Improving Network Protection and Performance with Network-Based Antivirus Technology

White Paper

October, 2002

Abstract

The predominant approach used by networked organizations to provide protection against viruses and worms has been to install antivirus software on host computers and servers. While generally effective, host-based antivirus (HAV) protection is not foolproof. Specifically, HAV solutions leave gaps in protection and also restrict network and application performance. Another type of antivirus protection, known as network-based antivirus (NAV), eliminates viruses and worms in the network, before they reach hosts. Until recently, NAV systems have been relatively unpopular because of their impact on network performance. However, advances in content processing technology now enable network-based antivirus protection with real-time performance, thereby mitigating the problems of previous systems and making it possible for any size of organization to enjoy effective, high-speed NAV protection. This paper reviews the capabilities and limitations of host-based antivirus solutions, explains the benefits of network-based antivirus technology, and describes how Fortinet’s FortiGate™ Antivirus Firewalls and FortiCenter™ Services enable enterprises and service providers to do combat in the constantly changing landscape of network threats.
Contents

The Changing Nature of the Virus Threat .................................................................4

Introduction to Antivirus Solutions .......................................................................5
  Common Virus-Detection Techniques .................................................................5
  To Scan or Not to Scan – Wild vs. Legacy Viruses ..............................................7

Two Virus-detection Approaches: Host-based vs. Network-based .....................8
  Approach 1: Host-based AV (HAV) Solutions ....................................................8
  Approach 2: Network-based AV Solutions ........................................................10

Fortinet’s Network-Based Antivirus Scanning Technology .............................12
  Challenges for Network-Based Antivirus Systems ..........................................12
  Key Elements of the Fortinet NAV Solution ......................................................13

Summary .............................................................................................................16

For More Information .........................................................................................16
The Changing Nature of the Virus Threat

The number of reported incidents of virus and worm attacks has increased dramatically over the past several years, as has the cost of dealing with these attacks. According to one study, the average number of attacks per company increased by 79% from July 1, 2001 to December, 2001 (Source: Riptech, 2002). The cost of recovering from attacks is skyrocketing also. Following the much-publicized 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 the Code Red worm 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).

Worldwide damage from malicious attacks in 2001

It would be tempting to interpret the data regarding the damage done by recent attacks as an indication of lack of investment by organizations in their antivirus defenses. However, penetration of antivirus technology is actually quite high, reaching over 90% in some market segments. This fact focuses attention on other causes for the problem, namely the nature of the evolving virus threat, and the limitations of current solutions.
The much-studied Nimda and Code Red attacks are examples of the increasingly sophisticated and disabling attacks commonly known as blended threats. Blended threats spread through networks with unprecedented speed by exploiting known vulnerabilities in widely deployed software applications. Even those organizations that maintain host-based antivirus software are successfully attacked, because the infection propagates to their PCs and servers faster than they can update their antivirus software. In addition, new vulnerabilities are exposed by the practice of allowing employees to access their personal, Web-based email accounts while at work, effectively bypassing most companies’ server and desktop AV defenses.

In the wake of these costly threats, organizations have been searching for solutions that can respond more effectively to fast-spreading attacks. Some organizations have resigned themselves to the fact that Internet connectivity poses risks, and simply prepare for the next inevitable outbreak. Other organizations are implementing means to automatically or manually cut off Internet access each time they learn of a major attack until they can verify that all of their hosts have updated antivirus software. Both of these approaches come at cost, and point to the need for alternative measures that can mitigate the weaknesses of host-based antivirus measures.

**Introduction to Antivirus Solutions**

This section describes the variety of virus scanning techniques used by most antivirus vendors, and compares host-based antivirus (HAV) systems with network-based antivirus (NAV) systems. The limitations of HAV systems demonstrates the need for a properly implemented NAV system that allows network administrators to deploy comprehensive antivirus protection faster, guarding against the rise of blended threats that endanger networks today.

In this paper, we use the term "virus" loosely to include security threats of all kinds, including:

- Viruses that replicate and perform malicious operations
- Worms that replicate and spread automatically via email, Web, or other protocols
- Trojans that hibernate on a host until awakened by a certain trigger

Most of the AV products in the market address all of these different kinds of threats.

