WHITE
PAPER

3-D Network Security

By Jon Oltsik

February, 2008

Table of Contents

Table of Contents ..... **i**
Executive Summary **1**
The Network in Transition **1**
Network Security Remains an Achilles Heel **2**
What about UTMs? 5
What's Needed? 3-D Network Security **6**
The 3-D Network Security Era Begins! 8
The Bottom Line **9**

Executive Summary

Sun Microsystems used to claim that "the network is the computer." This turned out to be a rather prescient but incomplete statement. With the increasing intersection between business processes and the Internet, the network is now the business.

Network-based business processes place increased importance and urgency on network security as more users, applications, and transactions crisscross over global pipes and private networks. Alarmingly, many large organizations are ill-equipped in this area. This white paper concludes:

- **Security coverage and sophistication remains lacking.** While networking and security attacks become more and more complex, many large companies still rely on old-standby security technologies like basic firewalls, IDSs, and gateway appliances. These systems lack network context – they see basic Layer 2-4 information and known attacks, but they don't inspect each packet or offer granular policy-based security enforcement.

- **Unified Threat Management devices provide little relief.** UTM systems aggregate security applications in a single box and may ease management but they are notoriously slow and lack integration into the network itself. This makes most UTMs a marginal improvement over existing tactical network security, point tools, and appliances.

- **Large organizations need 3-D network security.** ESG believes that the time is right for a new model it calls 3-D network security that combine broad security functionality and networking integration with massive scale and performance. While this type of "God box" was impossible in the past, it is now achievable to build a 3-D network security system because of recent improvements in microprocessors, IT economics, and development skills. As such, ESG believes that 3-D network security systems will become an enterprise staple over the next few years.

The Network in Transition

Global economic factors and new technologies are having a profound impact on large organizations. Enterprises distribute employees and business processes around the world to capitalize on new types of skill sets and lower labor costs. Companies share information in order to improve productivity and time-to-market. Firms outsource entire business functions like call center operations or manufacturing to global specialists in order to focus on core competencies. To meet these new business challenges, IT is taking advantage of technologies like Web services, SOA, and IP telephony and building dynamic communications-oriented applications in rapid fashion.

These business trends have a profound impact on corporate networks. Legacy 3-tiered LANs and remote WANs were never designed for today's demands for open perpetual communication. As a result, networks are in a massive state of transition. To service the business, networks must adhere to an architecture highlighted by:

- **Higher bandwidth demands.** Enterprise network backbones are rapidly moving from gigabit to 10 gigabit Ethernet while gigabit to the desktop becomes more pervasive. In terms of external connections, large organizations are eschewing fixed T1s and T3s in favor of fat Ethernet pipes or optical networks offering bandwidth on demand for inevitable traffic spikes.

- **Virtual connectivity.** Leased lines and dedicated circuits are giving way to a more virtual model that regularly cuts across public networks. Business partners communicate over the public Internet, home workers log on via IPSec and SSL VPNs, and remote offices are connected using MPLS through service provider clouds. Indeed, enterprise networks are taking on characteristics of the public Internet such as spiky traffic, multiple types of traffic and anonymous user access.

- **Massive mobility.** Devices are no longer tethered by wires and fixed connections. More than half of all business PCs sold are laptops with on-board wireless connectivity while smart phone and handheld device sales grew more than 20% in 2007. Multiple industry forecasts predict that there will be over 15 billion devices on-line by 2012. The inevitable result will be an ever-growing pool of mobile users and more IP devices on the network.

- **Network convergence.** The implementation may be a bit rocky but ultimately voice, video, data, and storage traffic will constantly traverse common IP pipes. As traffic increases over the next few years, large organizations will begin to re-architect their legacy 3-tiered networks into an intelligent end-to-end mesh based upon 10 gigabit Ethernet routing switches and edge devices built for intelligence and mobility.

- **Higher layer networking requirements.** The data link and network layers of the OSI stack continue to serve as a foundation but there is a rapidly growing amount of intelligence needed to support Layers 4-7 activities like load balancing, QoS, security, and network-based business logic.

