StillSecure®

White paper

NETWORK CONVERGENCE:

THE UNIFIED NETWORK PLATFORM™

Prepared by:

Mitchell Ashley
CTO and General Manager
StillSecure®

February 2007

Table of Contents

About the author

Mitchell Ashley is Chief Technology Officer and General Manager of emerging products at StillSecure. Mr. Ashley is currently leading StillSecure's research into the convergence of networking, security and software technologies. As CTO Mr. Ashley is responsible for technology and advanced product strategies for StillSecure's industry leading and innovative network security products. Since co-founding the company Mitchell conceptualized and led the development of StillSecure's network access control, vulnerability management and convergence products.

Mr. Ashley is a 20 year industry veteran in networking, network security and product development serving as co-founder, EVP, CTO, CIO, VP Engineering and GM at various companies including StillSecure, Jato Communications, BoldTech Systems, US West, and EDS. He has also consulted to a number of Fortune 500 companies. During his career Mitchell led many pioneering projects including digital interactive media video-on-demand and shopping services, hybrid fiber/coax broadband network and set top box services, broadband business and consumer data services, early Internet applications and services, and numerous IT operational systems in the telecommunications and financial industries. Mitchell is an in demand speaker at industry conferences, panels, security organizations and podcasts. He is published in numerous online and print publications, a featured author in the upcoming book Growth Strategies for Software Companies and frequently quoted by the industry news media. Mitchell blogs about the latest trends in network, security and software convergence at http://theconvergingnetwork.com. He also co-hosts the highly subscribed podcast StillSecure, After All These Years available at http://www.clickcaster.com/ss. Mitchell can be contacted through his blog or at mashley@stillsecure.com.

Mr. Ashley is a graduate of the University of Nebraska, Kearney, with a Bachelor of Science in Computer Science and Business Administration.

INTRODUCTION

The convergence of networking technology and security technology is the next phase in the evolution of the network. It’s already taking place. Multi-function security and networking devices, such as unified threat managers (UTMs) and branch-office-in-a-box systems (BOBs) are becoming commonplace, replacing traditional routers, firewalls, and specialized appliances.

These multi-function devices are simply the first wave of the convergence movement. While they combine networking and security functions, they are locked into the old way of doing things; that is, they have all the disadvantages of the proprietary, fixed-appliance approach to building out the network.

The true maturation of convergence is the unified network platform™ (UNP). The UNP is the new paradigm for networking and security. Beyond today's multi-function devices, the UNP provides an open, modular, customizable, virtual, software-based platform for delivering core networking and security functions.

This paper examines the industry trends that have led to convergence and, more specifically, the unified network platform (see graphic, below). Theses trends include:

1. The development of devices that integrate networking and security
2. The viability of software-delivered solutions and the rise of open-source
3. Advances in the price, performance, scalability of general computing hardware (i.e., Intel and AMD-based systems), and the obsolescence of proprietary network hardware appliances

This paper concludes with an in-depth description of StillSecure's UNP product concept. The UNP paradigm integrates the benefits of the trends discussed in this paper to deliver a software-based modular platform for network and security functions. This platform operates on a single system that can be implemented on off-the-shelf (OTS) hardware.

