The iForce™ VPN/Firewall Appliance

Powered by Sun and Check Point

Application Brief

Highlights

The iForce™ VPN/Firewall Appliance — powered by Sun and Check Point — integrates industry-leading Internet security software with the robust Sun Fire V60x/V65x rack-mount server running a hardened operating system to create a network security solution that's easy to configure, easy to manage, and easy to deploy

Financial Institutions can handle secure, high transaction workloads with high-availability configurations and also can incorporate branch offices into their core IT infrastructure

Government Organizations can use the Federal Information Processing Standards (FIPS)-certified appliance to protect internal sub-networks

Communication Companies can protect their own IT systems from intrusion, and can support customers with easy-to-deploy managed firewall services

Manufacturing Companies can integrate their supply chain through VPNs using the open Internet, reaping cost savings over leased-line connections

Retail Concerns can economically incorporate their outlets with the central office while simultaneously protecting them from intrusion

Check Point SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Re-Assessing Security Needs

Everywhere you look, organizations are re-assessing their security needs — and with good reason. Network-based security attacks are becoming commonplace, with ever more potent viruses and worms being unleashed onto the Internet.

Firewalls are a given today, and everyone understands the paradoxical need for strong perimeter security while providing secure access for remote sites and branch offices, and to partners, suppliers, and employees through Virtual Private Network (VPN) technology. VPNs help establish flexible, yet secure relationships to be established over the Internet, allowing authorized users to access internal resources with impenetrable encrypted communication, helping to eliminate the need for costly modem pools and leased-line connections.

Security at the perimeter is no longer enough. The recent SQL Slammer worm surprised companies with the swiftness of its spread throughout internal corporate networks, raising attention to the need for firewalls between corporate sub-networks and between layers in Web hosting infrastructure. In order to meet the increased need for security at the perimeter and at critical points within a company's internal networks, firewall solutions must be more cost-effective to deploy and easier to manage, especially when installed at remote locations.

Every Organization Needs Security

Every organization, regardless of industry segment, recognizes the need for both perimeter security and VPNs that support secure communication across the open Internet. Financial institutions need to protect their trading infrastructure with high-performance firewalls that can support transaction rates that don't keep their customers waiting — and they need to securely interconnect their main and branch offices. Government organizations can have large networks spread across the nation and the world — with each sub-network protected against unauthorized access. U.S. government organizations have Federal Information Processing Standards (FIPS) to guide their purchasing decisions, and they favor technology that meet their stringent qualifications. Manufacturing companies need to securely integrate their supply chains, and in today's competitive business climate, overseas communication via the Internet is the only economical choice. In addition to integrating supply chains, retail companies are faced with the need to interconnect all of their outlets into their core IT infrastructure. Communication companies and service providers must protect their own infrastructure, which is becoming increasingly Internet Protocol (IP)-based, and must also have economical, easy-to-configure, easy-to-manage, and easy-to-deploy firewall and VPN solutions for their managed service customers.

> "Today, Sun became the first major server vendor to deliver an enterprise-class dedicated security appliance."
>
> —Chris Christiansen, IDC Vice president for Security Products and Infrastructure Software

Best-of-Breed Solution

A solution that organizations of all kinds can trust is one that integrates the best hardware with the best VPN/firewall software — Sun's iForce VPN/Firewall Appliance.

The iForce VPN/Firewall Appliance is an integrated hardware and software solution that begins with the high-performance, economical, reliable, rack-mount Sun Fire V60x/V65x server equipped with up to two 2.8 GHz Intel® Pentium® III processors and up to fourteen Ethernet network interfaces, and an optional hot-swap redundant power supply for higher availability. This hardware is paired with the security solution used by 65 percent of the enterprise firewall/VPN market (Enterprise Firewall/VPN Software Market, IDC 2002) — Check Point Software Technologies VPN-1/ FireWall-1 software.

Check Point's VPN-1/FireWall-1 technology integrates access control, authentication, and encryption to help ensure the security and integrity of network connections. Security administrators can define and enforce a single, comprehensive policy that protects virtually all network resources while managing them from a central location. To meet high-availability requirements, Check Point ClusterXL software supports load-balancing and fail-over.

Server and Software Synergy

The result of this synergy between best-of-breed server and software products is a VPN/firewall appliance for new customers, companies deploying VPNs for the first time, those already using firewalls and also for those needing to upgrade their network infrastructure.

