WHITE PAPER

Virtualized Security: The Next Generation of Consolidation

The best way to predict the future is to invent it.
– Alan Kay.

A virtualized security Infrastructure is more than just an idea; in today's world of increased threats and rising costs, it's a necessity. More than anything else, it is Crossbeam's patented technology that has brought this idea to reality. This paper will take you through the components that comprise the Crossbeam Virtual Infrastructure; the X-Series high performance platform and best-in-class security applications, and demonstrate how Crossbeam invented the future.

TABLE OF CONTENTS

VITUALIZATION ADOPTION

As we begin a new decade, it is clear that enterprise IT departments are focusing attention on cost reduction programs to manage their increasingly diverse operations, which now include cloud computing initiatives. These programs include an increasing number of management technologies and tools designed to reduce such operational expenses as energy consumption, cooling costs, and travel.

As part of this effort, enterprises have been turning to infrastructure consolidation as a means of containing these costs. Unfortunately, this has left many network and security architects struggling to find the right technologies to both provide the strongest protection against network security threats, and still guarantee network availability and performance.

Virtualization technologies deployed across the data center have been successfully reducing IT costs while maximizing server and storage workloads. But the security infrastructure has been largely exluded from this effort due to the added burden of creating and managing virtual security appliances and the associated risk of accidental or malicious virtual machine mapping.

VIRTUALIZED SECURITY COMES OF AGE

Due to the geometric expansion of financially driven threats, increased traffic bandwidth, and a growing diversity of users accessing data, IT departments have resorted to creating hundreds of security segments with ever decreasing perimeters. Although this model reduces risk and helps provide visibility between segments, it has the negative effect of dramatically increasing the number of network and security devices and their security rules; leading to both appliance sprawl (See Fig. 1) and operational complexity.

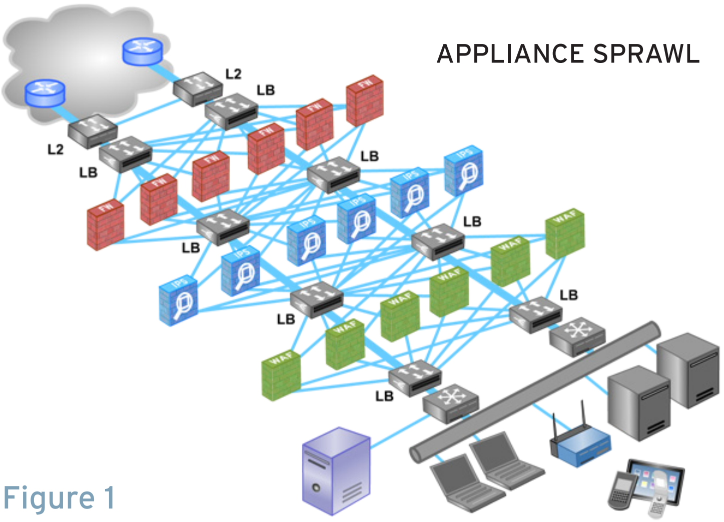


Figure 1

The logical approach to solving this problem is the creation of a virtual infrastructure that can accomodate the requirements of a robust network environment; but greatly reduce the need for hardware.

In order to achieve the goal of a virtual infrastructure and accompanying cost reduction, two important components are needed to create this system:

1. The ability for a security application to run on any number of hardware based Application Processor Modules (APMs) and still act as a single entity. (see Figure 2).

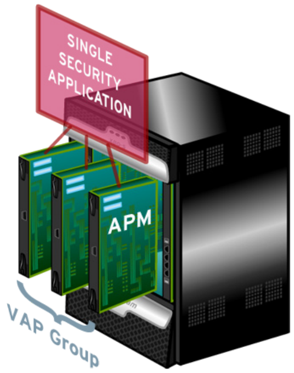


Figure 2

2. The ability for a security application to work as multiple independent security instances on a single APM. (see Figure 3)

