November 2004

Enterprise and Telco Network Security in a Box

With

IBM @server BladeCenter, Blade Fusion IP-X 1000 Secure Operating Environment

And

Check Point Software , Trend Micro and Aladdin

Best-of-Breed Security Applications Consolidated with High Performance, High Availability and Hot-Swap Maintenance

A Technical White Paper

Technical White Paper

Technical White Paper

Technical White Paper

Introduction

Best-of-breed security solutions have long been the most-effective choices for securing enterprise and telco networks. However, that approach has resulted in the deployment of a disparate set of products for firewall, intrusion detection, antivirus, vulnerability analysis and other network-centric security functions. That has led to gaps in protection and a high cost of ownership because of the need for multiple management consoles and a lack of integration. According to Gartner, the rise of network security platforms will enable best-of-breed security solutions to blur the lines between firewalls, network-based intrusion detection and vulnerability scanning, as well as other network-centric security technologies.

?????????Dedicated security appliance solutions customer challenges are updating the software and the cost of maintaining additional boxes on the network. Blade server products address many of the drawbacks of appliances and rack-optimized servers. The increasing number of security appliances, ranging from dedicated firewalls, VPNs, intrusion detection systems (IDS), SSL accelerators, gateway antivirus solutions and load balancers make the blades desirable for enterprise and telco use. Consolidating the solutions to a single network element dramatically reduces the management task (managing one box, as opposed to five); provides load balancing and failover support in a single solution, further reducing the number of solutions to be bought; and could improve performance.

In response to the above challenges, IBM with its leadership blade server platform—IBM @server® BladeCenter™—with integrated high throughput switches from Nortel® Networks and Cisco® Systems, in partnership with Blade Fusion's Secure Operating Environment and best of breed security software vendors have jointly created an integrated security infrastructure platform reference architecture for the enterprise and telco customers. This architecture is based on the BladeCenter platform, an open, high performance, highly available, scalable, and at a potentially much lower cost and better cost/performance ratio compared to the representative competitive vendors.

This white paper describes BladeCenter, including integrated Ethernet switching such as Nortel and Cisco with BladeFusion's Secure Operating Environment, Security in a Box solution reference architecture based on Check Point, Trend Micro, Aladdin and many other security applications. The integration and performance testing for this solution was conducted at the BladeFusion laboratory in Israel with support of IBM and other solution providers.

Solution Overview

BladeCenter with Blade Fusion IP-X 1000 platform is a Multi-Bladed Security Switch. It delivers a comprehensive multi-functional secure connectivity solution comprised of the following major components:

BladeCenter hardware: The BladeCenter server platform includes the BladeCenter chassis, HS20 server blades, embedded Ethernet switches and supporting options.

1. **Blade Fusion Secure Operating/Environment (SOE):** The Blade Fusion SOE uses rich security features to enable the operation of multiple security applications across multiple networks with BladeCenter while enforcing necessary network segregation and workflow management. In addition it delivers real-time blade/grid automation, N+1 high-availability, hot-swap maintenance and self healing for the applications and the hardware components that run on the system.
2. **Best of Breed Security Application Software:** ISV security applications software (Firewall, VPN, Antivirus, Antispam, Intrusion Detection /Intrusion Prevention etc.) some of which are pre-packaged (see next bullet below). The reference architecture is open to any X86-compatible software.
3. **Security filtering at line rate throughput:** The Nortel Networks Layer 2-7 Gigabit Ethernet Switch Module for IBM @server BladeCenter line rate load balancing and security filters provide acceleration and an extra layer of security by keeping out unwanted traffic to BladeCenter.
4. **Pre-packaged software** – Blade Fusion has pre-packaged pre-hardened, platform-optimized images from leading vendors such as Check Point, Trend Micro, Aladdin and others. These appliances are available packaged on the Blade Fusion management blade, which in turn can provision and deploy each of them on one or more blades automatically.
5. **Multi-Appliance Solutions (Blade Fusion “Models”)** – The Blade Fusion management blade is pre-packaged with multi-appliance solutions including one or more load-balanced clusters, and/or a combination of several security applications that can span a BladeCenter chassis full of

blades, applications and switches.

.

Hardware Description

BladeCenter

BladeCenter is a superior implementation of the blade server concept of physical consolidation of servers into a smaller, more manageable environment to achieve efficiencies of operation. The BladeCenter design brings the customers' computing resources into a cost-effective, highly reliable, modular new form factor at up to twice the density of comparable 1U Intel® processor-based servers. Coupled with Intel Xeon™ processors (up to 3.2 GHz), modular Fibre Channel and Ethernet switches and server load-balancers (layer 2, layer 2-3 and Layer 2-7) built into the BladeCenter chassis and advanced management of storage, networking, servers, and applications through IBM Director, organizations can take control of the computing environment and potentially reduce costs. Physical costs alone can potentially be reduced with a smaller footprint for multiple servers (14, 2-Way in 7U) and up to an 83% reduction in cabling. BladeCenter supports IBM's TotalStorage® and networking solution in a common fully managed architecture. Additionally, BladeCenter often takes less time to install, can require fewer people to manage and maintain, provides modular scalability, and provides an environment with almost no single points of failure.

BladeCenter Chassis

8677-2XX

The BladeCenter chassis comes with one KVM/management module, two power supplies, a 1.44MB floppy disk, a 48x CD-ROM and USB port. It supports optional Ethernet switches by IBM or major switch suppliers. For external storage there is an optional Fibre switch by IBM and Brocade. For installation of more that six blades an optional power supply module will need to be installed.

BladeCenter HS20

8832-XXX

The HS20 blade is a powerful Intel processor-based blade server that delivers uncompromising performance for mission-critical applications. A single blade can support up to two Intel Xeon processors with 533 or 800MHz front-side bus, 8GB of DDR ECC Chipkill™ memory, options for either two internal IDE or SCSI hard drives and integrated dual Gigabit Ethernet connections.

