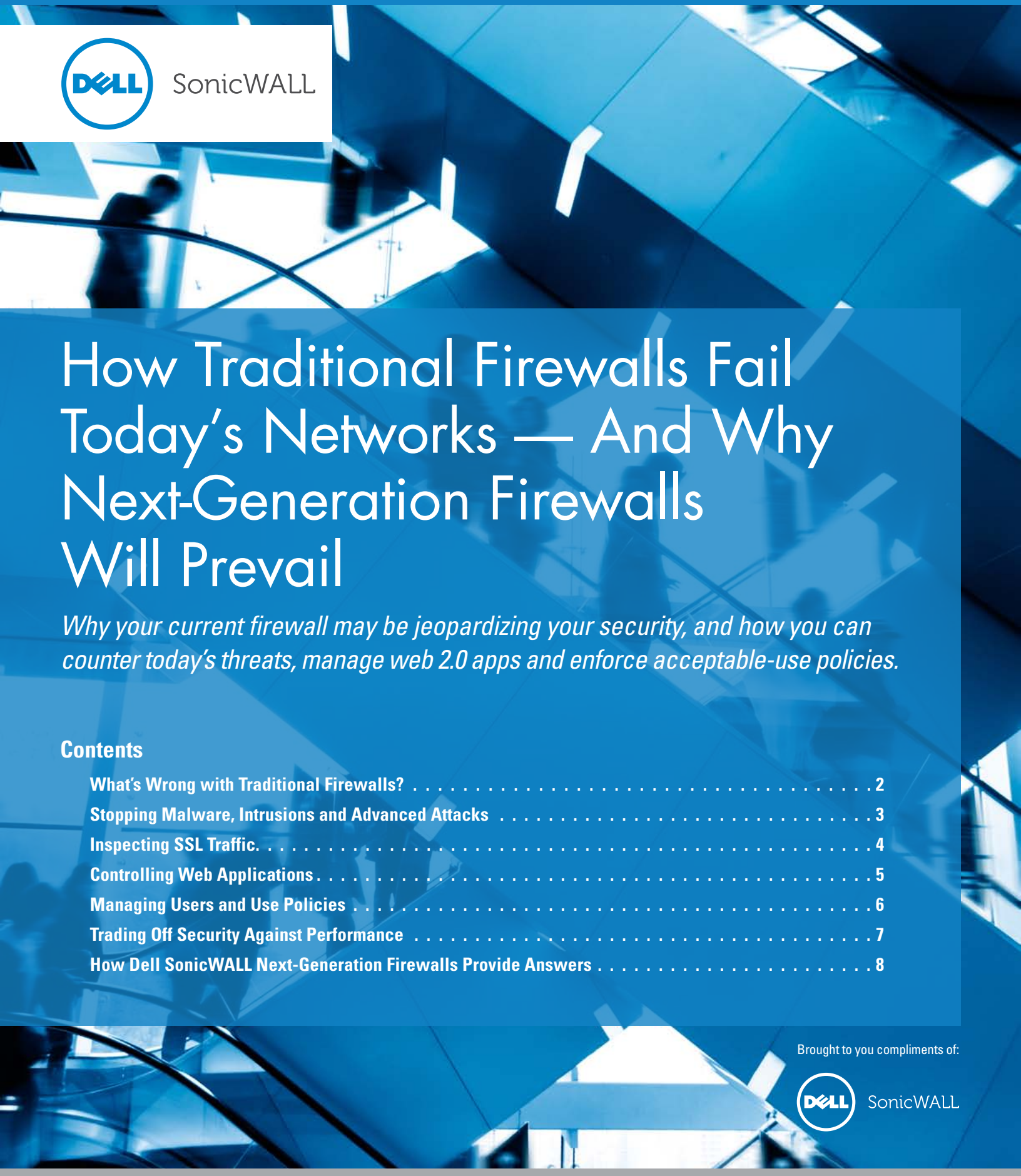


How Traditional Firewalls Fail Today's Networks — And Why Next-Generation Firewalls Will Prevail

Why your current firewall may be jeopardizing your security, and how you can counter today's threats, manage web 2.0 apps and enforce acceptable-use policies.

Contents

Brought to you compliments of:

TechTarget Custom Media

What's Wrong with Traditional Firewalls?

If your company has a traditional firewall, it is probably jeopardizing your security and costing you money.