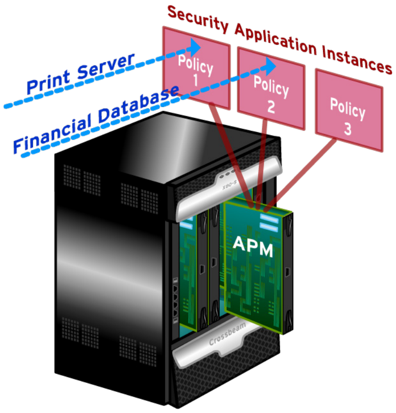
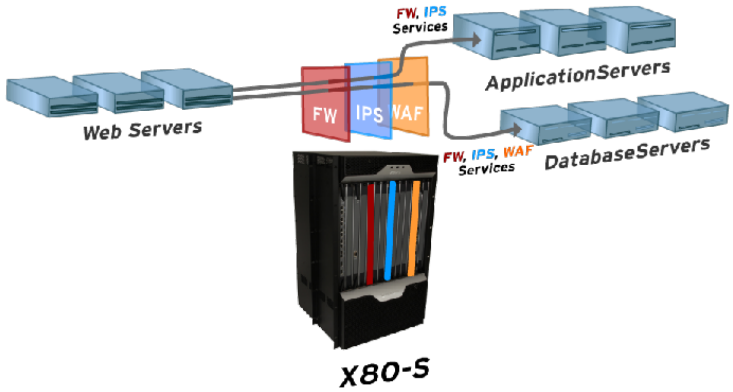


Figure 3

Using a virtual ifrastructure, network managers can create hundreds of firewall or IPS instances with distinct policies per segment on a single security platform while significantly reducing the number of network and security devices. For instance, one could apply specific firewall policies and IPS rules to the print server connection, and another set of IPS rules and firewall protection for the financial database zone and insure appropriate access to both these resources.

Large enterprises could use this technology to collapse firewall and IPS devices from remote locations into just one data center, but maintain unique security segmentation and rules for each location as represented in Figure 4.

Figure 4



THE CROSSBEAM X-SERIES PLATFORM

The underlying platform that enables these capabilities is the Crossbeam X-Series Security platform. The Crossbeam platform delivers best-of-breed virtualized security applications and services while consolidating network and security infrastructure with significant cost advantages. A virtual infrastructure significantly reduces the amount of equipment required by supporting thousands of enterprise users in a multi domain, fully virtualized platform with delegated administrative control to the individual network zone.

The Crossbeam X-Series architecture is the next generation security platform that provides carrier class resiliency and performance. Completely redundant hardware modules, switching fabrics, and control planes enable complete Single Box High Availability (SBHA) and Dual Box High Availability (DBHA) modes in configurations that provide up to 150Gbps utilizing up to 14 slots for module expansion and ranging over four different chassis types.

The Crossbeam X20, X30, X60, and X80-S Security Platforms.

X20

The X20 provides Enterprise customers with a flexible 4-Slot 5Gbps network security platform pre-configured for one security application. The chassis can be easily expanded to increase the performance of one application, or add a second application. The X20 can be field upgraded to a fully modular X60.

Click here to view a 3D model of the X20.

X30

The X30 provides Enterprise customers with a flexible 4-Slot 10Gbps network security platform pre-configured for one security application. The chassis can be easily expanded to increase the performance of one application, or add a second application. The X30 can be field upgraded to a fully modular X60.

Click here to view a 3D model of the X30.

X60

The X60 provides Enterprise & Service Provider customers with a fully modular 7-Slot 80Gbps network security platform that can be used to deploy up to 5 applications at once. The chassis is fully modular and can support a variety of Network and Application Processor modules to fit the necessary application and environment.

Click here to view a 3D model of the X60.

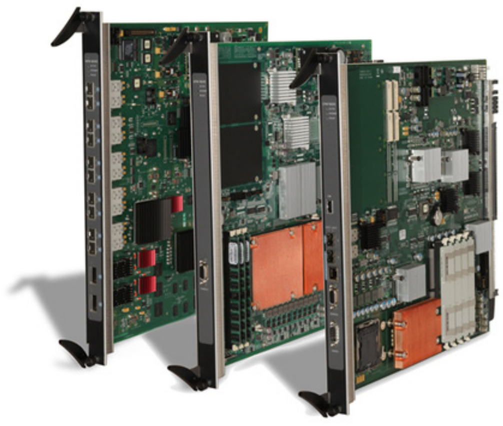
X80-S

The X80 provides Enterprise & Service Provider customers with the highest possible performance scalability, with a fully modular 14-Slot 150Gbps network security platform that can be used to deploy up to 10 applications at once. The chassis is fully modular and can support a variety of Network and Application Processor modules to fit the necessary application and environment.

