

NETGEAR® Stream Scanning Technology

Introduction

The proliferation of Web 2.0 technologies has dramatically increased the Internet's importance to small and mid-size businesses. However, it has also fueled a variety of new attack strategies, as attackers take advantage of the vast connectivity it provides, coupled with the confidence it elicits among users. Peer-to-peer sites encourage mass file sharing amongst strangers; accepting a browser plug-in to view a specific site is commonplace; popular social networking sites have taught many users that clicking on embedded email links is perfectly safe. These increasingly familiar behaviors have created new avenues for attackers to exploit.

According to a recent Gartner study, in 2007 the number of Web-hosted threats increased 800 percent and there were more than 275 browser plug-in vulnerabilities. Another recent study found that 79 percent of Web-hosted threats are hosted on legitimate sites which have been hijacked by hackers who have infected the site with the threat. The remaining 21 percent are found on rogue sites that have been designed to appear legitimate, with email "marketing" employed as the primary vehicle to direct users to these attacks.

The Challenge

The Internet has become an essential part of the day-to-day operations for small- and mid-size businesses, with email and Web access representing 90 percent of their business-critical applications. Though most companies are aware that some varieties of malicious software can enter their networks through web traffic, few are aware of the magnitude of the problem.

On average, security vendors receive more than 20,000 unique malware samples every day, and more than half of all network threats they receive have utilized HTTP as a vehicle. In a growing number of cases, a user only needs to visit a Web page or view Web mail to be infected by Web-based Trojans and spyware. Email is also a significant source of malware, and is frequently used to direct users to Web-based attacks.

This growing number of Internet-based threats has prompted the need for a robust gateway security solution that scans both inbound and outbound traffic to detect and remove threats before they reach individual desktops. However, comprehensive security and networking have historically been at odds with one another, due to the inherently inverse relationship between security and performance. Users demand speed, particularly when it comes to Web browsing. If a Web security solution is adding unacceptable amounts of latency, users will be the first to complain.

Traditional Batched-based Scanning vs. Stream Scanning

Most security solutions – from desktop security to gateway appliances – utilize "batch-based" scanning technology. This means that scanning commences only after the entire file is received, and outputting starts only after the entire file has been scanned (see Figure 1). As a result, end-users often experience long delays or sometimes even timeouts while the file is transferred and scanned.

Batch-based scanning was developed during an era when viruses were transmitted via removable media. It therefore employs algorithms based on the assumption that the entity to be scanned could be randomly accessed. This technology was tremendously effective for such media. However, when applied to the Internet-based threats in real-time Web traffic, this dated scanning approach introduces unacceptable levels of latency.