What does this mean for enterprise organizations? Network modernization is not an option. To attract top talent, out-maneuver the competition, and maximize productivity, networks must grow ever-more scalable, customizable and easily adaptable for dynamic business requirements.

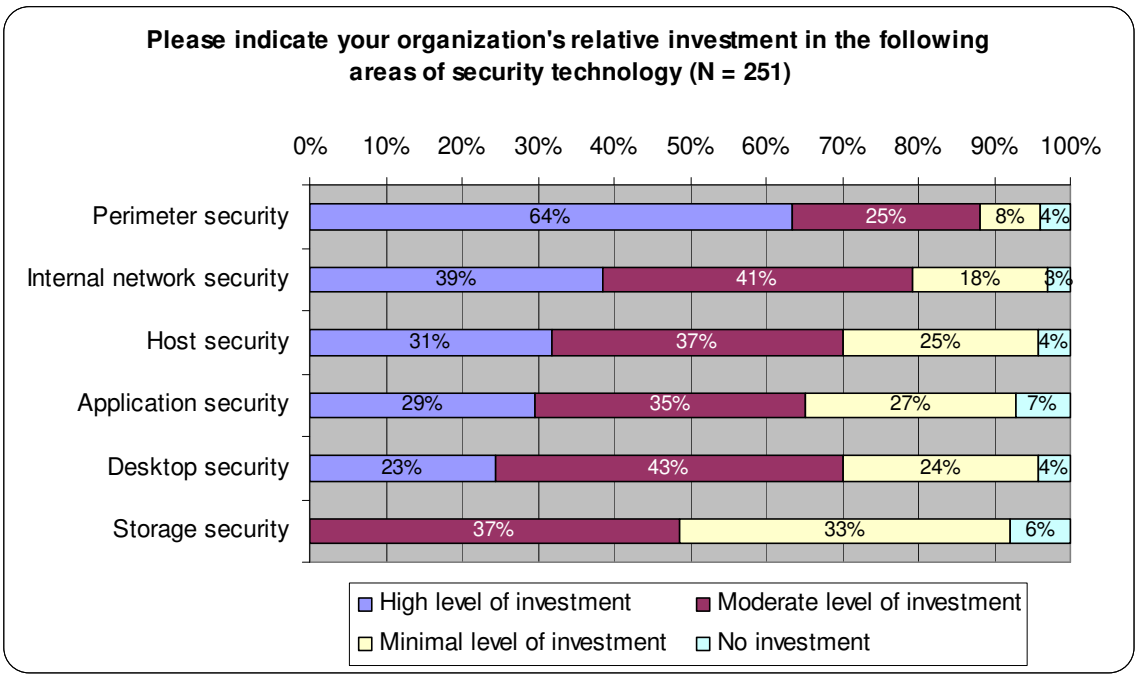
Network Security Remains an Achilles Heel

Two things about the network are certain: 1) The network must change to meet new business requirements and 2) Network security is far behind where it needs to be in order to support this transition. Why is there a security gap? Historically, network security was based on a series of individual point tools and filtering devices focused on the network perimeter. This equipment does an adequate job of blocking basic network attacks but does not provide an adequate amount of integration, intelligence, or policy enforcement.

These glaring weaknesses are illustrated in the data gathered in a number of ESG Research Reports. In multiple surveys of security professionals, ESG learned that:

- **Security investment remains fixed to the network perimeter.** In an era of pervasive network services, external users and mobile employees, security defenses remain anchored to the network perimeter. ESG Research indicates that the majority of security professionals believe that their organizations have a high level of investment in perimeter security while nearly 60% characterize their investment in internal network security as “moderate” or “minimal.” Alarmingly, less than one-third of organizations had a high level of investment in application security (see A.Figure 1).