The iForce VPN/Firewall Appliance integrates with Check Point SmartCenter software, supporting central management for VPN and firewall policies. SmartCenter helps to enable integrated VPN-1/FireWall-1 management for all iForce VPN/Firewall Appliances and gateways hosted on the Solaris™ Operating System, delivering a unified management infrastructure.

All of this comes with a package that challenges the competition to meet its price/performance. Depending on its configuration, the iForce VPN/Firewall Appliance can process from 1.4 Gbps to 3.1 Gbps of network throughput, and VPN performance from 390 Mbps to 1.2 Gbps using Advanced Encryption Standard (AES) encryption.

The VPN/firewall appliance integrates the Sun Fire V60x/V6x server, network interfaces, hardware configuration GUI, and Check Point's SecurePlatform, which consists of a hardened version of the Linux operating system and Check Point's VPN-1/FireWall-1 Next Generation (NG) with Application Intelligence software (Figure 1). Helping to reduce total cost of ownership by making the VPN/firewall appliance more quick and easy to deploy, SecurePlatform takes the guesswork out of operating system hardening and software installation

Five Server Configurations

Five different server configurations available, each with a minimum of four 10/100/1000 Ethernet interfaces; at least one Intel Pentium III processor; and at least 512 MB of memory. The five different configurations are flexible enough to meet the security and performance needs of the most complex networks, with the base system augmented with one or more of the following options:

- Dual Intel Pentium III processors
- Upgrade to 1 GB of memory
- Additional dual-port Gigabit Ethernet interface card (for a total of fourteen interfaces)
- Additional hot-swap redundant power supply

Hardened Linux Operating System

Forming a solid foundation for its firewall software, Check Point's hardened, customized, and optimized Linux operating system removes unnecessary software and services, while integrating drivers for the Sun Fire V60x/V6x peripherals.

Check Point VPN-1/FireWall-1 Software

The industry's leading Internet security software, Check Point VPN-1/FireWall-1 software is pre-integrated and pre-loaded for security right out-of-the-box, ready for fast and easy deployment. One of the key benefits of the VPN/firewall appliance is the ease by which it

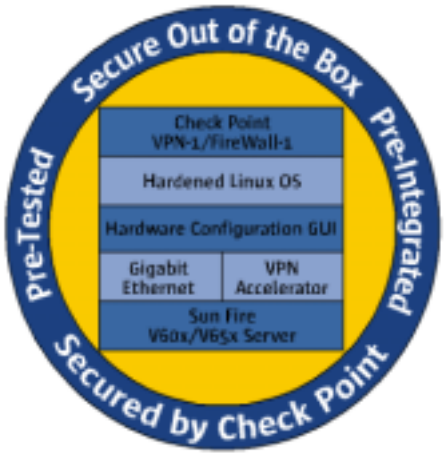

Figure 1: VPN/Firewall Appliance Components

can be managed through Check Point's SmartDashboard software, whether the appliance is located on site, at a remote office, or deployed as customer premises equipment by service providers. Features of Check Point VPN-1/FireWall-1 software include:

- One-click technologies for simple VPN deployment and management
- Patented Stateful Inspection technology for the highest levels of security
- Innovative active defense technology to detect and defend against network-based attacks
- Comprehensive, one-stop security management for maximum management ease and lowest total cost of ownership
- High availability and load sharing for transparent fail-over and increased performance
- Best-of-class performance, scalability, and flexibility
- Support for IPSec-based VPNs encrypted using AES, 3DES, DES, or CAST-40 algorithms

This extensive set of capabilities, along with Check Point's comprehensive management facilities, can be used to secure the most complex network architectures.

Certified Quality

Check Point's software has obtained SunTone℠ certification, and the iForce VPN/Firewall Appliance has undergone a rigorous testing process to obtain OPSEC "Secured by Check Point" certification. Government organizations can purchase the VPN/firewall appliance with confidence because it also has obtained FIPS 140-1 certification.

Example Architecture

Figure 2 illustrates the kinds of architectures supported by the iForce VPN/Firewall Appliance. A simplified enterprise network architecture is illustrated at the bottom of the figure (A), including an internal network containing workstations and servers and a De-Militarized Zone (DMZ) containing mail and Web servers accessible to the Internet.