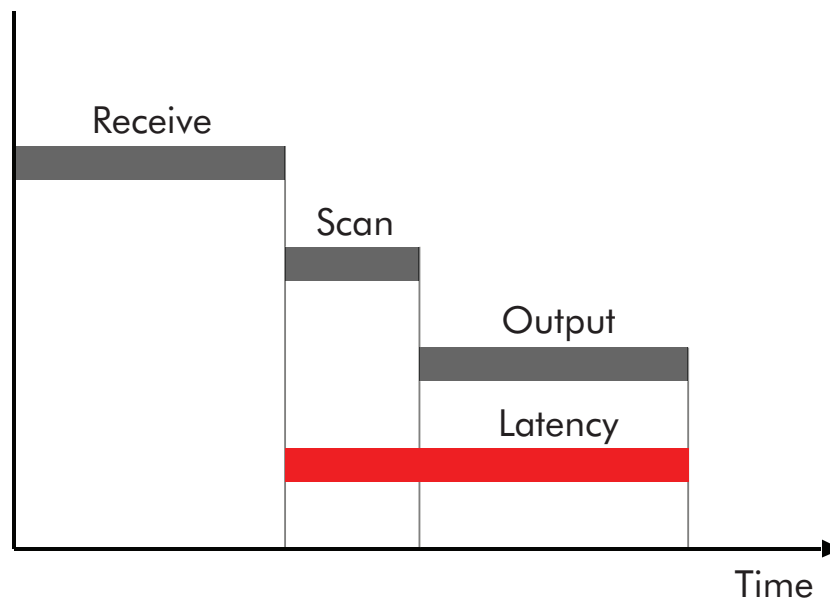


Figure 1: Traditional Batch-based Scanning

In contrast, stream scanning is based on the simple observation that network traffic travels in streams. Rather than wait for the entire file to arrive, the NETGEAR® Stream Scanning Engine begins receiving and analyzing traffic the moment the stream enters the network (see Figure 2). Once the minimum number of bytes is received, scanning commences. The scan engine continues to scan additional bytes as they become available, while another thread outputs the bytes that have been scanned. This multithreaded approach enables complete scans with minimal impact to network performance. File scans are many times faster than those of traditional security solutions – an easily visible increase in performance. NETGEAR Stream Scanning Technology is also highly scalable, so these performance benefits become increasingly pronounced as the volume of traffic increases. Organizations are therefore able to withstand significant spikes in traffic, as would occur in the event of an Internet-based threat outbreak.

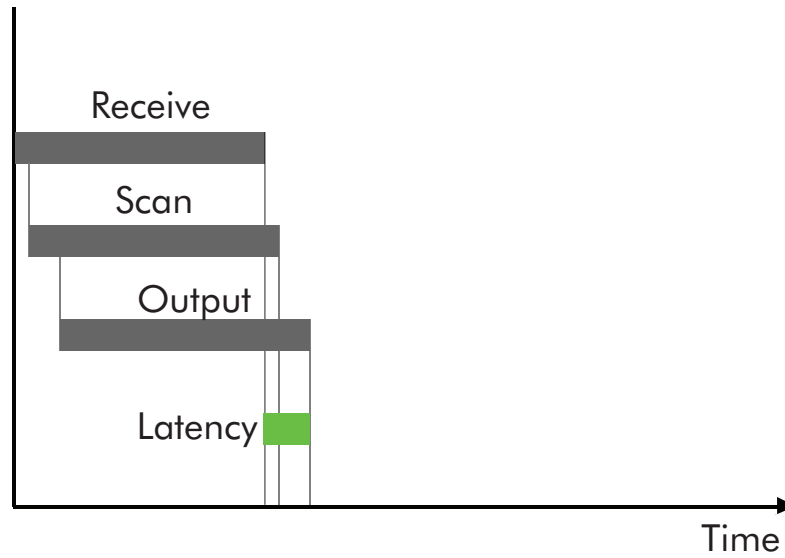


Figure 2: NETGEAR Stream Scanning

In comprehensive benchmark testing, NETGEAR Stream Scanning Technology consistently performed five times faster than traditional batch-based solutions. It has been successfully implemented in a wide range of industries – from government, to healthcare, to retail – with deployments ranging from small companies with fewer than 50 users, to geographically dispersed networks comprising thousands of users. For networks of all sizes, NETGEAR Stream Scanning Technology provides comprehensive, best-of-breed protection from Web- and email-based threats with minimal latency.

Conclusion

In today's dynamic business environment, small- and mid-size companies require a balance between networking and security. Security solutions must keep the company safe from the constant barrage of Internet-based threats, without becoming a communications bottleneck. NETGEAR patent-pending Stream Scanning architecture achieves this balance. NETGEAR scans high volumes of network traffic for security threats in real-time, without bringing the company's network communications to a standstill.

NETGEAR® ProSecure™ STM Web and Email Threat Management Appliance Solution

The ProSecure STM Appliance uses a unique technology that detects and blocks outbreaks based on their rapid and wide distribution behavior. This approach can detect spam and malware outbreaks as soon as they emerge, and block all associated messages in real time.

The ProSecure STM Appliance features patent pending Stream Scanning Technology that is designed to scan data streams as they enter the network. With Stream Scanning Technology, the NETGEAR STM is able to process large amounts of data in real-time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and Web content clean and without delay.

The ProSecure STM Appliance uses a proactive behavioral defense system that eliminates the gap between a vulnerability being exploited and the fix. The NETGEAR solution uses forensic analysis to identify suspicious characteristics of incoming and outgoing network traffic, and neutralizes them until they can be examined more closely.

NETGEAR, the NETGEAR logo, Connect with Innovation and ProSecure are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2009 NETGEAR, Inc. All rights reserved.