Reference Code: TA001894SEC

Publication Date: April 2010

Author: Graham Titterington, Karthik Balakrishnan, and Nishant Singh

TECHNOLOGY AUDIT

FortiGate with FortiOS 4.0

Fortinet

SUMMARY

IMPACT

Enterprise IT security functions have traditionally used several separately purchased stand-alone threat-prevention and remediation applications. This makes management an expensive and resource-intensive task. Fortinet's FortiGate UTM appliance cuts this cost by providing a tightly integrated portfolio of gateway security functions configured and managed through a single management console.

KEY FINDINGS

Strengths:	✓ Provides a fully integrated range of security services, with a low total cost of ownership. ✓ FortiNet's technical independence enables it to tailor its services to its clients' needs.
Weaknesses:	✗ Its URL categorisation system may be slow to spot a legitimate web page that has recently been compromised. ✗ Organizations that want to add to the protection offered by FortiGate will find it difficult to integrate with third-party products
Key facts:	i ICSA Labs, NSS Group, and Virus Bulletin 100 certified. i Targeted primarily at large enterprises and service providers; SMEs are also supported.

OVUM VIEW

The UTM application marketplace is extremely competitive, populated by more than a dozen key vendors from different backgrounds, including security product providers with a large installed base in the mid-to-large enterprise segment, vendors with a focus on SMEs, and the networking majors. Fortinet was founded to pioneer ASIC-accelerated UTM security appliances, and it continues to provide cost-effective protection to a wide range of organizations including service providers.

The FortiGate range of appliances offers a comprehensive unified security platform that provides organizations with a strong portfolio of integrated and centrally managed network security capabilities. Fortinet plans to build additional data loss prevention capabilities into its portfolio, adding to its usefulness, but it will stop short of providing a full DLP product. Fortigate also plans to enhance its core functionality and to expand its range of appliances with higher performance for large enterprises.

Fortinet scores well in terms of its installed base, distribution network, and global presence. It has a user base of more than 75,000 customers worldwide. In Asia-Pacific most of its sales are still in the SME sector, but the company is working to develop a base of larger customer markets, as it has done across North America and EMEA.

Recommendations

- **SMEs and large enterprises:** FortiGate is suitable for enterprises of all sizes. Fortinet's success in the SME segment is well documented, and FortiGate appliances have also been deployed by large enterprises throughout many industry verticals, especially by organizations operating in telecoms, financial services, and the public sector. Ovum understands that Fortinet is keen to move forward to increasingly target large enterprises. While the challenge in achieving this lies in widening the support network at a pace equal to the high growth rate of Fortinet, Ovum believes that the company could make deeper inroads into the large enterprise segment, as well as, expanding across geographies. The company went public on 18 November 2009, and this should allow it to gain scale and cater to large enterprises more effectively.

- **Service providers:** The service provider (SP) sector has identified a need to provide clean communications pipes to protect customers from an increasingly sophisticated range of malicious threats. Fortinet can satisfy this need. In addition it allows its appliances to be partitioned so that each customer of the service provider can be provided with a virtual appliance.

