Unchain Your Network with Application Intelligence and Control

Best practices for extending beyond blocking network threats to protect, manage and control application traffic in a Web 2.0 world

CONTENTS

SONICWALL®

Abstract

Today's workforce has access to more information, Web-based tools and rich media than ever before. As Web 2.0 applications permeate the corporate environment, they offer the promise of connecting people and enabling information exchange in novel and increasingly efficient ways. However, employees streaming video and music to their desktops are now stretching bandwidth to the limit. At the same time, this new paradigm of a business enhanced by Web-based applications threatens to undermine control and policy enforcement across network boundaries while evolving threats are finding new routes into the corporate network with potentially damaging effects.

The solution for many forward-thinking organizations is Application Intelligence. The next generation in firewall technologies, Application Intelligence advances the expected threat protection provided by traditional firewalls, so that organizations can empower users to access valuable applications, while enabling IT to protect the environment and ensure that bandwidth is available for mission-critical business processes.

This paper discusses the new risks facing organizations in light of the prevalence of Web-based applications and offers best practices for gaining control of applications, data and bandwidth. It also introduces SonicWALL® Application Intelligence and Control solutions, designed to help organizations of all sizes address the unique issues posed by Web 2.0, including employee use of unauthorized Web-based applications, streaming media, peer-to-peer applications (P2P) and protecting data sent in attachments and via email.

Introduction

Better collaboration, higher productivity and lower costs are just a few of the benefits enabled by a growing number of Web-based applications appearing in today's business environments. Unfortunately, these same applications also bring a new set of challenges. Some of these applications, such as social networking and streaming media applications, threaten to drain bandwidth and productivity as they compete with mission-critical applications. Other solutions, including those related to software as a service (SaaS) and service-oriented architecture (SOA), introduce new threats as they enable new ways of conducting business.

To gain the most value from these applications, organizations need a comprehensive security approach. In this new Web 2.0 environment, traditional firewalls fall short when it comes to ensuring protection of critical information and resources. Many organizations are unaware that their current network protection is insufficient. Other organizations who are aware of these challenges are shying away from allowing employees to use Web-based applications altogether. Yet, these applications offer tremendous benefits when used securely and within company-defined parameters.

Challenges to a Safe and Productive Workplace

As users become more technically knowledgeable, they often download and install Web-based applications into their work environment. While these applications can deliver an increased level of productivity, they also consume tremendous levels of bandwidth and serve as a conduit for a new class of security threats. This problem is exacerbated by the fact that employees are downloading files from social networking sites such as MySpace, streaming rich media from YouTube, accessing files from personal email accounts such as Yahoo® or Gmail®, and using P2P applications. In many cases, employees are unaware of the potential harm they are causing when downloading applications or streaming content.

There are several reasons that these activities make organizations vulnerable to attacks. For instance, a hacker can insert malformed data into packets, enabling Web applications to share too much information with the attacker. Cyber thieves can insert access controls into an application, allowing them to access specific content or functions meant only for authorized users. Some attacks generate high volumes of traffic to overwhelm certain applications, preventing legitimate users from using them. Combining this with an already-existing breed of advanced persistent threats, as well as attacks that increasingly target specific companies, the threat matrix continues to expand exponentially.

In addition to potentially damaging technical challenges to network protection, organizations must consider a number of business challenges as well. Streaming music and video sites consume lots of bandwidth, which can slow down mission-critical applications running on the network. Worker productivity can suffer as non-work-related Web 2.0 applications, such as streaming video, P2P downloads and online games distract employees.

In the midst of this new dynamic workplace, organizations are struggling to prevent data leakage, and ensure secure and uninterrupted access to necessary business resources. After all, as workers enter and leave a company, they may unintentionally introduce malware or infected data. In extreme cases, disgruntled employees may launch network attacks from within the company. To complicate matters even further, organizations are now receiving a greater amount of data entering the network by a growing number of remote workers and third-party consultants.