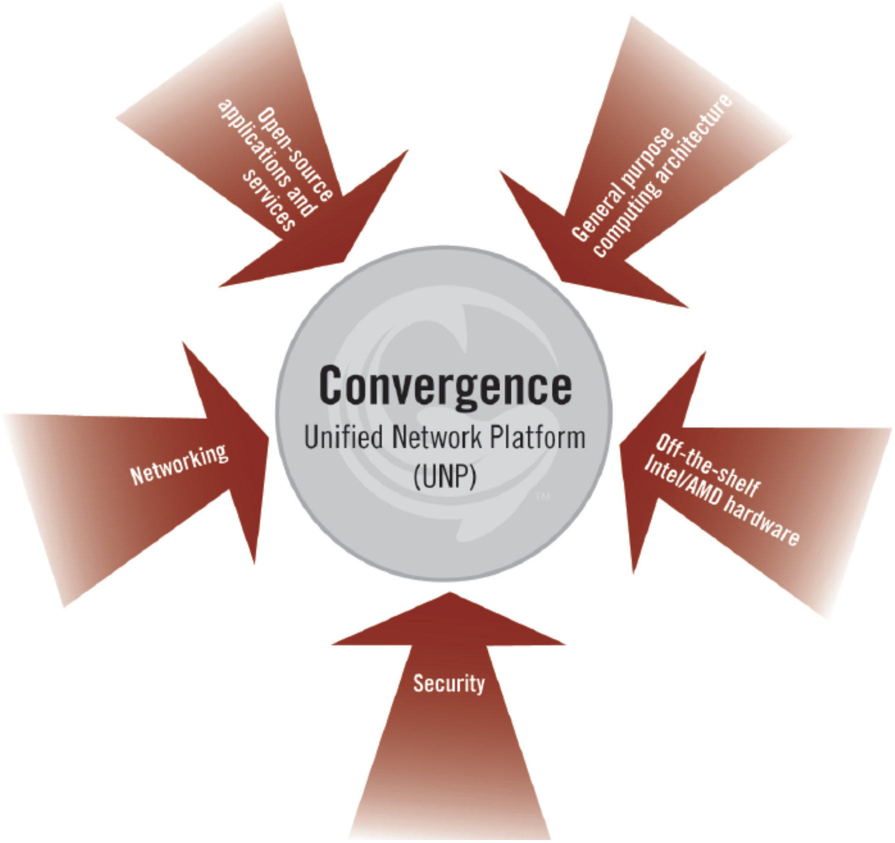
THE INTEGRATION OF SECURITY AND NETWORKING

A core component of the unified network platform concept is combining network and security functions in one product. The integration of these two once-separate disciplines has evolved in recent years and is now commonly available.

A few years ago, network security was viewed and treated as a specialized discipline and operation. Securing the network was accomplished utilizing standalone, specialized 'bump-in-the-wire' appliances to provide firewall, VPN, IDS/IPS, and many other security functions. With each additional appliance added to the network came additional overhead—more rack space, support and maintenance contracts, trained technicians and administrators, etc.

Security technologies were introduced into the network through specialized network security devices. As the application of these technologies matured, organizations learned how to deploy, configure, and manage them for maximum protection and efficiency. Everyone today understands that firewalls play an important role at the network perimeter, but now we frequently use firewalls inside the network and at remote offices to protect sensitive segments of the internal network.

Security applications have traditionally required a significant amount of computer power beyond what a typical router, switch, or other


Open-source applications and services
General purpose computing architecture
Convergence
Unified Network Platform (UNP)
Networking
Off-the-shelf Intel/AMD hardware
Security

network infrastructure device could accommodate. The additional resources required to inspect network packets for malicious traffic (as an IDS/IPS does) was beyond the design tolerances of then-current network equipment, requiring that these security functions be delivered on their own hardware, or as blades within switches and routers.

As network and security technologies matured, we began to see multi-function devices come to market. Today, firewall, VPN, IPS, AV, and many other network functions are delivered on one device. Some of the fastest growing industry security segments are Unified Threat Management (UTM) and Branch Office Boxes (BOB). Routers and switches have many of the same features embedded within them. It is commonplace to deploy network devices that provide all the network services (DNS, DHCP, routing, etc.) and security services (firewall, IPS, AV gateway, etc.) on vendor hardware appliances.

Current solutions utilize proprietary, specialized hardware appliances. Should history repeat itself, new security networking and security applications—likes UTMs and BOBs—will continue this cycle of standalone vendor appliances and specialized network hardware.

THE VIABILITY OF SOFTWARE-DELIVERED SOLUTIONS AND THE RISE OF OPEN-SOURCE

The unified network platform concept leverages the trend of delivering sophisticated network and security solutions as software. This is a major shift away from the proprietary, fixed-appliance approach that has always dominated the networking market. In the following paragraphs we examine how this came to be.

