WHITE PAPER

The Next Step in Network Security for Enterprises

Sponsor: Juniper Networks

Author: Mark Bouchard

AimPoint Group

keeping IT on target

Introduction

The mandate for enterprise IT is simple: facilitate transformation of "the business" or share in its eventual demise. To be relevant, viable, and—at least in the case of commercial entities—profitable, organizations must fully embrace information technology not only as a means to achieve greater operational efficiency and reduce costs, but also to differentiate themselves by offering customers and constituents a diverse range of compelling and increasingly sophisticated services. Moreover, to *remain* relevant, it is essential that enterprises treat transformation as a continuous process. New and innovative technologies are emerging seemingly on a daily basis and steadily incorporating them to unlock greater potential is really the only way to keep pace with the increasing "speed of business."

A significant obstacle to all of this transformation and differentiation, however, is the absence of a sufficiently capable network security solution to support an enterprise's most rigorous use cases. The vast majority of available security products are strikingly incapable of achieving the balance necessary to adequately address ongoing trends driving the need for substantially higher throughput, lower latency, and greater stopping power—not to mention other essential criteria such as adaptability, reliability, unified management, and cost effectiveness. The presence of capabilities and strengths in one or more of these areas is inevitably coupled with weaknesses in others.

What enterprises need instead is a next-generation network security solution, one that has been architected from the outset to meet all of the applicable requirements simultaneously. This would allow them to pursue new applications, technologies, and ways of doing business without having to make risky compromises or incur extraordinary costs. Accordingly, this paper explains why a next-generation network security solution is needed now, what such a solution entails, and the wide range of benefits that it yields.

A Challenging Scenario for Enterprises

Enterprise IT departments are in a difficult position. Their value is based on enabling new and better ways of conducting business, but all too often the underlying details of what this entails are not in alignment with each other. The concept of creating applications and leveraging available communications technologies to automate and accelerate various business processes is fairly straightforward. So is the need to provide an effective level of confidentiality, integrity, and availability—in other words, security—for the resulting services and associated infrastructure. It's when other real-world conditions and demands are accounted for that things get significantly more complicated.

Take user mobility and globalization, for example. Most organizations are pursuing related initiatives to help generate growth. These are somewhat at odds with a completely separate trend, data center consolidation, which is being undertaken to establish economies of scale and help reduce costs. Combined, the two sets of changes present a challenge, albeit a relatively manageable one, in that users are increasingly being separated from the applications and other information resources they require to get their jobs done. Layering in a third trend, however, makes a substantial difference. Specifically, the bandwidth requirements and latency constraints that accompany the growing sophistication of applications make it considerably more difficult to adequately support a highly dispersed user population.

One area in particular where this convergence of absolutely sensible, business-driven trends is proving problematic is network security. As it turns out, it's the very growth, richness, and diversity of the new approaches to conducting business and the applications being used to support them that is creating an increasingly challenging protection scenario and, in turn, eroding the effectiveness of conventional network security products.

The Growing Volume and Sophistication of Network Traffic

One of the major changes impacting the effectiveness of network security solutions is the growing volume and sophistication of network traffic. Just like the service provider community, most enterprises find themselves in the position of having to take greater advantage of information technology, not only to improve their ability to capture and retain customers, but also to reduce costs through increased operational efficiency.

The rising "speed of business" is practically dictating an increased pace of development and deployment of new applications to support both back office and customer-facing processes. The same reasons are driving greater "exposure" of applications that organizations already have, for example, by making internal systems and solutions externally accessible and/or by extending coverage to additional populations of users and devices.

Enterprises, of course, also need to react to pressure on the economic front. To this end, data centers are being consolidated to help establish economies of scale and to further reduce costs by centralizing and simplifying tasks associated with system administration, information security, and achieving regulatory compliance. In addition, organizations are steadily embracing cost saving practices and technologies such as teleworking, software as a service, and server virtualization. From a networking perspective, a key result is changing traffic patterns. Data centers are becoming even greater points of concentration and complexity at the same time that the average number of "hops" user sessions need to traverse is increasing.