Feature	Benefits
Modular system delivering raw processing power	• Ultra-slim and powerful, blade design delivers high density without sacrificing server processor performance. • Up to 84 servers in an industry-standard rack, packing more performance per square foot and saving you valuable central office and/or data center space. • Hot-swappable, designed to allow you to add or change servers without disrupting the operation of other servers in the chassis.
Supports up to two Intel Xeon processors with up to 800MHz front-side bus	• Equipped with Intel Hyper-Threading and NetBurst® technologies, the Intel Xeon processor delivers server performance ideal for compute-intensive, next-generation network and IT application workloads.
Up to 8GB of DDR ECC Chipkill memory	• Double data rate, error checking and correction, and Chipkill memory offer high performance with mainframe-inspired fault protection. • Able to handle your data-hungry applications with memory to spare
64-bit extensions	• Supports Intel® Extended Memory 64 Technology (Intel® EM64T) with embedded 3.6GHz Intel Xeon processor(s) on BladeCenter HS20 Modell 8832-XXX. • Provides 64-bit addressability while supporting both 64- and 32-bit applications, a smooth transition to 64-bit enabled applications while leveraging the price and performance of existing applications

Support for up to four hard disk drives	• Supports up to two internal SCSI disk drives and/or two hot-swap SCSI drives for flexibility and choice
Integrated dual Gigabit Ethernet connections	• Enabled to transmit large amounts of data at fast speeds for high-performance network applications • Robust design supports teaming and failover
Two high-availability midplane connections	• Provides durable and reliable connections to all chassis resources
Blade server interconnects	• Supports an optional 2-port (2Gb per port) Fibre Channel Expansion Card (Host Bus Adapter) to deliver a high-performance, highly manageable Storage Area Network (SAN) • Supports an optional 2-port (1Gb per port) Gigabit Ethernet Expansion Card to enable additional Ethernet bandwidth and allow for connection to multiple LAN segments
Light path diagnostics self-diagnosis panel	• Provides quick and easy guide to troubleshoot your server for higher availability and system uptime • Independently powered, allowing you to remove the server from the chassis and still illuminate the light path LEDs

Predictive Failure Analysis™ (PFA)	• Helps save time and money by decreasing planned and unplanned downtime • Helps increase uptime by allowing you to receive proactive alerts as much as 24 to 48 hours in advance
Integrated System Management Processor	• Helps increase server availability by continuously monitoring your system and notifying you of potential system failures or changes
IBM Director and IBM Director Extensions comprehensive systems management tools	• Exploits hardware capabilities by surfacing pertinent information about your system, allowing you to automate a response • Helps increase uptime, reduce costs and improve productivity via advanced server management capabilities • Provides intelligent system management for rock-solid reliability • IBM Remote Deployment Manager simplifies and automates deployment and redeployment for efficient installation and startup of your IBM @server BladeCenter T.
Operating system support	• Microsoft® Windows® Server 2003, Microsoft Advanced Server, Web (standard editions) • Red Hat® Enterprise Linux® 3.0 - Advanced Server (Carrier grade) • SUSE® LINUX 8.0 (Carrier grade)
3-year onsite limited warranty[1] for parts and labor	• The IBM Global Services organization provides reliable, dedicated and skilled assistance when you need it. • Provides peace of mind for an extended period of time

Nortel Networks Layer 2-7 Gigabit Ethernet Switch Module

It provides additional capabilities and benefits to the blade server offering, including increased application availability and performance, improved manageability and security protection, easier scalability and greater flexibility to support on demand computing.

Blade Fusion System Components

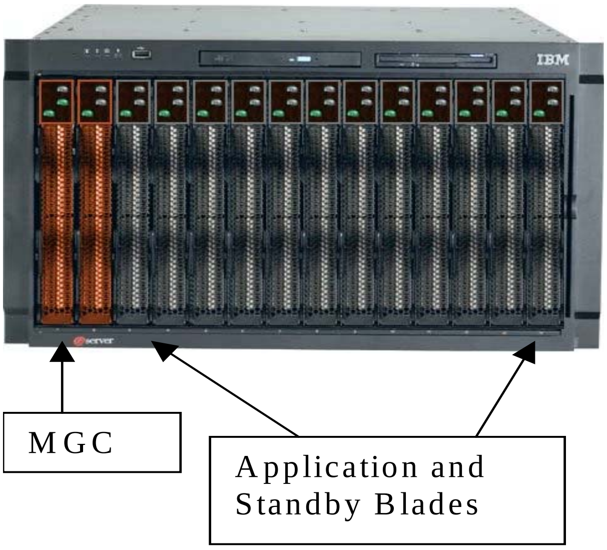
Blade Fusion IP-X 1000 is the Secure Operating Environment (SOE) that transforms the BladeCenter hardware into a cohesive and fully automated environment. Within the definitions of the Blade Fusion SOE, the system is comprised of four types of blades:

1. **Main Gateway Controller blades (MGC™)**. These blades are responsible for the management of the system. There are two MGC blades. One blade is always active, and the second is a hot backup for the central storage and management application. These blades and these blades alone contain the images of the security applications (appliance skeletons) and security solution 'models' that are created from combination groups of such appliances.
2. **Application blades.** These run the active applications (appliance instances) as well as the load-balancing units in the case that performance aggregation is required on one or more of the applications. Application blades run in 'diskless' mode, and they get their assigned images (O/S and application) over the backplane from the MGC or from an iSCSI storage redirected by the MGC.
3. **Standby blades.** These serve as hot standby for the applications. When the MGC detects a problem in the application, it migrates the application to a standby blade. A standby blade can replace any active blade in real-time. A standby blade need not be idle, and it could be running a low-priority application when it is pre-empted by the system due to the failure of a high-priority application.
4. **Networking blades.** These are the backplane networking components

providing the entire system with multi-gigabit connectivity both internally among the blades and externally with the outside world. Some of these blades have wire speed load-balancing features.

Comment #1: All blades above are standard issue BladeCenter hardware components with no hardware alterations whatsoever.

Comment #2: The MGC blades are the only ones that are pre-installed with software on their local disk. The other blades operate in 'diskless' mode and their function is determined by the MGC.



