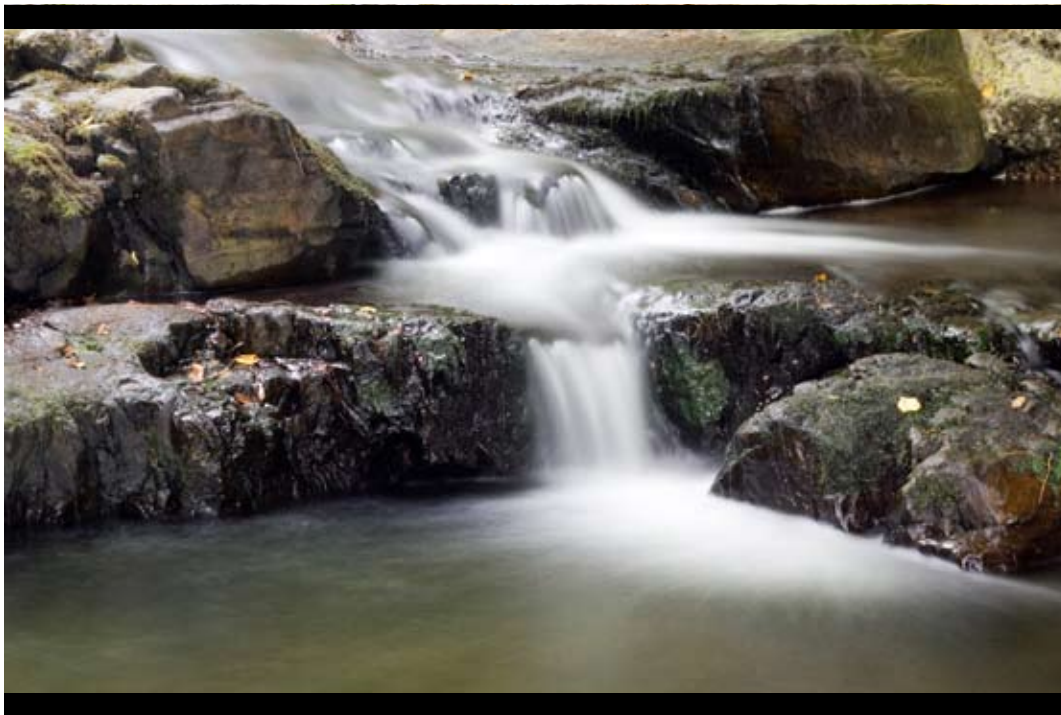


WHITE PAPER

Security Virtualization: Re-architecting the Appliance Mentality



Introduction

Undoubtedly, one of the hottest trends in IT today is the notion of virtualization. As Wikipedia defines it, virtualization is:

a technique for hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources. This includes making a single physical resource (such as a server, an operating system, an application, or storage device) appear to function as multiple logical resources; or it can include making multiple physical resources (such as storage devices or servers) appear as a single logical resource.

The promise of virtualization delivers some obvious benefits:

- higher resource utilization via device consolidation
- cost reduction associated with infrastructure consolidation
- improved scaling and operational flexibility
- improvements in operational uptime and business continuity

The obvious question that arises for many security and IT professionals is: can the benefits of consolidation and virtualization be achieved with respect to the delivery of security services?

Security Services Virtualization: What is Required?

In order to determine what “security virtualization” really means, it is useful to understand how companies define and enforce their security and accompanying compliance policies today. In defining a security policy, companies must identify what it is that they want to protect. Some assets and communications are more important than others. For example, a set of print servers on one segment of the network may not require stringent security protections; however, when data is extracted from a finance database, a much stricter set of conditions is likely to apply. Thus, the security policy becomes the set of business rules by which processes, people and technology are applied to affect asset protection goals.

To implement the processes and technology required to affect their security policies, most companies today deploy special purpose appliances running a host of security applications, from firewalls and content gateways to intrusion prevention devices and URL filters. To connect this plethora of appliances, enterprises are further required to deploy additional switching equipment and patch cabling to connect the appliances, along with load balancers to evenly distribute network traffic to the appliances. The typical “throw another box at it” architecture is commonly referred to as “appliance sprawl” (see Figure 1).