Why? Firewalls are an essential part of network security, but most are very limited. They can close unneeded ports, apply routing rules to packets and fend off denial-of-service attacks. But they can't look inside packets to detect malware, identify hacker activity or help you manage what end users are doing on the Internet.

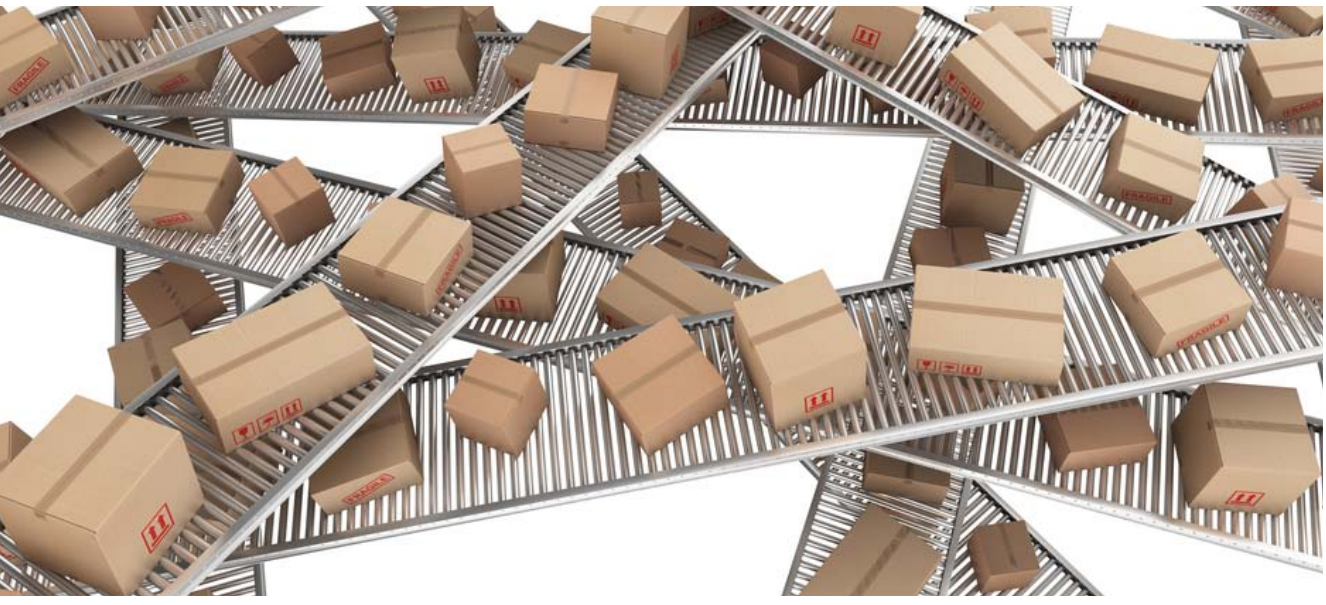
Basically, once a port is open (say, port 80 for Internet traffic), anything can come through disguised as legitimate traffic.

Traditional firewalls can also be expensive to operate, especially if you need to supplement them with additional security technologies.

This white paper will explain exactly where traditional firewalls fall short, how Next-Generation Firewalls fill those gaps, and how Next-Generation Firewalls can help you:

- Reduce costs.
- Detect more attacks.
- Enforce appropriate use of social media and web 2.0 apps.
- Ensure that high-priority business applications perform better.
- Identify departments and individuals who engage in risky or nonproductive behaviors.
- Provide excellent network performance without compromising security.

You can think of a traditional firewall as a receiving clerk at the loading dock. The clerk can open and close cargo bays and turn away some delivery trucks, but he has no visibility into the contents of the trucks. He can't tell if they contain illegal substances. He also can't stop people from flooding the mailroom with items unrelated to work, because he doesn't know who in the building is sending and receiving packages.



