



FORTIGATE

2005 COMPUTERWORLD HONORS CASE STUDY

BUSINESS & RELATED SERVICES

FORTIGATE SYSTEMS ENABLE COMPANIES TO SAFELY AND EFFICIENTLY CONDUCT BUSINESS ONLINE BY DETECTING AND ELIMINATING THE MOST DAMAGING, CONTENT-BASED THREATS FROM E-MAIL, WEB AND FILE TRANSFER TRAFFIC SUCH AS VIRUSES, WORMS, INTRUSIONS, INAPPROPRIATE WEB CONTENT AND MORE IN REAL TIME. **[20055300]**

A Search for New Horizons



Robert Carrigan,
Chairman of the Chairmen's Committee

Ron Milton,
Vice-Chairman of the Chairmen's Committee

Dan Morrow,
Chief Historian

SUMMARY

FortiGate systems enable companies to safely and efficiently conduct business online by detecting and eliminating the most damaging, content-based threats from e-mail, Web and file transfer traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time. FortiGate systems are the industry's first combination of hardware, software and specialized computer processors called ASICs.

APPLICATION

More than \$55 billion in damage was inflicted upon businesses last year by network viruses, worms and Trojans. Many of these so-called "content-based" network attacks are introduced into organizations via seemingly innocuous activities such as Web browsing and use of email. Attacks are initiated both outside the company and unknowingly inside companies as increasingly popular wirelessly connected computers travel on airplanes, internet cafes and public hot spots.

As organizations increasingly turn to real-time network applications like Web-based online ordering and instant messaging to remain responsive and competitive, this trend of constant exposure to content-based attacks will continue. Unfortunately, conventional network protection systems, such as single-function network firewalls and host-based antivirus software, lack the dedicated hardware and processing required to perform the deep analysis necessary to detect these threats without imposing unacceptable delays on real-time network applications. This gap in protection has left many organizations dangerously exposed to network attacks and often unnoticed exposure to spyware that can remotely steal passwords, credit card data or business contracts.

Fortinet's series of FortiGate unified threat management (UTM) systems were developed to meet small and large business needs for integrated, high-performance network and content security solutions to handle the increasingly sophisticated network threat environment. Maintaining healthcare data integrity, conforming to Sarbanes Oxley and even meeting financial banking Graham-Leach-Bailey regulations are among the thousands of reasons corporations are concerned with safeguarding their customers data – and ultimately their own business records.

FortiGate systems are the first and only in the industry to provide cost-effective, complete network-level and content-level protection with real-time performance. They enable threats to be caught before they enter an organization's network -- and do so at the highest network speeds far surpassing traditional solutions. Each of the 20-plus FortiGate systems is a dedicated, easily managed system with a consistent suite of security functions, including virus protection, content filtering, firewall, intrusion detection/prevention, VPN and traffic shaping functions. Whether used for one or all security functions, Fortinet consistently outperforms larger competitors by offering higher performance and dramatically lower capital and operating costs.

First introduced in May 2002, Fortinet's FortiGate family of systems have fast gained industry acceptance by more than 2,000 companies of all sizes -- from small businesses to the largest enterprises and service providers. To date, more than 80,000 FortiGate systems have shipped to leading banks, healthcare providers, retailers, and education institutions worldwide and Fortinet has been named the Unified Threat Management market leader by IDC. The company has 11 patents pending for its innovative software, hardware and ASIC processing technology, which has garnered numerous industry certifications, accreditations and awards.

BENEFITS

Since first introduced in May 2002, Fortinet's FortiGate devices have successfully protected thousands of

customers from hundreds of millions of attacks. In the last week of December alone, FortiGate systems have halted more than 13,000,000 viruses, worms and network intrusions. FortiGate systems have changed the network security landscape by breaking the mold of traditional security solutions in two main areas – the delivery of the best and most comprehensive integrated security functions and extremely high-speed network performance.