Then there's the changing nature of applications. This too is being driven by the realities of the business environment, but also by the natural evolution of technology. Applications are becoming far more complex, involving far more components and capabilities than were previously the norm. Take the concept of a Web 2.0 mashup, for example, where numerous underlying connections are made to compute and compile a useful aggregation of multiple, networked data sources and services, each typically representing an application in its own right. Or consider a multimedia collaboration application such as a telepresence solution. In fact, the latter serves to highlight yet another important characteristic, namely a growing sensitivity of many applications to latency—a product of the mounting interest to deliver ever richer content in conjunction with real-time interactions.

The impact of these various trends is twofold. First, there has been, and in all likelihood will continue to be, a veritable explosion in the amount of network traffic that enterprises are required to process and protect. The second issue is that whatever processing and protecting is done, it must be accomplished with a minimum of introduced latency—an objective that is becoming even harder to achieve given the growing volume and sophistication of threats.

The Growing Volume and Sophistication of Threats

No longer satisfied with merely building their reputations, hackers are now intent on actually making money. Rather than creating threats that "rattle our cages," they are now focused on designing exploits that successfully evade or overwhelm the majority of commonly installed countermeasures. This has led to a number of notable changes with regard to the nature of the threat landscape.

For starters, there has been a veritable explosion in terms of the sheer quantity of threats being released in recent years. The speed with which new exploits are developed and launched has also risen dramatically, particularly relative to when associated vulnerabilities are disclosed. Zero-day threats, once described in hypothetical terms, are now an all too common reality.

On top of everything else, increased creativity on the part of hackers has led to a threat population characterized by significantly greater diversity and, on average, significantly greater elusiveness. The predominate concerns of the past such as file level viruses and worms have been overshadowed by an array of new contenders that include spyware, spear phishing, keylogging trojans, rootkits, and targeted attacks. Even more troubling is the trend of threats "migrating up the stack" to take advantage of much harder to protect application-layer weaknesses.

Once again, the impact these changes have for enterprises is essentially twofold. First, in case it wasn't already clear, the prevailing conditions reconfirm the need to actively provide protection for the network traffic and associated computing infrastructure that represent the lifeblood of their companies. The second issue has to do with the scope of this protection. Multiple types of countermeasures—some involving intensive, in-depth inspection techniques—will need to be applied in order to adequately account for the diversity and elusiveness of today's threats. This latter item in particular has several important implications for what constitutes a suitable network security solution for today's enterprises.

The Impact on Network Security Infrastructure—Key Requirements Going Forward

The challenges outlined in the preceding sections are instructive in that they reveal the minimum set of requirements that now define an appropriate network security solution for an enterprise's most rigorous use cases. Specifically, to be considered effective, a solution must fully address the following set of essential criteria.

- **Security:** To meet the need for greater stopping power, a solution must incorporate multiple countermeasures that feature a blend of positive and negative model techniques providing protection not only at the network layer, but at the application layer and for individual elements of data as well. Firewall technology, even if it's used in conjunction with an antivirus solution, is simply not sufficient.
- **Scalability:** System capacity must be readily scalable from relatively modest traffic rates of a few Gbps to an aggregate throughput of greater than 100 Gbps. This is not enough, however. Session handling capabilities must also scale to match these throughput levels. For a portfolio including complex multimedia, real-time, and Web 2.0 applications, this translates into the ability to support several million simultaneous sessions.
- **Latency:** Given the performance characteristics of today's applications and the far-flung nature of their users, this criterion can no longer afford to be treated as secondary to having generous amounts of throughput. The two are definitely intertwined, but latency should also be considered in its own right. Solutions must be architected to minimize the amount they introduce, and should also incorporate capabilities to prioritize the processing of designated, time-sensitive traffic streams.
- **Unified management:** Administration of the solution's various capabilities should not require the use of multiple management tools or consoles. Ideally, it should be possible to configure all of the different inspections required for a given traffic stream within a single rule or policy statement. In addition, the solution should feature (a) extensive role-based administration capabilities to enable granular separation of duties, and (b) management coverage for other security products offered by the same vendor (for example, a branch office solution).
- **Reliability:** Highly proven software, redundant components, and support for high availability configurations are absolutely imperative given the potential impact of failures on enterprises and their customers and constituents alike.
- **Adaptability:** The solution should be able to accommodate additional functionality—especially new security capabilities as they become available—without the need for a major "rip and replace" exercise.

