



# Delivering Complete Network Protection Using Advanced Content Processing Technology

## White Paper

### Abstract

*Complete **Network Protection** addresses the full range of problems that threaten the security, productivity, and efficiency of enterprise networks, including network intrusion and attack prevention, virus/worm blocking, email spam prevention, and content filtering. Conventional solutions such as firewalls, VPN gateways and intrusion detection systems don't solve the problem: They only analyze packet headers and cannot detect threats embedded in network content, because they lack the processing power necessary to analyze content in real time to detect viruses, worms, or inappropriate content – and therefore leave the network edge open to a wide range of costly, content-borne threats. In response, most organizations deploy host-based anti-virus, content filtering, and spam elimination software to deal with application-level threats – and suffer increased exposure, reduced network performance, and increased costs.*

*This paper introduces Fortinet's ABACAS™ (Accelerated Behavior and Content Analysis System) technology, a powerful, patent-pending combination of software and ASIC-based hardware that breaks the Content Processing Barrier. ABACAS technology – the basis of Fortinet's FortiGate line of Secure Content Processing Gateways – delivers application-level services, like virus detection and content filtering, along with network-level services, including firewall, VPN, intrusion detection, and traffic shaping at the network edge, in real time. The result is reduced exposure to network attacks, better control over network content and resource usage, better performance, lower costs, and easier administration.*

© 2002 Fortinet, Inc. All rights reserved.

*The information contained in this document represents the current view of Fortinet, Inc. on the issues discussed as of the date of publication.*

*This white paper is for informational purposes only. FORTINET MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Fortinet Corporation.*

*Fortinet may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Fortinet, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.*

*Fortinet, FortiGate, FortiASIC, FortiOS, and ABACAS are either registered trademarks or trademarks of Fortinet Inc., in the United States and/or other countries.*

*FortiNet Inc.*

*1731 Embarcadero Road, Suite 200*

*Palo Alto, CA 94303; USA*

---

## Contents

<b>Network Protection - Past, Present, and Future .....</b>	<b>1</b>
Old Security Concerns: Physical attacks .....	1
Old Security Concerns: Protocol attacks .....	1
New Security Concerns: Content attacks .....	1
Other network protection problems: Bad Content, Spam, and More .....	2
<b>Conventional Approaches are Limited .....</b>	<b>3</b>
Conventional network security gateway technology .....	3
Conventional virus detection/prevention technology .....	3
Contentional content filtering technology .....	4
<b>The Content Processing Barrier .....</b>	<b>5</b>
<b>Fortinet Breaks the Barrier .....</b>	<b>6</b>
<b>Powered By ABACAS™ Technology .....</b>	<b>7</b>
<b>FortiGate Content Processing case study: Virus/Worm protection..</b>	<b>9</b>
Virus/Worm protection config options .....	9
High level protection .....	9
Medium level protection .....	10
Low level protection .....	10
Virus database options .....	10
Worm scanning .....	10
No user intervention required .....	11
Virus scanning methodologies .....	11
Signature scanning .....	11
Macro scanning .....	11
Heuristic scanning .....	11
Comprehensive protection .....	12
<b>Protection Against Network Misuse and Abuse .....</b>	<b>12</b>

---

---

**A Platform for Today and Tomorrow ..... 12**

**For more information ..... 13**

---

## Network Protection – Past, Present, and Future

Network protection in today's environment requires solutions that specifically address current and future threats to network security, employee productivity, and network usage efficiency. There have been significant changes in the information technology industry that create new challenges for companies that use e-commerce and on-line collaboration to drive their businesses.

Historically, network protection was focused almost exclusively on security concerns, and security solutions were focused primarily on so-called protocol level attacks: To fend off these threats, enterprises largely rely on firewalls, which scan packet headers only, to block network-level attacks.

However, content-borne attacks including viruses and worms embedded in email attachments, downloaded files from the internet, and macros in MS Office files are becoming the dominant cause of damage to IT resources. A successful virus attack may jeopardize confidentiality and result in loss of productivity and information. Facing these challenges are Internet based businesses as well as offline enterprises with internet connections (SOHO, SME, large enterprise) and service providers/Telcos.