Network Topology

The BladeCenter/Blade Fusion IP-X 1000 system uses the 802.1q protocol to separate the network into VLANs. The system manages three network types:

- **Management networks:** Allocated to the management of the system itself with no direct access other than indirectly through the UI of the MGC.
- **Access networks:** Allows the user to manage the system (access the MGC UI) using HTTPS and SSH protocols. Access to this network is available through the management port only, unless explicitly defined otherwise in a system firewall.
- **Application networks:** A list of networks used by the applications. These networks are defined and managed using the Blade Fusion central management UI . The user defines:

- Global Networks - The global list of all networks. In extreme cases up to 1000 segregated networks. More typically between 10 and 20.
- Externalized (uplink) Networks - Out of the list of global networks – which network(s) is (are) exposed to the external (to the chassis) world via the switch uplink ports. Some uplink ports may be defined as 802.1q trunks of multiple networks as is compatible with the large backbone switches to which they typically connect.
- Blade Slot Networks – Each slot in the chassis corresponds to a particular application. Each such application may require connectivity and access to 1 and in extreme cases even 500 to 1000 networks. This connectivity may also require switch redundancy.

Comment #1: Not all application networks need to be reflected to the outside world via the ESM uplinks. Some may be defined as internal only.

Comment #2: In case of failover, a standby blade is instantly 'rewired' corresponding to the application that was discovered to fail. This feature is called 'dynamic network topology' and it is a unique ingredient that enables N+1 redundancy. Without it, one would have had to 'pre-wire' a standby blade per each permutation of blade/application network connectivity (2N).

Security Enforcement: The following security measures are enforced by the Blade Fusion IP-X 1000 Secure Operating Environment:

1. No network can be seen by any blade in the chassis unless it is configured by an authorized user of BladeFusion's IP-X 1000 SOE.
2. The ESMs are not configured directly by the user via the Management Module or otherwise. The ESMs are configured indirectly by authorized users of the BladeFusion system.
3. The system polls the ESMs in regular intervals. If it detects a configuration that is in any way different from how it had been configured, its sets off alarms and forces a reconfiguration of the ESM back to normal.
4. The multiplicity of networks on each application blade and the network redundancy is enabled by BladeFusion's specialized secure networking agents, preinstalled on all the appliance images and monitored in real-time by the MGC blade.
5. Blade Fusion validates (a compilation type process) the configuration of a model prior to loading it into run mode. This compilation eliminates conflicts, errors and security hazards.

Major Features and Benefits

Easy Deployment of Load-Balanced Clusters - Scalable Performance

Blade Fusion enables the central management of load-balanced clusters of applications. Blade Fusion treats the load-balancers and their multiple application nodes as a single configurable entity. Blade Fusion automatically translates macro cluster configuration changes into appropriate individual blade configuration changes while enabling consistency and reducing human errors. This provides easy performance scalability and easy configuration.

IP-X throughput scales to 8Gbps. Supported servers scale to 12 blades, each with a single or dual Intel Xeon 3.2GHz processor with up to 8GB of DDR ECC memory. IP-X offers a simple upgrade path: as more capacity is needed, a blade is added either as a replacement or an addition. IP-X automatically configures the blade and the network. IP-X technology allows as many segments as needed to run off a single firewall blade. IP-X allows clustering applications to run across multiple blades and balances the load between these clustered blades.

Central Cluster Group Management

A high-performance cluster can be created by deploying one or more blades with load-balancing instances and by deploying one or more blades with an application instance. The cluster is configured centrally and the system maintains consistent configurations of all the cluster group members to avoid human error.

If one of the cluster members fails, an automatic failover occurs and the cluster is reconstructed within minutes to full capacity performance. The failed element can simply be hot swapped with a replacement blade. The technician is not required to have any proficiency with the application, the load balancer or the hardware. The system ‘remembers’ what is missing in its running model and uses the new blade to reconstruct the full model automatically.

Health Monitoring and Automated N+1 Fail-over

Blade Fusion’s blade management system offers an innovative, low-cost and reliable failover mechanism for hardware, software and networking. Instead of dedicating a standby node for every active node and manually replicating configurations, Blade Fusion sets a pool of one or more standby blades (which could even be ‘cannibalized’ from lower priority application blades as necessary). If Blade Fusion detects a failure in hardware, application or network, it automatically initiates a standby blade with the appropriate O/S kernel and parameters, application and network settings.

The entire failover process is completed within the order of one to two minutes with no human intervention required. Only one blade is necessary to recover for multiple different blades, each running a different application with possibly a different set of network connections while preserving network switch failover capabilities.

The system can monitor one or more of the following to determine failure:

- No response for a given protocol
- No response from blade agent
- Above threshold CPU or RAM usage of processes
- Process failures
- Response or no response from a script provided by the user to monitor the application

The system can respond in one or more of the following actions:

- Shut down failed blade and launch standby blade on same instance
- Shut down failed blade and cannibalize a lower priority blade to become the failover
- Launch an older instance saved in the system to back up the running instance
- Reboot the same blade with same or previous instance
- Any sequence of above events (first, second and third responses)

Virtualization and Dynamic Management of Network Topology

Blade Fusion's blade management system enables each blade to have as many network interfaces as needed by its topology requirements. This is enabled while providing for network switch failover and while enabling the above near real-time 1 to N blade failover scheme. Moreover, network topologies can be altered and network connections can be added or removed remotely via software controls with virtually no downtime required.

Virtually No Single Point of Failure

Blade Fusion's dynamic blade image resource allocation as well as its dynamic network topology enables fast and automated recovery from application and blade failures using minimal extra hardware resources. Dynamic network topology also enables rapid recovery from network and switch failures. In addition, Blade Fusion's twin management blade scheme eliminates another single point of failure while BladeCenter's native power supply and fan redundancy eliminate yet another.

Hot-Swap Maintenance and Servicing

All in all, there is virtually no single point of failure and all failed components are automatically recovered. After a successful failover of any kind (application, blade, switch, power, etc.), restoring the system to its previous state is a simple hot swap. The technician that hot swaps the appropriate component need not have expertise. The system 'knows' how to automatically configure the newly introduced element to what it is missing and eliminates human effort and error.