It is easy to slip into a “speeds and feeds” mentality when discussing the hardware features of network and security gear. The software component of these systems is often overlooked, yet it's software that makes it all happen. Innovation in networking and security software occurs within three domains: proprietary software, open-source software, and hybrids.

Within the context of network infrastructure, most of us are familiar with proprietary software operating environments, such as Cisco’s IOS and Juniper’s firewall/VPN ScreenOS. Proprietary software only operates on the vendor’s hardware, leaving organizations with the challenge of learning and supporting multiple technologies or standardizing on a single vendor, thereby limiting options when the time comes to expand or upgrade the network, or when hardware malfunctions.

Rarely is the software that powers these proprietary systems exposed or accessible to the customer. All configuration, upgrades, and expandability are limited to options provided by the vendor. Naturally they involve fees or new purchases. Implementation of new features may also require forklift upgrades (i.e., replacement) of proprietary vendor hardware due to insufficient memory and processor requirements, connectivity limitations, or end-of-life products.

The irony of this expensive status quo is that open-source software is the foundation of an increasing amount of network gear, particularly the recently introduced multi-function network and security appliances. Use of open-source is rarely exposed by the vendor to customers. This is understandable, as vendors seek to perpetuate the forklift upgrade and maintenance revenues they depend on.

But the story is bigger than proprietary appliances built using open-source components. Open-source software has revolutionized the way many networks are built, configured, and managed. The Linux operating system is the foundation for scores of network and security devices. The adoption of Linux for these purposes makes sense given its many network services and utilities, its broad base of support, and the vast number of software resources available. Many networks rely on Linux-based devices implemented on off-the-shelf (OTS) hardware. Homegrown OTS-hosted systems that include combinations of DNS, DHCP, firewall, VPN, traffic filtering, anti-virus gateway, email, file sharing, network monitoring, and other services are being deployed in production environments with increasing frequency.

Other open-source projects, such as snort.org, nagios.org, and nessus.org further exemplify the value open-source brings to networking and security. Entire vertical market segments have emerged from these technologies. The IDS/IPS and vulnerability management product verticals are prime examples. Many UTM, BOB, and even WiFi appliances rely on core open-source technologies. Even Cisco publicly disclosed its use of open source in a recent WiFi product, and has taken heat for not complying with the GPL license.

Network and security professionals have been quick to take advantage of the benefits open-source delivers:

1. **Control**—Open-source puts control back into the hands of the administrator. Linux and other open-source tools give admins powerful, accessible functionality.

2. **Transparency**—With open-source everything happening with in the device is visible and accessible. No proprietary vendor hooks or passwords block the administrator from accessing key information or understanding how the underlying system functions.

3. **Extensibility/expandability**—Open-source offers almost unlimited expandability. Additional functionality can be added just by installing or enabling existing software. OTS hardware can be easily expanded or resized to meet current and future needs.

In the past these benefits came at a price. They required that you have an administrator with solid working knowledge of Linux as it applies to networking and security. Currently, open-source network and security tools lack the structure and usability required for large-scale adoption at the corporate level—but that's changing. The unified network platform provides the structure and usability to bring these open-source-based systems into widespread use.

GENERAL COMPUTING HARDWARE

Thanks to open-source software such as Linux, general purpose Intel, and AMD-based hardware has demonstrated its viability as a networking and security platform. Generically referred to as general purpose computing architectures (GPCA), Intel and AMD-based hardware is now hosting many vendor appliances and network blades. The unified network platform concept also takes advantage of the outstanding performance available in off-the-shelf GPCA devices.

Let's take a look at why GPCA-based systems now compete successfully with fixed-appliances. First, manufacturing advances have led to further microprocessor miniaturization. Current chip fabrication is state-of-the-art 65-nanometer (nm), high-volume semiconductor manufacturing. This has led to the revolution of multi-core processing: multiple CPUs on a single processor chip. Working 45nm chips are due in 2007, first appearing in SRAM memory, with half the memory cell size of 65nm technology.