**Common Virus-Detection Techniques**

Viruses are executable programs, always embedded within otherwise ‘legitimate’ files. The challenge of antivirus science is to ensure that all infected files are stopped (100% detection rate) without creating “false positives”; that is, without mistakenly marking a clean file as being infected. Several methods are used to detect viruses.
The most common approach to virus detection is the “signature-based” approach. Signatures are telltale patterns of bytes that are unique to a particular virus. Signature-based AV products are composed of two key elements: a database that contains the signatures for known viruses, and a scanning engine that compares files under investigation with the signatures in the database to detect a match indicating the presence of a virus.

The simplest signatures are streams of bytes that are known to occur in a particular sequence within the code of a virus. Signatures can be made more complex by incorporating “wildcard” characters to account for known virus variations. In general, larger signature databases and longer, more complex signatures require more time for an AV system to scan a file.

Virus writers have taken a number of steps to further complicate life for AV vendors. For example, they often encrypt the bulk of the virus code, which randomizes the code and makes it much harder to develop a signature. Virus writers have also developed so-called “polymorphic” viruses, which actually modify themselves slightly at each replication, further complicating, and in some cases defeating the ability of AV vendors to develop signatures.

In the continuing AV arms-race, AV vendors have also taken counter-measures, by developing so called “heuristic” scanning that looks for patterns of “known bad behavior”, rather than looking for a specific virus signature. For example, some viruses read and write certain files or execute certain operations in a way that that would never be found in legitimate programs. The sequences of operations that constitute these behaviors can also be used to develop so-called heuristic signatures, which enable AV engines to detect some viruses without an explicit signature.

For many companies, the “holy grail” of antivirus technology would be a signature-less system that can detect and stop inappropriate behavior as programs execute on host computers. While appealing in concept, such systems are not commercially viable. A key problem is that the definition of appropriate vs. inappropriate behavior changes fairly rapidly in today’s modern computing environment. The rules that define acceptable behavior change with new releases of operating systems and application programs. Like virus signatures, the rules that govern “anomaly-based” virus prevention must be frequently updated to avoid an unacceptable number of false positive detections. Even so-called signature-less systems are not so different in practice from their signature-based counterparts.

Despite their known weaknesses and limitations, signature-based AV systems are still by far the most effective and widely used method of virus detection. Thus, the most practical approach at present to improving the performance of AV systems is to determine how to make signature-based systems more effective against today’s increasingly complicated and quickly spreading blended threats.
An obvious weakness of signature-based AV systems is that they can only detect known viruses. As a result, signature-based AV systems are generally ineffective against new attacks until the signature database is updated with the signature of a new virus or type of virus behavior. After a virus is released and begins to spread and infect users, several steps are necessary to update signature databases:

1. A new virus threat is recognized.
2. Antivirus companies gather suspected infected files and search for the virus code.
3. The virus is identified and a signature is developed that will uniquely identify it, without causing “false positives”.
4. The new signature is added to the AV vendor’s signature database.
5. Systems are “inoculated” against the new virus by propagating the new signature database to every device that runs the scanning engine.

Organizations are most vulnerable to new infections during the period between detection and inoculation, and any delays in the process increase the “window of vulnerability.” For large organizations especially, the biggest portion of the vulnerability window is the time required to update every PC, laptop, and server in their network with a new signature database.

Reducing the window of vulnerability maximizes the performance of signature-based systems. Network administrators can achieve this by deploying AV protection at the network edge, using network-based AV as opposed to relying solely on AV protection deployed on each computer and server in the network.

**Host-based and network-based AV windows of vulnerability**

![Host-based AV window of vulnerability](image1)

![Network-based AV window of vulnerability](image2)

**To Scan or Not to Scan – Wild vs. Legacy Viruses**

As explained above, the threat coverage provided by a signature-based AV system is determined by the signatures contained in the signature database. Traditionally, AV
Complement Your Host-Based AV Solutions with FortiGate Antivirus Firewalls

Vendors have tended to equate the size of their signature database with the quality and effectiveness of their products. As a result, it is not uncommon to see AV products that claim to scan as many as 60,000 different viruses.

Intuitively, it would seem that “more is better”; the more signatures processed by an AV scanner, the better the protection. However, this is not necessarily true. Of the 60,000 known viruses in the world today, fewer than 1,000 are “in the wild”. That means there are fewer than 1,000 viruses, today, that are actually spreading and infecting computers. The remaining 59,000+ viruses are legacy, or so-called “zoo” viruses. Many of them have never been released, and many of them were designed to infect operating systems and programs that are obsolete and no longer in use.

Scanning for non-threats can actually reduce antivirus protection, because it can increase the delays caused by AV systems. The impact of these delays cannot be overestimated - users routinely disable AV software because of performance impact. Unacceptable delay is the primary reason that Web traffic is almost never scanned for viruses, despite the fact that Web traffic easily transports these threats.

