WHITE PAPER

Network Security for 2010 and Beyond – The Impact of The Consumerization, Webification, Virtualization, and Consolidation of IT

Sponsor: SonicWALL

Author: Mark Bouchard

AimPoint Group

keeping IT on target

Executive Summary

Several high-level, business-driven IT trends are eroding the effectiveness of conventional approaches to network security, thereby forcing the evolution of related products and technologies. This paper explores four of these trends in particular – consumerization, webification, virtualization, and consolidation – identifying for each the drivers that make it matter, the characteristics that impact network security, and the resulting implications for network security strategies and solutions.

Overall, 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 (e.g., port, source/destination address) and inferred relationships to establish a corresponding level of trust. Furthermore, emphasis should be placed on integrated solutions that deliver multiple counter-measures and other helpful features – especially intrusion prevention and anti-malware capabilities – not only to reduce costs and complexity, but also to account for the reality that even a tighter degree of access control does not preclude threats from being conveyed within allowed traffic streams.

The Power of the People

To be clear, none of the four trends discussed herein is by any means new. Consistent with the definition of "trend", each has been underway now for at least a couple of years, and each is still going strong. Indeed, it could be said that all four have solidly reached the mainstream, which – along with how they overlap and reinforce one another – is what makes now a particularly appropriate time to hammer home the related security issues. First up: consumerization.

What is the Consumerization of IT?

Put succinctly, the consumerization of IT involves the introduction of consumer-oriented technologies, behaviors, and expectations into the realm of enterprise IT. And perhaps "introduction" is too passive to describe what's really occurring. Actually, it's more like IT is being force fed; it's being given no option other than to support the ongoing cross-over and melding of equipment, services, and activities of a personal nature with those historically identified as being "business-oriented."

Why is Consumerization Happening?

There are multiple drivers for this trend. First and foremost it is necessary to acknowledge that it's the people that make any business go and that ultimately ensure its sustainability. And over time these people have been able to obtain increasingly affordable, easy-to-use, yet very powerful tools – typically in the form of both devices and applications/services – that have helped them improve the quality of their personal lives, for example, by providing markedly better access to information and more efficient communications. Now, as employees, these same people want to apply these same innovations and the associated skills they've acquired to achieve similar benefits in the work environment. Beyond *wanting* to do this, they actually *expect* to.

Moreover, business managers are inclined to allow, even encourage, this very outcome. In addition to potential improvements in business-process execution and efficiency, they also stand to gain by being able to reduce their budgets for user devices, support, and training.

How Does Consumerization Impact Network Security?

So what does any of this have to do with network security? Well, one of the chief characteristics of the consumerization of IT is the corresponding proliferation of and loss of control over end-user computing devices. Practically speaking, this serves to erode and make variable the level of trust that can be attributed to any given device. The IT department, along with its network security infrastructure, must be able to account for a mixed bag. Not all devices will have a robust security model, not all devices will be corporate-owned and managed, and neither will there be clear relationships between a device's location (e.g., inside the network) and its type, security state, or category of user.

This implies the need for network security solutions that, at a minimum, can accommodate access and usage policies that vary based not just on device type but also on the actual security state of the device at the time it's connecting to the corporate computing environment. As good as this sounds, however, such policies involve a tremendous amount of detail and can quickly become complex and onerous to manage. Better yet then are solutions that reduce the need to rely on this approach by *also*:

a) supporting user identity, which is a higher-value and potentially over-riding attribute for establishing trust; and,

b) providing the means to simply treat all devices as untrusted, for example, by incorporating intrusion prevention and anti-malware capabilities that can be used to scan all traffic from all devices.

Two other side effects of consumerization also deserve attention. The first of these is that consumerization is inherently linked to mobilization. The types of devices involved are PDAs, smartphones, and other portable platforms. And the expectation is that they can be used not just while in the office but from remote locations as well. This points to the need for an organization's network security portfolio to also include SSL VPN technology.

The second item applies to both users and administrators and involves another expectation that consumerization brings with it: that tools be simple, straightforward, and easy to use. Going forward, network security solutions should ideally exhibit these characteristics as well.