SonicWALL

Stopping Malware, Intrusions and Advanced Attacks

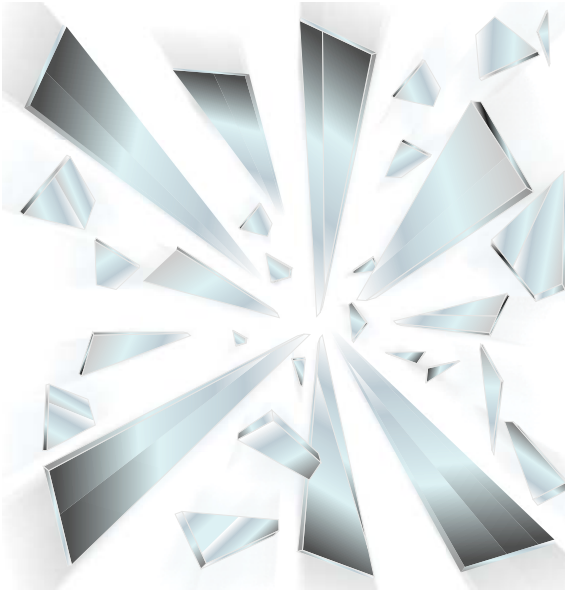
Traditional Firewalls

Traditional firewalls provide only a part of the network security organizations need.

Because they are so limited, most organizations supplement them with other network security technologies such as gateway anti-malware products, intrusion prevention systems (IPS), and content or URL filtering packages. These block malware, help detect attacks and prevent users from accessing web sites with malware.

But managing several separate security tools is costly. First, you need multiple licenses. Second, for each product, your systems administrators must master the intricacies of configuring hardware and software, setting rules, creating reports and monitoring events. You might even need to dedicate specialists to each system.

This duplication also undermines security, because it is very difficult to correlate data from multiple products to detect and respond to fast-moving attacks.



Next-Generation Firewalls

Next-Generation Firewalls provide multiple network security technologies in one package. They combine the features of traditional firewalls, gateway anti-malware products, intrusion prevention systems and content filtering packages.

All of these security technologies can be installed, configured, deployed and managed as a unit, which greatly reduces administrative costs.

And because all event data is available through one reporting system, it is much easier to identify threats early and take appropriate measures, before security has been compromised.

A Next-Generation Firewall can:

- *Block viruses, Trojans, worms, rootkits and polymorphic "zero-day" malware at the gateway, before they reach the corporate network.*
- *Prevent "drive-by downloads" from infected web sites.*
- *Mitigate denial-of-service and flooding attacks.*
- *Detect protocol anomalies and buffer overflow attacks.*
- *Stop network traffic from geographical regions and IP addresses associated with cybercriminals.*
- *Block outbound botnet "command and control" traffic.*
- *Prevent employees from visiting web sites containing content related to pornography, substance abuse, gambling, hate crimes and other objectionable topics.*

SonicWALL

Inspecting SSL Traffic

Traditional Firewalls

Retailers, banks and other organizations use the Secure Sockets Layer (SSL) protocol to protect sensitive information sent between their web sites and their customers'. Other companies can't block SSL traffic, because it has many legitimate and necessary uses.

Unfortunately, traditional firewalls can't decrypt and inspect SSL traffic.

That means that hackers and cybercriminals can smuggle malware right through the firewall just by concealing it in SSL traffic.

Also, botnets and the creators of advanced persistent threats (APTs) often create SSL tunnels from inside out to exchange command-and-control messages with their servers, and exfiltrate files.

Next-Generation Firewalls

Next-Generation Firewalls utilize Deep Packet Inspection (DPI) technology to decrypt and inspect SSL traffic into and out of the network.

That means you can detect and block malware concealed in SSL traffic.

It also means you can detect and stop botnet command-and-control messages, and prevent APTs from using SSL to exfiltrate your customer lists, engineering designs, trade secrets and other confidential information.

SonicWALL

Controlling Web Applications

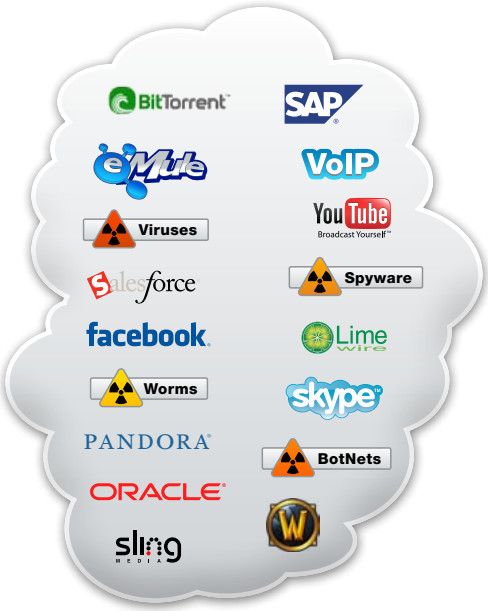
Traditional Firewalls

Traditional firewalls cannot associate network traffic with specific applications. They are not "application-aware."

