High Security at Low Cost with the iForce™ VPN/Firewall Appliance Powered by Sun and Check Point

A White Paper
August 2003

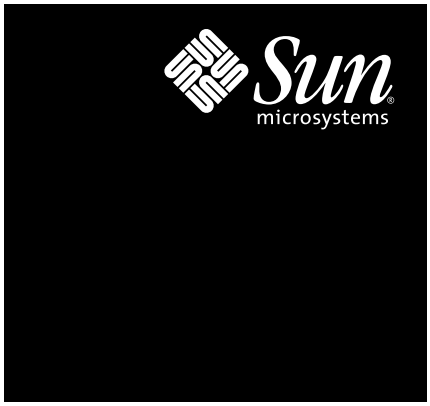


Table of Contents

Chapter 1

Introduction

Internet-based probes and attacks are a fact of life on today's networks. According to a CNET News report ("Worms boost cyberattack stats for 2003," April 3, 2003), Internet Security Systems found the number of security events detected by companies were up 84 percent during the first quarter of 2003 compared to the previous quarter, an increase attributed to more worms and automated attack software. Indeed, the increasing number of un-protected home computers using "always on" broadband connections provides a pool of easily-compromised systems that can be used as unwitting accomplices in carefully-crafted denial-of-service attacks that can bring corporate networks to their knees.

IT organizations understand the need for strong perimeter security, implemented via firewalls that are configured to inspect and filter both incoming and outgoing traffic. Virtual Private Networks (VPNs) have become a well-known tool to enable authorized, encrypted traffic to cross the Internet, making it possible to connect enterprise networks with remote sites and systems including suppliers, partners, consultants, and travelling or telecommuting employees — all without incurring the costs of leased-line connections or dial-up modem pools. In today's cutthroat economy, however, IT departments are being stretched thin as they are required to combat increasingly-sophisticated network attacks with less staff and reduced capital budgets.

The successful attack perpetrated by the Sapphire/SQL Slammer worm in January 2003 made IT organizations acutely aware of how much more attention they must pay to network security. The Sapphire/SQL Slammer worm was so virulent that the number of servers affected doubled every 8.5 seconds, and in only 10 minutes it had infected 90 percent of the Microsoft SQL servers that were vulnerable (Cooperative for Internet Data Analysis, www.caida.org). The worm's potency

 ©2003 Sun Microsystems, Inc.

surprised companies around the world as its propagation clogged enterprise networks and brought banking networks and ATM systems to their knees. The SQL Slammer worm served as a warning to many organizations that had a single vulnerable system at their network perimeter which in turn successfully attacked servers across their internal networks with astonishing speed. The SQL Slammer worm demonstrated that perimeter security is not enough, highlighting the need for improved security *within* enterprise networks, including traffic control between organizational subnets and between layers in Web-hosting architectures.

Reducing Total Cost of Ownership

Yet how do IT organizations increase the level of security despite their dwindling budgets? They do so with an eye on total cost of ownership — including the cost to configure, deploy, and manage their security systems. The iForce™ VPN/Firewall Appliance Powered by Sun and Check Point integrates best-of-breed solutions from Sun Microsystems and Check Point Software Technologies to create a secure out-of-the-box solution that is easy to configure, easy to deploy, and easy to maintain, making it easier and less costly for IT organizations to deploy additional firewalls in their enterprise networks and to upgrade the firewalls they already have.

The iForce VPN/Firewall Appliance — Powered by Sun and Secured by Check Point — combines the reliable, low-cost Sun Fire™ V60x/V65x server with a hardened operating system and the firewall technology used by 65 percent of the enterprise market — Check Point VPN-1/FireWall-1 software (Enterprise/Firewall/VPN Software Market, IDC, 2002). Using the appliance model, IT organizations can perform initial configuration over the network, without attaching a keyboard and monitor to the appliance; they can configure all of their Check Point software-based firewalls from a single console, regardless of their location; and they can centrally monitor and manage them once deployed. The iForce VPN/Firewall Appliance provides a low-cost solution for stretched IT organizations without compromising performance, flexibility, or availability. The appliance supports up to 2 Gbps of network throughput with up to eight Ethernet interfaces, and can be configured in high-availability configurations using load-balancing or fail-over techniques.

With the iForce VPN/Firewall Appliance, financial organizations can protect their trading infrastructure while maintaining the high transaction performance that their customers expect. They can securely interconnect their branch and main offices without incurring the cost of leased-line connections, and they can deploy systems remotely and mange them centrally. Government organizations, with large networks spread across the nation and the world, can use the appliance at their network perimeter and also between organizational subnets, making it difficult for attacks like the Sapphire/SQL Slammer worm to propagate. Manufacturing companies can use VPNs to integrate their supply chain, stepping ahead of the competition by using the Internet, rather than leased lines, to securely exchange orders, production status, and shipping information. Retail organizations can securely integrate their outlets into their core IT infrastructure with a low-cost, easy-to-deploy solution that doesn't require on-site maintenance. Communication companies can protect their increasingly Internet Protocol (IP)-based infrastructure, and communication service providers can use the iForce VPN/Firewall Appliance as customer-premises equipment that supports managed security with high performance and low cost.