In addition to security concerns, other issues related to network productivity are receiving increased attention. Most notably are email spam, and misuse and abuse of networks in the form of browsing/downloading inappropriate content and using the network for non-productive tasks. A comprehensive network protection solution must address these concerns in addition to network security.

### Old Security Concerns: Physical attacks

When networks were first used for storing and exchanging information, the major security threats were from physical attacks. The physical theft of discs and tapes, and the theft of data through wire-tapping were methods used by those attempting to gain access to private information. Protection from physical attacks was fairly simple and involved locating key network components in physically secure areas.

### Old Security Concerns: Protocol attacks

As physical security improved, attempts to gain access to private information moved to the protocol level. Probing networks and operating systems, the newly arrived "Hackers" employed their skills to gain unauthorized access to networks and file systems that contained information they wanted to steal or destroy. Hacking methods included spoofing, password cracking, denial-of service, and other protocol-level attacks. Prevention of protocol attacks led to the development of firewalls, VPN gateways, and intrusion detection systems (IDS), which can provide excellent protection from these attacks.

### New Security Concerns: Content attacks

We now know that the most potent dangers to computer networks are caused by malicious code contained in the content of Internet traffic. This malicious

---

code comes in the form of viruses, worms, active web content, and Trojan horse/agents. The newer, more sophisticated threats use a combination of network-based assaults in conjunction with content-based attacks to compromise and subvert networks and the resources they connect, often with devastating results:

- According to a recent analysis of network logs from hundreds of companies worldwide, content-based attacks are generating the most significant damage: **Over 63% of all attacks logged from July to December, 2001 were related to just two attacks, the Nimda and Code Red worms.** (Source: Ripstech)
- The cost of recovering from attacks is skyrocketing: Following the Nimda attacks, many major corporations cut off Internet connectivity for periods ranging from several days to several weeks. The combined costs related to damage and recovery from Code Red approached \$2.5 billion, and the related costs for Nimda were \$3 billion. **Worldwide, damage from malicious attacks in 2001 has been estimated at \$12-13 billion** (Source: eWeek).

Other network protection problems: Inappropriate Content, Spam, and More ...

Organizations suffer significant losses related to the misuse and abuse of network resources. For example:

- Email spam is top on the list of abuse of network resource for many enterprises. One large telecommunications company with 45,000 employees estimates that each “spam” message costs \$1 per piece in lost productivity. They also see the volume of spam doubling every 5 months. AT&T Worldnet estimates that 20% of its incoming messages are spam – and some ISPs estimate that spam accounts for over 50% of email traffic.
- Misuse is also a major concern. Non-productive activities such as Internet games, chat, music swapping, and inappropriate content browsing waste valuable network resources as well as productive time. Many public and private organizations are struggling to control access to appropriate content without overly restricting access to legitimate material and services.
- Non-essential or non-critical traffic can interfere with the ability to deploy new services that improve communications: Many organizations face expensive network upgrades in order to support new, bandwidth-sensitive network services, such as audio, video, and voice. In many cases these services could be deployed without costly upgrades by controlling the resources allocated to bandwidth-insensitive applications, such as email, web browsing, and file transfer.

---

## Conventional Approaches are Limited

### Conventional network security technology

In the early 1990's, Network Address Translation (NAT) addressed the problems associated with protocol-level attacks. NAT hides the IP addresses of protected private networks so that unauthorized users on the external network (the Internet) cannot target computers on the internal network. The NAT solution still provides effective protection against many protocol attacks.

In combination with NAT, most conventional firewalls use a technology called stateful inspection to examine and forward TCP/IP packets. Stateful Inspection examines the header of each packet received by the firewall and matches that header against a set of predefined policies based on network protocols and source and destination addresses. Packets are allowed or denied based on this information without any reference to the content of the packet.

While effective at providing protocol-level protection, NAT and stateful inspection do not fully meet the needs of today's network security climate:

- Neither are effective against attacks like viruses and worms that are hidden in the content of the network traffic
- Neither can effectively deny packets containing offensive material such as pornography or nuisance content such as inappropriate web sites.

The firewall products currently on the market are incapable of content level network attack and misuse protection, and therefore fail to deliver complete network protection.