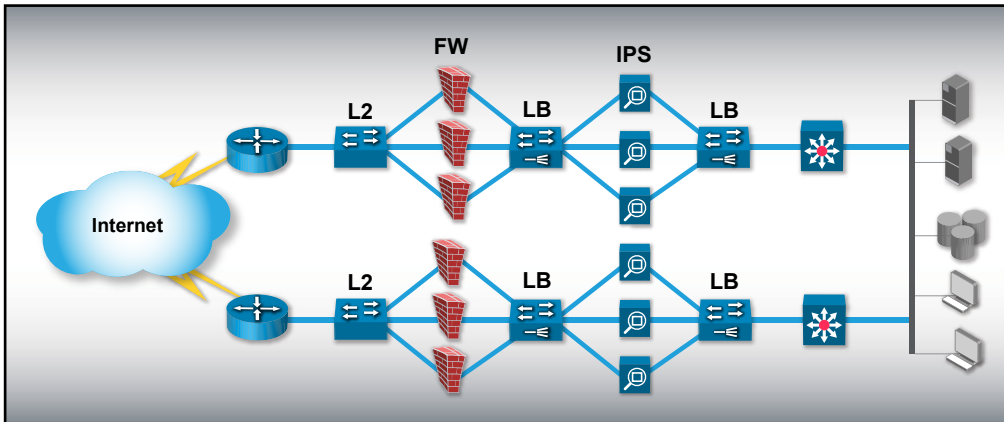


Figure 1 – Appliance Sprawl

In order to “virtualize” security services, the technology implementation must fully address the appliance sprawl issues. And it must do it in way that does not require changes to the security policies. More specifically, consolidation and virtualization of security services requires:

Application virtualization – The notion of virtualization of applications software is an increasing priority as IT organization try to efficiently take advantage of computing resources and so-called application blade servers. As applied to security, vendors of security appliances must figure out how to virtualize an application instance (e.g., a firewall) and apply it on-demand to a blade. This provides a first and significant step because it treats a set of blades as a pool of resources that can be profiled at will, according to capacity needs. However, a major obstacle for security appliance vendors exists: how do they ensure that applications running on virtual machines in one device sequence communications, consistent with the company security policy, with applications running on other virtual machines or other physical devices in the network. Furthermore, how do they prevent communications bottlenecks that could result from network-intensive applications like security? That’s where the next element of “security services virtualization” comes in.

Network virtualization – Most IT organizations today use network architecture as a way of enforcing security policies by deploying different security devices in different network segment or “zones.” The development of “zoning” or quarantined defenses has broken the traditional notion of “inside and outside.” Zones are areas whose boundaries are determined by some sort of firewall or intrusion prevention device and have become essential limiters of malware outbreaks. In a zoning model, one zone’s inside is another zone’s outside, even within a common building or organization. Yet trying to create zones based on geographic or wiring closet locations is very expensive and extraordinarily difficult to troubleshoot. Thus, in order to virtualize security services, a key element is the ability to virtualize the network switching fabric in a

way that facilitates “zoning” and simplifies deployment, all without compromising performance, architecture preferences or company security policies.

Control virtualization and policy implementation – Finally, the last critical element to enable security virtualization is the creation of a virtual representation of the appliance or chassis. The virtual chassis must control which services will run on which blades and how policy selection is governed and implemented. Additionally, the virtual chassis and its components must govern failover policies, service priority and service pre-emption rights. For example, the capability for a firewall service, on blade failure, to automatically “borrow” processing resources from a lower priority service must exist.

Today’s Daunting Security Challenge

Securing the corporate network used to be a fairly straightforward task. In the early 1990s, you would implement some access control lists (ACLs) on a router and you were set. As we all know, the days of straightforward security are gone.

As the advent of the Internet began, the need to block outside attacks ensued – enter the firewall. To add another layer of security, companies began to “zone” their network architecture with solutions like the “DMZ” where some or all traffic would be separated on an isolated network segment. Then, as companies wanted to leverage the Internet for remote users to get access to the corporate data center, virtual private network technology was added. Soon thereafter, the need for devices that scanned for so-called malware (Trojans, viruses, etc.) were required. As a result, physical devices/appliances started to literally “rack” up in the data center (see Figure 2)

