



# Total Cost of Ownership: Benefits of Comprehensive, Real-Time Gateway Security

## White Paper

*September 2003*

### *Abstract*

The network security landscape has changed dramatically over the past several years. Until fairly recently, many organizations felt protected against network-based attacks if they installed a conventional, network-layer firewall between their Internet connection and their internal, trusted network. However, beginning with the much publicized Code Red and Nimda worms, and continuing with the more recent Lovsan and SoBig attacks, the most damaging and fast-moving network threats are content-based, and are not prevented by conventional firewalls. Once these content-based threats enter a network they spread quickly and can often outrun conventional, host-based antivirus defenses. As a result, organizations that wish to implement a complete protection system are faced with the challenge of purchasing and integrating numerous independent systems at the network gateway in order to detect and defeat intrusions, viruses and worms, malicious Web and email content and the like. For most organizations the cost of purchasing and maintaining numerous individual systems is prohibitive. The problem is further exacerbated by the fact that software-based antivirus and content filtering products cannot keep up with today's (and tomorrow's) network speeds.

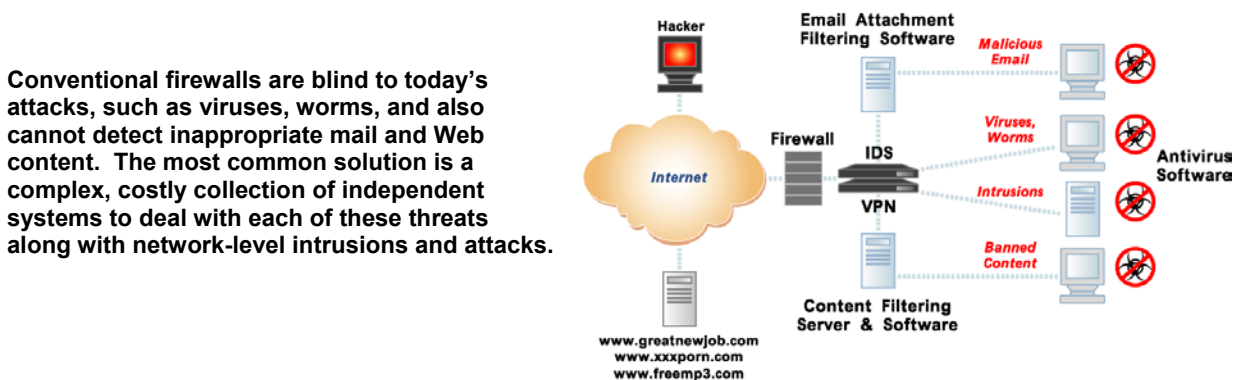
This paper examines the needs for comprehensive gateway security in a range of environments – including enterprise headquarters as well as branch office and small/medium business applications – and presents the total cost of ownership (TCO) benefits of Fortinet's integrated, ASIC-accelerated FortiGate™ Antivirus Firewall systems for delivering comprehensive security at the network gateway.

## THE REQUIREMENTS FOR COMPREHENSIVE GATEWAY SECURITY

Security at the network gateway must address both network-level and application-level, or content-based threats. Network level threats are typically addressed using the following devices:

- *Firewalls* that provide stateful inspection and network address translation to prevent unauthorized connections
- *VPN gateways* for network-level encryption to enable public networks to be used as secure virtual private networks (VPNs)
- *Network intrusion detection systems (NIDS)* and *intrusion prevention systems (IPS)* to detect and/or prevent attempts to exploit flaws in network protocols, server operating systems and applications

All of these systems – firewalls, VPN gateways, NIDS and IPS – are available as network devices that are deployed at the network gateway much like routers and other networking devices. By contrast, application-layer threats are typically handled using application software deployed on hosts at or behind the network gateway. These systems include gateway antivirus software (most often deployed on mail servers) and Web content filtering software. Finally, host-based antivirus software is deployed on servers, desktops and laptops to defend against the viruses, worms, Trojans and other content-based threats that bypass conventional edge protection. A typical configuration is shown in *Fig. 1* below.