Click here to view a 3D model of the X80-S.

THE X-SERIES PROCESSOR MODULES

There are three types of modules available to support a virtualized next generation firewall; Network Processor Modules (NPM), Application Processor Modules (APM), and Control Processor Modules (CPM). Complete flexibility for module configurations are supported to insure a stable configuration for the virtualized firewalls.

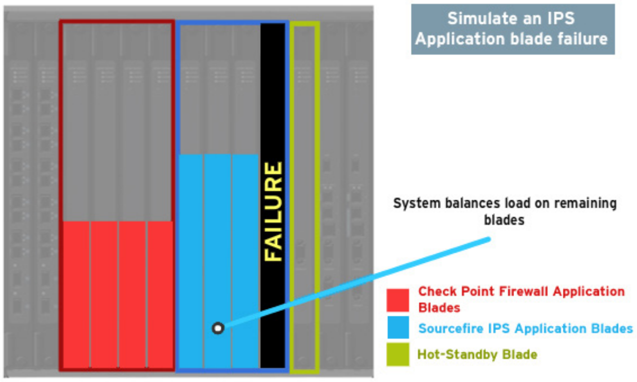


The Crossbeam NPM, APM, and CPM blades

THE NPM

The Network Processor Module (NPM) is fully enabled for next generation 10 Gb Ethernet networks and is designed to perform deep packet inspections, classifying the packets into flows that are switched through the system to the virtualized security applications. The flow switching mechanism is based on Crossbeams' load balancing algorithms (see Figure 5) and Crossbeam Secure Flow Processing. These technologies provide system network managers power and control to manage many virtual security domains-matching individual policies and rules to the appropriate entity.

Figure 5


Simulate an IPS Application blade failure
FAILURE
System balances load on remaining blades
Check Point Firewall Application Blades
Sourcefire IPS Application Blades
Hot-Standby Blade

Click here to watch Crossbeam load-balancing in action.

THE APM

Up to ten slots are reserved for Application Processor Modules (APM). These APMs manage the virtualized security applications applied to the traffic flows as they are switched through the system. Crossbeam Secure Flow Processing logically sequences network flows from one application to another using the application to manage the individual rules and polices set for each virtual firewall and IPS. This secure flow processing is managed at wire speeds regardless of the number of firewalls managed.

A key capability of the APM is the Virtual Application Processor (VAP) technology. A VAP (See Figure 2) clusters security applications, networking functions, and connections, allowing the XOS operating system to dynamically distribute the virtualized firewall and IPS applications to these processors. The security applications managing the virtual firewalls are automatically distributed and intelligently load balanced based on usage metrics. The result is an on-demand dynamic resource allocation for easy scaling, application redundancy, and self healing capabilities that enables redundancy inside the chassis. If one blade should fail, the system will automatically fail over to a second single or cluster of blades, insuring that all firewall entities are secured.

THE CPM

The health and management of the X-Series chassis falls to the Control Processor Module (CPM). On the CPM, a virtual representation of the chassis is created, blade services are assigned, and chassis management policies are governed. The CPM manages failover policies, service priority and service preemption rights. For example, one entity's firewall service may be provisioned so it automatically shares processing resources from a lesser used blade if data throughput should spike- insuring that all entities are always protected from attacks.

The X-Series system decouples network and security service processing to allow customers to take advantage of price/ performance improvements and innovation curves within each technology. The system offers significant consolidation of security equipment while preserving security policies, resulting in a safer and simpler network for a Virtualized Security System.

CERTIFIED SECURITY APPLICATIONS

A key benefit of the Crossbeam security solution is the ability to choose best-in-class security applications that fit your company's needs, and integrate them with the Crossbeam security infrastructure, giving you the best of both worlds.

The applications listed below can be serialized in any combination on the Crossbeam X-Series platform using our Secure Flow Processing technology. For example, the Check Point Security Gateway can be combined with Sourcefire 3D Sensor, the Actiance USG with the Imperva Database Firewall, or even a Check Point firewall with a McAfee firewall. The choice is yours.