To meet these many new business and technical challenges, today’s organizations need to take a closer look at the current state of their network security and ways in which they can allow productivity enhancing Web 2.0 tools without slowing business processes or opening their networks up to harmful threats.

Traditional Firewalls are Insufficient for a Web 2.0 World

Many organizations operate under the false assumption that their network firewalls adequately protect their corporate data and network resources in today's business environment. The inconvenient truth is traditional firewalls struggle to provide protection against Web application attacks. In fact, in certain instances, they do not even recognize these attacks as threats.

While some network security vendors are becoming aware of these threats, they are not meeting them sufficiently. For example, because traditional firewalls are inadequate to protect against new threats posed by social networking and other potential Web 2.0 applications, vendors have begun touting application-layer security, incorporating functionality from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) into their products. However, these solutions have proven ineffective against Web-based application threats for two fundamental reasons: they rely on static attack signatures and operate at network layers.

Static attack signatures are ineffective against many Web application threats because software programmers write security signatures to thwart attacks based on the behavioral patterns of known threats. Unfortunately, since programmers write these static signatures only for already-identified threats, they are reactive in nature. In addition, administrators must continually update security products with new signatures in order to fight the latest attacks. This leaves systems exposed to unidentified types of attacks and threats cloaked as normal traffic. More importantly, it leaves systems blind to targeted attacks exploiting the specific vulnerabilities of an application, for which there is no generic pattern.

These shortcomings are exacerbated by the fact that by using non-standard ports and SSL encryption, Web application traffic can evade detection and control by traditional firewalls. Solutions that operate at network layers are inherently limited by the information they are able to interpret. Because traditional firewalls and IPS systems inspect packets on the wire instead of entire requests and user session data, they lack the application-specific knowledge to discern an acceptable request from a threatening one. In spite of these issues, there are ways to uncover the potential risks to an organization's network and prevent them, while bolstering employee productivity at the same time.

Best Practices for Network Control and User Productivity

In the face of a rapidly evolving enterprise workspace, organizations should ensure the necessary level of network security while empowering users to take advantage of Web-based applications. To meet these challenges and improve employee productivity, companies are utilizing firewalls with Application Intelligence features that enable application access control with over 2,700 pre-defined user applications, regulate Web traffic, email, email attachments, and file transfers, and support bandwidth management. Here are a number of best practices that can reduce threats and control bandwidth consumption while improving worker efficiency.

1) Manage applications with custom access controls

With Application Intelligence, administrators can define custom access controls based upon user, application, schedule or IP subnet level. As a result, administrators gain the ability to manage the full range of applications that are available for access. Specifically, they can enforce approved application use and maintain control over P2P and other non-business related applications.

Figure 1: Allows you to classify, control and manage applications and data that pass through the firewall.

Enforce approved application use

One of the first practices a company wants to make is to mandate and enforce the use of preferred applications. For example, if a company has decided to standardize on a certain Internet browser, it can choose to pursue one of the following strategies:

1. Physically check everyone's system each day for unauthorized browsers

2. Set-up and run a script each day to check every system for unauthorized browsers

3. Define a policy for Application Intelligence that allows traffic for the preferred browser, while automatically blocking traffic from unwanted browsers

Clearly, the first two options are less than ideal, burdening the IT department with time-consuming manual tasks. In addition, these approaches fail to ensure an adequate level of protection. After all, if an administrator overlooks even a single system, malware can quickly spread like wildfire throughout the environment. The third option assures organizations of a robust measure that addresses security vulnerabilities while freeing IT resources to focus on strategic initiatives.

Maintain control over Peer-to-Peer (P2P) applications

Another essential practice is to ensure control over P2P applications, such as BitTorrent. These applications can steal bandwidth and introduce all types of mischievous files into the corporate network. The challenge for network administrators trying to manage P2P applications on their networks is the creation of new P2P applications or simple changes to existing P2P applications, such as new version numbers occur all the time, making it nearly impossible to keep track of P2P applications.