The list of active viruses, called The Wild List, is published at www.wildlist.org. This list is based on contributions from the world’s top antivirus researchers, representing essentially all antivirus vendors. The Wild List, of approximately 700 viruses (200 base viruses plus variants), is the definitive list of current threats that are infecting users’ systems worldwide. While many AV vendors continue to maintain databases that are 50-60 times larger than the Wild List, the benefit of doing so is highly questionable. In the world of antivirus protection, it makes little sense to look for attacks that are never there.

**Two Virus-detection Approaches: Host-based vs. Network-based**

Regardless of the specific techniques employed, today’s AV solutions fall largely into two camps – host-based, and network-based. Each is described below.

**Approach 1: Host-based AV (HAV) Solutions**

Host-based AV solutions are deployed in the form of software programs that run on standard host computer platforms. Most often, HAV software is used to provide protection solely for the host on which it is installed, such as an end-user’s desktop or laptop. In other cases, HAV software installed on a server is used to protect downstream hosts that access the server, as is the case with HAV software deployed on an email server.

HAV systems are file-based, meaning that they always work in conjunction with the file system installed on the host. This makes them especially effective at dealing with viruses that are spread by floppy disks or other shared media. HAV software is often used to scan email files before they are opened, preventing a common cause of infection and
virus propagation. In addition, most HAV software vendors require an understanding of the operating and file systems on which their software resides, and so are able to provide system clean-up utilities that enable their customers to recover from infections. For these reasons, HAV software is an essential part of any antivirus protection system. While HAV solutions can do an excellent job of dealing with viruses once they’ve reached a host’s file system, several inherent characteristics make them vulnerable in the shifting paradigm of today’s war against virus threats:

- **HAV products operate in an uncontrolled environment.** They are installed on the same platform that they protect, which renders the HAV software itself vulnerable to misconfiguration and attack. In addition, human error can circumvent HAV software. Users may inadvertently (or deliberately) open infected files even when cautioned by the HAV software not to do so. Users may also deliberately disable their host AV protection.

- **HAV products require significant administration.** HAV systems are not completely effective against new attacks until every host in an organization has been updated with the latest signature database. For HAV systems that scan for tens of thousands of legacy viruses in addition to known Wild List viruses, the database updates can take a substantial amount of time increasing the “vulnerability window.”

- **HAV software only operates on files that have been written to the host’s disk file system.** This means that some viruses will not be detected until after a complete disk scan, a process that can often take more than an hour. Some viruses, which persist within a host’s RAM, cannot be completely removed from the host until the system is rebooted.

- **HAV software typically reduces the overall performance of the host on which it runs.** Host performance is reduced because the content processing required to scan files for virus signatures is computationally intensive, and because HAV software typically scans all files whenever they are accessed. File operations can often take 2-5 times longer on hosts with HAV software enabled. The performance reduction can cause some users to deliberately disable their HAV software.

- **HAV systems are rarely used to scan real-time applications, such as Web browsers** because the poor performance of HAV systems introduce unacceptable delays. This is especially troubling, as many users access their personal, Web-based email while at work, effectively bypassing their company’s HAV systems.
Viruses enter an HAV protected internal network

Traditional HAV systems protect networks from infected files downloaded from CDs and diskettes to computers in the network; however, they can not provide sufficient performance or protection to networks from Internet-based, blended threats.

Approach 2: Network-based AV Solutions

Network-based AV (NAV) solutions are installed on a network gateway between two networks. Typically the NAV will be installed between an internal network and an external or public (e.g. Internet) network, between an organization’s network and its extranet partner’s network, or between different departmental networks within the same organization. The key characteristics of NAV systems are as follows:

- **NAV systems typically employ dedicated platforms.** Unlike the standard host computers of HAV systems, NAV systems use dedicated, security hardened operating systems that cannot be compromised.
- **NAV systems provide a single barrier behind which all hosts are protected.** This greatly reduces administrative effort and closes the “vulnerability window.” A single update of the signature database or scanning algorithms on the NAV gateway protects all of the systems on either side from viruses flowing in either direction.
- **NAV systems stop viruses at the network edge.** Viruses are stopped before they reach downstream PCs and servers, greatly reducing the risk that an unprotected
host will be compromised, and mitigating the risk of memory-resident and other viruses that are a challenge for HAV systems.