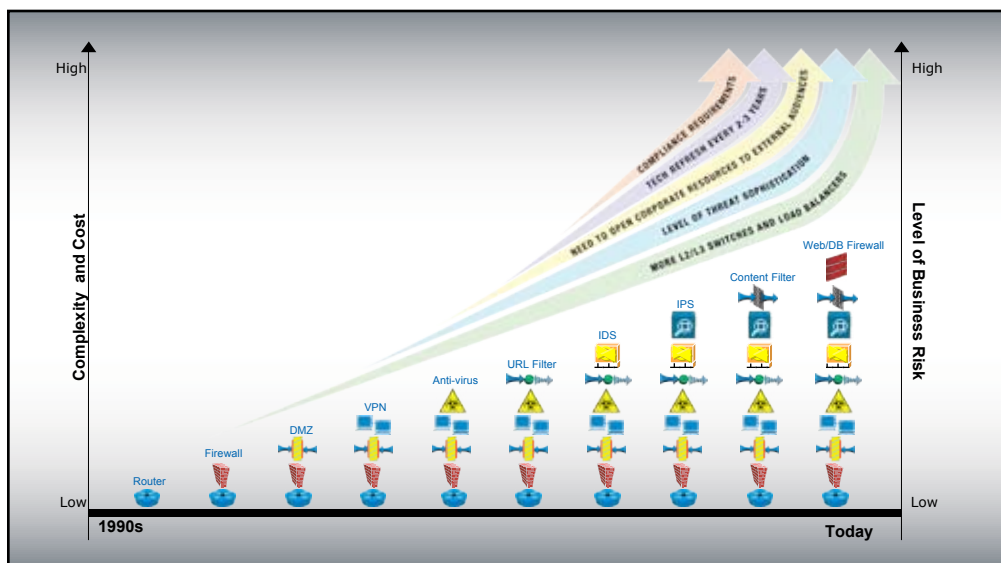


Figure 2 – The Daunting Security Challenge

As security threats were clearly starting to grow exponentially, it became clear that (best intentions aside) breaches were happening, and as a result companies started to deploy devices that provided alerts when a breach was detected – enter the intrusion detection system (IDS) – that’s right, another special purpose security box. The next step in the IDS evolution (and yet another appliance) came when companies not only wanted to detect intrusions, they wanted a device to act on them in real time. So the intrusion prevention system (IPS) was born. More recently, content gateways and filters were deployed as yet another special purpose security box to scan message and Web content for malware. Next on the list of appliance additions are Web and database firewalls that do deep packet inspection of database requests that might otherwise look harmless. In order to connect all of these devices and effectively segment network traffic, network administrators are required add more switches, more load balancers, lots on patch cabling and more data center floor space!

You can bet that the need for more of these special purpose security devices is NOT going to dissipate any time soon. Why?

- (1) The level of sophistication of those initiating the attacks is exploding – new threats are growing daily (see Figures 3 and 4).
- (2) As companies try to lock down their resources, the need to communicate with external constituents (e.g., partners, customers, suppliers, etc.) grows.
- (3) As network traffic grows and threats become more sophisticated, appliances “run out of computing gas” and need to be replaced, often before they have been fully capitalized.
- (4) And if that weren’t enough, regulatory and compliance requirements not only make the cost and complexity of security service deployments untenable, they elevate the business risks associated with the “let’s throw another box at the problem” mentality.

