eBOOK | FIREWALL TECHNOLOGY

THE NEXT GENERATION IS THE SMART GENERATION

How Application Intelligence and Control enables network security in the wake of Web 2.0, Cloud Computing and Mobility.

SONICWALL®

InfoWorld | NETWORKWORLD® Custom Solutions Group

INSIDE

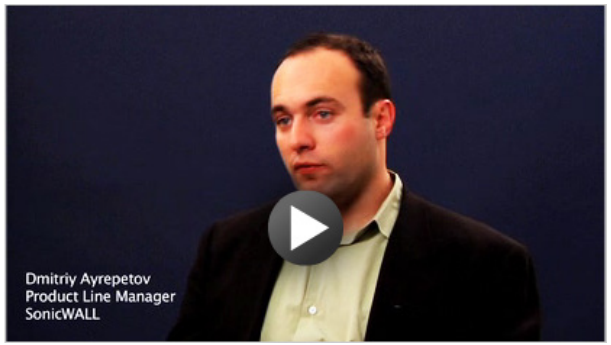
EXECUTIVE SUMMARY

This paper explores how innovations such as mobility, Web 2.0, social media and cloud computing have dramatically changed the IT landscape and introduced new security threats into corporate and government networks. Now traditional firewalls are coming up short as protocol and port number classifications have been rendered ineffective in blocking threats. In a bold move to reclaim control, CIOs and IT managers are looking to next-generation firewalls with application-layer intelligence that stands strong against today's threats. It's that kind of fortified protection that will enable organizations to fully embrace and leverage such innovations going forward.

INTRODUCTION

Firewalls are a long-standing tradition in network topography, implemented to help restrict unauthorized access to the corporate domain. They were originally designed to block network-layer threats. And whereas some have become more multidimensional by integrating additional security layers—such as anti-virus and intrusion detection—they are proving woefully ineffective against today's threats.

New vulnerabilities are wreaking havoc, partly due to a fundamental shift in the way business is conducted—particularly the manner in which employees, customers and other stakeholders



Attacks have now moved to the application layer. In this short video, Dmitriy talks about how administrators can take control and prioritize traffic on the network.

THERE ARE 223 MILLION CELL PHONE USERS OVER THE AGE OF 13 IN THE U.S. ALONE, AND 25 PERCENT OF THE MOBILE DEVICES SOLD DURING Q3 OF 2009 WERE SMARTPHONES.

SOURCE: NIELSEN

interact. Traditional interactions have been systematically replaced by more-innovative forms of communication and collaboration, all borne of the digital era. Of course, the extent and sheer volume of that electronic interaction are a far cry from what they were at the inception of the firewall.

Enterprises have invested heavily in unified communications. E-mail, instant messaging and VoIP applications such as Skype have since eclipsed traditional phone and fax interactions, making the Internet a minute-to-minute resource for employees and a primary point of integration for IT.

Additionally, social media is permeating the workplace. Facebook has more than 400 million users, and there are 70 million for LinkedIn and 16 million for Tagged. YouTube consumers are viewing two billion videos daily. Although social media has its place in daily employee interactions, enterprises are adopting Web 2.0 applications to accomplish corporate tasks—engaging shareholders via Facebook, pinging consumers on Twitter and collaborating with partners through BitTorrent.

Endpoint mobility—which is on a sharp upward curve—further muddies the waters. In fact, according to Nielsen, there are 223 million cell phone users over the age of 13 in the U.S. alone, and 25 percent of the mobile devices sold during Q3 of 2009 were smartphones. With hot technology such as notebooks, Androids, BlackBerrys and iPads in the palms of seemingly everyone between the ages of 13 and 73, the consumerization of IT is taking on a life of its own. Employees are now starting to pressure employers to embrace such tools and bring personal devices onto the corporate network.

At the same time, cloud computing has begun to infiltrate the IT infrastructure as well. Most notably, enterprises are moving more services into the cloud. Applications with sensitive information, including e-mail and customer relationship management (CRM), are being hosted by third-party vendors. As evidence, cloud computing services revenue is projected to hit $150.1 billion in 2013, according to research firm Gartner.