- **NAV systems reduce the load on email servers by eliminating infected emails before they reach the servers.** This is especially important during attacks by email-propagated worms which can generate thousands of messages and overwhelm an email server – even if it is protected by HAV software.
- **NAV systems are well positioned in the network to scan Web and other traffic that tends to bypass conventional HAV systems.**

*Using FortiGate Antivirus Firewalls to stop viruses at the network edge*

To perform AV scanning at network speeds requires 100-1000 times more processing power than is required for other security functions such as VPN and firewall processing. As a result, a major challenge to NAV solutions is the need to provide effective AV protection without reducing network performance. A sufficiently powerful NAV solution can provide protection for real-time and Web-based applications, shielding the network from the increasing risk of Internet-based, blended threats.
Fortinet’s Network-Based Antivirus Scanning Technology

Fortinet has pioneered the world’s first network-based antivirus system, proven to provide the highest level of AV protection while maintaining real-time performance – at data rates that reach gigabit/second levels. Through the combination of a unique architecture, new chip technology, and a comprehensive support infrastructure, Fortinet’s antivirus solution now sets a new standard for AV protection, price and performance.

Fortinet’s NAV functionality is standard in all members of the FortiGate Antivirus Firewall product line. In addition to antivirus protection, FortiGate Antivirus Firewalls provide firewall, VPN, content filtering, intrusion detection, and traffic shaping functions in robust, dedicated hardware units. The seven FortiGate models span SOHO to service provider, and support multi-gigabit performance levels.

Challenges for Network-Based Antivirus Systems

Conventional, signature-based HAV systems operate on files. They typically scan files for viruses when the files are stored (or opened) by the host’s operating system. The HAV software intercepts the files and streams them through a “scanning engine” which searches the files for patterns that match corresponding patterns in the virus signature database. The signature databases can contain several hundred kilobytes of information representing thousands of virus signatures. For a typical file, many millions of comparisons may be required to determine if it is free from infection. While the delays caused by virus scanning are often annoying to users, there is no hard limit on HAV system performance: if it takes 2 seconds, 20 seconds, or 2 minutes to scan a file, the results will be the same.

Compared with HAV systems, network-based antivirus systems operate under much more difficult constraints. Files are transported over networks in the payload portions of packets, each containing a small chunk of the file. A typical packet payload on the Internet is approximately 1,500 bytes in length. However, many viruses are substantially longer than 1,500 bytes, and can exceed 100K bytes in length. As a result, it is not sufficient for NAV systems to simply scan each packet individually. If a virus is longer than 1,500 bytes, and the signature for the virus relies on patterns that occur in portions of the packet that are separated by more than 1,500 bytes, then a packet-by-packet scan will never detect it.

To deal with this challenge, some NAV systems contain hard disks, and function essentially as HAV systems that are deployed at the edge of a network. Packets are reassembled into files on the disk, and streamed off the disk at a rate that will not overwhelm the software scanning engine. Such systems do not achieve network-speed performance, and while potentially acceptable for email, are generally not usable for real-time, Web traffic.

To operate effectively, a NAV system must be able to scan both Web and email traffic without causing noticeable delays. This requires the ability to reconstitute packets into
application-level content streams and compare the streams to the patterns in the signature database in real time. The content reassembly and scanning processes must take place at network speed, or the NAV system will run out of space to store the contents from new, incoming packets, resulting in data loss. On a 1 gigabit/second link, a delay of only 2 seconds can fill 256 megabytes of memory! Since the processors used in conventional computing and networking systems are not designed to scan large data sets (files and streams) for complex patterns (signatures) at high speeds, effective NAV systems require a dedicated architecture designed specifically for this type of processing.

**Key Elements of the Fortinet NAV Solution**

Fortinet’s high-performance NAV solution is powered by two key elements:

1. Fortinet’s Advanced Behavior and Content Analysis System (ABACAS™) Technology.
2. Fortinet’s Threat Management Team (TMT) and FortiCenter™ Services infrastructure.

These key elements have enabled Fortinet to deliver the highest performing NAV system on the market, as well as the only ASIC-based AV system that is certified by the International Computer Security Association (ICSA).

**ABACAS Technology Provides High Performance Content Processing**

ABACAS Technology forms the basis of the FortiGate NAV system. The two primary components of ABACAS Technology are the FortiASIC Content Processor and the FortiOS Operating System.