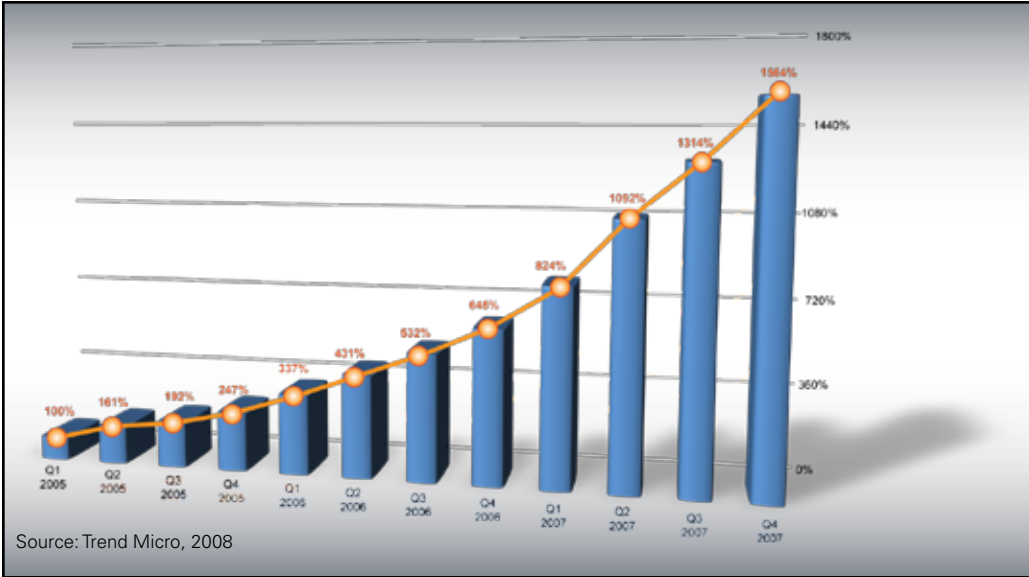


Figure 3 – Web Threats: Total Growth of Newly Created Web Threats Since 2005

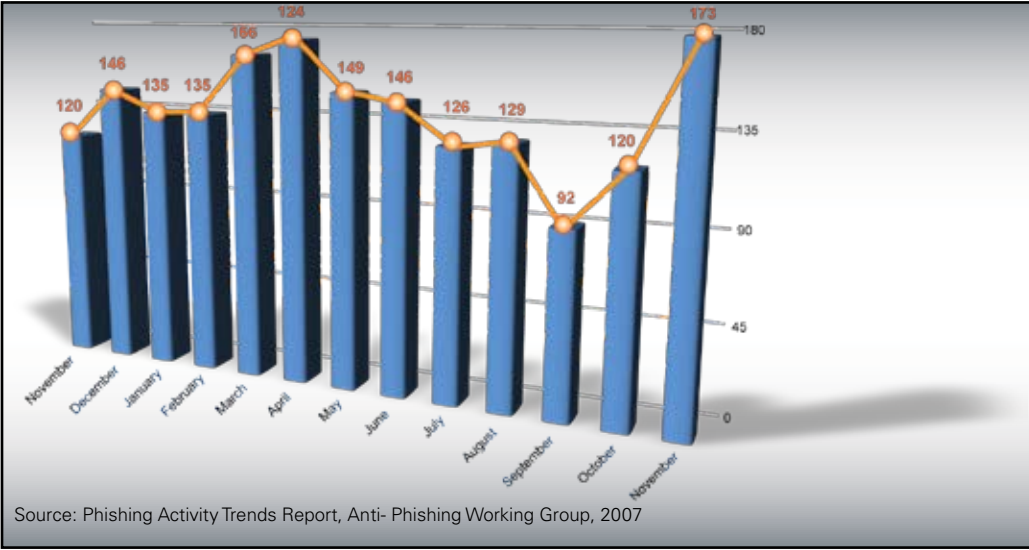


Figure 4 – Phishing Attacks in 2007

As a result, it is increasingly difficult for companies to:

- Implement and track business processes and controls that eliminate risk
- Decrease “time to compliance”
- Preserve the integrity of corporate assets
- Instill confidence and trust among customers, employees and shareholders
- Maintain and enhance corporate brand/reputation

So how have security vendors responded to this daunting challenge?

Today's Security Solution: How About Another Box?

The security vendors' response to the growing threat challenges is essentially, "Have I got a box for you, and by the way, you are going to need a lot of them."

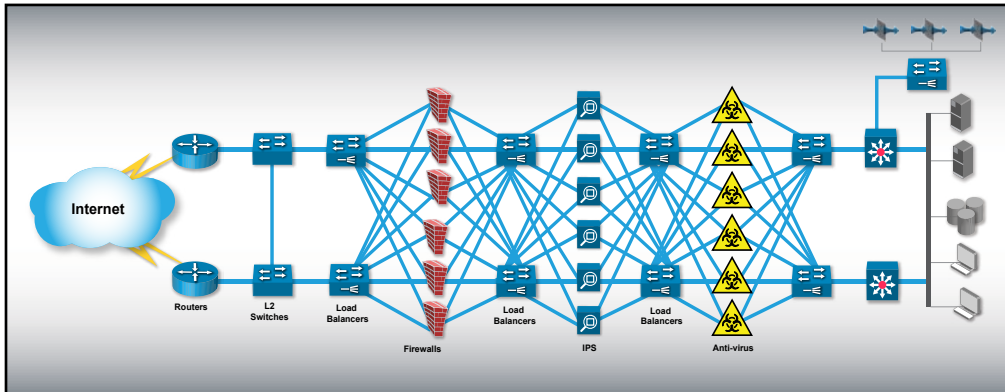


Figure 5 – Security Appliance Sprawl

The good news is there are lots of tech companies focusing on a particular security threat area. That focus is big plus for customers; however the downside is that these focused companies typically require another box to be added to deploy their solution. Redundancy and traffic growth requires that the number of these boxes grows over time along with the growth of all existing appliances like firewalls and IPS devices. This phenomenon has come to be known as "appliance sprawl" (see Figure 5).

Unfortunately, appliance sprawl yields extraordinarily complex data center architectures, leading to wasted data center space, growing power usage and difficulty in fault diagnosis. Moreover, since these devices require connections to layer 2/3 network switches and load balancers, and have limited networking and application processing power, they essentially become embedded elements in the network. This means that when the security services need to be expanded or upgraded, so does the network – an extremely expensive and inefficient use of IT and security resources.