FIGURE 1. SECURITY INVESTMENT IS FOCUSED ON THE NETWORK PERIMETER

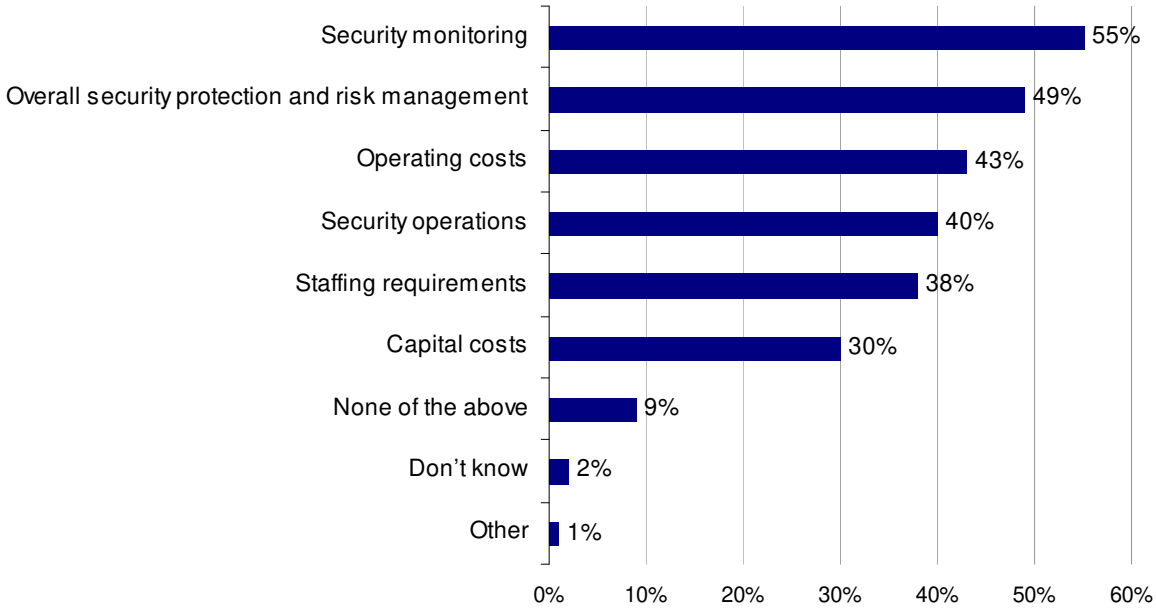


Source: Enterprise Strategy Group, 2007

- **"Best of breed" solutions resulted in lots of complexity and overhead.** Since network security was built organically over time as new threats arose, many companies emphasized "best of breed" security functionality over integrated solutions. This "point tools-centric" network security led to predictable operating problems around processes and staff and also adversely impacted security monitoring and overall security protection and risk management (see Figure 2). This is a real issue in an era highlighted by increasing volume and sophistication of network security attacks.

FIGURE 2. . ADVERSE EFFECTS OF LIMITED SECURITY MANAGEMENT TECHNOLOGY INTEGRATION

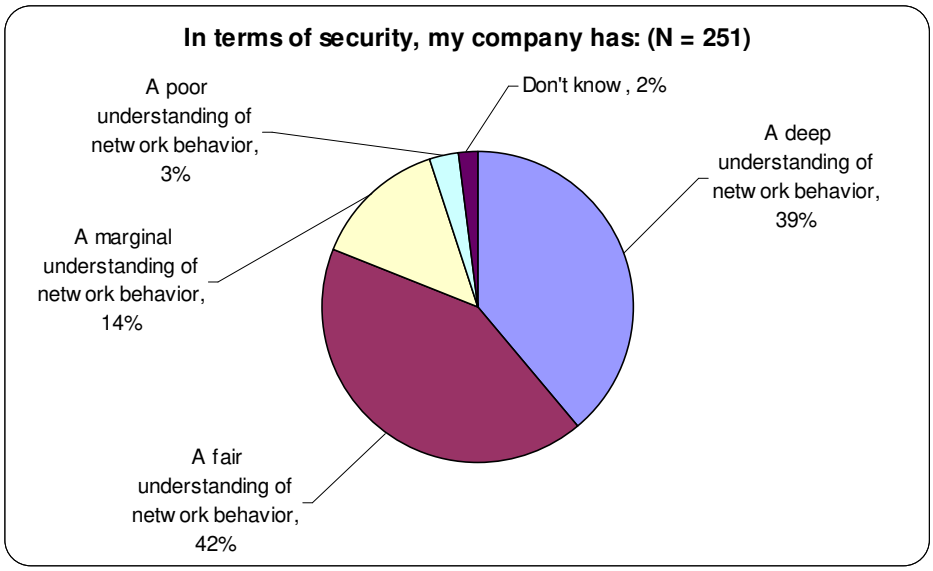
In your organization, which of the following areas do you believe are adversely impacted by limited security management technology integration? (Percent of respondents, N = 207, multiple responses accepted)



