Reduce Your Virus Exposure with Active Virus Protection

A White Paper

by SonicWALL, Inc.

SONICWALL

Executive Summary

Viruses are the leading Internet security threat facing businesses of all sizes. Viruses spread faster and cause more damage than ever before, and according to Computer Economics, it is estimated that they have created $12.3 billion in damages. Unlike other forms of security threats, viruses are not particular about which network they attack. Viruses disrupt your employee productivity, waste expensive IT resources, and destroy your company's most valuable asset – your information.

Your anti-virus software is only as good as the last virus update. Anti-virus software is primarily a reactive measure against known virus threats, and as a result is out of date the moment a new virus is released. Therefore, updating, detection, and policy enforcement play a key role in meeting the latest threats and protecting your networks. The challenge is not only having anti-virus software installed on your company's computer systems, but also ensuring that your network is protected when a new virus outbreak occurs. Distributing the anti-virus updates, the instant they become available, is essential for complete virus protection.

The best defense against today's virus threats is an active virus protection system that automatically acquires the latest anti-virus software, updates all appropriate systems and enforces anti-virus software updates. This approach provides two services for your business: It ensures that your systems are updated in the fastest time possible, and it removes the "human factor" by automatically updating every system on the network. With active virus protection, your exposure is greatly reduced and your protection is significantly improved.

This white paper describes today's virus environment, why you need to reevaluate your current anti-virus strategy, and how your business can deploy SonicWALL's active virus protection system to provide cost-effective, comprehensive virus protection that keeps your business secure.

Brave New World of Today's Internet Virus Threats

Today, a sophisticated virus can spread to millions of computers via the Internet in a matter of hours and cost businesses billions to clean up. How bad is the virus threat?

- **More Virus Attacks**. The Computer Emergency Response Team (CERT) Coordination Center reported the number of virus attacks jumped 160% in 2001.
- **Fast Spreading Viruses**. The Internet enables viruses to spread like wildfire to business networks. Computer Economics, estimated that Nimda alone infected more than 2.2 million servers and 700,000 PCs within 24-hours.
- **More Virus Breaches**. According to the Information Security Survey of 2001, 89% of the more than 2,500 of those surveyed said they experienced a virus security breach.
- **More Expensive to Recover from Viruses**. Experts estimate U.S. corporations spent about $12.3 billion to clean up damage (restoring disk drives, recovering files, IT staff time, and so on) from computer viruses in 2001 (Computer Economics). A virus named Code Red alone caused an estimated $2.6 billion in damages.

New, More Powerful Virus Strains

Today, hackers create sophisticated viruses that attack network vulnerabilities on multiple fronts and use a variety of propagation methods. Virus payloads can enable hackers to launch Denial of Service (DoS) attacks that bring down mission-critical servers. Virus writers have also found it easy to trick people into opening e-mail attachments with tempting subject lines like “I LOVE YOU!”

One of the most dangerous characteristics of the new and more powerful strains of viruses is their ability to spread without human intervention. Traditional viruses typically required some human intervention in order to spread, such as sending an infected file to another user, or opening an e-mail attachment to trigger the propagation.

Nimda is an example of the new, more powerful virus strains spreading across the Internet. This virus injected malicious text into each .exe file on the system; escalated the privilege level of the guest account; created readable and writeable network shares; made numerous registry changes; and interjected script code into html files, etc. Cleanup of a Nimda type virus becomes difficult because the damage is permeated throughout the entire network infrastructure.

Proliferating Virus Entry Points

Before the Internet, floppy disks provided the primary medium for viruses. Now, Internet viruses can spread through any network from any number of network ports, including e-mail, Web content, file downloads, and so on. These multiple entry points not only increase network vulnerability to viruses, but also increase the speed that a virus can spread.

An emerging concern for businesses is the proliferation of remote access points that can carry viruses to the business network. Telecommuters, day-extenders, and mobile workers all represent new network entry points for viruses. For these remote users, the blending of work and personal computing on the same computer opens up new virus threats for your business network. Even with secure access through a VPN (Virtual Private Network), viruses can be transferred to the corporate network from insecure remote locations.

New Threats Require New Measures

Anti-virus scanners are the front line technology for preventing virus attacks. They can reside on a server, gateway, or client. The heart of an anti-virus product is the scanning engine, which conducts the scanning of files as it looks for viruses. A database of known virus signatures is what the scanning engine checks against. A signature is a search pattern, characters or bytes that are usually unique to each virus.

Because anti-virus software is primarily a reactive measure against known threats, updating, detection and policy enforcement play a key role in meeting the latest threats and protecting networks from infection. Anti-virus software is only as good as the last known virus because the software doesn't know what the new threat is unless it has the latest virus signature definitions. Updating your anti-virus software in the fastest time possible is the only way to minimize damage to your network. Today's virus protection is all about time-to-protection.