### Conventional virus detection/prevention technology

To provide protection from viruses, most organizations attempt to install virus scanning software on all of the computers in their network. While a necessary part of any complete network protection solution, these so-called "host based anti virus" products do not provide complete protection on their own. In particular, without virus protection at the network edge, organizations are vulnerable to attack with each new threat until every host in their network has received updated anti-virus software. With new attacks reported almost weekly, organizations are constantly exposed, and spend significant resources ensuring that all hosts are constantly updated. If even one host on the network is not protected, a successful virus attack can result.

Conventional virus protection also does not prevent the spread of malicious material throughout a network. Email users may still spend a portion of their valuable time each day deleting virus-containing emails that have passed unchanged through their organization's firewall.

Most importantly, most of the current virus scanning solutions do not protect against threats from files downloaded from the World Wide Web. Instead, they only scan email attachments. In fact, a common way for email-based viruses to enter a protected network is through employee use of personal web-based email accounts (such as Yahoo, and Hotmail) while at work.

---

### Conventional content filtering technology

Currently, the most popular solutions for blocking unwanted web activity is to block access to a list of banned (or “blacklisted”) web sites and pages based on their URLs. The URL blocking approach can be unnecessarily restrictive, preventing access to valid content on sites that may contain only a limited, localized amount of unwanted material. And as with virus scanning, the list of blocked URLs requires constant updating. Further, certain URLs may have little to do with the content included in the website and these URLs might never make their way into the URL blocking database.

Many of the popular email spam elimination systems also use blacklists to eliminate unwanted email messages. These systems match incoming email messages against a list of mail servers that have been pre-identified to be spam hosts, and drop messages from these servers. As with URL blocking for web content filtering, blacklist-based spam elimination has a number of limitations. For example, spammers often launch email spam from different hosts every time, and may even manage to compromise a victim’s host (e.g., your channel partner’s mail server) and use it as a spam server. Simply maintaining a list of spam servers barely helps solve the problem.

Conventional content filtering using a blacklist approach cannot provide a complete solution to the problems of inappropriate web activity and email spam. Intelligent, detailed analysis of content is the key to managing these problems.

## The Content Processing Barrier

Host-based anti-virus and content-filtering solutions are expensive to deploy and manage and also suffer significant limitations. A better approach would be to provide anti-virus and content filtering services at the network edge, where they'd be most effective – just as with firewalls, VPN gateways, and intrusion detection systems. However, application-level content processing requires enormous computing resources as compared with network-level processing – in many cases by a factor of 100 or more. As a result, it has not been possible to deploy content-processing applications at the network edge without severely degrading network performance. This is the Content Processing Barrier.

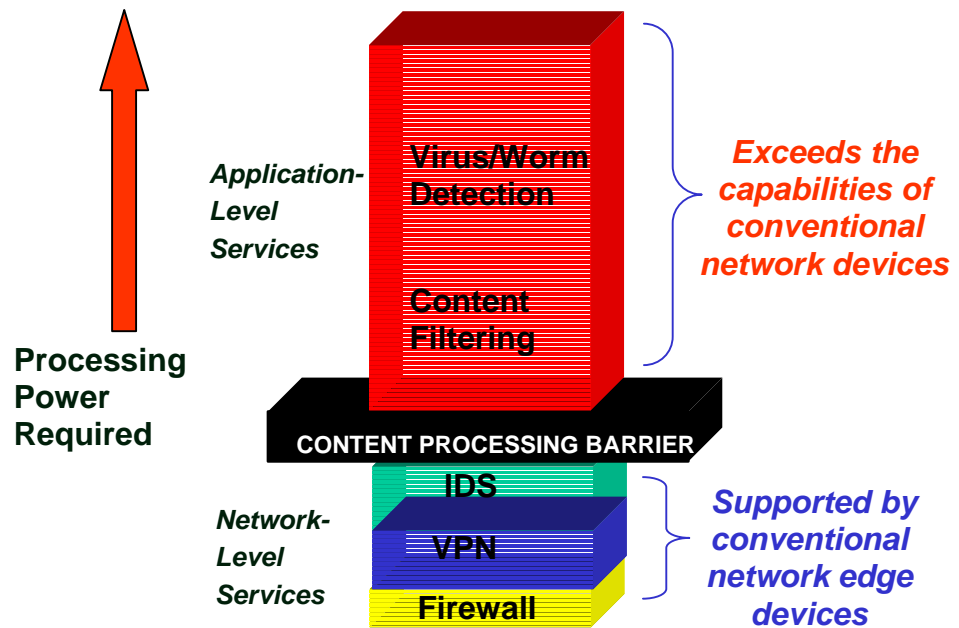


Figure 1. The Content Processing Barrier Limits the Capabilities of Conventional Network Devices