Source: Enterprise Strategy Group, 2007

- **Network sophistication is a mismatch for security skills and safeguards.** When it comes to security, understanding network applications and flow is essential. Why? A pronounced spike in traffic over UDP port 1434 may indicate the next incarnation of SQL Slammer while a malformed HTTP request could represent a SQL injection attack. While this information can be critical, many organizations maintain separate networking and security groups that haven't adequately integrated their organizations, skills, or technologies. Little wonder then that so many security professionals admit that their organizations simply don't have the right skills to understand and analyze network behavior as it relates to security (see Figure 3).

FIGURE 3. ADVERSE EFFECTS OF LIMITED SECURITY MANAGEMENT TECHNOLOGY INTEGRATION



Source: Enterprise Strategy Group, 2007

Aside from these deficiencies, some existing network security technologies just haven't kept up. Many firewalls are configured to inspect packet headers but ignore payloads that could contain malicious code or confidential data. IDS/IPS systems react to known attacks but may be useless against zero-day or tunneled exploits. Traditional network security defenses also tend to ignore everything above Layer 4 of the OSI stack placing applications in harms way. This level of risk is bound to impact the business, thus it is simply unacceptable.

What about UTMs?

The need for new network security defenses and tighter integration has not gone unnoticed by the security industry. In an attempt to simplify network security for customers, many vendors now offer Unified Threat Management (UTM) devices that combine multiple network security technologies in a single chassis or appliance and wrap all security applications with a common management interface. This is certainly a step in the right direction, but most UTM offerings are insufficient because they lack:

- **True network integration.** Regardless of the packaging, most UTM devices act as "pass through" boxes on the network that examine packets upon network ingress and egress. Customers still need to process packets for networking decisions so they supplement UTMs with an infrastructure consisting of switches, routers, and wireless access points adding cost and complexity to network operations and security.

- **Performance headroom.** Many UTMs become a network bottleneck when on-box security functions such as firewall, IDS/IPS, and gateway antivirus, are run simultaneously. It is not unusual to see UTM systems that advertise "gigabit speed" performance reduce actual throughput to a few hundred megabits. Too often, network security administrators are forced to "dial down" protection features in order to meet service level requirements – a Faustian technology compromise that favors performance over protection.

- **Application knowledge.** A good number of UTMs don't know much about the network other than IP addresses, ports, and protocols. These systems can't look "up the stack" in order to prevent application layer attacks or guard against data leakage. The problem here is that in most organizations, these

defenses have moved from "nice to have" and become absolute requirements.

Most UTMs are also a mismatch for today's dynamic networking needs. To balance security and networking requirements, organizations may want to base network security rules based upon user identity, application type, or network location. Hard-and-fast security locks no longer apply; today's defenses must be tightly linked to business policies and network throughput requirements.