Time to Protection

Virus protection is ultimately about how quickly the anti-virus software can be updated to protect your network against the latest virus attack. Traditional anti-virus software is vulnerable during two critical gaps. First is the gap between the release of a new virus and the release of the anti-virus update. Second, the time it takes to implement virus updates to every PC on your network.

When a virus outbreak happens, virus vendors analyze the virus, identify its unique signature, and create the anti-virus. This process can take hours or days to complete. Virus vendors often send out incremental anti-virus updates as they develop more knowledge about the threat. Unless the anti-virus software has a mechanism to get these updates instantly instead of at scheduled intervals, the network remains vulnerable.

The biggest time-to-protection gap is getting the new virus updates to all the computers on a network. Anti-virus software deployed on PCs without centralized enforcement requires users or administrators to update the virus software one at a time. Even with a centralized anti-virus management console, an administrator needs to manage the updates.

Removing the Human Factor in Enforcement

The human factor in virus protection represents a potential risk to your business network. Keeping up with the rapid-fire changes in anti-virus updates places a heavy burden on administrators. Employees can easily turn virus protection off, as, for example when installing new software. Without a method of ensuring that the anti-virus software is always active, virus protection across the network will degrade as more and more users fail to restore their virus protection.

Enforcement is an essential element of virus protection. Virus policy enforcement isn't just about getting updates quicker, it's also about ensuring virus protection is always running on every PC on the network.

Automatic Anti-Virus Management

While virus protection is most effective at the desktop where the exposure risk is highest, it's also the most difficult to maintain anti-virus effectiveness.

Centralized enforcement is an economic necessity for any business with more than a few computers. It's simply not viable to manage every desktop's anti-virus software by manually installing and configuring each time there is an update. Besides the enormous costs involved, there is too much margin for error in a manual process.

On the downside, most centralized anti-virus management products create more cost and complexity to your virus protection infrastructure. Typically, the virus management software runs on a network server and requires IT resources to set up and maintain.

A centralized virus management solution that automatically installs, maintains, and updates anti-virus clients eliminates nearly 80% of the total cost of implementing virus protection.

Integrated Firewall Protection

Today's virus threats can carry sophisticated payloads designed to attack network vulnerabilities that require a firewall to protect against. A good firewall provides the first line of defense against Internet hackers and a solid foundation for your anti-virus protection. Any weakness in your firewall capabilities opens up vulnerabilities in your virus protection.

The International Computer Security Association (ICSA) classifies firewalls into three categories: Packet Filters, Application-Level Proxy Servers, and Stateful Packet Inspection firewalls.

- **Packet Filter**. A packet filtering firewall simply examines the packet header and decides whether or not to let the packet proceed. Decisions are made in accordance with a set of rules or filters. The inability of packet filtering to dig deeper into the packet exposes your network to Denial of Service (DoS) attacks and a host of prevalent Internet attacks. Most broadband routers include packet-filtering firewalls.
- **Application Level Proxy Server**. Proxy server firewalls provide upper level examination of IP packets. While providing superior firewall protection compared to packet filtering, a proxy server firewall causes significant performance degradation at the Internet gateway. Also, proxy servers are difficult to set up and maintain, and they require updates for each new application on the network.
- **Stateful Packet Inspection**. A stateful packet inspection firewall intercepts packets until it has enough to make a determination as to the state of the attempted connection before passing judgment. By maintaining a table of current connections and their most recent events, these firewalls are able to spot abnormal sequences inherent in hacker

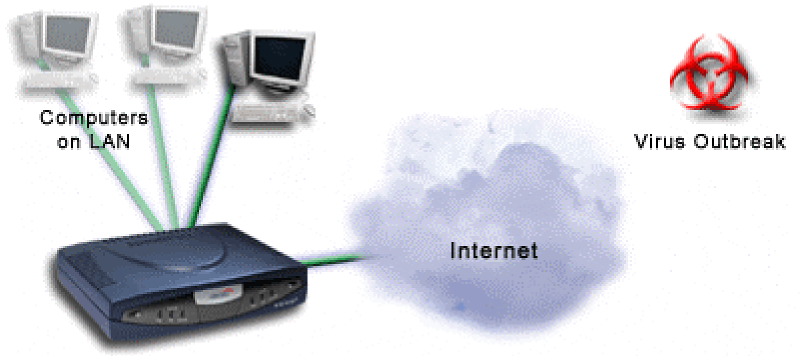
attacks. Stateful packet inspection is the most trusted firewall technology and is widely used in enterprise-class firewalls.