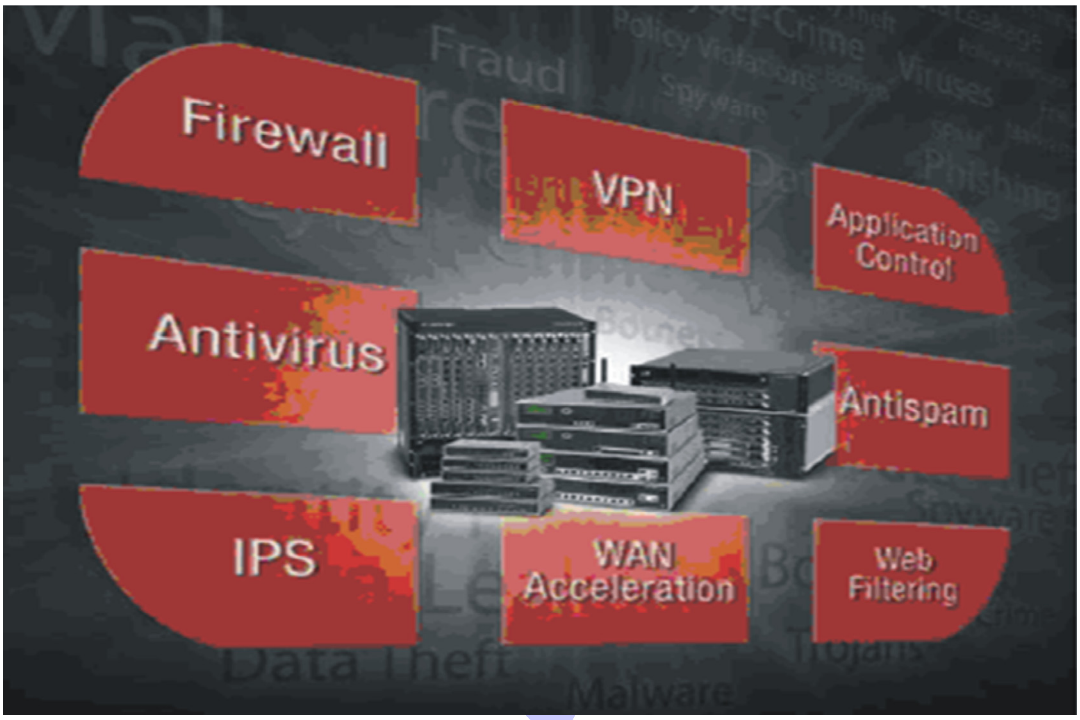
- **Small office/home office:** While FortiGate security appliances can scale up and down to meet the needs of small organizations, Ovum believes that there are more efficient ways to meet the need for basic IT security functions. However, small organizations could deploy the FortiClient unmanaged free edition, which in terms of functionality is similar to standard FortiGate appliances.

FUNCTIONALITY

SOLUTION OVERVIEW

The FortiGate appliance-based Unified Threat Management (UTM) applications combine several gateway security components including a stateful-inspection firewall, gateway antivirus, anti-spyware, IPsec and SSL VPN, web filtering, IPS, traffic shaping, WAN optimization, application control, DLP, and anti-spam applications. The FortiGate product line of integrated network security appliances (as shown in *Figure 1*) is now large enough to cater to the specific requirements of organizations of different sizes, as well as service providers. It ranges from the blade- and chassis-based products that are required to meet the operational demands of large enterprises and service providers to the smaller end of the hardware range that suits the needs of SMEs and remote branch operations.

Figure 1: FortiGate security infrastructure



Source: Fortinet OVUM

Fortinet delivers a completely home-grown and integrated set of hardware and software products. Forty-nine percent of Fortinet's employees work in research and development (R&D), illustrating its independence from other vendors in the delivery of its hardware and software products. Fortinet has its own security operating system (FortiOS) which is used to provide end-to-end product and service integration.

FortiGate's strength as a security appliance lies in its ability to maintain business continuity and sustain normal processing speeds while maintaining an effective defense against network and application threats that are being launched against business systems. Through its high-performance security ASIC processor (FortiASIC) and its Content Pattern Recognition Language (CPRL) Fortinet also speeds up routines for rigorous content protection.

To satisfy the need for a dynamic throughput approach, FortiGate security platform embeds FortiASIC processors that provide content analysis and scanning capabilities, as well as acceleration for firewall and encryption/decryption operations. FortiGate's ASIC-based architecture enables it to analyze the network content and its behavior in realtime.

Fortinet's Complete Content Protection (CCP) approach can reassemble packet-level payloads at gigabit network speeds into application-level objects, such as files and documents. Fortinet uses this technology to scan and analyze the reassembled content against a list of thousands of virus and worm signatures. Fortinet's CCP approach enables it to detect a variety of threats, including inappropriate web content, email spam, spyware, and phishing attacks.

FortiGate configurations range from the FortiGate-30 Series (30Mbps FG-30B model) to the FortiGate-5000 Series (182Gbps FG-5140 Chassis model). FortiGate appliances also support voice-over-IP (VoIP) protocols such as Media Gateway Control Protocol (MGCP), Skinny Client Control Protocol (SCCP), and SIP. They can interpret the VoIP signaling protocol to open and close ports for each call to maintain security.