- **Networking/compatibility:** To ensure applicability in the broadest set of use cases, the solution should include at least basic support for a wide range of networking technologies (NAT, address assignment, VLANs, and security zones). Further infrastructure consolidation and simplification can be realized, however, if full featured instances of certain technologies are fully incorporated, such as routing and switching capabilities.
- **Cost effectiveness:** This is already accounted for in part by each of the preceding criteria, but the general idea is that the solution should be designed to reduce infrastructure complexity and total cost of ownership relative to available alternatives.

These requirements and the solution they represent are particularly relevant when it comes to securing data centers. This is certainly the most intensive deployment location that enterprises have for security and networking equipment—not to mention one that is receiving heightened levels of attention as compliance auditors continue to elevate the importance of securing internal networks and systems. Larger enterprises, however, may also find a solution matching these requirements to be appropriate, if not actually necessary, at their boundaries to the Internet. After all, aggressive e-commerce strategies, the increasing size and dispersion of user, consumer, and constituent populations, and higher degrees of interconnectivity—driven in part by Web services and Web 2.0 technologies—are all causing rapid growth in the volume/rate of traffic destined to and from the Internet.

Conventional Approaches Come Up Short

The different types of network security products currently in use by most enterprises address the requirements identified above to some extent, but they typically have significant limitations as well.

Best-of-breed appliances. Single-service products featuring best-in-class security software continue to receive a lot of attention, particularly for countering new classes of threats or implementing newly emerged security technologies. Even with specialized hardware, however, multiple instances are often needed to achieve sufficient scalability. And this gets multiplied, of course, by the need to have a similar set of devices for each and every countermeasure an enterprise decides to deploy. Security and throughput objectives can generally be achieved, but not without substantial cost—not to mention latency, complexity, and rigidity.

Blade systems. Chassis-based systems that accommodate multiple server blades are definitely a step in the right direction but, unfortunately, not a very big one. New functionality or greater throughput is supported by simply adding more blades. As such, these systems definitely deliver a measure of consolidation and reduced complexity, at least relative to best-in-class appliances. However, they fail to address the need for lower latency. To be fully "processed and protected," packets need to transit the system's backplane multiple times and be reprocessed by each of the different security "modules." In addition, little if anything has been done to unify management. And enterprises can still run into throughput constraints due to all of the redundant processing that is required and the fact that most of these systems rely on generic hardware (and operating systems) for the individual blades.

Unified threat management (UTM) appliances. Combining multiple countermeasures with a purpose-built appliance platform has a few interesting advantages. Products with true service integration not only provide a complementary set of security capabilities, but do so with unified management and a fairly efficient processing model that introduces minimal latency. On the downside, throughputs above 1 Gbps are practically unattainable, at least not without adversely impacting latency or cutting back on the different types of inspections that are conducted. Numerous units will be needed to support many use cases, leading to commensurate increases in cost and complexity. Having a fixed form factor also limits the adaptability of such products.

The net result is that enterprises are caught between a rock and a hard place. They can choose: not to pursue new applications, technologies, and ways of doing business because there isn't really an effective way to economically secure them; to pursue these business-critical items but not bother with securing them at all; or, to negotiate various trade-offs and compromises to pursue and protect them as best they can with the less-than-ideal security solutions that are available. In fact, chances are good that most enterprises are employing all three of these approaches to some extent, at any point in time.

A Next-Generation Architecture that Delivers

What today's enterprises need is another alternative: a network security solution architected to maximize attainment of the previously identified requirements, one that is capable of fully enabling the various initiatives that enterprises must pursue to drive operational efficiency and reduce costs yet still remain competitive. Based on their respective strengths and weaknesses, a combination of the traditional chassis and UTM approaches would certainly be a logical foundation from which to build. Indeed, a very attractive option would be a chassis-based design that features:

