

Virtualized Security: The Next Generation of Consolidation

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

A consolidated security infrastructure is more than just an idea; in today's world of increased threats and rising costs, it's a necessity to be responsive cost-effectively. Crossbeam's patented technology to virtualize network security into a consolidated platform has made a consolidated security infrastructure practical. This paper will take you through the components that comprise the Crossbeam X-Series high performance platform and best-in-class security applications, and demonstrate how Crossbeam invented the future.

TABLE OF CONTENTS

Virtualization Adoption _____	2
Virtualized Security comes of Age _____	2
The Crossbeam X-Series Platform _____	3
The X-Series Processor Modules _____	4
Crossbeam Management System _____	4
Security Applications _____	5
Summary _____	6

VIRTUALIZATION ADOPTION

It is logical that IT departments focus attention on cost reduction programs to manage their increasingly diverse operations, including 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.

Consolidation of the infrastructure has successfully contained costs, but consolidation of the security infrastructure is more difficult. Virtualization technologies deployed across the data center have been successfully reducing costs while maximizing server and storage workloads. But the security infrastructure has been largely excluded 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. Many network and security architects have struggled to find the right technologies to both provide the strongest protection against network security threats, and still guarantee network availability and performance.

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.

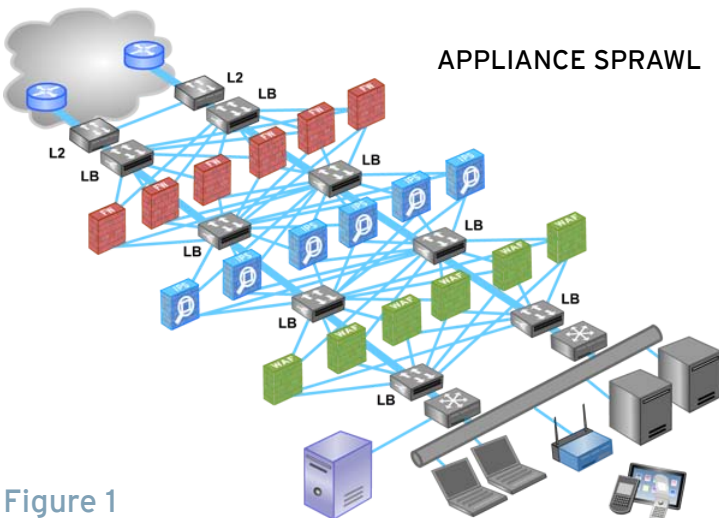


Figure 1

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

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

1. The ability for a security application to run on specific hardware, such as a hardware-based Application Processor Modules (APMs) but still act as a single entity for resiliency and performance scalability (see Figure 2).

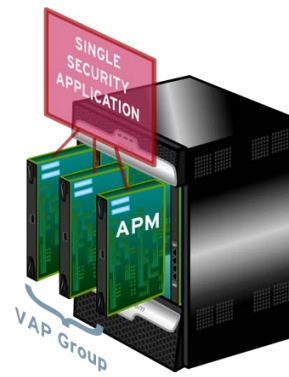


Figure 2

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

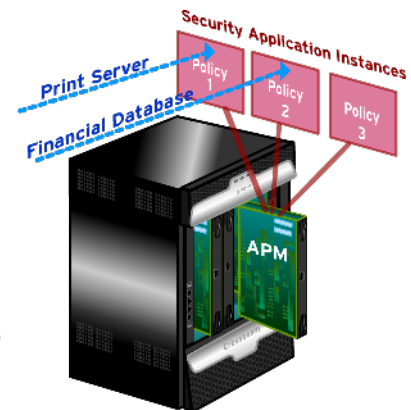
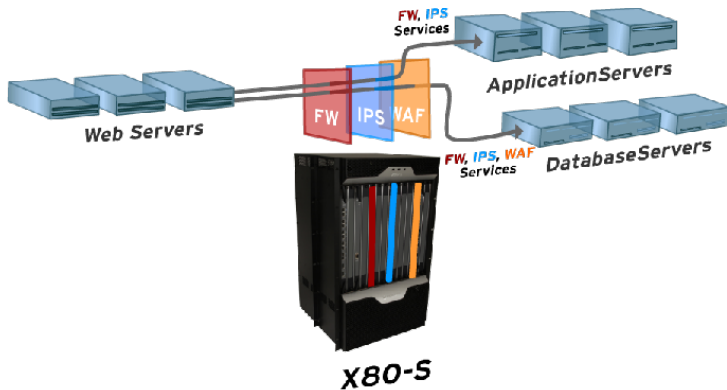


Figure 3

Using a virtual infrastructure, 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, insuring appropriate access to both these resources.

Large datacenters 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 security applications and services, and virtualizes them onto the X-Series platform, consolidating network and security infrastructure with significant cost advantages. This approach not only significantly reduces the amount of equipment required to support thousands of users in a multi-domain environment, but also to delegate administrative control to the individual network zone and automate failover and load balancing across a series of application modules in the platform.