Check Point® SOFTWARE TECHNOLOGIES LTD.	

APPLICATION	
• **Security Gateway R75**	Check Point's Security Gateway on Crossbeam offers a very unique approach to tailoring solutions to meet your exact business security needs. The software blade architecture provides the ability to easily add security services as new threats emerge, such as adding the Application Control blade to help identify block and limit usage of thousands of applications based on user identity. The Crossbeam X-Series hardware bladed platform adds to the approach by being able to quickly adapt and scale the performance of these security services, as well as create a very robust and self-healing system.
• **VPN-1 Power VSX R67**	VPN-1 Power VSX on Crossbeam provides a virtualized security gateway that can be used to create up to hundreds of individual security systems per APM or across multiple APMs depending upon performance needs. This allows the consolidation of hundreds of individual appliances into a single X-Series platform. Based on the proven VPN-1 Power software, VSX on Crossbeam provides best-in-class firewall, URL filtering, VPN and intrusion prevention technology for each security instance.
• **Firewall-1 GX 4.0**	FireWall-1 GX delivers the market leading security to GPRS (2.5G) and UMTS (3G) enabled wireless networks. Together with Crossbeam, FireWall-1 GX secures connectivity between wireless carriers, the GRPS infrastructure as well as the auditing and tracking of GRPS traffic. The Crossbeam X-Series incredible performance allows GX to scale and meet the demands of mobile traffic growth for years to come.

actiance™	

APPLICATION	
• **Actiance Unified Security Gateway**	The Actiance Unified Security Gateway (USG) provides granular security and compliance controls for Web 2.0, instant messaging, and social media, all while adding an extra layer of protection for firewall deployments. The USG enables Web 2.0 content monitoring, feature access and content-posting controls as well as logging and archiving social media.

SOURCEfire®	

APPLICATION	
• **Sourcefire 3D Sensor (IDS/IPS/RNA) V4.10**	Built on the de-facto industry standard for IPS, (SNORT), Sourcefire 3D Sensor on Crossbeam delivers a scalable and powerful IPS solution- with the fastest IPS throughput on the market. Couple Sourcefire 3D Sensor and Sourcefire RNA with a best of breed firewall from Check Point and you have the world's hottest Next Generation Firewall – only from Crossbeam.

iMPERVA Protecting the Data that Drives Business	

APPLICATION	
• **Imperva SecureSphere Database Security Suite (DSS) v8.0**	SecureSphere on Crossbeam delivers the full SecureSphere web application, database, and file security feature set in a very high performance, self-healing and scalable platform. SecureSphere Data Security Suite is the market leading data security and compliance solution that protects sensitive data from hackers and malicious insiders, provides a fast and cost-effective route to regulatory compliance and establishes a repeatable process for data risk management.

McAfee	

APPLICATION	
• **McAfee Firewall Enterprise V8.1.1**	McAfee Firewall Enterprise on Crossbeam delivers the world's most powerful and scalable application-aware firewall ideal for large Enterprise and Government deployments. This Next Generation Firewall on Crossbeam provides the latest high performance Identity and Application Awareness, Global Threat Intelligence and integrated Web filtering, A/V, IPS and SSL Encryption all on one platform.

SUMMARY

Crossbeam, along with Check Point, Imperva, Actiance, and McAfee have developed a comprehensive, total solution for enabling cost effective security deployment for large enterprises. The X-Series Virtual Security Platform provides the highest hardware scaling and high availability solutions for a growing list of state-of-the-art security application deployments. The end result for is a high performance, scalable virtual service delivery platform that provides revenue generation and cost reduction opportunities through a competitive managed service offering. This promotes competitive differentiation and reduces the total cost of deployment and management of infrastructure.

Crossbeam Systems®, Inc. offers a proven approach to deploying network security that meets the extreme performance, scalability and reliability demands of large enterprises, service providers and government agencies. Its leading X-Series security platform offers an open, high-performance architecture that easily provisions and scales multiple best-in-class security applications to meet the ever-changing threat landscape. Companies rely on Crossbeam to intelligently manage risk, accelerate and maintain compliance, and protect their businesses from evolving threats. Crossbeam is headquartered in Boxborough, Mass., and has offices in Europe, Latin America and Asia Pacific. More information is available at www.crossbeam.com.