All components are hot-plug enabled. A failed component is simply replaced while the system is online, and IP-X restores the system to its original state. Upgrades are also straightforward: simply add a new blade, designate it as either a replacement or a new member of a cluster, and IP-X will automatically configure it appropriately.

The Lifecycle of an Application on Blade Fusion

When installing a new application or set of applications to run on a given blade, the system allocates a version of an operating system on that blade according to the user's selection. The operating system already has a Blade Fusion agent installed. The next step is to use the application vendor's native installation process. More than one application can be installed on the blade's instance.

The user defines the names of the processes to be monitored and defines failure thresholds of various kinds. Also, the user defines start and stop commands as well as prescripts and postscripts. These scripts can contain monitoring services of various kinds that can, among other things, define application failure criteria for Blade Fusion's failover schemas.

A snapshot can be created and saved in the system as a skeleton for the future creation of duplicate instances. The system is pre-installed with best-of-breed security application skeletons but the user can add more by creating a snapshot of one of the instances.

A skeleton can be copied to become an instance that runs on a blade and several snapshots of an instance can be saved for various purposes. Therefore, a given blade may have a running instance and several saved instances that are earlier snapshots of it.

Low Downtime and Low-Risk Hardware Upgrades

Blade Fusion’s architecture enables blade upgrades with minimal downtime and little, if any risk. This is because Blade Fusion enables an automatic rollback to the system’s previous state at any time during the upgrade process. To affect a blade upgrade one can simply plug the new blade into the chassis and request the system to swap the application from the old blade to the new. The upgraded system is up and running almost instantaneously. If problems occur, a rollback to the previous state can be just as fast.

Low Downtime and Low Risk Software Upgrades

Blade Fusion’s architecture enables application and operating system upgrades with minimal downtime and little, if any risk. This is because Blade Fusion enables an automatic rollback to the system’s previous state at any time during the upgrade process. To affect a software upgrade, simply create an image copy and use regular and native upgrades. After the upgrade is performed satisfactorily offline, the appropriate blade can be reallocated to the upgraded image copy instead of the old image. The upgraded system is up and running almost instantly. If problems occur, a rollback to the previous state can be just as fast.

Managed Entities and Hierarchies and Relationships Among Entities

Each blade can run an instance of an application. This blade-instance association is the simplest resource allocation. The system also associates with that instance-blade entity a network topology, a network failover schema and an application failover schema. Older instances can also be saved as well as the original skeleton (if the instance originated from a skeleton).

A cluster group is a group of instance-blade entities of the same kind and originating from the same skeleton that also has instance-blade entities comprised of load-balancing instances. A cluster group constitutes an even larger resource allocation that involves multiple blades. A cluster group enjoys central and consistent management and configuration.

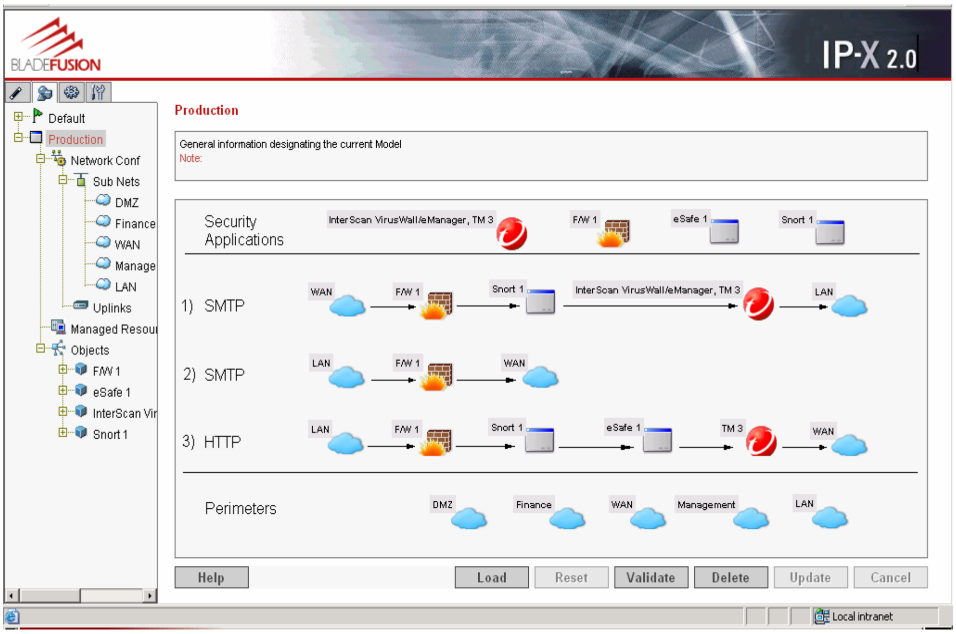
The next entity up in the hierarchy chain is the model. The model contains multiple other entities such as cluster groups and blade-instance associations of various kinds. It also contains failover pools that use same resources for the various recovery schemas of the various entities that make it up.

Each entity can be active (running) or designated to be the active (preloaded). Additional entities can be saved and those are not active and are not designated to become active.

All entities can be saved, renamed, copied and moved from one chassis to another or saved for DRP purposes. In addition, models or any other solution or subsolution can be reused and duplicated from one chassis to the next.

Consolidated Management

Configuration, including hardware, operating system, applications and network, is performed with the graphical Web-based IP-X console. IP-X orchestrates services, hardware, network configuration, topology and segments automatically.



Production

General information designating the current Model
Note:

Simple Network Topology

No wiring. The network is embedded in the blade server chassis, and IP-X controls all network settings. IP-X automates adding/editing network segments and the number of external ports per segment.

Workflow Enforcement

Each blade in the Blade Fusion architecture is equipped with a low-level network agent that is capable of performing routing and packet enforcement tasks. All such modules are activated and synchronized from a central configuration tool.