"Innovations such as mobility, Web 2.0 and cloud computing are a huge benefit to business," says Jason Tate, director of networking for Aaron Rents, a specialty retailer of residential and office furniture, consumer electronics, home appliances and accessories based in Atlanta, Ga. "IT needs to be on board."

Still, adoption can bring about heated debate: How much personal freedom is too much? Who should be allowed access to which applications? Should sensitive data leave the network? What's the protocol for controlling rogue devices? «

POLL

WHAT IS YOUR COMPANY'S POLICY REGARDING EMPLOYEE ACCESS TO SOCIAL NETWORKING SITES—SUCH AS TWITTER AND FACEBOOK—USING THE CORPORATE NETWORK?

- ☐ WE ALLOW EMPLOYEES TO ACCESS ALL SOCIAL NETWORKING SITES
- ☐ WE RESTRICT ACCESS TO A FEW SOCIAL NETWORKING SITES, BUT ALLOW OTHERS
- ☐ WE RESTRICT SOME EMPLOYEES' ACCESS TO SOCIAL NETWORKING SITES
- ☐ WE BLOCK ALL SOCIAL NETWORKING SITES FOR ALL EMPLOYEES

VOTE

NEW TECHNOLOGIES, NEW THREATS

As the argument rages on with the promise of increased productivity, adoption is having the opposite effect in some respects, says Patrick Sweeney, vice president of product management for SonicWALL™ Inc., a network security provider based in San Jose, Calif.

Employees are socializing on the "company dime," hogging bandwidth for non-work-related activity at the expense of critical business tasks. For example, in a company that has ESPN streaming to PCs on the network and 100 employees tuning in to watch soccer's World Cup, the network is bound to get congested, slowing the performance of business applications. The answer cannot be as monolithically simple as blocking all streaming sites; rather, greater granularity in policy is needed to solve the problem.

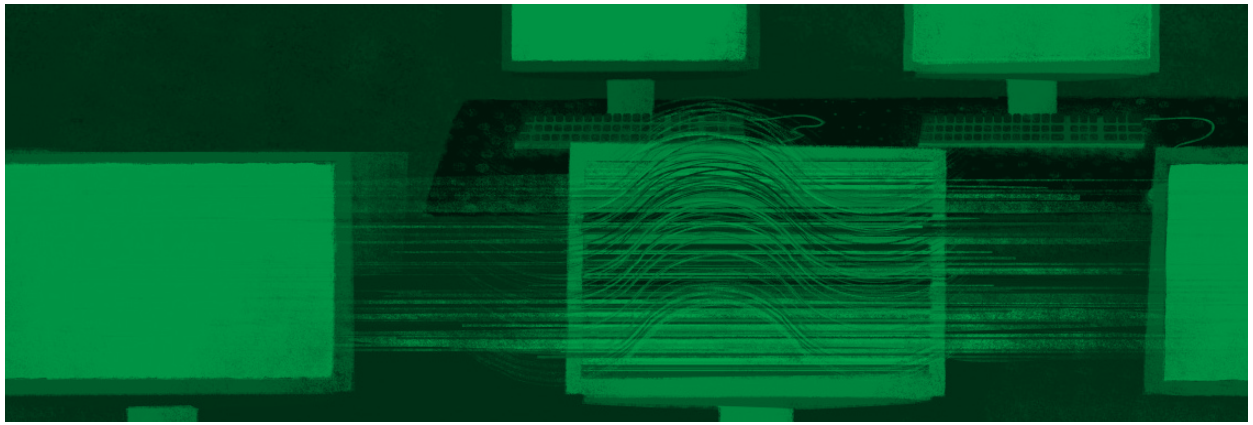
A bigger drain on productivity, though, is the new security risks. "The traditional virus threat is gone," says Tate. "Now Web applications and the cloud expose networks to potential drive-by malware attacks to which even legitimate sites and diligent users are susceptible."

Popular Web applications and social media sites—not just the typical pornography, pharmaceutical and gambling sites—are opening dark new doors when users unwittingly download infected content. All the while, traditional threats are spreading to new business tools, as experienced in the recent password attack against iPads and various spam campaigns targeting Facebook and Twitter.