Traditional firewalls have no way to:

- Block dangerous applications.
- Control applications that have legitimate uses but are also subject to abuse.
- Visualize and control traffic by application.

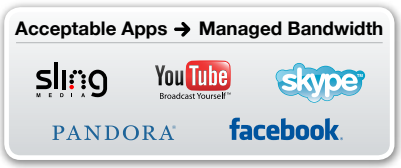
In today's world, where software applications are the lifeblood of business, this lack of application control is a serious deficiency.

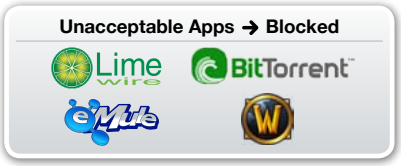


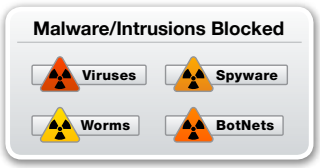
Next-Generation Firewalls

Next-Generation Firewalls offer application intelligence and control. That means they can recognize traffic belonging to specific applications and enforce corporate acceptable-use policies. They can even allocate bandwidth to high-priority applications.

In addition, Next-Generation Firewalls allow administrators to monitor and visualize network traffic. They can observe traffic volumes by application, spot bandwidth hogs and determine why traffic slows at peak periods during the day. Application traffic visualization gives you a powerful new tool to troubleshoot problems and plan network capacity.







Next-Generation Firewalls can:

- *Block applications that endanger security or reduce productivity, such as peer-to-peer file sharing and FTP file transfers.*
- *Control legitimate applications that are subject to abuse — for example, allowing instant messaging programs to exchange text but not transfer files.*
- *Limit applications to certain times of day — for instance, allowing access to multi-player games only after business hours.*
- *Ensure that high-priority applications (customer relationship management, order processing) will get more bandwidth than less urgent applications (chat, video streaming).*

TechTarget Custom Media

SonicWALL

Managing Users and Use Policies

Traditional Firewalls

Traditional firewalls have no way of connecting network traffic with users. Suspicious traffic cannot be associated with individual users, except through the laborious process of pouring through log files.

Traditional firewalls cannot:

- Enforce Internet acceptable-use policies.
- Provide insight into application usage.
- Identify which users are using dangerous applications or surfing to compromised web sites.
- Limit social networking applications to groups that have a business need to use them.
- Improve network performance for high-priority groups.

Next-Generation Firewalls

Next-Generation Firewalls allow application control to be applied at user group and individual levels, which allows you to enforce acceptable-use policies at a granular level.

Facebook, Twitter, LinkedIn and other social media sites may account for hundreds of nonproductive hours for many employees. However, the marketing and human resources departments may have good reasons to access these sites, including to promote products and services, assess consumer sentiment and find job candidates. A Next-Generation Firewall could:

- Enforce company policies by giving marketing and HR access to social media sites while blocking access for employees in other groups.
- Allow everyone to post text and photos on Facebook, but not play Facebook-related games.
- Permit engineering and IT to stream technical videos during work hours, but allow other employees to stream video only at night.
- Allocate more bandwidth to executive management and selected departments.

Traffic visualization allows administrators to not only monitor network traffic by application, but also identify specific employees who pose security risks or inadvertently affect productivity — for example, by downloading massive files or streaming long videos during peak periods.

TechTarget Custom Media

SonicWALL

Trading Off Security Against Performance

Traditional Firewalls

Traditional firewalls often force administrators to trade off security against performance.

If administrators activate all security measures, the firewall may hold up network traffic. Then users complain about bad network performance, slow response times and long file downloads.

So administrators compromise by turning off monitoring on certain ports, disabling firewall rules and limiting deep packet inspection.

Or they limit the size of email attachments, which affects user productivity.

This creates a dilemma: Face user complaints today, or increase the risk of a security breach tomorrow.