1. Comprehensive, Integrated Security – For years, companies had no choice but to purchase and attempt to integrate numerous independent security solutions to protect their networks. This “congo line” approach is expensive to buy, laborious to manage, and most importantly, ineffective in solving the increasingly-sophisticated slew of cyber threats, which often take the form of blended attacks.

The advent of Fortinet’s FortiGate systems changed all this, and essentially created a market for unified threat management solutions – which is currently the fastest-growing segment of the \$3.4 billion security market. FortiGate devices offer companies a full range of security functions -- including antivirus, content filtering, firewall, intrusion detection/prevention, VPN, anti-spam and traffic shaping – onto one easy-to-manage system to effectively thwart content and network based viruses, worms, Trojans and other attacks.

2. Real-Time Performance – Utilizing a specialized computer processor called an Application Specific Integrated Circuit (ASIC) to offload computationally-intensive security tasks, FortiGate systems perform deep security at high-speeds with no slowdown of common Internet and network-based applications including email, file transfer, web video conferencing and online commerce. This real-time network scanning is critical in enabling companies to securely leverage the benefits of high-speed networks, and sets Fortinet apart from larger, more entrenched competitors in the market.

FortiGate systems are the only ASIC-accelerated antivirus gateway products in the world and the only security products in the world with four certifications from the leading independent Security Certification lab called ICSA (firewall, virtual private networking, intrusion detection, and antivirus). ICSA is analogous to Underwriters Laboratories for security, providing the most reliable and respected third-party testing services in the industry.

Another major differentiator of FortiGate devices is the global FortiProtect virus update service, which provides 24x7x365, automatic updates for FortiGate systems to protect them against security threats as they arise. With FortiProtect, network administrators do not need to worry about or spend time patching systems with the latest updates. More than 100 engineers in the United States, Europe and Asia can quickly develop a new virus blocking script and post it to FortiProtect providing real-time protection to customers.

With more than 80,000 units shipped to date, FortiGate systems have helped thousands of customers worldwide improve network security and reduce capital equipment and administrative costs.

IMPORTANCE

FortiGate security systems leverage breakthroughs in computer processor design, software development, network analysis and content inspection.

To provide iron-clad security without performance penalties, Fortinet developed a high-performance security processor ASIC (FortiASIC) and patent-pending Content Pattern Recognition Language (CPRL) software specifically designed to speed up the computationally-intensive routines commonly associated with complete content protection. The integration of these cutting-edge technologies is unique to Fortinet and goes far beyond the Deep Packet Inspection capabilities available in other security solutions. FortiGate systems also offer customers new security algorithms and behavior-based heuristics – or a set of rules developed to resolve abnormal network behavior when a specific algorithm cannot be designed – to stop known and unknown cyber threats. This technology allows Fortinet to increase its detection capabilities against modern, ‘zero-day’ or previously unknown virus or worm attacks that are designed to bypass traditional network security defenses.

ORIGINALITY

Around the turn of the millennium it became apparent that conventional network security solutions were inadequate for addressing the millions of modern network threats. Content-based viruses, worms and Trojans were causing major damage to company computing systems and networks, threatening the viability of open networks like the Internet as a critical tool for delivering information, entertainment and commerce. Recognizing the need for integrated, high-performance network and content security solutions to handle the increasingly sophisticated network threat environment, Ken Xie founded Fortinet in October 2000, with a vision to create the industry’s first high-performance unified threat management system.

He did this by leveraging specialized computer processors (ASICs) that accelerate numerous security applications within a single dedicated device. FortiGate systems are the only ASIC-accelerated antivirus gateway products in the world, and the only security products with four certifications from the industry-certification expert ICSA (firewall, virtual private networking, intrusion detection, and antivirus). FortiGate systems provide cost-effective, complete network-level and content-level protection with real-time performance -- enabling threats to be caught at the network gateway before they enter an organization's network, and at speeds which far surpass traditional solutions.

With FortiGate systems, Fortinet essentially defined, introduced, and is leading a new market called unified threat management (UTM) with a 30% marketshare. UTM is currently the fastest-growing equipment market within the security sector, estimated to be more than \$3.4 billion in the next three years (source: IDC, 2004).