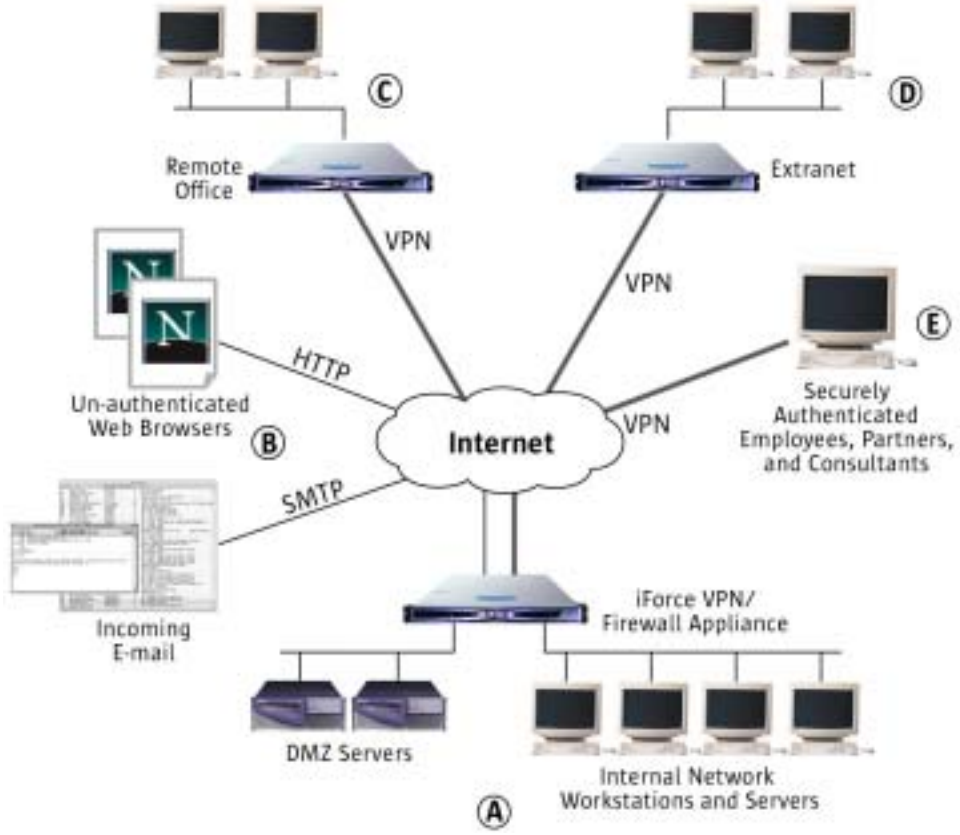

Figure 2: Example Architecture using the iForce VPN/Firewall Appliance

Firewall Features

Check Point's stateful inspection technology is used to create a firewall between the enterprise and the open Internet, allowing unauthenticated traffic from Web browsers and other mail servers (B) to reach the DMZ, and for internal systems to reach resources outside of the local network. Check Point's rich set of supported services and application proxies enable an additional layer of filtering to protect internal servers from protocol-based attacks.

Organizations of all kinds need at least this minimum level of protection, and many need significantly more of the firewall features found in the iForce VPN/Firewall Appliance. Large organizations like government agencies and communications providers need security at the perimeter, and also to control traffic between multiple internal networks to limit propagation of any successful attacks — like the SQL Slammer worm that surprised so many organizations in its ability to navigate through supposedly secure networks.

Site-to-Site VPNs

Virtual private networks can be established to link remote offices (C) with a central office, and to establish extranets (D) that link suppliers and other business partners into the company's infrastructure (Figure 2). Using Site-to-Site VPNs, external sites can operate as if directly connected to the central office, with encrypted communication secure from intrusion. Because of the low cost of Sun's VPN/firewall appliance, companies can deploy appliances within the internal networks of their suppliers, helping them to limit the scope of the extranet to only the few authorized users of company resources.

Using VPNs, financial organizations, manufacturing companies, and retail concerns

can easily and cost-effectively interconnect their core networks with their branch offices, outlets, suppliers, and contractors. With the ability to so easily integrate elements of their supply chains, those companies leveraging the power of VPNs will continue to stay ahead of the competition.

Because so many organizations depend heavily on VPNs to conduct their day-to-day business, performance is key. Fortunately, Sun has designed the iForce VPN/Firewall Appliance with several options for optimizing VPN performance — including Check Point's Performance Pack, upgrading from 1 to 2 CPUs, and utilizing the power of hardware encryption with the optional VPN Accelerator card.

Client-to-Site VPNs

There are many benefits to enabling authorized partners, consultants, and telecommuting employees to access selected services on the company's internal networks — but not all of them merit the deployment of a dedicated VPN/firewall appliance. For these situations, Client-to-Site VPNs (E) provide the same level of security offered by Site-to-Site VPNs, but instead establish encrypted connection between a single workstation and the company's local-area network (Figure 2).