There are specific hardware ranges for FortiManager and FortiAnalyzer, the Fortinet management, analysis, and reporting appliances. Also available are hardware appliances that provide the company's Secure Messaging (FortiMail) services, client software (FortiClient), security subscription services (FortiGuard services), web and database security appliances (FortiWeb and FortiDB), FortiMobile the end-point security software, and the FortiCarrier platforms which help protect critical applications across a service provider's IP network.

Fortinet's FortiWifi range of appliances includes a built-in wireless access point to the existing range of FortiGate appliances, offering standard 802.11a/b/g/n support, a WAN port for securing Internet connections, as well as four integrated switch ports that enable easy deployment across multi-user environments.

For service providers and other organizations that want independent users to share a firewall appliance, the FortiGate product set is able to offer multiple, separately provisioned and managed instances of a single physical appliance through the use of multiple virtual domains (VDOMs). Across its product portfolio, Fortinet's dynamic approach to virtualization supports the management of multiple domains and brings with it scalability and performance capable of supporting thousands of virtual networks.

FortiGate devices can be deployed in parallel to deliver very high availability, either with the two appliances working in parallel or with one in standby mode. Furthermore, in the mid-to-high-end models, redundant power supplies have been included while add-on modules can provide power-failure bypass facilities for fail-to-wire operation. Devices that store security data (in particular FortiAnalyzer appliances) can support redundant disk approaches to strengthen their fault tolerance.

SOLUTION ANALYSIS

Anti-spam

Utilizing Fortinet's range of anti-spam services – such as dynamic scoring, domain classification, IP and email address blocking, identification scanning, and spam probing – the Fortinet Anti-Spam application is capable of blacklisting and whitelisting websites and domains, scanning emails for keywords, and leveraging dynamic scoring to deliver its user-level protection services.

Anti-malware (including anti-spyware and antivirus services)

Fortinet's gateway-based AV applications combine advanced signature and heuristic detection engines to detect and remove viruses, worms, spyware, and other malware at the gateway in realtime (using automatic antivirus signature updates from the FortiGuard Antivirus Service). Fortinet seeks to identify generic families of malware to avoid an excessive proliferation of malware signatures, and it focuses on malware that is currently active. Its scanners check both inbound and outbound files, including email attachments, and cover SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, FTP, HTTP/HTTPS traffic, and web mail.

Fortinet maintains several malware databases, to support its monitoring tools. Fortinet users can report suspicious system behavior which may be caused by malware that is not registered in the current malware database. Fortinet performs four regular threat updates every day, while additional updates may be provided when a serious threat is detected.

Firewall

FortiGate includes a functionally complete stateful-inspection firewall that delivers strong protection while maintaining enterprise-level throughput performance and scalability. Fortinet's FortiASIC chip is used as an accelerator to the firewall's processing and inspection capabilities, enabling multi-gigabit line-rate performance for inline network deployment.

Intrusion prevention

The alerting and blocking capabilities of the Fortinet Intrusion Prevention System (IPS) are supported by a customisable database of known security threats and an anomaly detection engine to detect unknown and evolving threats. The role of the IPS is to identify and stop threats that are directed to both network servers and browsers (clients).

Traffic shaping and application control

The Fortinet Traffic Shaping and Application Control service allows end-user organizations to maintain control over network communication. It includes protocol awareness, meaning that it doesn't rely on assigned ports for common applications; for example, it does not assume that HTTP traffic using port 80. It eliminates unwanted application communication, optimizes performance, reduces latency, and minimizes bandwidth demands. The Application Control service utilizes a dynamic application identification engine, which helps identify and classify applications based on their behavior and in turn enables administrators to define more granular application control policies. The appliance comes with a control list that is capable of classifying and defining policies for more than 1,000 applications to help administrators to define granular policies.