*Fig. 1*

The situation depicted in *Fig. 1* is problematic for both large and small organizations:

- For small companies as well as for the branch offices of larger companies, the cost of equipment, system integration and ongoing maintenance is prohibitive.

- For headquarters locations and other large enterprise sites, software-based gateway antivirus products are generally ineffective against attacks embedded in real-time, non-email (e.g. Web) applications, or else they add unacceptable delays when attempting to screen real-time, HTTP traffic.

An increasing number of attacks, such as Lovsan and SoBig, are best characterized as “blended threats.” They utilize a combination of network-level and content-based attacks to evade conventional defenses. In order to deal with these new, more potent threats, network protection systems must become more integrated, flexible and real time while remaining affordable and manageable.

### **THE FORTINET SOLUTION: FORTIGATE ANTIVIRUS FIREWALLS**

Fortinet’s award-winning FortiGate Antivirus Firewalls represent a new type of platform that delivers comprehensive security with real-time performance, and also provides key TCO benefits relative to conventional products. FortiGate systems employ a unique, ASIC-accelerated architecture that provides the ability to perform network-level and content-level security without slowing critical network applications, including real-time applications such as Web traffic. The 10-member FortiGate product series offers models that span from telecommuter and SOHO applications as well as small business, branch office, and large enterprise applications. All FortiGate units are capable of providing a complete complement of integrated services including:

- Antivirus (ICSA certified)
- Content filtering
- Intrusion prevention
- Intrusion detection (ICSA certified)
- VPN (ICSA certified)
- Firewall (ICSA certified)

For small organizations and branches, FortiGate systems provide an “all-in-one” solution that delivers complete network and content security at the gateway. For enterprise headquarters and data centers, FortiGate systems can be deployed as a complement to existing firewall, VPN, NIDS and other network-level security products to provide high-performance antivirus and content protection for email, Web and file transfer traffic. For all types of organizations and deployments, FortiGate systems offer significant TCO benefits, as illustrated next.

### **TCO COMPARISON IN AN ENTERPRISE ENVIRONMENT**

Many enterprises have installed “best of breed” firewalls, VPN gateways and intrusion detection systems at their network perimeter, and have also installed antivirus software on their email servers (as well as on servers, desktops and laptops across their companies). Yet even with these protections in place, numerous enterprises succumb to content-based attacks for several reasons:

- Firewalls do not detect or stop content-based threats. They simply pass all traffic from Web servers, email servers and many other sources on the Internet, relying on downstream systems (such as intrusion prevention or systems or antivirus software) to detect malicious content.
- Most antivirus software deployed at network gateways is used to scan email traffic. However, an increasing number of attacks evade detection by gateway antivirus software by using non-email protocols (such as HTTP) to initiate and propagate.
- New attacks are very disruptive to IT organizations, which are forced to divert key people and resources to updating laptops, desktops and servers with the latest antivirus signature database each time a new threat is unleashed.

In view of the issues above, every enterprise should include comprehensive gateway antivirus protection as an essential element of its network security strategy to complement its host-based antivirus protection. Unfortunately, very few enterprises have done so because of the high costs and low performance of software-based antivirus technology. Antivirus software deployed on conventional computing hardware is very slow and causes significant performance delays that are especially noticeable for real-time applications such as Web traffic. Providing adequate performance using standard computing hardware requires significant investments in server hardware and gateway antivirus software licenses.