The Blade Fusion workflow enables the ability to:

- Enforce rules between two nodes in the same network segment
- Add an additional layer of security, reducing or eliminating intrusion and malicious penetration

- Enforce ‘next hop’ by MAC address
- Enforce ‘previous hop’ by MAC address (reducing or eliminating man in the middle and other threats)
- Force certain protocols to follow one and only one path among blades
- Reduce unwarranted access from one blade to the next and between the blades and the management blades
- Design and enforce deterministic network behavior from a central console

Model Replication and Rollback

A snapshot (model) can be produced with a push of a button that includes the entire configuration in a single location, including hardware, network, operating system kernel and parameters and applications and parameters. The model is used for both rollback in case of a failed upgrade and for creating instantaneous replicas of the entire gateway.

Illustration of the ‘model’ concept: If an MGC blade is swapped out of an active system and swapped into an ‘out of the box’ BladeCenter, it will replicate the entire solution of the original platform to the new one. Comment: the original box would still be fully operational, because the secondary MGC took over as soon as the primary was swapped out.

Enhanced Security Quality

IP-X offers a complete solution that enhances the quality of the gateway. Security services are all best-of-breed incorporating the most advanced and comprehensive set of features. The cohesive approach covers the entire range of services and processes of configuring the gateway, from network to blades to the operating system to applications resulting in fewer configuration errors and fewer security vulnerabilities. The unique high availability mechanism reduces many of the problems associated with failover. The ability to pretest the entire configuration before deployment and to produce exact copies of the entire gateway for replication across the enterprise slashes time to upgrade and enables a more robust and stable gateway.

Reduce Capital Costs (CAPEX)

IP-X runs on open-system blade servers available from multiple leading hardware manufacturers. These platforms are available at a fraction of the cost of proprietary security hardware while offering comparable performance. In addition, when retired, the platform may be used for other less demanding applications. Inventory is also reduced because a single type of blade can replace any failed security appliance. IP-X reduces software license costs as well because its unique high-availability scheme eliminates the need for licenses for idle standby nodes.

Reduce Operational Costs (OPEX)

IP-X reduces operational costs in all stages of the gateway's life cycle. Set up is compressed from days to minutes. The ability to replicate the gateway across multiple sites without resident experts further increases these savings significantly. Upgrades and patches are also greatly simplified and are easily replicated and distributed throughout the organization's multiple gateways. The ability to automatically roll back to a previous setting reduces the penalty of any configuration problem or error.

Reduction of Total Cost of Ownership

From all the above it is clear that Blade Fusion provides the most comprehensive solution features and qualities while dramatically reducing the cost and effort involved in owning, maintaining, upgrading and servicing mission-critical enterprise and telco solutions.

Reference Architecture Applications: Implementations with Key Security ISVs

With BladeCenter, Blade Fusion IP-X 1000 supports cluster/high availability (Active/Active or Active/Passive), load-balancing and monitoring applications such as:

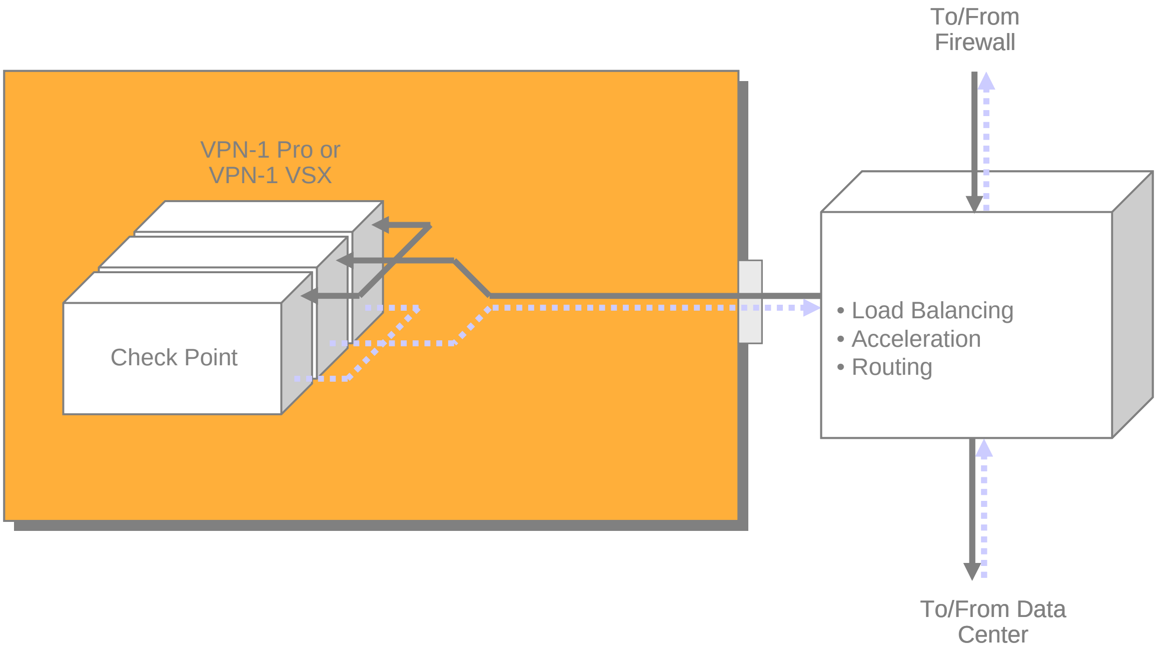
- **Firewall/VPN (FW/VPN):** Check Point VPN-1 VSX and VPN-1 Pro
- **Intrusion Detection System (IDS)**: ISS Realsecure, Snort, Enterasys Dragon
- **Antivirus (A/V):** Trend Micro, Symantec, Aladdin eSafe
- **Antispam:** Symantec BrightMail
- **Content Filtering**: WebSense
- **Generic Applications Support (GAS)**: Any application can be added.

Firewall/VPN: Check Point – High-Performance Clusters

VPN-1 Pro and VPN-1 VSX

Check Point® is a worldwide leader in securing the Internet. It is a leader of both the worldwide VPN and firewall markets and through its next-generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web-security solutions that help protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets.

One of the most popular 'models' of BladeCenter with Blade Fusion is a high-performance, session-persistent cluster of Check Point's perimeter security products, VPN-1 Pro or VPN-1 VSX. An ongoing need within enterprises and ISPs is to scale up the throughput of Firewall and VPN gateways.