The Web, Web 2.0, and Enterprise 2.0

The webification of IT is a general term meant to capture three high-level developments:

- The long-running transition from applications with thick clients to those which use a Web browser as a universal client;
- The evolution from simple publishing sites used to convey static information, to revenue-garnering transactional Web applications, to the rich and highly interactive Web 2.0 services of today; and
- The emergence of Enterprise 2.0, another symptom of the consumerization of IT whereby what were once classified as frivolous, user-oriented Web 2.0 services and technologies are now being used to facilitate a wide variety of business operations (e.g., marketing, support, research, and development).

Why is Webification Happening?

Once again, there are multiple drivers for this trend. The tremendous reach the Web provides organizations is an obvious one. Standardization and related cost efficiencies are also powerful motivating factors. Looking more specifically toward Web and Enterprise 2.0, businesses are attracted to the potential of having applications that "self-improve" as more people use them. In addition, with the proper approach, the network effects afforded by the Web can be harnessed not just to obtain more users/customers, but also to learn from them and to build on their contributions. New ideas can be vetted, modified, re-evaluated, confirmed, and quantified in terms of their potential at a speed and with a degree of thoroughness unlike any before. In a nutshell, webification paves the way for organizations to dramatically improve their operational efficiency and competitive posture in the marketplace, and that is why it's here to stay.

How Does Webification Impact Network Security?

In terms of how network security strategies and solutions need to evolve, the primary implications of the webification of IT are threefold.

(1) Protocol and port details have been rendered practically useless when it comes to setting and enforcing security policies. Webification means that an estimated two-thirds of network traffic is HTTP and HTTPS over TCP ports 80 and 443, respectively. The actual applications being used can be virtually anything and everything, even email. And although Web traffic is the worst offender in this regard, the potential is there for other ports and protocols to be used and/or abused in a similar fashion. The net result is that network security solutions can no longer rely on port and protocol, but instead must have sufficient visibility and fluency such that traffic can be controlled (in part) based on the specific applications that are generating it.

(2) A combination of the participatory nature of Web 2.0 and the susceptibility of the technology used to enable related capabilities has made it virtually impossible to reliably pre-classify web sites/services as trusted or untrusted. It is simply too easy for hackers either to exploit associated vulnerabilities or to make content contributions that are malware (or include pointers to malware). The result, much like with the consumerization of IT, is the need to treat all sites and services as untrusted and, therefore, the need to scan all associated network traffic for malware and other threats in real time.

(3) The participatory nature of Web/Enterprise 2.0 also facilitates data sharing and exchange. This increases the risk of both intentional and unintentional disclosure of sensitive information, in turn driving the need for network security solutions to incorporate at least some basic capabilities for controlling the flow of content and individual elements of data – such as being able to block files of a certain type, specific files known to contain sensitive data, and files and other communications traffic that is detected on-the-fly to contain sensitive material.

Virtualization is Virtually Everywhere

As described by market leader VMware Inc, virtualization entails "the separation of a resource or request for a service from the underlying physical delivery of that service." In more practical terms, the point of abstracting the interface to a resource in this way is to allow it to be shared among multiple "consumers" of its services, each of which remains isolated from the others. For example, with server virtualization a single instance of server hardware can effectively support multiple workloads, or virtual machines, each of which is comprised of an application, operating system, and associated data files.

Why is Virtualization Happening?

Server virtualization, in particular, is extremely popular among organizations of all sizes and types due to the compelling benefits it conveys. Organizations can substantially reduce server counts, in turn slashing expenditures for hardware, administration, energy, facilities, and so forth. In addition, the portability of virtual machine workloads simplifies the process of achieving high availability and business continuity objectives while also making it extremely easy to adapt to changing business conditions and operational models. For example, with server virtualization technology and a corresponding set of management tools, additional instances of a workload can be spun up (or down) on demand, resources can flexibly be re-provisioned as needed, and cloud computing infrastructure can dynamically be engaged to augment existing datacenters during periods of high demand.

To be clear, desktop, application, and other flavors of virtualization are also gaining traction. None of these is as pervasive as server virtualization, however, and neither do they have as significant an impact on network security. That said, worthwhile to note is the potential for desktop virtualization to help with the device proliferation issue introduced by the consumerization of IT. Specifically, desktop virtualization is attractive in this regard because it facilitates an approach where applications and sensitive data remain accessible yet need never leave the datacenter.