This white paper provides a technical overview of the iForce VPN/Firewall Appliance. It presents solution architectures that can be used to support scenarios such as those outlined above, and it provides technical details on the product's features including hardware configuration options and software features.

Chapter 2

Product Overview

The iForce VPN/Firewall Appliance helps lower total cost of ownership with a system that is pre-integrated, pre-tested, and secure out-of-the-box — resulting in a solution that is easy to configure, deploy, and maintain. Customers don't have to configure CPUs, memory, network peripherals, or locate appropriate drivers because the integration is complete and from a single source. The hardened operating system comes pre-installed, saving time and also the possibility of errors in the hardening process. Check Point VPN-1/FireWall-1 software is pre-installed, and desired features are simply enabled or disabled through Check Point's licensing mechanism, eliminating the need to install additional software. Finally, a Web-based hardware configuration interface is pre-installed, making it easy for administrators to perform initial configuration without needing a directly-attached monitor and keyboard.

Pre-Integrated Stack

The iForce VPN/Firewall Appliance is built from the server platform on up through the software stack with best-of-breed technology from both Sun Microsystems and Check Point (Figure 2-1)

Sun Fire V60x/V65x Server

The foundation for the iForce VPN/Firewall Appliance is the low-cost, high-performance, reliable, rack-mount Sun Fire V60x/V65x server. Depending on the appliance configuration purchased, the server is equipped with up to two 2.8 GHz Intel Pentium III processors, 512 KB Level 2 ECC cache, either 512 MB or 1 GB of main memory, and an redundant power supply option for those requiring higher availability. These servers are data center ready with its rack-mount form factor, and both front and rear status LEDs.

©2003 Sun Microsystems, Inc.

The iForce VPN/Firewall Appliance

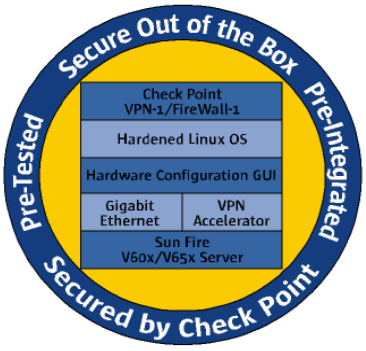


Figure 2-1: The iForce VPN/Firewall Appliance's hardware and software stack is pre-tested, pre-integrated, and is secure out-of-the-box.

Network Interfaces and Peripherals

The Sun Fire V60x/V65x server has two on-board 10/100/1000 Mbps Ethernet ports. Depending on the desired configuration, the additional PCI slots can be equipped with additional dual 10/100/1000 Mbps Ethernet interface card (for a total of four to fourteen ethernet ports)

Hardware Configuration GUI

Available first on the iForce VPN/Firewall Appliance is Check Point's Web-based interface for initial configuration, including interface IP addresses and netmasks. With the hardware configuration GUI, customers can perform initial appliance configuration, then use Check Point's SmartDashboard to establish VPN and firewall rules, or use Check Point's SmartCenter management software to configure and manage a number of appliances or other Check Point firewall installations from a single location.

Hardened Linux Operating System

Check Point's SecurePlatform software incorporates both a hardened version of the Linux operating system and Check Point's VPN-1/FireWall-1 Next Generation (NG) software into a single package. Check Point takes a version of Linux and eliminates unnecessary components and services to reduce the chance of firewall mis-configuration that could result in an operating system intrusion. Check Point then integrates drivers for the Sun V60x/V65x server components and peripherals, and optimizes the system for performance. This process, carefully audited by Check Point's security experts, eliminates manual, error-prone operating system minimization and hardening, reducing administration time and increasing security and performance.

Check Point VPN-1/FireWall-1 Software

Check Point's VPN-1/FireWall-1 software is the leading Internet security software, combining both firewall and VPN capabilities in a single product. Because Sun's iForce VPN/Firewall Appliance incorporates Check Point's flagship security suite, the appliance is completely compatible with existing Check Point firewalls, including software installations on Solaris™ Operating System servers, firewalls installed with Sun's iForce™ Perimeter Security Solution, and even Check Point systems running on competitors' platforms. Because of the flexibility afforded by this level of compatibility, organizations can deploy new firewalls with the assurance that they will be compatible with any future Check Point software purchases; they can upgrade their technology with the iForce VPN/Firewall Appliance, and they can add firewalls to their existing infrastructure and manage them all from a central Check Point SmartCenter management console.