Virtual private networking (IPsec and SSL VPN)

Fortinet provides industry-standard, secure communication services using its extensive range of IPsec, PPTP, and L2TP VPN facilities. Fortinet also provides an integrated SSL VPN remote access feature which is capable of intercepting the SSL traffic and inspecting it for any possible threats before passing to the host. It is also possible to integrate the VPN with other existing Fortinet security services in order to provide complete network-level protection. The application interoperates with Radius, LDAP, local database, SecureID, and X-Auth protocols to provide users with authentication support for IPsec clients. FortiGate VPN is FIPS 140-2 certified and its integrated traffic-shaping capability enables prioritizing VPN traffic when there is contention for bandwidth.

Given that FortiGate is already designed to intercept application traffic and reassemble it for analysis, Fortinet's recent move to enable WAN optimization capability (including caching and compression techniques) on the appliance is a logical step. This feature accelerates applications passing through slow networks, while also ensuring that all of these communications are clean and secured by its integration with FortiGate's security services.

Web filtering

FortiGate can block inappropriate and malicious material and scripts, including Java Applets, cookies, and ActiveX scripts. Fortinet's Web Filtering service currently categorizes more than 25 million domains and billions of web pages. Fortinet categorizes identifiable content into one of 77 discrete categories so that its customers are able to enforce an appropriate usage policy, as well as avoid suspect websites and the malware that they may contain. FortiGate appliances use advanced techniques to detect proxy avoidance, further enhancing the effectiveness of the overall Web Filtering service. FortiGate appliances do not check the URL's embedded in a web page (it checks the linked pages only if the user clicks on the link). However, it does automatically check URLs embedded in email messages in order to block phishing attacks.

Data leakage prevention

Fortinet provides some basic DLP functionality – it has a pattern-matching engine to help identify sensitive information and prevent it from being transmitted outside of the network perimeter. For example, it can detect social security number formats or bank account number formats, based on predefined patterns and regular expressions (which can also be customized by the administrator, according to the organization's needs). This technology is also capable of providing audit trails for data and files, which in turn can support legislative compliance initiatives. However, this does not amount to a comprehensive DLP product as it does not perform data discovery functions, even though Fortinet plans to enhance this area of FortiGate's functionality.

Centralized management console and reporting services

Fortinet provides an enterprise with support for the information reporting needs of its security and systems management administrators. This capability is enabled through Fortinet's FortiManager and FortiAnalyzer platforms which can be deployed along with the FortiGate appliances.

FortiManager platforms are appliances that enable end-user organizations to manage all Fortinet products from a central console. The centralized FortiManager facility allows enterprise-wide management and administration of all networked and remote FortiGate appliances, allowing defensive policy changes and updates to be deployed quickly and effectively in response to newly identified threats. FortiManager and FortiGate reduce the administrative effort needed to deploy, configure, and maintain all Fortinet applications. Multiple FortiManager platforms can be deployed in a tiered configuration to support a hierarchical and delegated decision-making structure, reflecting how the enterprise is managed.

Fortinet recognizes that the delivery of up-to-date information and alerting services is key to providing an effective security infrastructure. To fulfill this requirement, it offers FortiAnalyzer – an appliance for the delivery of activity forensics, information archiving, and graphical reporting services. FortiAnalyzer provides comprehensive views of network usage and the associated security information requirements. It has important discovery capabilities and can be used to provide alerts and reports on vulnerabilities that are found across the whole organization.

PRODUCT STRATEGY

FortiGate appliances are designed to reduce overall protection costs both in terms of capital expenditure and operating costs, when compared to the deployment and management overheads of running multiple point-based security products.

Across its product range, Fortinet sells exclusively through its channel partners, and this strategy has made Fortinet build FortiGate appliances that are readily deployable across all market sectors (except the consumer market).

Consolidating security infrastructure usually provides end-user organizations with two distinct advantages: improved security that is delivered by reduced product fragmentation, and cost & time savings. Therefore, as an end-to-end provider of core protection services, Fortinet focuses on the savings that customer organizations can make in reduced renewal costs as point-based, third-party security contracts come up for renewal, and through reductions in other legacy support, maintenance, and associated running costs.

Key Fortinet business partners include Alcatel, BT, Dimension Data, Siemens, and Unisys. HP ProCurve, Riverbed, and VMware are all viewed as strategic technology partners (although none of these vendors provide technology that is sold by the company).