SonicWALL's Active Virus Protection

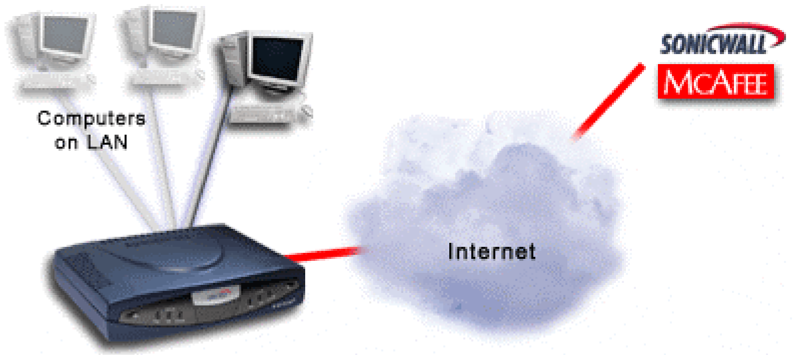
What is active virus protection? Technically, it’s a distributed, gateway-enforced anti-virus solution. What it delivers is always on, always updated anti-virus software to the network. With SonicWALL active anti-virus protection, no employee can access the Internet without the latest updates. If a virus attack happens, you can be assured that SonicWALL is updating your business' anti-virus software as soon as it is available.

SonicWALL Network Anti-Virus (NAV) includes the automatic policy enforcement and management of McAfee anti-virus signature and client software updates, and SonicWALL's attachment blocking service—all as an affordable per-client subscription.

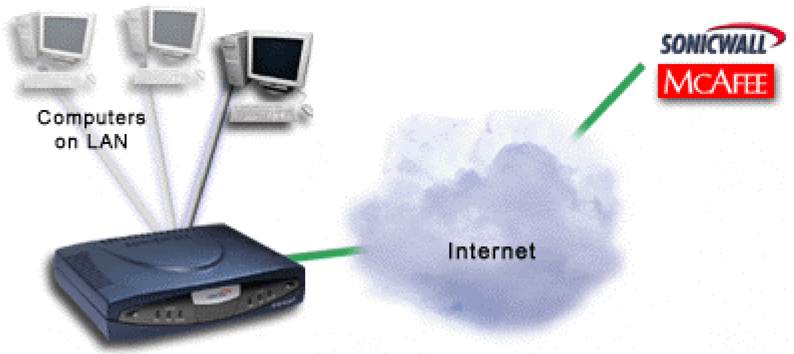
Here's how SonicWALL Network Anti-Virus works.



At the first sign of a virus, SonicWALL appliance blocks suspect attachments



Virus alert updates the policy on SonicWALL Internet security appliance



Updates are automatically enforced on every client

Auto-Enforcement and Management

The key to the SonicWALL Network Anti-Virus enforcement process is based on a series of communications between the McAfee VirusScan client residing on each desktop and the SonicWALL Internet security appliance.

The SonicWALL Internet security appliance stands on guard at your Internet gateway for virus update alerts and handles all the virus enforcement and management.

SonicWALL's Auto-Enforcement works like this:

1. Whenever a PC attempts to send traffic to the Internet through the SonicWALL Internet security appliance, a request for the version of the VirusScan files is automatically returned to the desktop.

2. If the PC does not respond, or if it responds with an outdated version, the SonicWALL Internet security appliance triggers a transparent, automatic update by the client. All users are kept updated before accessing the Internet.

Rapid E-Mail Attachment Blocking

The SonicWALL Internet security appliance can also block new viruses even before the virus signature is available. When a new virus outbreak occurs, the virus filename is instantly relayed to the SonicWALL Internet security appliance. Any infected e-mail file attachment from the Internet is blocked at the SonicWALL Internet security appliance. This early detection system protects your network from new viruses even before their inoculations are available.

Zero Administration

SonicWALL takes anti-virus protection a giant step forward with zero administration. Auto-Enforcement manages all aspects of virus protection from client software installation to virus policy enforcement. This means no administration and no hidden IT costs inherent in other centralized virus management solutions.

Integrated Security

SonicWALL Network Anti-Virus is a member of the SonicWALL family of security products and services. The foundation of SonicWALL's comprehensive security solutions is our line of easy-to-install and easy-to-manage SonicWALL Internet security appliances. They provide enterprise-class firewall protection with an ICSA-certified, statetful packet inspection firewall, IPSec VPN for secure remote access, IP address management, and fully integrated support for SonicWALL security applications like VPN services, NAV (described here), Integrated Content Filtering, and Strong Authentication. SonicWALL's intuitive Web-interface management makes security setup and management easy.

The SonicWALL family of Internet security appliances

Reduce Your Virus Exposure with SonicWALL Active Virus Protection

Today's viruses are faster, stronger, and more destructive. You can’t fight today’s viruses with yesterday’s defenses. SonicWALL’s active virus protection is built on a new architecture that protects at the desktop with automatic enforcement at your Internet gateway using the SonicWALL Internet security appliance. Together, they deliver the best time-to-protection solution on the market today.

Find out more on how SonicWALL Network Anti-Virus can affordably protect your business against today’s virus threats, call 1-888-557-6642 (U.S./Canada), or the SonicWALL reseller partner in your region www.sonicwall.com/sales/index.html.

SonicWALL, Inc

E-mail: info@sonicwall.com

Web: www.sonicwall.com