By implementing policy for Application Intelligence, companies can block or limit these applications through bandwidth and time-based restrictions. And because advanced Application Intelligence delivers application signature updates automatically, they eliminate time spent updating application signature rules so system administrators can focus on more business-critical tasks.

Gain visibility and control over encrypted application traffic

Frequently, Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL) protocols encrypt transactional Web-based application traffic, making it invisible to traditional firewall scans. The capability to decrypt, inspect and re-encrypt HTTPS and SSL traffic at wire speed can extend the functionality of Application Intelligence to encrypted application traffic.

Automate application signature updates

Establishing automated updates and notifications can ease administration, ensure Application Intelligence signatures are always up-to-date, issue alerts of potential policy violations, and notify end users of standard policy upon blockage or restriction.

2) Prevent data leakage and incoming threats with proactive policies

Once applications are under control, companies need to ensure that sensitive information is not leaked (whether accidentally or intentionally) or stolen by employees, contractors or partners. Application Intelligence includes the necessary controls to help organizations mitigate Web-mail and data loss, restrict FTP upload, protect confidential documents and block forbidden files.

Mitigate Web-mail and data loss

A good place to start with controlling data is email, the most popular workplace tool. The fact is that a company's existing anti-spam protection may fail to prevent data leakage when an employee or contractor sends information from a networked remote or mobile device using a Web-mail service such as Hotmail® or Gmail®, as well as corporate SMTP and POP3 email . By implementing policy for Application Intelligence, the company can detect and block any outbound email that contains sensitive or confidential information.

Protect confidential documents

In addition to measures that protect the information within Web-mail messages, organizations must also consider email attachments. While most companies can block viruses and spam from entering the environment via approved email applications, such as Microsoft Outlook®, they are typically at a loss when it comes to protecting attachments sent via email. In some companies, outbound email does not pass through an email security system. Or the email security system does not check the content of email attachments. In either case, attachments containing confidential information can easily leave the organization.

With Application Intelligence, the organization can proactively address this security vulnerability when sensitive information is sent using the company's approved email application. The company simply creates a policy for Application Intelligence to block email attachments carrying a watermark indicating sensitive information. The firewall will then block these files from leaving the company network. Organizations can even apply such a policy to protect documents transmitted via their FTP servers.

Restrict FTP upload

FTP services are often used when people have to exchange large files, although there are many other uses. However, FTP sites can also serve as a conduit for unwanted content to enter the organization. To counteract this potential, organizations can limit FTP upload privileges to trusted parties, such as the project manager in a partner's company. Certain Application Intelligence feature sets enable administrators to create policies allowing FTP uploads by only authenticated users. Simultaneously, these features can empower the organization to disallow any FTP commands deemed unnecessary on a given FTP server.

Block forbidden files

While the best practices discussed so far go a long way toward helping organizations take control of their information, organizations need to understand that malicious or unapproved files can still find their way into the environment. For example, many traditional network firewalls are unable to block files that pose potential harm, such as those containing source code (SRC) or executable code (EXE) files. Whether downloaded from a Web page, received as an email attachment, or transferred via FTP, these files can cause a computer to perform tasks according to encoded instructions.

Then there are personal information files (PIF), which tell the operating system how to run an application. And Visual Basic Scripts (VBS) that can access and modify data on the user's computer. Rather than remain helpless in the face of these threats, organizations can create a forbidden file extensions list in their policy for Application Intelligence to block these files. As a result, the company can mitigate the risks associated with these types of files.

3) Manage bandwidth to ensure application availability

To ensure that the use of Web-based applications does not interfere with the availability or performance of mission-critical applications, companies must manage network bandwidth. For example, while some employees may enjoy streaming video and music on their desktops, this can affect employee productivity as well as the availability of business applications for others in the organization. To that end, bandwidth management has taken on new significance. Advanced Application Intelligence provides the functionality needed to control bandwidth usage throughout the organization for controlling access to streaming video and music, and ensuring availability of mission-critical applications.