Some vendors have responded to this problem by trying to develop their own firewall, IDS, IPS, malware filtering, etc. on their own appliance. While on the surface, a vendor's integration of its multiple security applications on a single device is appealing, it comes at the untenable expense of choice of best-of-breed security applications. In other words, enterprises lose the ability to leverage the focused R&D efforts of multiple security software vendors – a shoddy trade-off.

The bottom line is that appliance sprawl is difficult to deploy, operate, scale and manage, and VERY expensive.

So, is it possible to consolidate these security and networking appliances without having to make untenable trade-offs?

What Do Enterprises and Services Providers Want?

What would an ideal enterprise security solution look like? It would avoid the “yet another security box” sprawl and instead offer an architecture that had the following characteristics:

- Consolidation of security appliances and network gear required to deliver security services
- Virtualization of implementation of security application software
- Preservation of best-in-class third-party security application choice
- Highly scalable and resilient platform
- Reduced complexity of security services deployment and on-going management
- Compelling ROI and dramatically lower total cost of ownership

This security wish list is available today – only with Crossbeam.

A New Architecture: Consolidation, Virtualization, Simplification and Choice

Crossbeam has a fundamentally different approach to deploying security services. Our Next Generation Security Platform (NGSP) allows enterprises and service providers to consolidate network infrastructure (switches, load balancers, patch cabling and power cords) and appliances supporting security applications, virtualizing the delivery of security applications and dramatically simplifying deployment and on going management.

Our NGSP consists of a number of key components including: our high performance chassis, special purpose blades (the Network Processor Module, the Application Processor Module and the Control Processor Module) and our patent-pending operating systems software, XOS™ (see Figure 6)

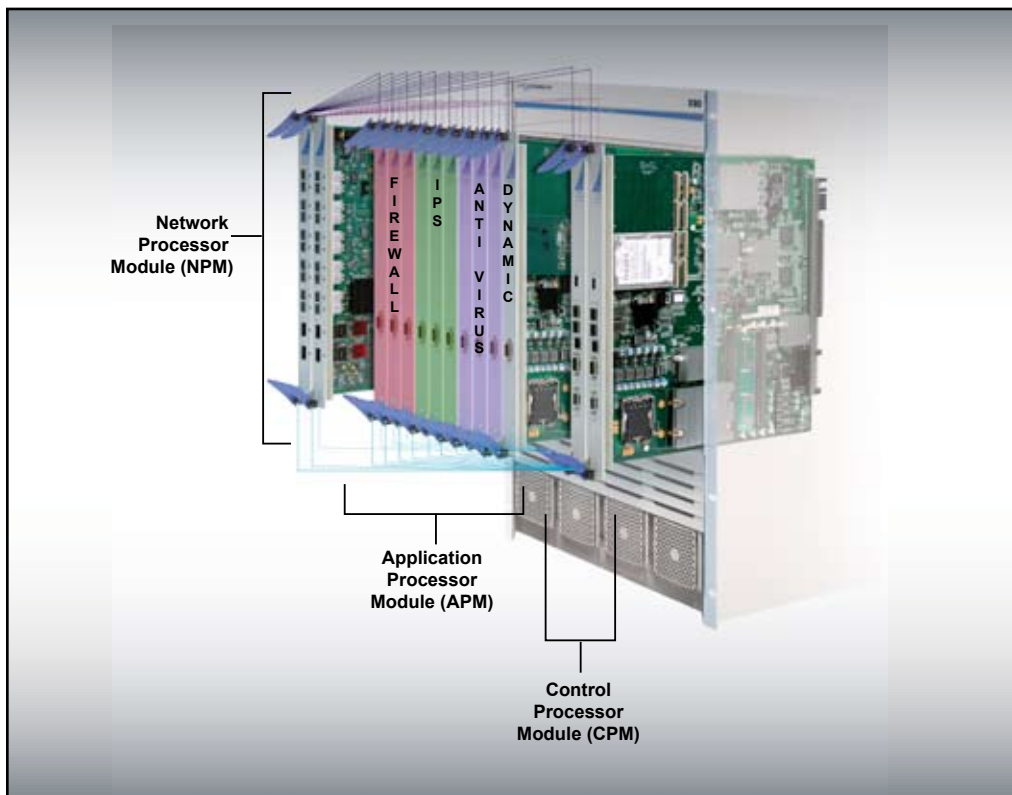


Figure 6 – The Crossbeam Virtualization and Consolidation Architecture

Each of our Network Processing Modules (NPM) creates a high-performance switching fabric (10Gbps of super low latency forwarding capability) that consolidates layer 2 switches and load balancers. Crossbeam replaces each of the layers of network “glue” in our NPMs. We then create a virtual instance of these capabilities so that it can recreate the sequence of security services through a sequenced flow of network traffic (e.g., IPS first, then firewall).