Customers deploying Check Point security solutions have additional assurance that the software and the appliance has been carefully examined and certified by a number of different organizations. Check Point's software has obtained SunTone^{SM} certification, and the iForce VPN/Firewall Appliance has undergone a rigorous testing process to obtain "Secured by Check Point" certification. Government organizations can purchase the VPN/firewall appliance with confidence because it has obtained FIPS 140-1, ICSA, NSA, and E3 certification.

Check Point's VPN-1/FireWall-1 software helps organizations secure their network perimeters from intrusion, control traffic flow between different internal subnets, and also between layers in e-commerce architectures, for example between Web and application servers, and between application and database servers. Through virtual private networks, companies can interconnect networks at their main offices with branches, outlets, and establish extranets within the networks of partners and suppliers, all using secure, encrypted communication over the Internet. Client-to-Site VPNs enable authorized suppliers, consultants, partners, and travelling or telecommuting employees to securely connect to enterprise networks using a single workstation. Highlights of Check Point's VPN-1/FireWall-1 software include the following:

- Patented Stateful Inspection and Application Intelligence technology for the highest levels of security
- One-click technologies for simple VPN deployment and management
- Content-filtering capabilities that can be used to protect users from undesirable Web content, malicious ActiveX components, and viruses.
- Innovative active defense technology to detect and defend against network-based attacks
- OPSEC framework that enables third-party products like sophisticated virus scanners to integrate with the firewall's packet-filtering functions
- SmartMap, providing an intuitive, graphical representation of the security environment
- Comprehensive security management to minimize administrator time and reduce total cost of ownership
- High availability and load-sharing configurations for transparent fail-over and increased performance
- Support for IPSec-based VPNS encrypted using AES, 3DES, DES, and CAST-40 algorithms

©2003 Sun Microsystems, Inc.

Chapter 3

Solution Architectures

The iForce VPN/Firewall Appliance is built to serve the needs of a number of different industries, including financial, government, health care, communications, manufacturing, and retail organizations. Each industry — indeed each company within an industry — has unique security requirements that can be addressed using the wide range of features supported by the VPN/firewall appliance. From a network architecture perspective, however, most solutions derive from one or more of three basic VPN/firewall configurations:

- Perimeter security configurations control network traffic in and out of enterprise networks, and between internal networks, for example between organizational subnets and between layers in a Web services infrastructure.
- Site-to-Site VPNs help organizations securely extend their networks over the open Internet from a central enterprise network to remote networks at branch offices, retail outlets, trading centers, and to networks within supplier and partner companies.
- Client-to-Site VPNs make it possible for companies to allow individual client systems — ranging from home PCs to IP-enabled PDAs — to securely connect to an enterprise network and access services to which they are authorized. Client-to-Site VPNs help companies integrate supply chains, provide access to business partners including law firms, marketing organizations, and consultants, and they allow traveling or telecommuting employees to access resources like e-mail and internal Web sites as if they were on the corporate network.

This chapter provides examples of these three basic network architectures and how they can be used to create unique solutions that meet challenging security requirements.

©2003 Sun Microsystems, Inc.

Perimeter Security

Every organization connected to the Internet must provide for perimeter security, and firewalls are the primary mechanisms used to control network traffic between internal networks and the Internet. Firewalls are typically deployed as a central point of control through which all traffic to and from the Internet pass. They are most often configured to allow specific protocols to pass to and from a De-Militarized Zone (DMZ) containing servers accessible to the outside world, including Web and mail servers. They allow systems on internal networks to access services outside the organization, carefully filtering return traffic so that only responses to previous requests can return from the Internet to internal systems. Good practices dictate that both internal networks and the DMZ use ingress and egress filtering so that in the event that security on an individual system is compromised, it can't pass arbitrary traffic out to the Internet or to other servers.

Good firewalls, like the iForce VPN/Firewall Appliance, provide features that help organizations to make their networks much more secure than those using less sophisticated products. Firewalls implementing stateful packet inspection not only filter based on packet headers. They look into packet contents down to the application level, so that responses inconsistent with a previous request are dropped, making it difficult to compromise applications. Check Point's patented Stateful Inspection technology included in the iForce VPN/Firewall Appliance is so sophisticated that in most cases it eliminates the need for application proxies. In some cases, however, application proxies can provide extraordinary features — for example Check Point VPN-1/FireWall-1 software incorporates a Secure Socket Layer (SSL) proxy that allows the firewall to act as the endpoint of SSL connections from authorized users, enabling internal resources like Web sites to be securely accessed without clients installing VPN software.