Client-to-Site VPNs are key technologies for organizations needing to integrate small branch offices, single workstations at supplier sites, consultants, and telecommuting employees with high-speed broadband connections.

The low cost of Check Point's VPN-1 SecuRemote software makes it easy and cost-effective to extend an organization's network to those needing access. VPN-1 SecuRemote software implements IPSec encryption with Internet Key Exchange (IKE) that's compatible with the iForce VPN/Firewall Appliance or any other Check Point VPN-1/FireWall-1 installation.

For higher levels of security, Check Point VPN-1 SecureClient software establishes secure VPNs while protecting the client system with the same stateful inspection technology that makes the VPN/firewall appliance itself so secure.

First Line of Defense

The iForce VPN/Firewall Appliance is the first line of defense against intrusion at the network perimeter and between networks internal to large organizations. With up to two CPUs and hardware encryption acceleration, it is powerful enough to support heavy amounts of VPN traffic, helping organizations to more easily integrate their partners, suppliers, consultants, branch offices, and telecommuting employees into their enterprise networks.

The iForce VPN/Firewall Appliance offers a compelling option for financial, government, retail, and communications companies searching for low-cost, easy-to-configure, easy-to-manage, and easy-to-deploy security solutions.

What's even more compelling about Sun's VPN/firewall appliance is that it is compatible and can integrate with existing Check Point solutions, including those installed with Sun's iForce™ Perimeter Security Solution and those deployed on Sun servers running the Solaris Operating System. For organizations with investments in the Check Point SmartCenter management console, the iForce VPN/Firewall Appliance integrates virtually seamlessly, providing the utmost in network security while helping to protect existing investments.

Figure 3: The iForce VPN/Firewall Appliance

Learn more about the iForce VPN/Firewall Appliance at: sun.com/checkpoint

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** +1-800 555-9SUN OR +1 650 960-1300 **Web** sun.com

Sun Worldwide Sales Offices: Argentina: +5411-4317-5600, Australia: +61-2-9844-5000, Austria: +43-1-60563-0, Belgium: +32-2-704-8000, Brazil: +55-11-5187-2100, Canada: +905-477-6745, Chile: +56-2-3724500., Colombia: +571-629-2323, Commonwealth of Independent States: +7-502-935-8411, Czech Republic: +420-2-3300-9311, Denmark: +45 4556 5000, Egypt +202-570-9442, Estonia: +372-6-308-900, Finland: +358-9-525-561, France: +33-134-03-00-00, Germany: +49-89-46008-0, Greece: +30-1-618-8111, Hungary: +36-1-489-8900, Iceland: +354-563-3010, India: Bangalore: +91-80-2298989/2295454, New Delhi: +91-11-6106000, Mumbai: +91-22-697-8111, Ireland: +353-1-8055-666, Israel: +972-9-9710500, Italy: +39-02-641511, Japan: +81-3-5717-5000, Kazakhstan: +7-3272-466774, Korea: +822-2193-5114, Latvia: +371-750-3700, Lithuania: +370-729-8468, Luxembourg: +352-49 11 33 1, Malaysia: +603-21161888, Mexico: +52-5-258-6100, The Netherlands: +00-31-33-45-15-000, New Zealand: Auckland: +64-9-976-6800, Wellington: +64-4-462-0780, Norway: +47 23 36 96 00, People's Republic of China: Beijing: +86-10-6803-5588, Chengdu: +86-28-619-9333, Guangzhou: +86-20-8755-5900, Shanghai: +86-21-6466-1228, Hong Kong: +852-2202-6688, Poland: +48-22-8747800, Portugal: +351-21-4134000, Russia: +7-502-935-8411, Saudi Arabia: +9661 273 4567, Singapore: +65-6438-1888, Slovak Republic: +421-2-4342-94-85, South Africa: +27 11 256-6300, Spain: +34-91-596-9900, Sweden: +46-8-631-10-00, Switzerland: German: 41-1-908-90-00, French: 41-22-999-0444, Taiwan: +886-2-8732-9933, Thailand: +662-344-6888, Turkey: +90-212-335-22-00, United Arab Emirates: +9714-3366333, United Kingdom: +44-1-276-20444, United States: +1-800-555-9SUN OR +1-650-960-1300, Venezuela: +58-2-905-3800