Next, the Application Processor Module (APM) virtualizes processing power for various best-of-breed third-party security applications. Each APM is a fully hot-swappable dual-core, or dual dual-core Intel-based processor, supporting up to 4GB of memory and one or two 100GB disks that can mirror each other. The actual services (i.e., security applications) that are absorbed into the APM have no inherent profile. As a result, one APM or multiple APMs can become any service (e.g., firewall or IPS) that the administrator assigns. Thus, racks of IPS devices and racks of firewalls or any other security appliance can be virtualized in a highly scalable and efficient way.

Finally, the Control Processor Module (CPM) provides the key management interfaces and capabilities to the rest of the chassis. On the CPM, administrators create a virtual representation of the chassis, assign which services will run on which blades and determine how policy selection is governed. As the chassis and its components come on line, they assume the identity and behaviors that the administrator

has previously assigned in the virtual representation. The CPM also governs failover policies, service priority and service preemption rights. For example, a firewall service may be provisioned in such a way that on failure, it will automatically “borrow” processing resources from a lower priority service.

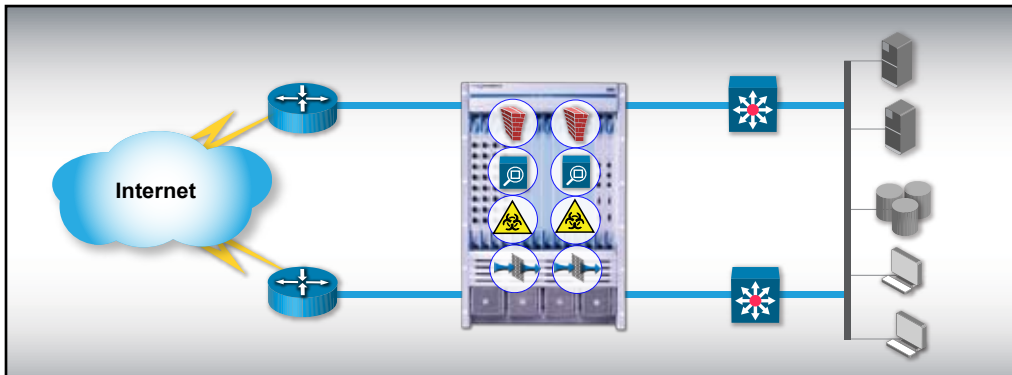


Figure 7 – Consolidation, Virtualization and Simplification of Security Services

The result is that security services are no longer embedded in the networks as racks of special-purpose appliances, switches and load balancers. Instead, these racks of special-purpose appliances, switches and load balancers are consolidated (see Figure 7). This is a revolutionary way to think about security services in that it separates (or decouples) the deployment and management of security services like firewall and intrusion prevention from the LAN switching infrastructure. We do this by consolidating application processing and virtualization capabilities in a device that “plugs” into any customer LAN. In other words, we create a security plane that sits on top of (or overlays) the company LAN. And what makes this concept even more powerful is that we do this in way that seamlessly integrates best-of-breed third-party security applications – we give our customers choice. No other vendor can offer this.

Our customers get best-of-breed security application choice and a super high performing and resilient platform that has unparalleled scaling ability. The result is a simpler architecture that reduces capital costs, operating expense and licensing costs and provides dynamic and flexible expansion capacity for multiple services. While our chassis, and our network, application and processing modules are critical components of our Next Generation Security Platform, our core innovation resides in the Crossbeam-developed operating system.

Crossbeam enables the Next Generation Security Platform via our highly sophisticated and patented Crossbeam Software System – XOS. We have invested \$75 million of research and development and over “500 man years” of software development in XOS. Moreover, we have nine patents pending.