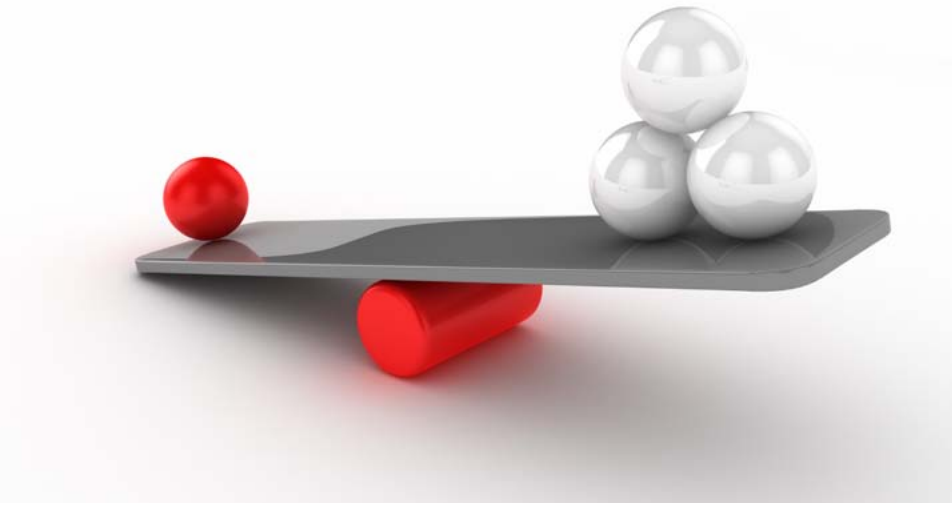
Next-Generation Firewalls

Next-Generation Firewalls have far higher throughput, so administrators don't have to trade off security for performance.

Factors that enhance performance include:

- Processors with faster clock speeds.
- CPUs designed to understand network communications and perform security scanning.
- Parallel processing architectures.
- More efficient approaches to deep packet inspection.

You should never have to compromise security to maintain acceptable performance.



TechTarget Custom Media

SonicWALL

How Dell Sonicwall Next-Generation Firewalls Provide Answers

Dell SonicWALL offers a wide range of Next-Generation Firewalls that address the shortcomings of traditional firewalls.

Stop malware, intrusions and advanced attacks

Dell SonicWALL Next-Generation Firewalls, unified threat management firewalls and related products offer a complete set of network security technologies in one package, including gateway anti-malware, intrusion prevention and content filtering.

The integrated package is easy to install, configure and manage.

Inspect SSL traffic

The firewalls perform high-speed decryption and inspection of inbound and outbound SSL traffic.

Application intelligence and control

Dell SonicWALL Next-Generation Firewalls recognize over 4,500 enterprise, desktop and web-based applications; block and control them individually; and provide charts to visualize network traffic by application.

Visibility into users

The firewalls integrate with Active Directory and LDAP directories so they can identify network traffic by user and user group, and apply application usage and bandwidth control policies selectively by group and user.

They also allow administrators to drill down to application use by individuals and enforce acceptable-use policies at a high level of granularity.

High performance and scalability

Dell SonicWALL Next-Generation Firewalls feature CPUs designed for security processing and parallel-processing hardware architectures.

A unique Reassembly-Free Deep Packet Inspection™ (RFDPI) engine can scan against multiple application types and protocols at extremely high speeds, with no upper limit on file size or the amount of concurrent traffic.

A wide choice of models allows a single set of security features to be deployed very cost effectively in small offices, and with massive scalability in very large ones.

Dell SonicWALL Next-Generation Firewalls provide:

- *Traditional firewall stateful packet filtering*
- *Gateway anti-malware*
- *Intrusion prevention*
- *Content filtering*
- *Spam filtering*
- *Application intelligence and control*
- *User visibility and management*
- *Email security*
- *Secure remote access for IPsec and SSL VPNs*

SonicWALL

Backed by an industry leader

Dell SonicWALL is an industry leader with an outstanding malware research group, comprehensive 24/7 customer support and an unparalleled track record of innovation. As such, Dell SonicWALL has received numerous industry awards and top-ranked results from independent research organizations such as ICSA Labs and NSS Labs.

If you have a traditional firewall…

If you have a traditional firewall, you are getting too little security and wasting too much time and money.

Dell SonicWALL Next-Gen Firewalls & Unified Threat Management Firewalls

To learn more about Next-Generation Firewalls from Dell SonicWALL, please visit http://www.sonicwall.com/us/en/products/Network_Security.html**.**