The Content Processing Barrier makes networks less secure, less productive, and more expensive to operate, because it leaves networks vulnerable to attacks, blind to unproductive content, and burdened with the costs of acquiring and integrating numerous point solutions. Conventional solutions cannot provide complete network protection and meet the requirements of today's cost-conscious organizations. A new approach is required.

---

## Fortinet Breaks the Barrier

Fortinet's FortiGate Secure Content Processing Gateways (SCPGs) are the first products that have been designed to provide complete, cost effective network protection in a single, integrated solution. Built using dedicated hardware/software platforms and powered by Fortinet's FortiASIC Content Processor chips, FortiGate systems provide tremendous processing power and application-level service intelligence. FortiGate systems enable network-based deployment of traditionally host-based services such as virus/worm protection and content filtering, along with network-level services, without compromising network performance.

Each FortiGate series SCPGs provides high-performance network-level services, such as firewall, VPN, intrusion detection, and traffic shaping, in addition to anti-virus and content filtering, at data rates up to 2 gigabits/second. The FortiGate gateways complement or eliminate the need for other point solutions, resulting in lower costs for equipment and maintenance and greatly simplified installation and management.

The FortiGate product line includes models that address a wide range of price/performance needs, from telecommuter and SOHO through branch office, enterprise, and service provider environments:

- FortiGate-50 for home and SOHO users
- FortiGate-100 and 200 for branch offices and small businesses
- FortiGate-300 and 400 for medium-sized and large businesses
- The FortiGate-2000 for large enterprises and service providers requiring Gigabit+ performance.

*For more information on FortiGate product suite, go to: <http://www.fortinet.com>.*

**Powered by ABACAS™  
Technology**

Fortinet's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which includes the FortiASIC™ Content Processor and the FortiOS™ Content Processing Operating System, is the basis of the FortiGate systems' high performance capabilities. The FortiASIC Content Processor contains a powerful, flexible signature scanning engine that can match a wide range of content types against the "signatures" of thousands of viruses, intrusion attacks, keywords, or other patterns without compromising network performance. The FortiASIC chip also includes a cryptographic acceleration engine to support high-performance VPN encryption and decryption. By functioning as VPN gateways, the FortiGate units are able to "see inside" VPN tunnels and prevent harmful material from entering the private network that would otherwise pass through unchecked. In addition, the FortiASIC chips contain hardware engines that accelerate packet header analysis (for firewall processing and intrusion detection) as well as a flow management engine to support traffic shaping.