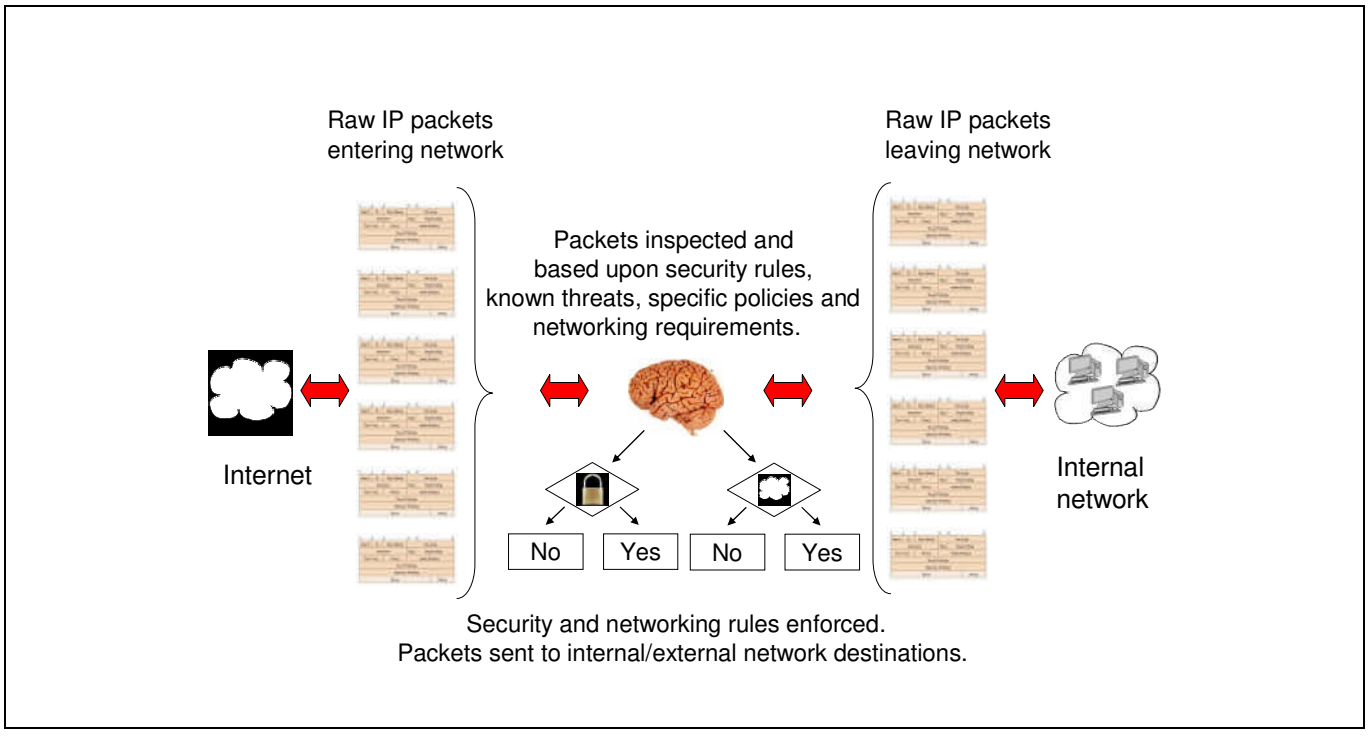
What's needed? 3-D Network Security

Network security isn't magic; it is simply a matter of examining each IP packet and then making a series of decisions based upon risk tolerance. For example, before sending an external user to the web server, each packet should proceed through security and asked a series of questions such as:

- Is the source IP address real? Is it from an acceptable source?
- Is this really HTTP traffic or is there something tunneled inside?
- Does the payload contain known malicious code?
- Does the HTTP protocol conform to acceptable standards?
- Is there something suspicious about the traffic pattern?
- Does this activity conform to security policy?