Control access to streaming media

Employee access to streaming video sites such as YouTube is sometimes useful but often abused. While blocking such sites might work in the near term, the most effective remedy is to limit the bandwidth available to streaming video sites using Application Intelligence.

Similarly, streaming audio sites and streaming radio sites consume precious bandwidth. However, users often have legitimate business reasons to access them. Organizations can manage this challenge by instituting controls per Web site and by file extension. A policy for Application Intelligence can detect, block or limit the bandwidth available to streaming audio sites and files.

Ensure availability of mission-critical applications and content

With the growing need for bandwidth throughout a company to access key applications and content, few things lower productivity more than non-business use of the network. As employees download P2P files and play online games via the network, other workers, business partners and contractors can struggle to access critical resources and information. Some organizations respond by easing bandwidth restrictions across the company. However, a better approach is to enact group-based bandwidth management. For example, Application Intelligence can specify that executives and key decision makers have unfettered access to streaming videos and the bandwidth while other employees have limited access during business hours.

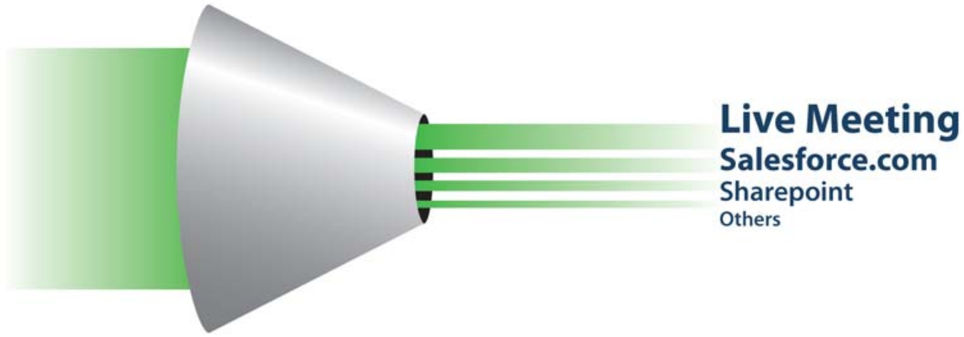

Figure 2: Ensures mission-critical applications get the network bandwidth they need to operate and contribute to business productivity.

Likewise, many mission-critical applications (e.g., Live Meeting®, Salesforce.com® and SharePoint®) are cloud-based or run across geographically dispersed networks. Prioritizing network bandwidth for these applications is critical to ensuring business productivity. Again, organizations can create a policy for Application Intelligence that ensures bandwidth priority for critical applications. Advanced Application Intelligence even enables administrators to prioritize bandwidth availability by date, such as end-of-quarter for sales-related applications.

SonicWALL Application Intelligence and Control

Delivering performance, protection and application control

While these best practices can go a long way to ensuring network protection and employee productivity, one Application Intelligence solution goes beyond traditional firewalls to meet the needs of today's organizations and picks up where traditional network firewalls leave off. SonicWALL® Application Intelligence and Control solutions not only block traditional network-layer threats, but also extend protection, management, and control over application-layer traffic, enhancing compliance, content filtering and data leakage prevention, while ensuring performance-under-attack from advanced persistent threats that particularly target cloud-based applications. Application Intelligence can dedicate throughput for mission-critical or latency-sensitive applications like Live Meeting and restrict productivity-draining applications like YouTube based on user group, time of day, or mobile device type.

Leveraging high-performance SonicAWALL Reassembly-Free Deep Packet Inspection™ technology, SonicWALL Application Intelligence can identify and control unauthorized browsers, Web 2.0 sites, IM clients, and EXE, SRC, PIF or

VBS files—as well as dynamically evolving P2P applications like BitTorrent. Continuously and automatically updated with an industry-leading 2,700+ unique application signatures, Application Intelligence can identify and control application traffic regardless or port, protocol, platform or even encryption[1].