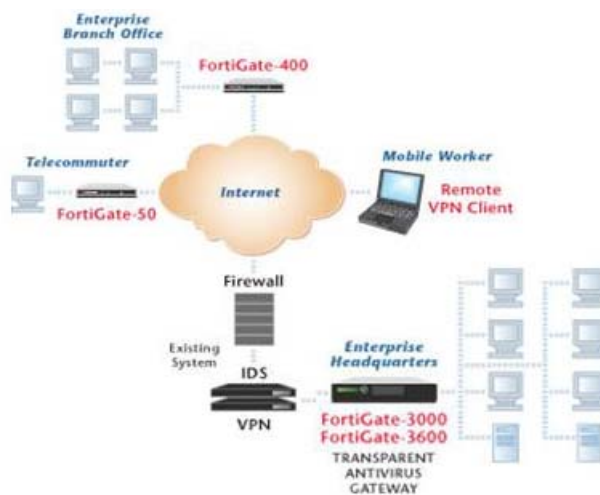
Fortinet's unique, ASIC-based architecture changes the price/performance equation for real-time gateway antivirus protection. FortiGate antivirus firewalls screen email (SMTP, POP3, IMAP), Web (HTTP) and file transfer (FTP) with performance that exceeds several hundred megabits/second (depending on the FortiGate model, protocol and traffic mix).

The following is an example taken from a real customer application in which Fortinet was compared (and chosen) versus a software-based gateway antivirus solution:

- A large publishing company required content security to protect its central data center containing confidential, proprietary information. Peak bandwidth in and out of the data center is approximately 100 Mbps. In order to meet the requirement for real-time performance, a leading AV software company configured a solution that required 15 general purpose servers and 15 licenses for the antivirus software, plus load balancers and integration services.
  - Total cost of acquisition for antivirus software licenses, server hardware and load balancers:
    - \$225,000.00
  - Annual hardware maintenance and antivirus software subscriptions:
    - \$85,000.00

- 3-Year cost of ownership:
  - \$480,000.00
- Comparable Fortinet solution: Two FortiGate 3600 Antivirus Firewalls configured in a high-availability (HA) arrangement. Either FortiGate unit can deliver the full 100 Mbps bandwidth requirement – the additional unit is for backup in the event of a failure.
  - Total cost of acquisition:
    - \$60,000.00
  - Annual hardware and software maintenance and antivirus subscription:
    - \$15,000.00
  - 3-Year cost of ownership:
    - \$105,000.00

The Fortinet solution saves \$375,000 over three years.



Fortinet's enterprise systems plug the gap left by conventional, email-centric antivirus software. They can be deployed transparently, in conjunction with existing firewall, VPN and other legacy systems to close the vulnerability window and stop content attacks in email and Web traffic in real time. High availability features eliminate costly downtime.

*Fig. 2*

## TCO COMPARISON IN A BRANCH OFFICE/SMB ENVIRONMENT

There are several reasons why all organizations including small businesses, branch offices and even telecommuter locations require complete network protection. One key reason is that content-based threats are indiscriminate, and spread with equal ease to large and small companies. Another reason is that in today's increasingly connected environment, both large and small companies are establishing intranets and extranets that link them with remote sites whose security status cannot be verified. As a result, large organizations are vulnerable to attacks that may first penetrate the home networks of

telecommuters (or the networks of their business partners) and then propagate over “secure” VPN tunnels. Small businesses are equally vulnerable to attacks originating at larger companies with whom they communicate.

Regardless of total company size, few organizations can afford the initial capital outlays and maintain the skilled people required to purchase, integrate and maintain disparate security technologies at SOHO, small business and branch office locations. As a result, most small and mid-sized locations are not fully protected.

By integrating multiple, high-performance security technologies into a single system, FortiGate antivirus firewalls enable complete, affordable network protection for any environment, at costs that are dramatically lower than those required with disparate, older-generation technologies, as shown below in *Fig. 3*:



*Fig. 3*

The following table (*Fig. 4*) shows a TCO comparison for a FortiGate 60 Antivirus Firewall versus a collection of conventional products. The FortiGate 60 is typically deployed in small offices with between 10 and 50 users (depending on traffic). In this scenario, the 3-year life cycle cost of the FortiGate unit, which is between \$1,750 and \$2,250, is less than 1/6<sup>th</sup> that of the conventional system, which costs between \$12,800 and \$13,300 over a 3-year period. Note that this comparison does not attribute any savings to the FortiGate unit for its inherently lower costs for initial installation and ongoing management and administration.

