



Seven Reasons Security and Performance Must Coexist - And How to Get Them To

A Cymphonix White Paper



Introduction

As Internet threats increase organizations must build defenses to protect employees, productivity and data. Yet, at the same time, on-demand applications, remote resources and online content usage are at an all-time high – requiring better performance from network infrastructure and Internet circuits.

Network administrators must implement a broader set of security features yet improve application performance to meet the needs of the organization. This introduces major challenges; the implementation of numerous security platforms increases network latency, interface management and troubleshooting complexity. Additionally, treating Internet security and performance as opposing functions eliminates any hope of diagnosing Internet data stream issues or correlating the events that impact security and performance.

The following list outlines the seven reasons security and performance must coexist on corporate networks and introduces Cymphonix's recommendation for solving each issue.

1.

Most Multiple/Blended Threat Management Approaches Create Latency

A recent article published by Network World points out the incredible latency introduced by popular Unified Threat Management (UTM) devices. Stating, "it's not uncommon for the UTM products on the market today to suffer as much as a 50% loss in performance..."¹ Most UTM solutions on the market function similarly to the disparate devices they attempt to replace. Simply put, these devices process packets at least one time for every threat they attempt to stop. By scanning once for spyware, once for viruses, once for unsafe URLs, once for inappropriate content, once for infected file transfers, etc gateway throughput diminishes significantly.

UTM devices often evolve from previous security devices like firewalls or proxies. Unfortunately this evolution causes underpowered hardware configurations that aren't optimized for processing the deep-packet scanning required to protect against blended threats. Organizations should implement solutions that utilize a scan-once-reference-many approach to blended threats. By scanning once, then referencing multiple threat, file and application libraries latency is reduced significantly.

2.

Security Issues Become Apparent When They Impact Committed Service Levels.

Organizations often don't discover security issues until they impact performance and access to online resources. For example, spyware protection recently has become high priority to network administrators. This is due primarily to the impact spyware has on productivity. In 2005 IDC estimated that spyware issues represent 30% of all help desk calls.²

Organizations benefit greatly when Internet circuit performance is monitored along with security breaches. Network administrators should look for solutions that report on Internet circuit performance, producing alerts when service levels drop below committed levels.

3.

Layer 7 Shaping Provides True Insight and Control over the User Experience

The legacy approach of port-based application rate limiting or threat blocking is no longer sufficient for delivering an effective user experience. Blended threats and mission-critical applications may now share common ports and function similarly to HTTP or HTTPS traffic. QoS tags may also be insufficient for VoIP calls that don't rely on MPLS queuing (e.g., Skype). For this reason, gateway security devices and application shaping appliances should share at least one major attribute in common: Layer 7 application recognition and control. By implementing Layer 7 application recognition and control and coordinating it with other networking communication attributes, organizations will be able to identify packet attributes and then set policies on those attributes – creating a more productive user experience. For example, only a solution that can identify Layer 7 application attributes (in coordination of other network communication attributes) can identify and stop or filter non-port 80 HTTP traffic – a common approach of utilizing proxy anonymizers to bypass Internet content filtering policies.

4.

Integrated Policy Management

Network security, access and application policies vary by department, group, job function and even individual. While traditionally viewed as disparate, security, access and application policies should actually compliment one another for both management and efficiency. Administrators should implement solutions that deliver Internet policy management tools with application bandwidth, Internet content, time-of-day, threat and access policy features integrated into a single interface. This approach allows administrators to manage the Internet data stream by user/group, application and threat.

5.

Event Correlation of Disparate Internet and Network Events

Internet performance is slow – what's causing it and how do you start troubleshooting? Most network administrators look immediately to online connection speed tests, IDS/IPS reports, traffic logs, and potentially even packet sniffers to identify problem areas. While these traditional approaches can yield results, it's often difficult to identify the root cause of performance issues. For example, poor Internet performance is often a symptom of spyware infection. The infected device utilizes its Internet connection to run zombie processes – calling home to transfer data or even pass data through other infected machines. But, when such infectious activity appears as HTTP traffic, how is an administrator to identify and correct the issue? An integrated approach to security and performance should provide true event correlation for troubleshooting the problem. In this case, when performance stalls, the administrator would check real-time reports showing total upload and download volumes, drill down to identify the top bandwidth consumers, and then verify the applications used by those machines or individuals. Through Layer 7 application identification the administrator would quickly see the spyware/zombie traffic

and have the control to immediately stop data transfer from that machine – either by application (spyware) or by total traffic. Within moments, performance would be restored and the administrator could tend to cleaning the infected machine. With true event correlation, the administrator would also be able to identify what activity caused the spyware infection and where it came from – to establish preventative policies and prevent future infections.

6.

Data-Driven Decision Making

Disparate systems generate separate reports and often produce conflicting data. While savvy administrators may be able to deduce causes of performance issues and security breaches, such work is often time consuming and fails to deliver effective reports for communicating reasoning with management. According to the Standish Group only 29% of IT projects finish on time and on budget³ – it's no wonder administrators are looking for better data. By integrating security solutions with performance solutions administrators are able to generate better data about what's really happening with their Internet connection – and communicate their decisions to management.

7.

Users, Applications and Threats Will Always Demand More Resources

When it comes to calculating bandwidth circuit requirements for any particular organization there are three time-proven concepts to consider:

1. Users and groups of users will always attempt to download, upload and use larger and larger files
2. Applications work on a first-come-first-serve basis and demand sufficient resources to function. As applications become more complex, more resources are required
3. Threats come with connectivity – so if you're connected to the Internet, you have to deal with them. Unfortunately threats also use/demand connectivity resources. The new breed of spyware/adware/malware threats consume bandwidth resources that mission-critical applications need to function

Buying more bandwidth, a larger Internet circuit, is never a permanent solution to performance issues. As connectivity resources increase users, applications and threats will quickly fill the gap. Administrators must implement policies to manage user access to content, application priority and stop threats from impacting resources. Implementing policies with a unified Internet data stream control device is more effective and cost efficient than attempting to manage multiple disparate security and performance devices.

Gateway threat management tools, whether single-purpose or blended, help organizations become more protected from both internal and external threats. Application performance solutions increase organizations' ability to prioritize mission-critical information. However, by combining security with application performance, organizations can correlate isolated events and more easily identify and control the problems created when users, applications and threats compete for network resources.

About Cymphonix

Cymphonix Corporation, headquartered in Sandy, Utah, uses patent-pending Cross-Layer Intelligence™ (XLI™) technology to provide unmatched network threat protection and resource optimization. With the powerful XLI engine, Cymphonix products seamlessly integrate network protection, application performance, and traffic visibility into a single, easily managed solution.

For more information about Network Composer™ and other Cymphonix solutions visit www.cymphonix.com or call toll free 866-511-1155.

References:

1. *All-in-one security devices face challenges* by Ellen Messmer, 08/14/06
<http://www.networkworld.com/news/2006/080906-all-in-one.html?page=1>
2. *Spyware costs plague SMBs* by Linda Tucci, 05/18/06
http://searchsmb.techtarget.com/originalContent/0,289142,sid44_gci1089658,00.html
3. *Trim the Fat* by Harry J. Harczak Jr., 06/2006
http://www.biztechmagazine.com/article.asp?item_id=141

Cymphonix Corporation
8871 S. Sandy Parkway, Suite 150
Sandy, Utah 84070
866-511-1155
www.cymphonix.com