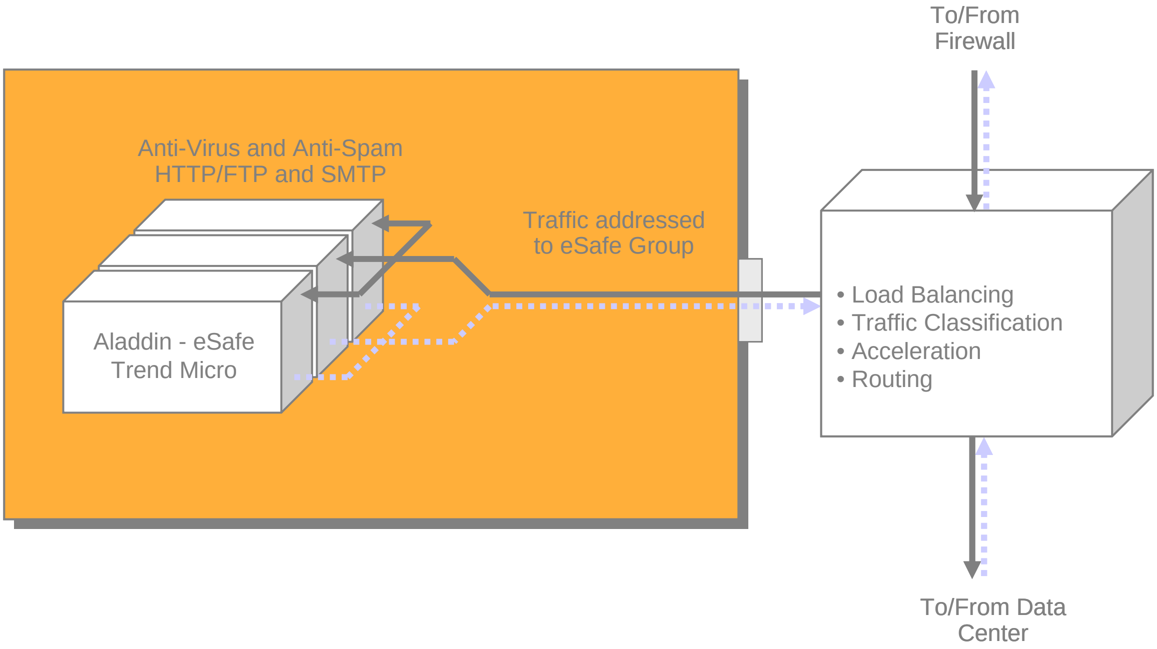
Check Point's VPN-1 Pro is a tightly integrated solution combining the market-leading FireWall-1 security suite with sophisticated VPN technologies to offer a comprehensive proactive and intelligent attack protection for the network, application and Web layers in addition to providing an easy-to-deploy and manage secure-connectivity solution The cornerstone of Check Point's Intelligent Security Solutions, VPN-1 Pro meets the demanding requirements of Internet, intranet, and extranet VPNs by providing highly secure connectivity to corporate networks, remote and mobile users, branch offices and business partners.

VPN-1 VSX is a high-speed, multi-policy security solution designed for large-scale environments like data centers and campus networks. The VSX gateway supports replacement of complex network topologies consisting of physical routers and firewall/VPN gateways. It allows multiple networks to be protected, connected to shared resources such as the Internet and DMZs, and interacts with each other safely, while providing simplified and centralized management that will result in increased flexibility and cost-savings.

Highly scalable, yet easy to manage and deploy, VPN-1 Pro and VXS help the world's largest organizations secure themselves with the world's most intelligent security solutions.

High-Performance Content Filtering (SMTP, HTTP, FTP)

The BladeCenter/Blade Fusion platform is also ideal for accelerating deep packet inspection applications such as antivirus, antispam, content filtering and intrusion detection.



Aladdin - eSafe

Aladdin is a leading provider of secure content management. It's unique 'inline' technology and traffic classification options enable high throughput for all kinds of traffic including HTTP, FTP and SMTP.

eSafe Gateway from Aladdin is a modular multi-layered content security solution that deals with all the content security aspects. eSafe Gateway integrates both mail and Web security into one solution over major Internet protocols—HTTP, FTP, SMTP and POP3.

Mail Security: eSafe Mail is a single product that combines protection against seven threats to help secure e-mail.

1. Known viruses are blocked with eSafe's fast antivirus engine. Unknown viruses and other malicious active code (ActiveX, Java) are blocked by eSafe's various proactive technologies.
2. Exploits compromised security and is used by hackers to introduce fast-spreading malicious code. eSafe helps detect and block malicious code attempts to exploit security holes.
3. Malicious code is easy to construct and spreads rapidly. eSafe proactively blocks malicious code.
4. Spam is a major nuisance, wasting time and resources. eSafe antispam software blocks the majority of spam, saving time and money.
5. Cookies can compromise privacy and encourage spam. eSafe can block cookies from untrusted sources and from all e-mail.
6. MS Office Documents can contain macro viruses as well as embedded malicious code. eSafe removes macros and embedded objects arriving from untrusted sources.
7. Hacker attacks are numerous: Denial of Service (DoS), relaying, e-mail spoofing, attachment spoofing and manipulation. eSafe provides built-in e-mail protection mechanisms.

Web Security: eSafe Web is a single product that combines protection against seven threats to secure email.

1. Super-fast HTTP and FTP scanning (30-200Mbps) is achieved through the awarded NitroInspection^{TM} inline technology
2. URL filtering for non-productive and dangerous or illegal content
3. Application Filtering, the next generation of security threats, protects from malicious code in P2P, Instant Messaging, Adware, Spyware and Unauthorized HTTP tunnelling.

