewall platform, with the release of FortiOS™ 2.8, which also includes IPv6 support, virtual domains for high end systems, enhanced email filtering for Spam protection and dynamic Web filtering.

The FortiOS firmware, which is shipped on all FortiGate platforms, has been enhanced in Release 2.8 with the addition of a number of significant features and benefits including:

- Dynamic Attack Prevention Technology: A major step forward in responding automatically to new, content-based threats by combining key elements of antivirus, intrusion detection and intrusion prevention technologies.
- IPv6 Support: The first of a 3-phase rollout to support the next generation of Internet technology, especially important for the Asia-Pacific markets because it provides virtually “unlimited” unique addresses and supports ubiquitous Internet connectivity on all types of devices including mobile phones, PDAs and even home appliances.
- Virtual Domains (FortiGate 3000 and 3600): Serves the needs of the managed security services market being addressed by large carriers and service providers

because it enables a single FortiGate unit to deliver security services to multiple customers.

- Enhanced Email Filtering for Spam Protection: Provides more extensive messaging filters for detecting Spam, such as reverse DNS lookup, subject line checking, and checking in real-time against databases of known spammers.
- Enhanced Web Content Filtering: Provides real-time integration with Cerberian's extensive URL database containing millions of Web sites and pages, and provides granular Web filtering policies for individuals and groups.

“The new release of Fortinet's FortiOS strengthens the FortiGate system as a high-performance, integrated Secure Content Management (SCM) platform,” according to Chris Christiansen, IDC vice president of security products. “As customers struggle with the administrative overhead of managing separate SCM solutions, Fortinet's consolidated approach offers the benefits of greater security and lower operational costs.”

Dynamic Threat Prevention, Automated Real Time Protection

The new Fortinet Dynamic Threat Prevention technology enables FortiGate systems to scan any protocol for malicious content or behavior and take preventive action – such as dropping packets, resetting connections, or even proxying connections – and to update attack detection and preventive actions dynamically from the FortiResponse Network . Together, with Fortinet's antivirus, firewall, and other capabilities, Dynamic Threat Prevention provides the industry's most complete, real-time system for stopping today's sophisticated attacks.

Conventional antivirus systems have missed some of the latest worms and other attacks such as LovSan and SoBig because their scanning engines were not designed to screen for the protocols used to launch the threats. Further, many intrusion prevention systems were ineffective against these new attacks because their detection signatures are updated manually, a process which is too slow for attacks that can spread to thousands of systems in minutes.

Fortinet's Dynamic Threat Prevention technology addresses these limitations by combining the ASIC-accelerated, application-level content analysis of Fortinet's antivirus technology with the extensive and flexible attack recognition capabilities of the network intrusion detection systems (NIDS) and the real-time, in-line response capabilities of Fortinet's intrusion prevention system. With Dynamic Threat Prevention, a wide range of techniques can be used to detect and stop an attack, and the fastest, most effective response can be deployed in minutes to all FortiGate systems via the FortiResponse Network.

When a new threat is detected, the Fortinet Threat Response Team determines the most effective means for stopping the attack – whether via antivirus scanning, protocol anomaly detection, or other proactive means – and will send updates in real time to FortiGate systems worldwide that, at the customer's option, can take effect immediately. Because the FortiGate units include firewall, VPN and other capabilities, they can implement all elements of an attack response without the need to integrate and coordinate with 3rd party firewalls or other systems.

IPv6, Virtual Systems, Email Spam Protection, Dynamic Web Filtering

IPv6 is the next generation of the Internet Protocol that provides virtually unlimited addresses and supports the ability for essentially any device to be “on the network.” The Fortinet IPv6 Phase I implementation in FortiOS 2.8 is a “dual-stack” implementation that enables assignment of IPv6 addresses to and routing between physical and virtual interfaces, and also supports IPv6 addressing server functionality.

Targeted at managed service providers and very large enterprises, the new virtual domain feature is supported on the FortiGate 3000 and FortiGate 3600, which are high-end, multigigabit, carrier- and enterprise-class systems. Each can support up to 250 virtual domains (VDOMs) per system. This is especially important for service providers who

want to offer different services (antivirus, content filtering, intrusion prevention) for multiple customers powered by the same FortiGate unit.

In addition to the FortiGate systems' native content filtering functions for email, FortiOS 2.8 provides enhanced capabilities to filter email content for Spam attacks. These features include services for checking and marking messages with Spam characteristics based on keywords and phrases in an email message's body and subject line, blacklists of known Spam senders, invalid return email addresses, MIME header checks, as well as blocking of SMTP Messages based on IP address blacklists, reverse DNS lookups, and checks against the Real-time Blackhole List (RBL) and the Open Relay Database (ORDB).

Fortinet is adding enhanced Web content filtering via a partnership with Cerberian to embed real-time Web filtering into the FortiGate product line. When the optional Cerberian Web Manager service is activated, all URL requests are sent to one of the global Cerberian service centers for a categorization request, which replies to the FortiGate unit with the categories matched by the URL, such as pornography, gaming, etc. The FortiGate system then makes an allow/deny decision based on the policy for the user that made the original request. Detailed logging enables dynamic report creation for historical and specific user or group tracking.

“The recent wave of attacks shows that the sophistication of threats is increasing, as attackers continually work to exploit the limitations of disjointed, conventional defenses,” said Richard Kagan, vice president of marketing, Fortinet. “The Dynamic Threat Prevention capabilities we're delivering in FortiOS Release 2.8 prove that the benefits of a single, integrated security platform are more than simply lower hardware cost and ease of deployment. In addition, a platform like Fortinet's – conceived, designed, and supported by a single company – provides the best platform for the deployment of the multifaceted, real-time security measures that are essential to dealing with today's and tomorrow's threats.”

Availability and Distribution

FortiOS release 2.8 will be available for beta customers in December 2003 and will be available for new and existing FortiGate systems in Q1 2004. All features in FortiOS Release 2.8 are provided at no additional charge to customers with valid maintenance contracts, with the exception of Virtual Domains and the Cerberian Web Manager service, which are priced separately. Pricing will be available from Fortinet’s global network of authorized resellers and distributors.

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. FortiGate systems, the only ICSA quadruple-certified security products (antivirus, firewall, IPSec, NIDS), also deliver a full range of network-level services – including firewall, VPN and traffic shaping – in addition to application-level services in integrated, easily managed platforms. Fortinet, named to the “Visionaries” category in the 2003 Gartner Enterprise Firewall Magic Quadrant, is privately held and based in Sunnyvale, California.

#