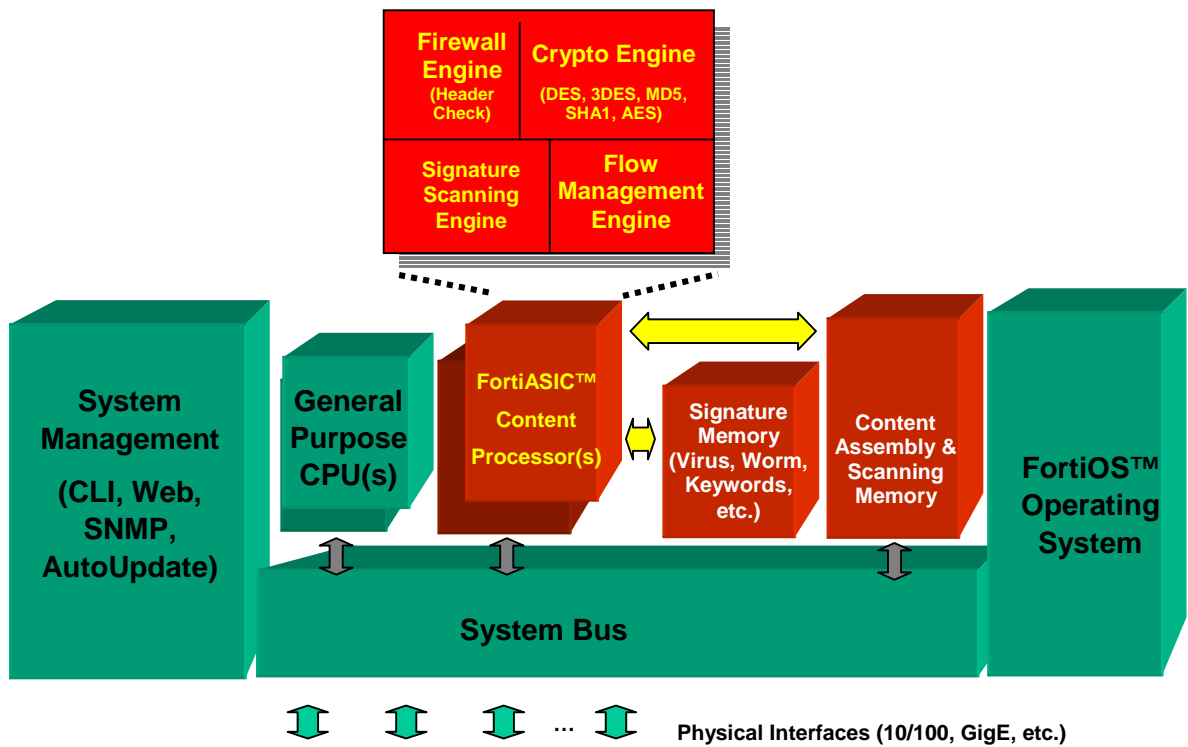


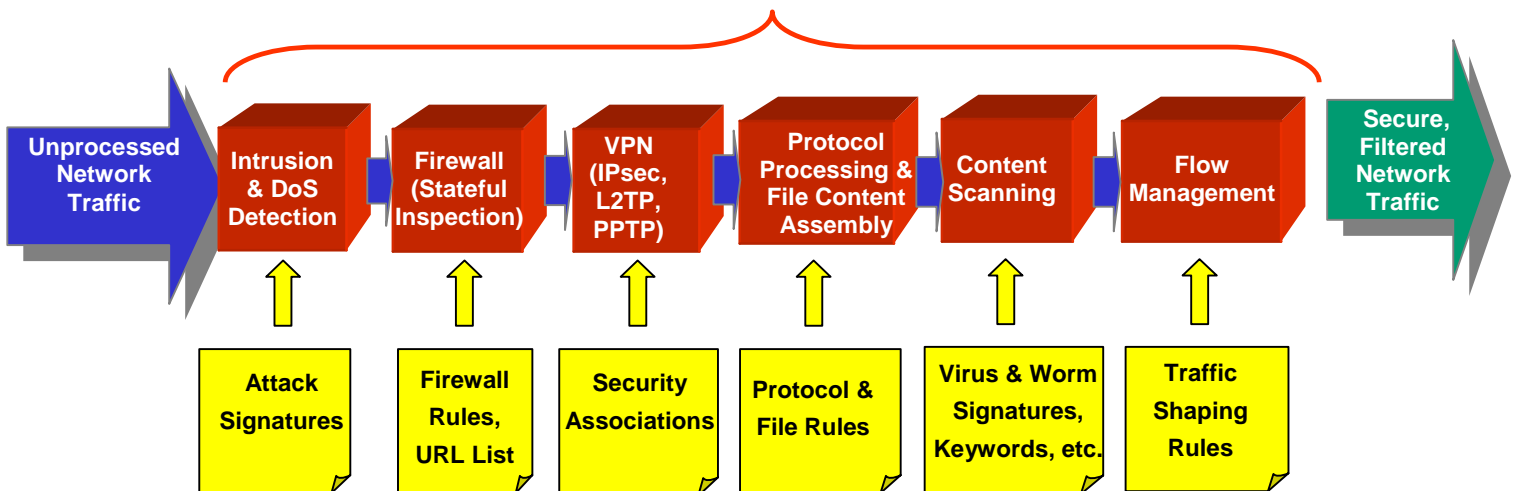
Figure 2. FortiGate Systems Leverage Advanced ASICs and Software for Unparalleled Performance

FortiGate systems protect networks from content borne attacks such as viruses and worms, and prevent networks from being penetrated by unwanted email and inappropriate content by screening the information carried in content protocols. The content protocols carry web traffic (HTTP) and email traffic (SMTP, POP3, and IMAP). Content scanning begins when the FortiGate receives network traffic and re-directs all content protocol traffic to the FortiTCPIP stack. The high-performance, hardware-assisted FortiTCPIP stack controls the processing of all content protocols. When a content stream is first received, the FortiTCPIP stack creates connections to both client and server to begin the transmission of the packets. The stack then receives the packets and converts them to a content stream.