Multi-core processing significantly improves the handling of network traffic. Other advances such as increased cache sizes and virtualization allow GPCAs to perform many network, security, and application functions in parallel at much faster speeds. Hardware bus advances such as those offered through PCI-Express improve data path throughput between processors, memory, and applications. High-speed communications can now be supported on a wide range of GPCA hardware. Consider that today's OTS systems offer bus speeds in the 1300 Mhz range and that a PCI-Express bus can handle 8GB of bandwidth.

GPCAs are changing the networking and security landscape. The proprietary appliance paradigm is no longer the only game in town. When network and security appliances performed a single or limited number of functions, hardware could be tailored to meet that specific feature set. As networking and security features are added to these appliances, reliance on special purpose hardware becomes unnecessary. While proprietary hardware simplifies the acquisition process, GPCA hardware gives customers the freedom and flexibility they need to cost-effectively deploy multi-purpose devises using off-the-shelf (OTS) machines.

Using GPCA systems has additional benefits and efficiencies built in. Support, for example, is readily available. GPCA manufacturers such as Dell, IBM, HP, etc. have extensive and highly responsive support organizations. Additionally, it is common for both large and small business to have established relationships with one or more of these vendors, so the purchase of additional hardware occurs through a routine process.

The ingredients for the next-generation network device are in place: integrated security, the open-source software model, and GPCA hardware. Networking and open-source enthusiasts are typically the ones with the skills and inclination to create the systems that leverage these. Maybe you have somebody like that in your network group. But the build-it-from-scratch development model isn't sustainable or scalable. What's missing is a model that brings these into a unified paradigm; a platform of networking, security, extensible and transparent software, and expandable, scaleable, cost-effective hardware.

What's missing, in short, is the concept of a unified network platform.

INTRODUCING THE UNIFIED NETWORK PLATFORM

The Unified Network Platform, or UNP, is an open platform architecture that enables the convergence of network applications including:

- Data networking
- Security
- Network infrastructure
- Network applications
- Network management

StillSecure® is developing the UNP product concept with the intent of releasing a first-generation UNP product in 2007.

The UNP delivers core network functions via a foundation of open-source software and general purpose Intel/AMD computing hardware. With this foundation, the UNP offers full flexibility, transparency, scalability, and expandability.

The StillSecure UNP product concept comprises layers of software components, called modules, operating on a substrate of a hardened Linux operating system running on general purpose Intel/AMD-based hardware, illustrated in the figure on page 5. Rather than relying on traditional proprietary hardware/software appliance structure, the UNP allows the administrator to select the appropriate network and security applications that run on each device. Rather than the “least common denominator” approach of combo network appliance solutions, the UNP gives the administrator the ability to choose the best solutions to operate on each UNP device within the network. Through this flexible approach, administrators can change, remove, or migrate various network and security functions between UNP devices to meet new business demands or changing network architectures.