Markets: eSafe flexibility provides a solution for small to medium enterprises, large corporations/organizations as well as the xSP market (ISP, MSP, ASP…). For the xSP market, eSafe poses numerous opportunities and benefits especially when powered by BladeCenter Blade Fusion:

1. New revenue stream thru new ISP-level services (new in the marketplace)

2. Beat competition and improve service/product positioning
3. High-capacity inspection
4. Scalable solution
5. Tiering—ability to offer different service levels to optimize the business model

TREND MICRO – IMSS AND IWSS

InterScan Messaging Security Suite

Trend Micro™ InterScan™ Messaging Security Suite integrates antivirus security, content filtering technology, and an antispam module on a single server-based platform. This comprehensive solution blocks malicious code, spam and unwanted content at the messaging gateway—the network's most critical entry point. With centralized policy-based management, the suite deploys a powerful, coordinated defense against mixed-threat attacks, like Bagle and Netsky. Compared to point products, this integrated suite delivers higher security with minimal cost and effort.

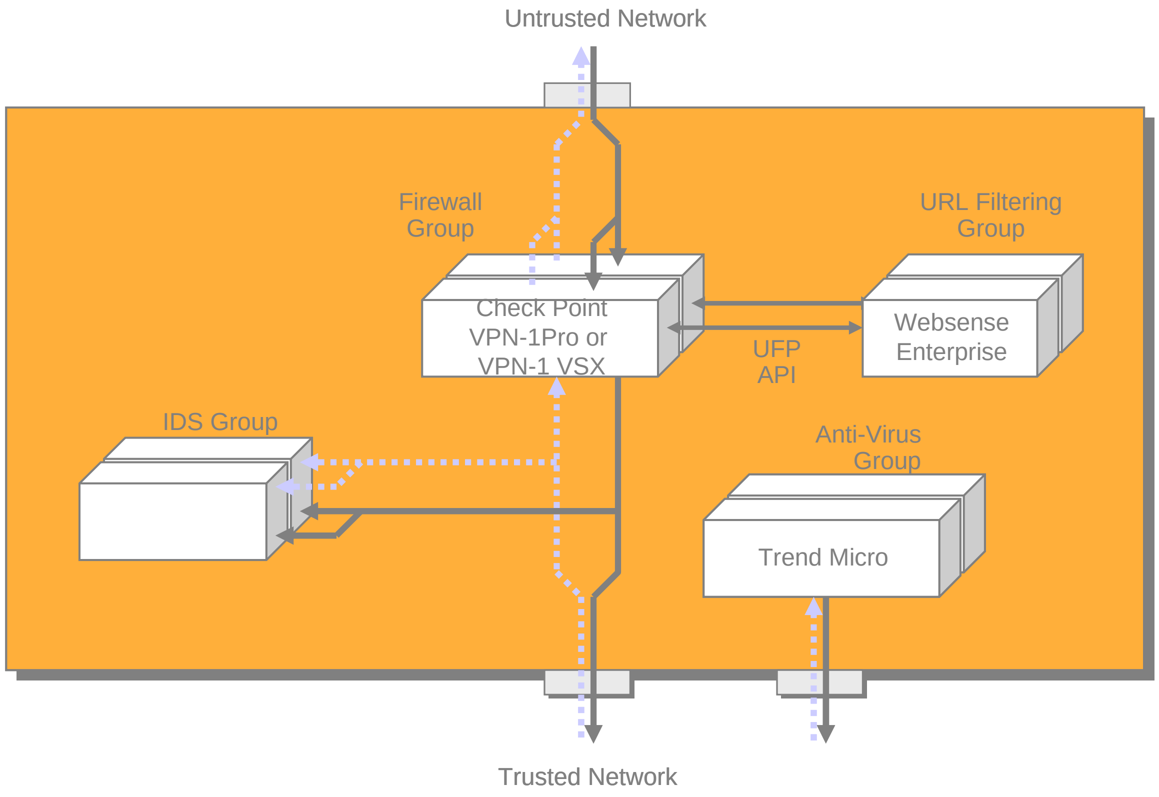
InterScan Web Security Suite

Trend Micro™ InterScan™ Web Security Suite delivers high-performance security for HTTP and FTP traffic at the Internet gateway. The suite integrates antivirus, anti-phishing, anti-spyware, and optional URL filtering technology. This comprehensive solution is designed to scan Web content and block malicious threats—without sacrificing Web performance. It is also highly flexible and scalable, even on large, complex networks. With a centralized management console, IT managers can deploy a rapid, coordinated defense against emerging threats.

Multi-Functional Security Gateways

FW/VPN clusters with IDS, Antivirus, Antispam, URL Filtering and more

One of the key advantages of the BladeCenter/Blade Fusion platform is its inherent flexibility, openness and scalability. The platform can consolidate any combination of security applications, each one of which could be in a high-performance cluster or just in active/passive high availability.



Performance and Price/Performance Advantages

No other single platform can deliver performance for best of breed security software applications like the BladeCenter/Blade Fusion platform. That's because this centrally managed multi-bladed platform combines the power of multiple Xeon powered blades in conjunction with a multi-Gigabit backplane and powerful switches and load balancers.

The BladeCenter/Blade Fusion multi-bladed security gateway appliance outperforms traditional stand-alone appliances as well as proprietary multi-bladed competitors.

Just as important as performance is price/performance. The combined BladeCenter/Blade Fusion solution is not only more powerful, it is often less expensive than competing multi-bladed appliances. As a result the price/performance advantage can be very pronounced.

Capital Expenditures (CapEx)

The BladeCenter/Blade Fusion Capex (Capital Expenditure) can be significantly lower than either competing bladed security solutions or assemblies of traditional stand-alone appliances resulting in a potentially faster return on investment. Most important of all, this ROI is achieved with little or no loss or compromise in the performance of the system which is superior to leading competitive solutions.

Operating Expenses (OpEX)

As with the capital expenditure required to purchase and begin using IP-X, the yearly operating costs for maintaining the Blade Fusion solution can also be a fraction of the cost when compared to the operating costs incurred for leading competitive solutions.

Blade Fusion's IP-X solution often costs a fraction of what other solutions cost, and yet it often delivers similar or better performance, offers more features, and relies on standards based IBM BladeCenter platform.