Content streams are separated according to their service type and sent to an associated command parser. There is one command parser customized to understand each content protocol. The command parser analyses the content stream for content that could contain viruses, worms, banned content, and other content borne attacks/network intrusion. For example, if the content is an HTTP stream the command parser screens for uploading or downloading files. If the content is an email stream the command parser screens for attachments or embedded code. If the stream contains attachments or upload/download files, it is diverted to the virus scanning engine. All other content is routed to the content filter engine where, if content filtering is enabled, the stream is either blocked or allowed depending on the content filtering settings.

Figure 3. The FortiASIC Chip Accelerate All Phases of Network Protection

### FortiASIC Content Processor



---

## **FortiGate Content Processing Case Study: Virus/Worm Protection**

When the patent-pending FortiGate virus scanning engine receives a new content stream, it scans the stream for target files that may contain viruses or worms. The virus scanning engine scans all files being uploaded or downloaded using HTTP or in email attachments. The virus scanning engine is looking for target files that may be executable (exe, bat, and com), visual basic files (vbs), compressed files (zip, gzip, tar, hta, and rar), screen saver files (scr), dynamic link libraries (dll), MS Office files, etc.

Most HTTP files and email attachments use the MIME (Multipurpose Internet Mail Extensions) format. The virus scanning engine is able to parse MIME files to find the target files.

All target files that are found are intercepted by the virus scanning engine. The virus scanning engine then processes these files according to the FortiGate virus protection configuration.

### Virus/Worm protection config options

You can configure FortiGate virus scanning for three levels of virus protection: high, medium and low. Several configuration options are available for each level of virus protection. By changing the protection level and the configuration options for each level, you can quickly and easily react to new virus threats before your network becomes infected.

### **High level protection**

You can configure High-level protection to remove all target files from HTTP transfers and email attachments before they enter your private network. With high level protection turned on, the FortiGate does not perform virus scanning. Instead, all files and attachments are identified and removed from content protocol data streams.

You can switch on high-level data protection separately for the HTTP, SMTP, POP3, and IMAP content protocols. For each content type, you can also select target file types to be removed. The virus scanner replaces deleted files with an alert message that is forwarded to the user.

High-level protection can be used to remove all content that poses a potential threat before it reaches your protected network. This security level provides the best protection from active computer virus attacks. It is also the only protection available from a virus that is so new that no effective virus scanner is available for it.

You would not normally run the FortiGate with high-level protection turned on. However, it is available for extremely high risk situations, where there is no other way to prevent viruses from entering your network.

---

### **Medium level protection**

When you configure the FortiGate for Medium-level virus protection, the virus scanning engine scans all target files for viruses. You can configure the virus scanning engine to perform up to three different types of virus scans on each target file.

If a virus is found in a file, the virus scanner deletes the file and replaces it with an alert message that is forwarded to the user. If a virus is not found, the file is added back into the data stream and forwarded unchanged to the user.

### **Low level protection**

The low level of virus protection can be used to temporarily suspend virus protection. With the FortiGate configured for low-level virus protection, all target files are forwarded unchanged to their destinations.

### **Virus database options**

When configured for virus scanning, FortiGate offers you three options of virus database size as follows:

1. Standard virus database. This virus database option covers the most dangerous virus in the wild-list. Typically, the wild list contains approximately 800 viruses that are known to be active. Customers selecting this option are effectively shielded from the known virus attacks that have the ability to damage your infrastructure.
2. Extended virus database. This option covers over 6,000 viruses. This list includes the viruses in option 1, and also includes a large number of viruses that, while rarely propagated over the Internet, are nonetheless still found and may be introduced inside your network via floppy disks or CDs.
3. Extreme virus database. This option includes essentially all known viruses, and provides protection from virus attacks of any kind.