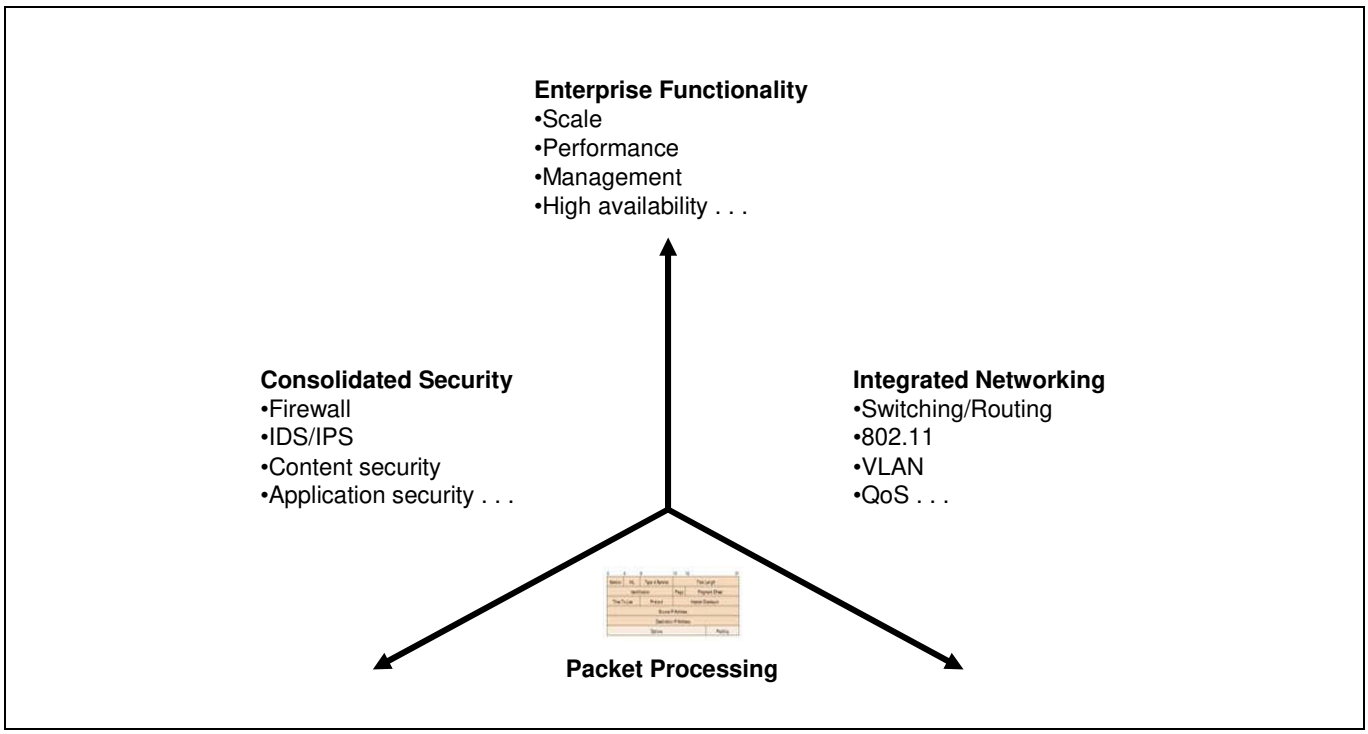
As these questions are answered, the network security system can make decisions based upon based upon security rules, known threats, and specific policies. Packet processing isn't just limited to security enforcement however, networking activities such as routing, switching, and QoS are also based upon the network's ability to scrutinize packets and take appropriate actions (see Figure 4).

FIGURE 4. PACKET PROCESSING MODEL FOR SECURITY AND NETWORKING



ESG believes that increasing network sophistication combined with growing security threats is driving a new model called "3-D network security" (see Figure 5). Unlike monolithic network security add-ons of the past, 3-D network security uses deep packet processing as the foundation for aggregating the enforcement of networking and security rules. The three dimensions of 3-D network security include:

FIGURE 5. THE ESG 3-D NETWORK SECURITY MODEL BASED UPON PACKET PROCESSING



- **Consolidated security functionality.** Like a UTM, 3-D network security must include stateful firewall, signature-based IDS/IPS, gateway filtering (i.e. anti-virus, anti-spyware, etc.), and VPN functionality but 3-D security builds in additional protection from there. Once each packet is "cracked," the 3-D network security model also can provide for content security such as URL filtering, Data Loss Prevention (DLP) and application security. The real benefit provided by 3-D network security is fine-grained security enforcement. Rather than binary "allow/disallow" security enforcement, 3-D network security can enforce multiple rules with multiple enforcement responses. A purchasing manager may gain full access to financial systems from his office but not from the local Starbuck's. Users may be allowed to IM with outsiders, but bandwidth for this application will be given a low priority. A DOS attack that would normally gain access to the web server over open Port 80 can be blocked at the network perimeter.