A Case Study

BladeCenter with Blade Fusion, Check Point Software and eSafe-based solution

Recently, a large Health Management Organization (HMO) with 1.7 million insured members, needed to streamline the process of authorization, procurement and payment clearing for insurance covered prescriptions, while improving the service given to customers, doctors and partners. To accomplish this task, the HMO decided to implement an Extranet between it and its network of doctors and partner pharmacies.

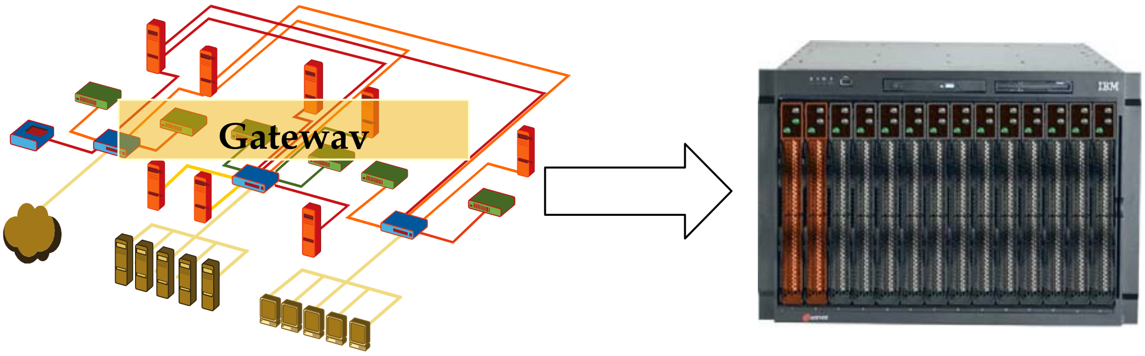
The HMO determined that the Extranet gateway should have the following features:

- Full redundancy (always active)
- Multiple layers of security (including firewall, VPN, A/V and IDS)
- High performance

Initially, the HMO investigated using traditional appliances, load balancers and switches, but found that a total of 20 devices, accompanied by an expensive integration project would be required to meet these needs. Next, the HMO investigated the BladeCenter/Blade Fusion with Check Point alternative and found that the addition of the Blade Fusion solution would dramatically reduce the total number of elements while delivering the required performance and functionality required. The upfront cost of equipment and integration was also dramatically reduced, and the ongoing cost of support and maintenance contracts was similarly found to be a fraction of the anticipated cost.

The Blade Fusion solution was quickly deployed within a single BladeCenter chassis and the fully redundant solution currently includes:

- 16 segregated network zones
- Full switch redundancy for all applications
- 1 load balanced Check Point VPN-1 VSX cluster
- 1 active/passive Check Point VPN-1 VSX cluster
- 1 Aladdin eSafe gateway A/V
- 2 Snort IDS blades (each tapping several networks)



BLADECENTER

The system requires only one standby blade that provides failover for the entire solution (n+1 high availability) and delivers hot-swap maintenance, plug-and-play scalability and near-zero downtime upgradability for software and hardware. All of these features combine to help support the solution with significantly less effort and less expertise.

The satisfied customer has used the remaining open slots to provide high availability and redundancy for additional DMZ applications that are non-security related (such as a Web server, an application server and a DNS server).

Summary

The BladeCenter/Blade Fusion-based Enterprise and Telco Network Security solution reference architecture provides an excellent roadmap to creating a tailored solution with best-of-breed security ISV applications such as Check Point, Trend Micro, Aladdin eSafe and others, with enablement layer provided by Blade Fusion. The resulting BladeCenter “Security in a Box” integration-tested solution provides an open, industry-standard-based hardware that is a cost-effective, highly available, and high-performance scalable solution—on demand.

This integrated solution delivers high performance at a fraction of the cost of competing solutions. It delivers automated performance and response monitoring, as well as systemwide automated rollback, disaster recovery, replication and auditing.

Additional Information

IBM eServer BladeCenter

www-1.ibm.com/servers/eserver/bladecenter/

BladeFusion Technologies

www.bladefusion.com/

Check Point Software Technologies Ltd

www.checkpoint.com/

Trend Micro

www.trendmicro.com/en/home/us/enterprise.htm

Aladdin Knowledge Systems

www.ealaddin.com/

Visit *www.ibm.com/pc/safecomputing* periodically for the latest information on safe and effective computing. Warranty Information: For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven or ClusterProven.

Telephone support may be subject to additional charges. For onsite labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician.
All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time without notice. IBM is not responsible for photographic or typographic errors.

This publication was developed for products and services offered in the United States. IBM may not offer the products, services or features discussed in this document in other countries. Information is subject to change without notice. Consult your local IBM representative for information on offerings available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of a specific Statement of General Direction.

The examples given in this paper are hypothetical examples of how a customer can use the products described herein and examples of potential cost or efficiency savings are not based on any actual case study. There is no guarantee of comparable results. Many factors determine the sizing requirements and performance of a systems architecture. IBM assumes no liability for the methodology used for determining the configurations recommended in this document nor for the results it provides. Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements quoted in this presentation may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this presentation may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information in this presentation concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. IBM has not tested these products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices do not include tax or shipping and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Price may include applicable discounts. Reseller prices may vary. Unless otherwise specified, pricing information is current as of original publication of this document.

MB, GB, and TB = 1,000,000, 1,000,000,000 and 1,000,000,000,000 bytes, respectively, when referring to storage capacity. Accessible capacity is less; up to 3GB is used in service partition. Actual storage capacity will vary based upon many factors and may be less than stated. Some numbers given for storage capacities give capacity in native mode followed by capacity using data compression technology.

Maximum internal hard disk and memory capacities may require the replacement of any standard hard drives and/or memory and the population of all hard disk bays and memory slots with the largest currently supported drives available. When referring to variable speed CD-ROMs, CD-Rs, CD-RWs and DVDs, actual playback speed will vary and is often less than the maximum possible.

IBM, the eight bar logo, the @server logo, xSeries, BladeCenter, Chipkill, ClusterProven, ServerProven, ServeRAID and TotalStorage are trademarks or registered trademarks of International Business Machines Corporation in the U.S. and other countries. For a list of additional IBM trademarks visit **ibm.com**/legal/copytrade.shtml.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.