<b>FUNCTION</b>	<b>FortiGate 60</b>	<b>CONVENTIONAL TECHNOLOGY</b>
<b>Firewall</b> (NAT, Stateful Inspection, ICSA Certified)	Included	Firewall/VPN Appliance
<b>IPSec VPN</b> (ICSA Certified)	Included	Firewall/VPN Appliance
<b>Gateway Antivirus</b> (SMTP, POP3, IMAP, HTTP, FTP)	Included	Standalone server and antivirus software; Poor performance for Web traffic
<b>Intrusion Detection</b> (1,400 attack signatures, ICSA Certified)	Included	Standalone NIDS device
<b>Intrusion Prevention</b> (34 attack signatures)	Included	Included
<b>Web &amp; email Content Filtering</b> (URLs, keywords & phrases, senders, ActiveX, Scripts, File Block, etc.)	Included	Standalone server, Web content filtering software, antis spam service
<b>Base Cost</b>	\$995 (10 users) \$1,495 (unlim)	\$700 (10 users) \$1200 (unlim)
Cost for Antivirus	Included	\$1,500
Cost for NIDS	Included	\$4,000
Cost for Content Filtering	Included	\$1,500
Total Acquisition Cost	\$1000- \$1,500	\$7,700 - \$8,200
Annual Maintenance & Subscriptions	\$250	\$1,700
<b>3-Year Cost</b>	\$1,750 - \$2,250	\$12,800 - \$13,300

**Fig. 4:** For a small office, the TCO of a FortiGate 60 is roughly 1/6<sup>th</sup> that of a collection of conventional systems, and also offers additional advantages in terms of security, performance and administration.

A similar analysis in *Fig. 5* for a mid-sized business or branch office shows the advantages of a FortiGate 300 versus a conventional solution:

<b>FUNCTION</b>	<b>FortiGate 300 Antivirus Firewall</b>	<b>CONVENTIONAL TECHNOLOGY</b>
<b>Firewall</b> (NAT, Stateful Inspection, ICSA Certified)	Included	Firewall/VPN Appliance
<b>IPSec VPN</b> (ICSA Certified)	Included	Firewall/VPN Appliance
<b>Gateway Antivirus</b> (SMTP, POP3, IMAP, HTTP, FTP)	Included	Standalone server and antivirus software; Poor performance for Web traffic
<b>Intrusion Detection</b> (1,400 attack signatures, ICSA Certified)	Included	Standalone NIDS device
<b>Intrusion Prevention</b> (34 attack signatures)	Included	Included
<b>Web &amp; email Content Filtering</b> (URLs, keywords & phrases, senders, ActiveX, Scripts, File Block, etc.)	Included	Standalone server, Web content filtering software, antispam service
<b>Base Cost</b>	\$5,995	\$7,000
Cost for Antivirus	Included	\$6,000
Cost for NIDS	Included	\$8,000
Cost for Content Filtering	Included	\$3,000
Total Acquisition Cost	\$6,000	\$24,000
Annual Maintenance & Subscriptions	\$2,000	\$6,000
<b>3-Year Cost</b>	<b>\$12,000</b>	<b>\$42,000</b>

*Fig. 5:* For a mid-sized business or branch office, the FortiGate 300 provides high throughput (up to T3 connections) and has a TCO which is less than 1/3 of conventional systems over a 3 year period.

## **CONCLUSION**

Traditionally, many companies have faced the difficult tradeoff of better security vs. higher costs. As the only firewall/VPN security product line with integrated AV, content filtering and IDP from telecommuter/SOHO through multi-gigabit, enterprise and service provider models, FortiGate Antivirus Firewalls set new standards in affordability and value for money, allowing organizations to access enterprise-class network security at substantially lower total costs of ownership, without sacrificing competing corporate initiatives worthy of strategic investment, while gaining a greater defense in depth network protection strategy.

## **FOR MORE INFORMATION**

Please visit our web site at [www.fortinet.com](http://www.fortinet.com) or email us at [info@fortinet.com](mailto:info@fortinet.com)