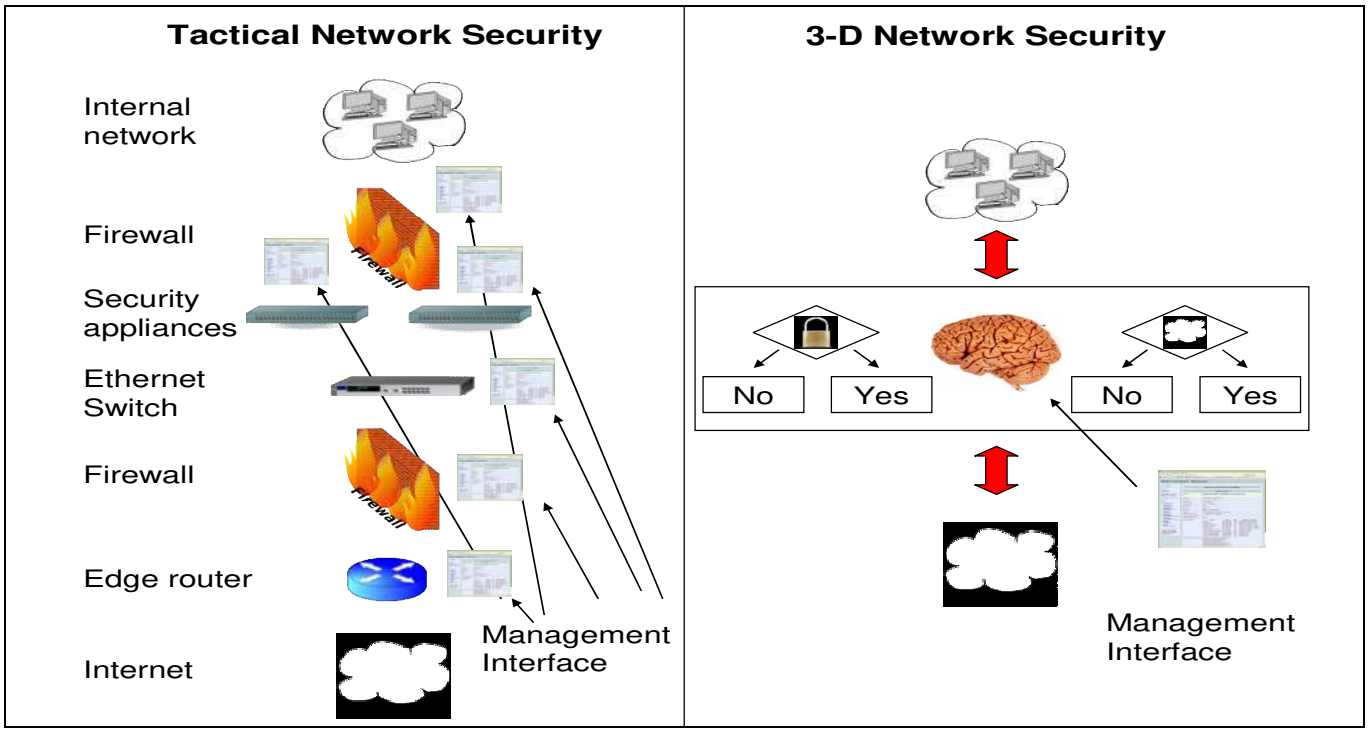
- **Networking integration.** To optimize packet processing and simplify network architectures, the ESG model marries critical elements of networking and security into integrated packages. As such, 3-D security must offer basic routing (OSPF, RIP, multicasting, etc.) and switching (VLAN, QoS) wireless (802.11 a, b, g, and n) and other networking capabilities (i.e. NAT, traffic shaping, load balancing, etc.). The goal here is not to replace existing infrastructure but to integrate functionality where it can simplify the network, avert complexity, or lower cost. For example, a 3-D network security device could obviate the need for a separate edge router or DMZ switch while a branch office could use an integrated wireless Access Point (AP) precluding the need for additional equipment.

- **Unprecedented enterprise features and functions.** Aggregating all of this security and networking goodness demands plenty of uptime, scale, performance and management. First off, this means real "wire speed" performance where packet processing doesn't interfere with network throughput. This

requires lots of multi-core and specialized processing engines. Second, 3-D network security systems must be built for high availability calling for redundant everything (i.e. fans, power supplies, failover clusters). Finally, 3-D network security devices must support stateful load balancing in a grid architecture for overall scalability and "five 9s" availability.

With the ESG model, network security is turned on its head (see Figure 6). Today, packets are detoured through multiple security boxes looking for individual threats or policy violations. Typically, each of these security systems has its own element management system requiring security administrator time and attention as well. With 3-D security, packets: 1) Flow through a single or set of networking/security systems, 2) Get a complete examination based upon security threats and policies, and 3) Are acted upon accordingly. Additionally, 3-D network security is based upon centralized management. The benefits here are obvious: Higher network throughput, improved security, and streamlined operations – all at a lower cost.