The core of the FortiOS is a dedicated, security hardened, real-time kernel optimized for packet processing. It provides a common framework and environment for all of the FortiGate applications: AV, content filtering, firewall, VPN, NIDS, and so on. The FortiOS also supports APIs to applications that run on standard (e.g. Linux) operating systems, making it easy to integrate third party utilities (such as a Web server, and Secure Shell) into the products. Because the FortiOS is a closed system, it is not susceptible to being attacked by any of the threats that the FortiGate units process.

FortiGate units derive their primary performance advantage from the FortiASIC CP-1 Content Processor, a new type of chip designed by Fortinet. The FortiASIC chip contains multiple functions that contribute to high AV performance:

- The **Firewall Engine** processes packet headers, and accelerates the identification of the application-level flow to which each packet belongs.
- The **Signature Scanning Engine** reassembles packet payloads into content streams in the Content Memory, loads the appropriate portions of the signature database, and performs hardware-based pattern searches.
The Content Memory associated with the FortiASIC chip varies in each FortiGate unit depending on its rated throughput, and ranges from 64 MBytes in the FortiGate-50 to 1 GByte in the FortiGate-2000.

*Fortinet’s ABACAS high-performance content processing*

Each FortiGate unit can be configured by the system administrator to reassemble, stream, and scan attachments to email messages transported using SMTP, POP3, or IMAP protocols, and Web pages and downloads transported via the HTTP protocol. The system is expandable without any changes to hardware and can support the processing of additional protocols, such as FTP.

**FortiCenter Infrastructure Keeps Signature Databases Up to Date**

The Virus Signature Database in each FortiGate unit is supplied by Fortinet’s FortiCenter™ infrastructure and services. The FortiCenter services ensure that customers receive up-to-the-minute information on network threats, and ensure that FortiGate units include the latest signature databases needed to detect and stop attacks.

FortiCenter services are managed by Fortinet’s Threat Management Team (TMT), which includes leading antivirus researchers who continuously scan global sources for new viruses, worms, and other attacks. Working in concert with customers, partners, and a worldwide network of antivirus experts, the Fortinet TMT identifies new threats, isolates virus samples, determines the nature and level of the threat, and develops new signatures when needed.
When a new threat is identified, the FortiCenter sections of the Fortinet Web site are updated with relevant information for review by customers, and if needed, a new signature is added to the Virus Signature Database and pushed to a FortiCenter Server. FortiCenter Servers can be accessed at any time by authorized FortiGate units in order to download the latest signature database, a process that generally takes less than a minute. Each FortiGate unit can be configured to load the latest signature database daily or weekly, and can be directed by an administrator – remotely if desired – to download the latest database at any time. In the event of an especially dangerous threat, the Fortinet TMT can issue an alert telling all FortiGate administrators to download the latest database immediately. The FortiCenter architecture also supports the ability of the FortiCenter Servers to automatically alert FortiGate units that a new database is available and to trigger an immediate download if so configured by the administrator.

World-wide TMT and FortiCenter server locations

In order to ensure high availability, there are several FortiCenter Servers located in different parts of the world, including North America, Europe, and Asia. Each FortiGate unit can be configured to communicate with two FortiCenter Servers, and the Servers can re-route update requests if needed to handle peak demand.
Summary

Host-based antivirus systems serve an important purpose and should be a part of any well-conceived virus protection strategy. However, host-based AV protection alone is no longer sufficient to deal with today’s fast-spreading, blended threats. Network-based antivirus systems can stop threats at the network edge before they reach host computers, and provide the time needed to update host AV software. Fortinet’s ABACAS technology includes a dedicated, FortiOS Operating System and ASIC-based hardware content processing that can deliver Network AV protection at the network edge to prevent attacks that bypass even the best host-based AV systems. The patent.pending ABACAS technology provides application and network level services in real time, providing the performance required to protect networks from the increasing number of blended threats and Internet-based attacks. FortiCenter services provide continuous, up-to-the-minute protection from new threats.

Based on ABACAS technology and FortiCenter Services, Fortinet’s FortiGate family of Antivirus Firewalls represent the industry’s first and only ICSA-certified, ASIC-based, real-time network antivirus systems. FortiGates provide an important new defense in the war against network attacks.

For More Information

In the constantly evolving network security environment, the FortiGate Antivirus Firewalls provide the strongest and most effective protection available for your network. More information about Fortinet’s products is available from the following sources.

Business Information

Please visit us at www.fortinet.com.

Potential Partners

Please contact us at partner@fortinet.com or visit us at www.fortinet.com.

Additional Resources

Please contact us at (1) 408-235-7700 for engineering/technical support.