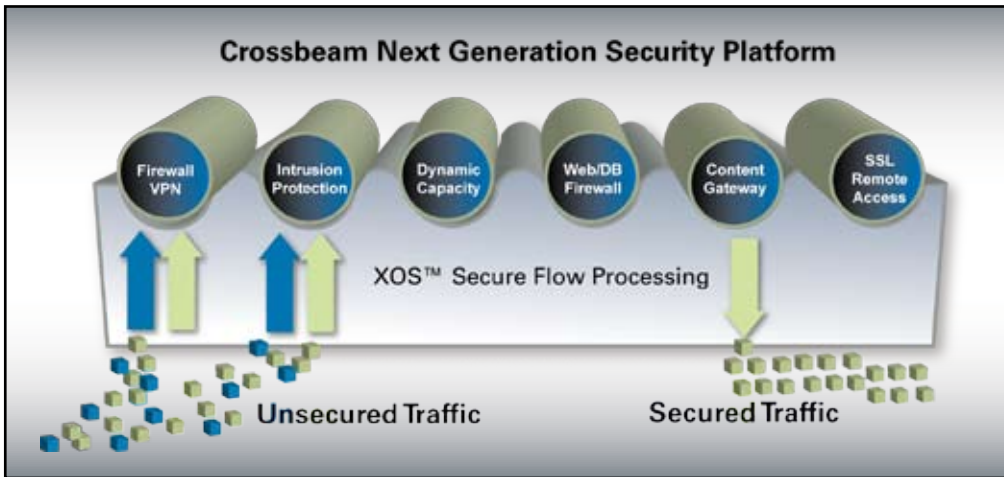


Figure 8 – Secure Flow Processing

One of our key XOS innovations is the ability to logically sequence network flows from one virtualized instance of a security application to another. We call this “secure flow processing.” So as an example, if your company’s security policy requires that all traffic go through a DMZ in which an IPS does deep packet inspection first then hands off traffic that passes its rules set on to a firewall for inspection, our secure flow processing enables this as if switches, load balancers and patch cables were all physically installed between the IPS and firewall (see Figure 8). In other words, your security policy via our consolidated and virtualized implementation! This secure flow processing is all done at wire speed, with active management of data flows and load balancing with “state” maintained for firewalls and content gateways.

Additionally, security applications are virtualized on a pre-hardened Linux image that is dynamically applied to any application blade. Security applications and configuration data are automatically distributed to multiple computing modules. The result is easy scaling for virtualized clustering and application redundancy, and the ability to enable single box high availability with self-healing.

Crossbeam offers a comprehensive product line that includes our cost-effective C-Series for small office and remote locations tied to larger corporate data centers, and our flagship X-Series that delivers unparalleled scalability and a blistering 40Gbps of firewall performance. All of our products can be configured and managed by our network management system, SecureShore (see Figure 9).

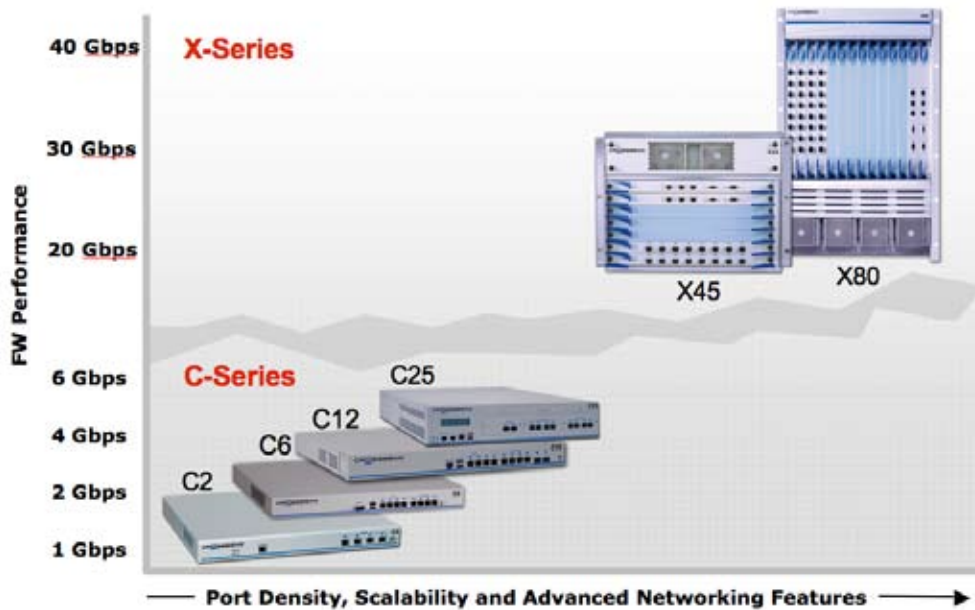



Figure 9 – Crossbeam Product Portfolio


In connection with this comprehensive product line, Crossbeam partners with best-of-breed ISVs to deliver our security solutions. Those ISVs partner with Crossbeam and Crossbeam's Professional Services Organization to deliver our Next Generation Firewall Solution, our Next Generation Content Gateway Solution and our Virtual Security Services Solution. Each of these ISVs security solutions are certified on the Crossbeam Next Generation Security Platform. The integrations ensure that these best-of-breed security applications are tightly integrated, operate seamless and take full advantage of Crossbeam scalability, virtualization and secure flow processing capabilities.