- Interface flexibility, ideally in the form of modular cards/blades
- Dedicated, distributed hardware and software-based intelligence for ingress processing (for example, denial of service screening, session lookup), internal distribution and balancing of session traffic, and egress processing (for example, traffic management)
- A high speed, non-blocking switching fabric that provides any-to-any connectivity between all slots/blades
- Scalable processing capacity, ideally in the form of blades that are dynamically programmable and that automatically inherit the configuration of all other processing cards (thereby avoiding the management overhead and inevitable utilization inefficiencies associated with having each blade configured to perform a specific subset of tasks)
- A dedicated control plane to enable full time accessibility to management functions
- Redundant hardware components and support for high availability configurations
- A modular operating system capable of being incrementally upgraded (for adaptability purposes) and serving as the "central store" for a robust set of security services that are tightly integrated (to avoid redundant packet processing)
- Fully unified policy and configuration management
- A robust networking feature set, including routing, switching, and virtualization capabilities

A network security solution designed to these specifications is attractive not only due to the tremendous capabilities it provides (see Table 1), but also because it is based on a highly proven architecture. After all, the architecture described herein is basically the same as that used in today's large enterprise and carrier-grade routing and switching platforms.

Table 1: Comparison of Different Network Security Product Architectures

	Best-of-Breed Appliances	Traditional Chassis	UTM Appliances	Next-Gen Architecture
Security	☆	☆☆☆	☆☆☆	☆☆☆
Scalability	☆	☆☆	—	☆☆☆
Latency	—	☆	☆☆☆	☆☆☆
Management	—	☆	☆☆☆	☆☆☆
Adaptability	—	☆☆☆	—	☆☆☆
Cost/Complexity	—	☆½	☆½	☆☆☆
Networking	☆	☆	☆	☆☆☆

The Benefits of a Next-Generation Network Security Solution

The technical advantages and capabilities that can be attributed to a next-generation network security solution—one that is consistent with the previously described architecture—have already been fairly well illuminated. They include substantially greater scalability and security coverage with considerably less latency and infrastructure complexity. However, there are numerous business benefits that should also be acknowledged. For enterprises, a next-generation network security solution:

- **Enhances responsiveness and competitiveness**—rapid deployment of new and innovative applications and services is enabled by removing the obstacle of always having to first acquire and then deploy more security infrastructure to ensure their integrity
- **Lowers IT cost of ownership**—the availability of a high capacity, low latency network security solution eliminates potential constraints to pursuing imperative cost saving initiatives such as data center consolidation, virtualization, and teleworking; furthermore, the associated security and networking infrastructure, along with its management, is greatly simplified
- **Facilitates current and future growth**—new and increasingly sophisticated technologies and latency-sensitive applications can be fully embraced to drive near term growth, while a high degree of adaptability ensures solution applicability even as the threat, application, technology, and business landscapes continue to change
- **Reduces risk**—compute-intensive security functions such as intrusion prevention can be widely deployed without the need to scale back on other inspection and control mechanisms, and without having to worry about degrading the end user experience
- **Helps achieve compliance**—having a feasible solution for deploying essential countermeasures in enterprise data centers makes it easier to fulfill regulatory requirements that pertain to establishing reasonable and appropriate defenses for internal networks and systems

The bottom line is that a next-generation network security solution enables enterprise IT not only to support but accelerate the transformation, innovation, and differentiation required to sustain growth of "the business" while still containing costs. New applications and the infrastructure that supports them can easily be scaled without the usual delays and capital expenditures required for new hardware installations.

Summary

Today's CIOs are under mounting pressure to implement advanced technologies and dynamic, content-rich applications to help sustain business growth, while also reducing the cost of IT operations. However, their ability to pursue these increasingly crucial initiatives is being impeded by the lack of a product that can adequately address the resulting demands placed on their network security infrastructure—particularly at hotspot locations such as the data center core and/or edge. What they require is a next-generation network security solution, one that takes a page from the book used to design carrier-grade routing and switching platforms. By employing a similar architecture and taking advantage of similar design principles, such a solution is capable of delivering superior protection with minimal added latency and greater scalability, adaptability, and cost-effectiveness than would otherwise be possible. The net result: enterprises can pursue new applications, technologies, and ways of doing business without having to make risky compromises or incur extraordinary costs.

About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and advisory services company specializing in information security, compliance management, application delivery, and infrastructure optimization strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security and networking topics for more than 12 years. During this time, he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and high-level architectures to the justification, selection, and deployment of their security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about helping enterprises address their IT challenges.

A Word From the Sponsor

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

2000303-001-EN Apr 2009