As new holes pop up all over corporate and government networks, the malware defense landscape has been upended. "It's becoming harder for network administrators to distinguish between good and bad," Sweeney says. And that puts enterprises—and their digital assets—at risk. Data loss, in particular, looms heavily today, causing increased oversight by regulators. So, how is compliance affected? Where is data most vulnerable? Can these Web applications be managed and controlled?

With this widening attack surface, IT would probably prefer to unplug entirely, says Tate. Parents may tell their children "no," given the perils of Web 2.0, "but we need to find a way to say 'yes,'" he argues, "without coming across as overbearing 'network storm troopers.'" One way to do that is by updating antiquated firewall technology to deal with the complexities of today's IT landscape. «

TRADITION FALLS FLAT



"THERE SIMPLY ISN'T ENOUGH INTELLIGENCE BUILT INTO TRADITIONAL FIREWALLS TO BLOCK WHAT'S GOING ON, SO THE CONCEPT OF BEING ABLE TO IDENTIFY AND MANAGE APPLICATIONS IS BECOMING CRITICALLY IMPORTANT."

— PATRICK SWEENEY, V.P.. PRODUCT MANAGEMENT, SONICWALL

Yesteryear's firewalls simply weren't designed for the modern ways of IT consumerization and Web 2.0. Certainly no one could have predicted the extent to which things would change in a couple of decades. And now those firewalls are coming up short. "Traditional firewalls can handle amateur-hour attacks," Tate explains, "but these new attacks are sophisticated, so we need to be more selective in how we grant access."

In particular, these older firewalls are Layer 3 network devices. Operating in network layers means that the firewalls inspect traffic based only on the information pertaining to a combination of the packet's source and destination address—that is, its protocol and port number. But with nearly two-thirds of traffic today being HTTP and HTTPS, "protocol and port details have been rendered practically useless when it comes to setting and enforcing security policies," according to the AimPoint Group, an analyst firm based in Maryland.

Traditional firewalls also prove ineffective against Web-based application threats, because they rely on static attack signatures and have no application-specific knowledge to determine what actually represents a threat. Their policy configurations are based only on known threats. By using SSL encryption and nonstandard ports that have traditionally been closed, Web applications can slip through undetected. For example, an instant messaging program can open port 80 and then dynamically reprogram itself to look like a standard stream, Sweeney says.

"Unfortunately, there simply isn't enough intelligence built into traditional firewalls to block what's going on," Sweeney says. "So the concept of being able to identify and manage applications is becoming critically important." «

FIREWALLS GET "SMART"

So as the onslaught of Web 2.0 applications continues unabated—becoming unwieldy yet integral to and ingrained in day-to-day business activity—firewalls need to get "smart."

'SMART' FIREWALLS IN THE REAL WORLD

So what does this concept of application intelligence and control look like in the real world? SonicWALL Vice President of Product Marketing Patrick Sweeney describes how these capabilities can be rolled out for everyday protection:

- ✓ **Enforce the use of approved applications only.** Enterprises can systematically block access to all social networking sites such as Facebook or just the ones that represent the most risk. This prevents employees from inadvertently downloading infected content to the corporate network.
- ✓ **Maintain control over applications.** Enterprises can allow access to bandwidth hogs such as YouTube but limit usage to the employees who need it in order to do their jobs. They can also rate-limit usage based on the media or the time of day, preserving bandwidth for mission-critical applications.
- ✓ **Prevent loss of sensitive data.** Enterprises can stop employees from e-mailing documents with a watermark or tag built in. With greater visibility and control over encrypted traffic, they can prevent sensitive customer data and intellectual property from being unnecessarily exposed.
- ✓ **Combine application policy, control and data loss.** Most importantly, enterprises can combine all of the controls on a per user / per group basis to create the exact policy required—whether prioritizing bandwidth for critical applications or restricting bandwidth for unproductive groups—for the greatest productivity gains while maintaining vigilant inspection for malware and data leakage.