FIGURE 6. 3-D NETWORK SECURITY COMPARED TO TODAY'S TACTICAL MODEL



The 3-D Network Security Era Begins!

Historically, users may have dismissed concepts such as 3-D network security claiming that it would be impossible to pack the necessary horsepower needed into a single box. Yes, in the past this was in fact true leading to an avalanche of fixed-function security appliances and the subsequent operations challenges. More recently however, 3-D network security has started to become a reality because of:

- **New processing capabilities.** Today's lightning fast multi-core processors can now emulate the work that used to require multiple physical processors or individual systems. Multi-core processors also enable a new kind of system flexibility. Groups of cores can be dedicated for system-level activities or designated for applications. Processing loads can be balanced across multiple cores based upon queues, policies, or processing algorithms. This scale will only increase as the number of cores per processor increases while processor speeds follow Moore's law with enhanced performance as part of each new product cycle. .

- **Low cost networking hardware.** Now that the world's communication flows over IP pipes, the cost of basic networking hardware like Ethernet ports, network service processors, and 802.11 chips continue to decrease rapidly. Given this decline, 3-D network security vendors can design multi-function systems without betting the company on R&D while users can consume multi-function small form factor devices at an affordable price. .

- **Advanced operating systems.** 3-D network security devices take advantage of years of network device operating system experience combined with a growing global development community. Today's operating systems include features once confined to supercomputing such as guaranteed resource availability (i.e. memory space and processing cycles), shared libraries, and parallel processing.

Several vendors offer first-generation 3-D network security devices today and continue to make great progress in fulfilling the ESG vision. One vendor that stands out from the pack is SonicWall. Mostly known for its mid-market products, SonicWall recently introduced its new E-Class Network Security Appliances (NSAs) which provide the company with a 3-D network security device it can bring to enterprise customers. The SonicWall E-Class NSA combines the hardware horsepower of multi-core processors with deep packet inspection and integrated networking functionality. Like the ESG 3-D network security model, this means that the E-Class NSA can process and inspect packets and then make security and networking enforcement decisions from a single device. While this in itself is noteworthy, the E-Class NSA most attractive feature may be its overall ease-of-use. SonicWall's heritage with smaller customers has taught the company how to simplify security management without sacrificing advanced functionality. This experience will be welcome by over extended enterprise CISOs looking to improve security without hiring an army of MIT network engineers.

The Bottom Line

CISOs must constantly deal with business and security issues including from security threats to compliance mandates, to asset amortization and replacement. Security threats and technologies become more complex each day yet somehow security managers must meet security challenges AND simplify operations, and reduce costs. 3-D network security has the potential do deliver in all of these areas.

ESG believes that 3-D network security is available today so there is no time to waste. Large organizations should prepare for 3-D network security with a pragmatic and effective plan of attack including:

- **Assessing current and future risk.** This should include both business and IT risk. In other words, assess if there are any impending initiatives or applications that include the need for things like remote network access, mobile devices, regulatory compliance controls, and new protocols, and compare this list with existing network security risks. With this information in hand, IT managers can prioritize areas where network security issue could have dramatic implications on the business.

- **Assess the network architecture.** Most modern networks have too many underutilized devices that require an army of administrators, software licenses, and service contracts. Ask your network engineers to provide a "blue sky" network concept that would greatly simplify the overall design. Use this as a template for assessing where 3-D network security systems could replace numerous others.

- **Examining security operations.** Ditto for security operations. How many IT staff members are dedicated to security operations? Is this number growing and if so, by how many? How do these folks coordinate their activities? Does the current security operating processes and procedures impact emergency response? The answers to these questions will tell you: 1) Where you need to simplify security operations and 2) Some possible benefits of doing so.

Once these activities are completed, it ought to be fairly clear where 3-D network security makes immediate sense. This background can then serve as the foundation to justify expenses, plan projects, and begin conversations with leading 3-D network security specialists like SonicWall.

20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com