You can switch between different virus database options at anytime. Meanwhile, Fortinet's Threat Response Team closely monitor virus attack patterns on a daily basis and all of the three databases are updated constantly and automatically.

### **Worm scanning**

When configured for worm scanning, the virus scanning engine scans HTTP requests by scanning their originating web page for known viral patterns such as Code Red attempts to gain entry to MS IIS servers by trying to exploit a known buffer overflow bug in these servers.

---

To scan email attachments for worms, the virus scanning engine looks for filenames known to be used by worms. For example, the Nimda worm uses files named readme.exe and sample.exe.

Just as with virus scanning if the virus scanning engine detects a worm, the virus scanner deletes the file containing the worm from the data stream and replaces it with an alert message.

### **No user intervention required**

FortiGate content screening is transparent to the end user. Client and server programs require no special configuration. Fortinet dedicated high-performance FortiASIC hardware and high-performance software ensures there are no noticeable download delays.

### **Virus scanning methodologies**

The FortiGate virus scanning engine is designed to support a combination of strategies to find viruses in target files, including signature scanning, macro scanning, heuristic scanning (static heuristic scanning), and simulated execution (dynamic heuristic scanning). Signature scanning is the least processor intensive method of virus scanning and most viruses are found by signature scanning. The other scanning strategies require progressively more processing power, with simulated execution being the most demanding.

To reduce processing demands, virus scanning always starts with the least demanding virus scanning strategy before moving on to the more intensive options if appropriate. As soon as a virus is found, scanning stops.

### **Signature scanning**

Signature scanning scans the target file for byte-strings that are known to identify viruses. If all of the byte strings for a particular virus are matched, then the virus is considered present in the file.

### **Macro scanning**

Macro scanning extracts macros from MS Office files and scans them for known macro virus strings. Macros are also analyzed for peculiar behavior such as importing and exporting code, writing to the registry, and attempting to disable security features. If any of the macro tests produce a positive result a macro virus is considered present in the MS Office file.

### **Heuristic scanning**

Heuristic scanning, also called static heuristic scanning, scans files for known byte strings that indicate the presence of a virus. For example, in the following program bytes:

**B4 09 BA 20 01 CD 21 B8 02 3D BA 12 34 CD 21 CC B8 FF 4C CD 21**

---

The virus scanning engine can match the following signatures:

B8 02 3D BA ?? ?? CD 21 – This program opens a file.

B8 ?? 4C CD 21 – This program terminates itself.

### **Comprehensive protection**

Working together, the virus scanning strategies provide the best virus scanning protection available. The FortiGate virus scanning engine is also optimized for dynamically scanning network traffic and to provide the best performance possible. The result is thorough and efficient virus protection that stops viruses from entering protected networks while minimizing file transfer delays.

### **Protection Against Network Misuse and Abuse**

Using the same FortiASIC content processing technology, FortiGate provides web and email content filtering. As shown in Figure 3, the FortiASIC Content Scanning Engine scans for banned content such as key words and phrases. In finding a match for undesirable content, FortiGate will block the entire message or that particular page that contains the content, sending an appropriate notification to the intended recipient in place of the blocked content.

### **A Platform for Today and Tomorrow**

The FortiGate Secure Content Processing Gateways address today's most pressing network protection challenges. However, the history of the Internet makes it clear that network protection has been and will remain a constantly moving target. A great advantage of ABACAS technology and the FortiGate series architecture are their inherent ability to support real-time coordination between threat detection and preventive action. With the integrated capabilities and common operating environment, policies can be quickly modified and dispatched across all of the sub-systems in real time. And the entire system, including threat databases and operating code can be updated over their network, securely, at any time. This ability to adapt and respond dynamically to new threats makes FortiGate systems especially capable of delivering comprehensive network protection now, and in the future.

---

## For more information

More information about Fortinet secure gateway products is available from the following sources.

### **Business Information**

Please visit us at [www.fortinet.com](http://www.fortinet.com).

### **Developer Information**

Please contact us at [support@fortinet.com](mailto:support@fortinet.com).

### **Potential Partners**

Please contact us at [partner@fortinet.com](mailto:partner@fortinet.com) or visit us at [www.fortinet.com](http://www.fortinet.com).

### **Additional Resources**

Please contact us at (1) 650-493-6800 for engineering/technical support.