The Crossbeam X-Series architecture 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 scale up to 640Gbps of full duplex network connectivity, throughput up to 135Gbps of IMIX real-world traffic, and up to 100 million concurrent connections. X-series platforms can utilize up to 14 slots for module expansion and are available in the following range of chassis types.

The Crossbeam X20, X30, X50, 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.](#)

X50

The X50 provides Enterprise customers with a flexible 4-Slot 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 X50 provides real-world application performance scalability to 18Gbps.

[Click here to view a 3D model of the X50.](#)

X60

The X60 provides enterprise & service provider customers with a fully modular 7-Slot network security platform that can be used to deploy best-in-class security applications. The chassis is fully modular and can support a variety of Network and Application Processor modules to fit the necessary application and environment. The X60 provides real-world application performance scalability to 70Gbps.

[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 network security platform that can be used to deploy best-in-class security applications. The chassis is fully modular and can support a variety of Network and Application Processor modules to fit the necessary application and environment. The X80-S provides real-world application performance scalability to 140Gbps.

[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, or other security applications: Network Processor Modules (NPM), Application Processor Modules (APM), and Control Processor Modules (CPM). Complete flexibility for module configuration is supported to insure a stable configuration for the security workloads.

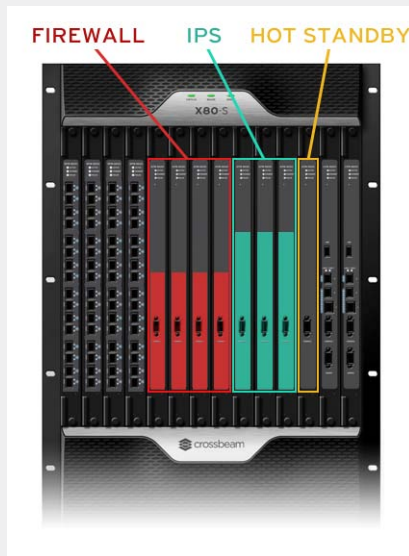


The Crossbeam NPM, APM, and CPM blades

THE NPM

The Network Processor Module (NPM) provides the switching fabric, physical interfaces, load balancing, and routing functions for the X-Series platform. The NPM can effectively consolidate networking gear, and fully enables next generation Ethernet networks. The NPM 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 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



Virtual application processor (VAP) groups run security applications such as firewall and IPS, and can be reconfigured on the fly to accommodate different physical APM permutations since the license, configuration and application data is on the CPM. In the event of an APM failure, the application can be automatically moved to a standby blade and re-combined with the VAP group, without affecting service.

[Click here to watch Crossbeam self-heal.](#)

THE APM

Up to ten slots in an X-Series platform 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 and Figure 5) 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.


CROSSBEAM MANAGEMENT SOLUTION


Consisting of the X-Series Management System (XMS), Greenlight Element Management (GEM), and Command-line Interface with Automated WorkflowSystem (AWS), the Crossbeam Management System provides visibility and control across the entire X-Series infrastructure allowing. This visibility extends from the entire solution, to individual platforms, to modules, to flows and applications that IT needs to effectively and time-efficiently recognize, diagnose, and remediate performance-impacting issues. Having a comprehensive view minimizes operational costs, reduces downtime, and improves efficiency, freeing personnel to focus on managing the network and not the infrastructure.


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.

	
APPLICATION	
<ul style="list-style-type: none"> • Security Gateway R70, R70 HCC, R70 IPv6 Pack, R71, R75, and R75.20 	<p>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.</p>
<ul style="list-style-type: none"> • VPN-1 Power, VSX R65, R67, & R68 	<p>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.</p> <p>Check Point VSX enables organizations to consolidate multiple instances of firewalls, VPNs, URL filtering and IPS on a single Crossbeam APM. This ability allows organizations to maximize their processing resources and minimize total cost of ownership and effectively consolidate the data center.</p>
<ul style="list-style-type: none"> • Firewall-1 GX 4.0, 5.0 	<p>Check Point VSX enables organizations to consolidate multiple instances of firewalls, VPNs, URL filtering and IPS on a single Crossbeam APM. This ability allows organizations to maximize their processing resources and minimize total cost of ownership and effectively consolidate the data center.</p>

	
APPLICATION	
<ul style="list-style-type: none"> • Actiance Unified Security Gateway 4.2 	<p>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.</p>

	
APPLICATION	
<ul style="list-style-type: none"> • Sourcefire 3D Sensor (IDS/IPS/RNA) V4.10 	<p>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.</p>

	
<p>APPLICATION</p> <ul style="list-style-type: none"> • Imperva SecureSphere v8.0, 9.0.1* 	<p>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.</p>

	
<p>APPLICATION</p> <ul style="list-style-type: none"> • McAfee Firewall Enterprise V8.2.1* 	<p>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.</p>

*Expected Release: Q1 2012

SUMMARY

Crossbeam, along with Check Point, Actiance, Sourcefire, Imperva, 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 the 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.