Licensing is on a per-hardware-device basis with no usage restrictions, and the only price variations are based on the level of support services that is required. These services may include firmware upgrades, technical assistance, and hardware replacement. Additional security-related subscription services, which are offered either as bundles or separately, include AV, AS, IPS, and web filtering services. These subscriptions are necessary if the customer wants to use the corresponding services on the appliance (some customers buy FortiGate just for its firewall and network traffic management capabilities).

IMPLEMENTATION

FortiGate appliances are designed and built for ease-of-use and fast deployment. However, as would be expected, the more complex configurations that are required to support the protection requirements of enterprise environments often require pre-deployment planning, and support from the company's network of value-added resellers (VARs). Therefore deployment timescales vary depending on the FortiGate appliance model or models being deployed and the network infrastructure complexities.

FortiGate systems can be deployed using a modular approach. Many of the company's security protection services can be delivered with the appliance, but activated when they are needed by the end-user organisation. FortiGate permits each of these services to be configured individually.

Post deployment, management is normally controlled using a central console approach (FortiManager). As its automated update capabilities and administrated privileges can be controlled in a hierarchical way, the post-deployment management and support efforts are minimized.

Fortinet provides both classroom-based and online training facilities. Technical support on complex issues is provided from the company's Technical Assistance Centres and, where appropriate, via partners worldwide with routine level-one support being provided by Certified Support Partners.

Fortinet's technical support options include:

- FortiCare 8×5 Enhanced Support offering (charged at 5–10% of the appliance cost) supporting customers via a web portal and online chat system. This also includes a return and replace (three Days) hardware support service

- 24×7 round-the-clock mission critical service (charged at 15–20% of the appliance cost) delivered by online ticket access, online chat, and telephone. This service also includes a hardware replacement service that allows customers to maintain high levels of availability.

Deployment examples

Banco do Brasil: Banco do Brasil has deployed the FortiGate appliances to provide firewall, intrusion prevention and virtual private network protection at its headquarters and at 145 other locations across Brazil. It also uses FortiManager and FortiAnalyze to help monitor and analyze network activity and attempted attacks. Nine FortiGate-3600A appliances are deployed in its headquarters to connect to the branches using VPN connectivity. They also help to secure self-service applications at branches and over the Internet. These include applications running on ATM machines. The bank has 80 FortiGate-311B appliances deployed in high-availability mode to protect the bank's data center. These are managed through two FortiManager- 3000 and two FortiAnalyzer-2000A appliances. The branches have two FortiGate-1100C appliances deployed in high-availability mode to secure their end of the connections with head office. The network of appliances allows the bank to change rules quickly and effectively throughout the bank without the need for technical staff at the branches.

Elsag Datamat: E-Security, the IT security division of Elsag Datamat, chose FortiGate to secure the G8 summit in Italy in July 2009. It wanted an integrated network security solution with high performance, reliability and ease of management. The FortiGate-3600A appliance provided ten Gigabit Ethernet interfaces having up to 6Gbps of throughput. From a security perspective it provided:

- network perimeter protection
- segmentation of wired and wireless areas and the definition of policies for trusted and untrusted user profiles on specific areas
- high availability.

FortiGate's virtual domains were used to virtualize, separate, and distribute multi-layer security through the various components of the portal: the application, the web, and the database. FortiAnalyzer provided centralized analysis and reporting of more than 1 million security events that occurred during the conference.

Table 1: Contact Details

US Headquarters
1090 Kifer Road
Sunnyvale
CA 94086, USA
Tel: +1 408 235 7700
Fax: +1 408 235 7737
www.fortinet.com

EMEA Tech Support and Training Centre
120 Rue Albert Caquot 06560
Sophia Antipolis
France
Tel: Tech Support: +33 4 8987 0555
Tel: Sales Support: +33 4 8987 0510
Fax: +33 4 8987 0501

Source: Fortinet

OVUM

Headquarters
Shirethorn House,
37/43 Prospect Street,
Kingston upon Hull,
HU2 8PX, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Australian Sales Office
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

End-user Sales Office (USA)
245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684

For more information on Ovum's Subscription Services please contact one of the local offices above.

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Ovum cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Ovum will not be liable for any interpretations or decisions made by you.