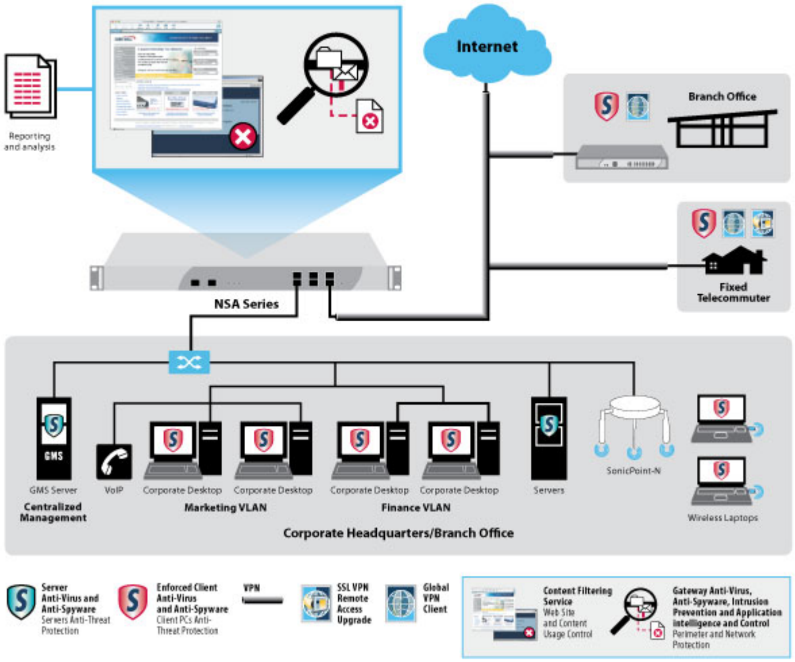
Reporting and analysis
Internet
Branch Office
Fixed Telecommuter
NSA Series
GMS
GMS Server
Centralized Management
VoIP
Corporate Desktop
Corporate Desktop
Marketing VLAN
Corporate Desktop
Corporate Desktop
Finance VLAN
Servers
SonicPoint-N
Wireless Laptops
Corporate Headquarters/Branch Office
Server Anti-Virus and Anti-Spyware Servers Anti-Threat Protection
Enforced Client Anti-Virus and Anti-Spyware Client PCs Anti-Threat Protection
VPN
SSL VPN Remote Access Upgrade
Global VPN Client
Content Filtering Service Web Site and Content Usage Control
Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Perimeter and Network Protection

Figure 3. SonicWALL's NSA Series combines powerful Application Intelligence controls with high-speed intrusion prevention, file and content inspection, and an extensive array of advanced networking and flexible configuration features.

[1] Optional DPI SSL feature

A set of customizable protection tools, SonicWALL Application Intelligence offers administrators precise control and inspection capabilities over their network traffic. An intuitive wizard makes it easy for administrators to configure the solution to address the most common scenarios that Application Intelligence will likely encounter. Administrators can easily change rules to adapt to unique business situations. In addition, granular controls enable IT administrators to create and enforce policies that ensure bandwidth for critical processes. This unique combination of control and flexibility leads to improved productivity throughout the organization.

Conclusion

Organizations that turn a blind eye to the use of new Web-based applications infiltrating the environment are opening the door to security and productivity issues that will only increase over time. After all, employees, contractors and partners will continue to introduce them as they seek ways to be more productive. What today's organizations should focus on are ways to control the potential threats and bandwidth shortages posed by these applications while empowering users to make the best business use of them.

SonicWALL, the leader in dynamic security for the global network, provides Application Intelligence and Control solutions that adapt as both organizations and threats evolve—dynamically and globally. Unlike “application-control-only” appliances, SonicWALL seamlessly integrates Application Intelligence with Intrusion Prevention and industry-leading firewall defenses, forming a unified next-generation solution that is easy to deploy and manage.