Next Generation Firewall



- ▶ Firewall (FW)
- ▶ Web Application FW
- ▶ Intrusion Detection (IDS)
- ▶ Intrusion Prevention (IPS)
- ▶ VPN
- ▶ Virtualized IPS
- ▶ Professional Services



C-Series



X-Series







Figure 10 – Next Generation Firewall Solution

The Next Generation Firewall is a new class of solution that provides the foundation of enterprise security – tightly coupled firewall and IPS capabilities. Firewall and IPS provide complimentary protection and a multi-layered defense, maintaining low latency while performing complex inspection and blocking. Simply having an IPS in the same appliance as the firewall does not constitute a Next Generation Firewall; both components need to leverage each others’ inspection capabilities, have intelligent traffic handling and work together to block attacks. Crossbeam provides the optimal solution by tightly coupling and certifying the leading firewall and IPS solutions (see Figure 10). Crossbeam’s unique architecture and operating system, XOS, allows secure flow processing between leading firewall ISV Check Point, leading IDS/IPS vendors IBM ISS and Sourcefire, and Web and database firewall ISV Imperva. The Next Generation Firewall running on Crossbeam’s platform replaces complex network topologies consisting of routers, switches, load balancers, firewall/VPN gateways and network intrusion prevention systems.

Next Generation Content Gateway

- ▶ URL Filtering
- ▶ Content Scanning
- ▶ Spyware Detection
- ▶ Malware Blocking
- ▶ Message Scanning
- ▶ Anti-Phishing
- ▶ Professional Services





C-Series



X-Series

Figure 11 –Next Generation Content Gateway Solutions

The Next Generation Content Gateway consists of the Crossbeam Next Generation Security Platform running customer-preferred combinations of best-of-breed security content applications including: URL filtering, malware scanning, anti-virus, P2P protection, bot-net protection, proxy/cache and reputation services (see Figure 11). Other functions such as SSL decryption and data leak prevention are also easily added. Additionally, the order and specific functions to be applied may be determined entirely by the customer. In delivering this solution, Crossbeam has certified applications from industry leading best-of-breed vendors such as Trend Micro and Websense. The flexibility and intelligence of the Crossbeam Next Generation Content Gateway Solution helps customers consolidate from 20 to 50 existing separate appliances into one highly available, scalable system.

Virtual Security Services

- Multi-domain FW
- Virtualized IPS
- Virtual Secure Layer 2/3 Processing
- Virtual System LB
- Policy Segmentation
- Professional Services

INTERNET SECURITY SYSTEMS*

CHECK POINT™
Software Technologies Ltd.

X-Series

Figure 11 – Virtual Security Services

Finally, Crossbeam has introduced a new Virtual Security Services solution that delivers best-of-breed security services while reducing cost through leveraged infrastructure, giving large enterprises and service providers a sustainable competitive advantage (see Figure 12). This solution dramatically increases the number and management capabilities of services by adding a full suite of managed content security services. It significantly reduces the amount of equipment required by supporting thousands of subscribers (enterprises to end users) in a multi-domain, fully virtualized, single platform with delegated administrative control down to the individual subscribing entity. Crossbeam partners with Check Point and IBM ISS to deliver a fully virtualized security gateway that embraces network, application and policy virtualization. It enables the creation of up to 250 virtual systems – firewall, VPN, intrusion prevention and content filtering – all on a single highly resilient, scalable chassis.

Conclusions: The Best of Both Worlds— Consolidating and Virtualizing Without Compromises

Only Crossbeam can deliver on the promise of security services virtualization and simplification. And only Crossbeam can offer over 10Gbps of “multi-application” performance and virtualization, all in way that facilitates the implementation of a company’s security policy without compromises. You choose the best-of-breed certified security applications and you, via your security policy, choose the secure flow processing sequence. Add in single box high availability with self-healing and linear scalability, and you have an unparalleled Next Generation Security Platform.

And finally, the benefits our customers achieve are a testament to the efficacy of our solutions. And what is the Crossbeam customer experience? Consistently, our customers find that our Next Generation Security Platform:

- Reduces the complexity of security services deployment and management
- Improves network performance and resiliency
- Facilitates scalability and future growth
- Eliminates trading-off functionality for performance or tight integration for choice of security application
- Accelerates “Time to Compliance”
- Delivers exceptional ROI and materially reduced TCO



Corporate Headquarters

Crossbeam Systems, Inc.
80 Central Street
Boxborough, MA 01719
Tel: +1 (978) 318 7500
Fax: +1 (978) 287 4210