How Does Virtualization Impact Network Security?

With regard to network security, the primary challenges as a result of server virtualization are how to protect virtual networks and how to protect dynamic networks.

The issue with the first of these items stems from the presence of virtual switching features and the ability, therefore, to create portions of networks within a single physical host. The problem that arises is how to apply the appropriate security policies and filtering capabilities to the communications traffic flowing between the virtual servers operating in such an environment. The answer is that network security solutions must themselves become "virtual-izable." In other words, versions must be available that take the form either of virtual appliances or of unadorned software that administrators can combine with an operating system and then "package" as a virtual machine.

The second challenge is bit thornier. Live migration is a popular, value-add capability for most server virtualization solutions that enables individual virtual machines to dynamically be re-located from one physical server to another – for instance, in the event the first server is overloaded or about to crash. The concern in this case is that an associated/nearby security device could suffer from a loss of context – that is, a loss of session state, the relationship between networked systems, or the identity of the migrated system – and thereby become unable to properly enforce the appropriate security policies. To account for this situation, network security solutions must evolve such that their dependence on details like session state, location, directional orientation, and network-layer attributes is reduced in favor of items that are agnostic/independent of both the physical *and* logical environment – such as the specific applications and services that are being used and who is using them.

Consolidation and Centralization are Core Objectives

The final macro-level trend on the table is the consolidation of IT. Succinctly put, organizations today are intent on reducing the number of distinct instances and overall amount of infrastructure they own, operate, and maintain. And in this case infrastructure refers to anything and everything, from applications, servers, storage, and network devices all the way up to entire datacenters. Inherently linked to this trend is centralization, or the removal of infrastructure from remote locations in favor of running larger instances of the same solutions at fewer locations that are then accessed remotely.

Why is Consolidation Happening?

Consolidation and centralization are being fervently pursued by today's organizations in large part because they are among the most effective ways to cut infrastructure related costs and complexity and improve operational efficiency. Beyond these bottom line benefits, they also simplify security and ease the burden of demonstrating compliance with privacy and industry specific security regulations. Heightened requirements for disaster recovery and business continuity also become easier to address, both by making secure remote access available on a widespread basis and by making it less costly to provide advanced HA capabilities for the majority of business-critical systems.

How Does Consolidation Impact Network Security?

IT consolidation creates both a problem and an opportunity when it comes to network security. The problem is that having so much of an organization's infrastructure in one place translates into having a substantially greater amount of network traffic at that place. As a result, network security solutions must be available in high-capacity, high-performance versions. In today's computing environments, the ability to process and fully protect multiple Gbps of traffic without introducing too much latency along the way is not an option; it's a necessity.

The opportunity, on the other hand, is for network security solutions to become part of the trend, that is, to help reduce infrastructure cost and complexity by themselves providing a significant measure of consolidation. It has already been noted that in addition to enforcing access control policies, effective network security requires intrusion prevention, anti-malware, content control, and SSL VPN capabilities – at a minimum. It would certainly be advantageous then, if organizations could obtain all of the essential countermeasures they require in a single, integrated solution. The catch, of course, is that such solutions must not result in making any significant compromises relative to point products in terms of feature set, effectiveness, manageability, and performance.

Bringing It All Together

Just like IT must continuously evolve to adequately support the business so to must network security evolve to adequately support IT. In particular, the specific capabilities and characteristics that network security solutions need to provide in response to the consumerization, webification, virtualization, and consolidation of IT are:

- The ability to accommodate access and usage policies that vary based on the type and security state of the source device;
- The ability to set and define access, usage, and filtering rules based on higher-layer attributes, including user identity, the specific applications being used, and the actual content being transmitted;

- The ability to scan all traffic for malware and other types of threats (due to the proliferation of un-trustable devices, sites, and services);
- The ability to dynamically support secure remote access for a wide variety of device types;
- Greater ease of use for both administrators and users;
- The ability to be delivered/deployed as part of a virtualized network;
- A high-performance architecture that can fully process and protect high volumes of network traffic; and,
- The ability to meet many (if not all) of an organization's network security requirements with a single, integrated, enterprise-class solution.

About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis firm 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 13 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 security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about helping enterprises address their IT challenges.