SUCCESS

The development and market adoption of FortiGate systems have far exceeded Fortinet's internal goals and industry benchmarks for offering this level of security application performance and integration. Since introducing the first FortiGate systems in May 2002, Fortinet has introduced a continuous stream of products and technology advancements rivaling the productivity of companies 10 times larger. The FortiGate product line has grown to include more than 20 models targeted for all types and sizes of businesses -- from small offices to the largest enterprises and service providers. There have been three major FortiOS software releases, which have more than tripled the number of features offered on FortiGate systems.

Fortinet's FortiGate systems defined and introduced the unified threat management (UTM) market -- of which Fortinet was recently named the market leader, surpassing more established security vendors like Symantec, Trend Micro and others. Additionally, FortiGate systems have received dozens of prestigious industry awards -- including the 2003 Networking Industry Awards "Firewall Product of the Year" and Network Computing's 2004 "Security Product of the Year" Award.

Market adoption of FortiGate systems has grown exponentially. In just over two years, more than 80,000 FortiGate units have been shipped to more than 2,000 customers worldwide -- including many blue chip companies in the financial services, government, healthcare, education and telecommunications sectors. FortiGate systems have put Fortinet on customer's network security "short-list" of vendors, often winning out over industry heavyweights like Cisco, Check Point, Symantec, McAfee and Juniper.

But perhaps the biggest testament to the success of FortiGate systems comes from the mouths of Fortinet customers:

- "FortiGate systems provide all of the security functions we need to safeguard our patient's online medical data in a single, cost-effective security platform." -- Tavares Marsh, Caritus Christi Healthcare
- "The Fortinet device massively outperformed the other single point devices we looked at and we were very impressed with its combination of best-in-class VPN, anti-virus, firewall, IPS and content filtering functions." -- Michael George, Europe's National Exhibition Centre
- "Since implementing the Fortinet solution, we have had no known incidence of malware on our center PCs." -- Jeff Nelson, Jenny Craig Weight Loss Centres
- "We knew we needed to improve our network security to better protect us from attacks and also to reduce the amount of time and resources we were using to respond and clean up afterwards. We evaluated a number of security solutions and selected Fortinet's FortiGate system for the complete content protection it provides, combined with easy configuration, simple management and highly competitive price point." -- Mark Giorgis, Long Beach Transit.

DIFFICULTY

Fortinet was founded with the goal of solving the continuously-evolving modern-day network and content security threats facing businesses of all sizes, but doing so posed significant challenges for this start-up venture.

Until the introduction of Fortinet's FortiGate systems, it hadn't been possible to build networking devices with the processing power and specialized software intelligence needed to perform application-level content processing in real time. Industry giants in both networking and security weren't dealing with new, content-based network threats within the fabric of the network itself, and continued to pursue network off-load software-based solutions relying on host computers first being attacked before they could be protected. No one

believed that it was possible to “do antivirus in the network, at network speeds.”

To bring the FortiGate systems to market required a commitment by Fortinet to develop many interrelated technology components that would daunt even the largest companies, including:

- A new hardware architecture for processing content in the network at exceptionally high speeds
- A custom computer processor or ASIC for providing real-time content processing in the network
- Two distinct network antivirus and content filtering update services (FortiProtect and FortiGuard), distributed through 11 points throughout the world
- A new secure, real-time operating system leveraging a hardened Linux software kernel
- Seven best-in-class security applications that can be used alone or integrated (antivirus, firewall, VPN, intrusion detection & prevention, Web content filtering, email content filtering, & traffic shaping)
- A complete global infrastructure of people & systems deployed around the world to find new attacks, characterize them, and deliver updates in real time to systems deployed anywhere in the world

Additionally, potential customers needed to be convinced that a new, unknown company competing against leading industry providers like Cisco, Juniper and Check Point could be trusted to provide critical network protection systems and services for their organizations.

Many would have balked at such an undertaking, but an audacious vision combined with a team committed to working hard to take on a multitude of challenges and execute exceptionally was key to Fortinet’s success.