According to the AimPoint Group, "Organizations must increasingly focus on network security solutions that are able to define and enforce policies based on higher-layer attributes, such as user identity, the specific application being used and the actual content being transmitted—rather than those that continue to rely primarily on network-layer information, such as the port source/destination address."

To do this, CIOs must look toward the next-generation firewall, which addresses application intelligence. This means being able to identify and understand applications and their potential risk to the corporate network as well as protect, manage and control everything that passes through the firewall—whether social media, peer-to-peer or software as a service (SaaS) applications. They should expect their firewall to dynamically adapt to changing business demands and emerging security threats while maintaining high levels of performance.

"The pace of hardware advancement today enables the firewall device to do more," Tate notes. "The technology is here now to do it all—including deep packet inspection—and still switch packets at high speed." Not surprisingly, Tate has switched over to a

WHAT IS THE GREATEST THREAT TO YOUR COMPANY WHEN IT COMES TO PROTECTING DATA IN TODAY'S IT LANDSCAPE?

- ☐ HACKERS
- ☐ MALWARE
- ☐ DATA LEAKS
- ☐ INEFFECTIVENESS OF CURRENT SECURITY TECHNOLOGY

VOTE

FIREWALLS GET "SMART" *continued*

next-generation firewall from SonicWALL to protect Aaron Rents' IT infrastructure.

An obvious core capability of this next-generation firewall is active threat management through integrated layers of security. This includes seamless interoperability with other areas such as anti-virus, anti-spyware, intrusion prevention and anti-spam services.

The next-generation firewall takes security a step further, extending traditional network-layer threat protection to include application-layer inspection. It will still flag port and protocol violations, but its real value lies in intelligent traffic management that also enforces policies based on application, user/group and content. By identifying and classifying application traffic, it will enable enterprises to control access and regulate Web traffic, e-mail and file transfers.

Equally important is the dynamic nature of the firewall's threat signature configurations. It starts with a baseline of predefined threat signatures from which to enforce policies but also allows for continuous and automatic updates as well as customization to handle the most likely threats through granular creation and enforcement of policy.

Deep packet inspection of network content is also critical. Not only must the firewall inspect every packet of information for malware across the application layer but it must also do so without degrading the network performance. Inspection involves decrypting and analyzing inbound and outbound SSL traffic, no matter the port or the protocol. That traffic can then be re-encrypted and sent on to its destination—unbeknownst to the user.

Indeed, the next-generation foundation seamlessly integrates application intelligence with core capabilities such as intrusion prevention and malware blocking for "a unified and comprehensive network security platform," says Sweeney. That's the future of firewall technology. «

THE NEXT-GENERATION FIREWALL TAKES SECURITY A STEP FURTHER, EXTENDING TRADITIONAL NETWORK-LAYER THREAT PROTECTION TO INCLUDE APPLICATION-LAYER INSPECTION.

BOTTOM LINE

So what does all this really mean to the enterprise – public or private? A next-generation firewall can block access to social networking sites that pose the greatest risk; flag transmissions of sensitive or watermarked data via uploads or attachments in Webmail to prevent data leakage; and restrict bandwidth usage levels based on application, user or time of day to optimize performance. With this kind of protection, enterprises can fully embrace innovative business tools—including mobility, Web 2.0 and cloud computing—and reap all the rewards they promise.

To Tate, that means a lot. "We can now grant reasonable requests quickly and feel good about being protected." That unbridled access to applications and innovations, he concludes, yields a more successful, profitable business. «

APPLICATION INTELLIGENCE THROUGH SonicWALL

SonicWALL, Inc. is a premier provider of network security solutions that help reduce costs and complexities while delivering a more secure infrastructure. In particular, we've taken firewalls to the next level, integrating application intelligence and control. Extending protection beyond network-layer threats, our next-generation firewall is designed to lock down the enterprise against today's threats, with maximum control over all data and applications that traverse the network. As a result, you'll enjoy application-level access controls, restrictions on the transfer of specific files and documents and greater bandwidth management. For more information, visit www.sonicwall.com.

SONICWALL®

InfoWorld | NETWORKWORLD® Custom Solutions Group