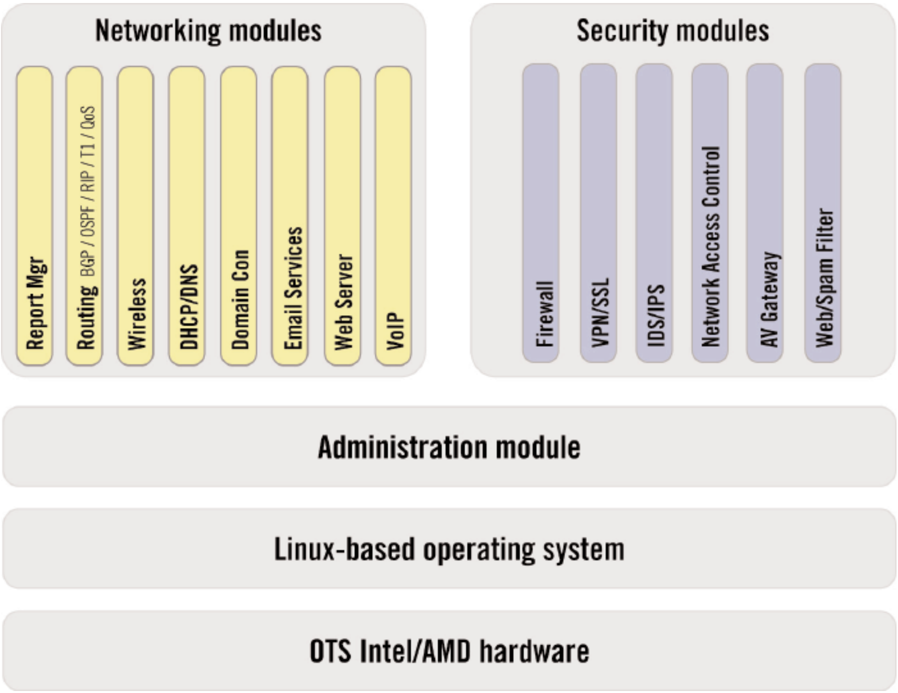
UNP utilizes a plug-n-play modular software architecture. Rather than being limited to the fixed set of options available in typical network appliances, UNP modules are installed, upgraded, or uninstalled at the discretion of the network administrator. UNP modules provide core networking functions, such as:

- Routing
- DNS
- DHCP
- WiFi
- Other network services.

Security functions are also available through modules:

- Firewall
- VPN
- IDS/IPS
- Antivirus gateway
- Additional security functions.

The true power of UNP lies in its expandability of both software and hardware. First, the UNP is an open platform, the core of which is a software framework for implementing, operating and managing network and security applications. This framework supports the services required of any UNP-compatible module. Since the UNP platform is open, administrators have full access to



adapt, customize, and expand UNP to include the network, security, and applications services needed.

UNP modules can be sourced through a variety of means. A large body of open-source software is available today which can easily be adapted to UNP. Vendors already leveraging Linux can adapt proprietary product to operate on the UNP's open software framework. Individuals can extend UNP through their own installation and customization of software.

Through this modular software architecture, any number of additional applications can be supported such as voice-over-IP (VoIP), email, file-sharing, printing, and Windows domain services. As new demands for network and security/applications occur, additional UNP modules can emerge to satisfy these needs.

Since UNP operates on GPCA technology, hardware is readily available. Rather than suffering the woes of over saturated appliances breaking under performance demands of running multiple network and security services, OTS hardware can be easily installed and upgraded. Cost-effective hardware can now replace costly proprietary hardware to increase the number of applications, improve performance capacity, and network throughput, or to take advantage of the latest hardware improvements and cost efficiencies. As mentioned above, GPCA hardware brings with it a high level of support from well established, global manufacturers.

The UNP operates on a pre-hardened Linux operating system. This provides an open foundation to customize network and security services, or add new networking and security functions. Network administrators can now take advantage of the wide range of network and security open-source solutions available and be assured of the stability and security of underlying UNP OS. This also removes the burden of setup and configuration traditionally experienced with 'build-it-from-scratch' Linux networking devices that administrators patched together in the past.

The UNP product concept can take advantage of virtual operating environments such as VMware or open-source Xen software. UNP operates on any platform that supports virtualization software. This means that dedicated hardware is no longer required in every case, and the network can be more flexibly configured or reconfigured to meet changing needs and network architectures. Simulating network configurations with limited hardware can easily be accomplished. New networks can be constructed immediately by virtualizing the network on one or more GPCA devices.

CONCLUSION

The unified network platform presents a new paradigm for addressing the needs of network and security functions. Breaking the mold of the proprietary vendor hardware appliance solutions, UNP provides an open platform architecture consisting of open software and general purpose hardware, enabling the convergence of network applications. Through the use of UNP, organizations can design, build, manage, and maintain secure networks without the limitations and expense of vendor proprietary hardware and software.