Good firewalls support network address translation, enabling organizations to use internal IP addressing schemes that best support their needs, and which obscure internal addresses from potential intruders. They can be used to keep malicious content like worms and viruses from entering internal networks, and they can restrict access to external resources like pornographic Web sites. In the event that malicious activity is detected, the VPN/firewall appliance can automatically respond by denying all access from the offending source IP address. or terminating TCP connections that are established as part of a denial-of-service attack.

Finally, good firewalls are scalable, making it easy for organizations to deploy configurations that handle the maximum amount of expected network traffic without impacting performance. They support high-availability configurations so that single component failures don't impact application availability. They are easy to configure, easy to deploy, and can be securely managed from anywhere within the organization.

It should come as no surprise that the iForce VPN/Firewall Appliance provides all of the features described above, and many more, providing organizations with a secure, high-performance, scalable, and low cost-of-ownership product that can be deployed not only at the network perimeter but within enterprise networks as well.

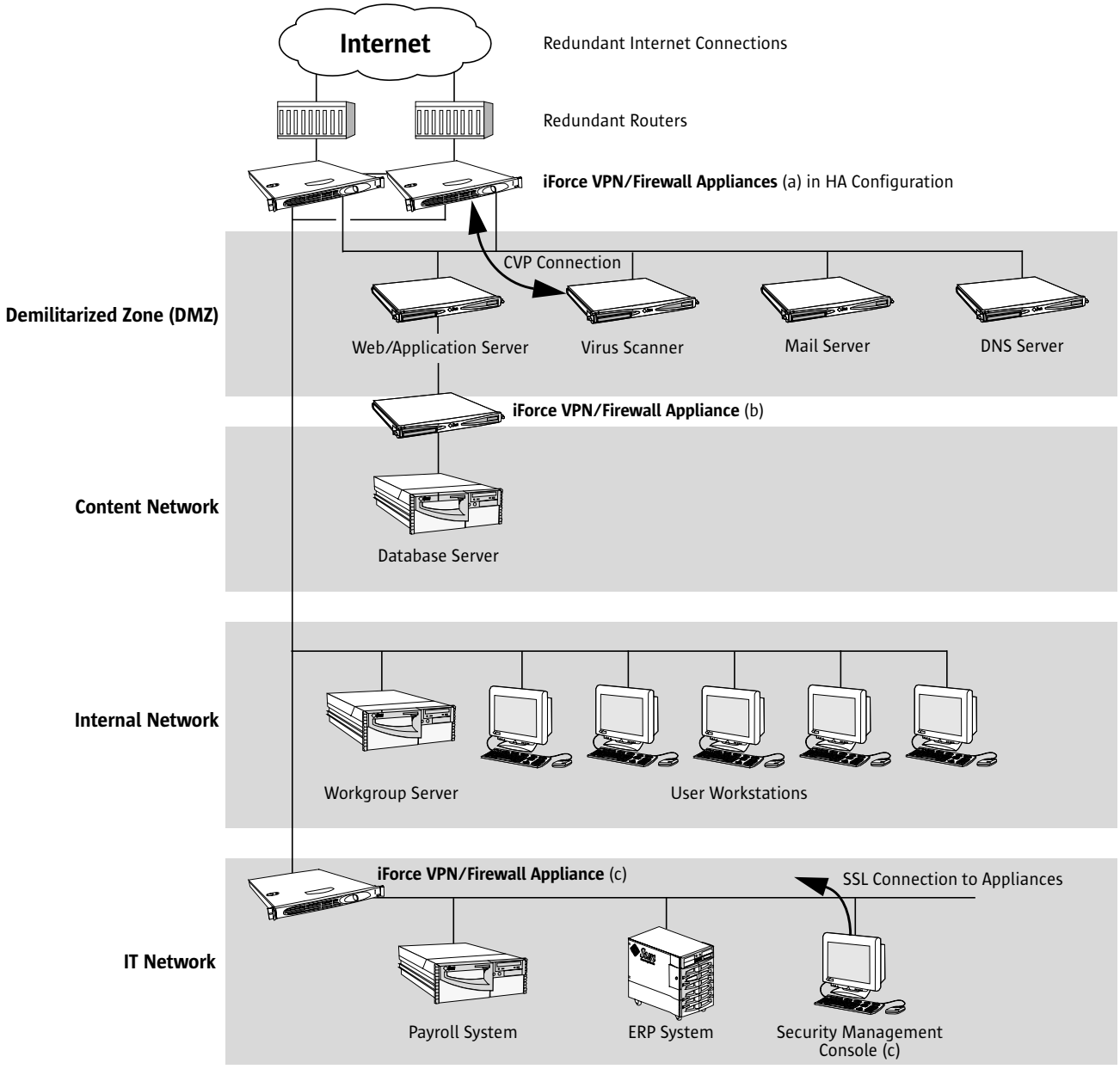
Since most IT organizations are familiar with Check Point's firewall capabilities including stateful packet inspection and network address translation, the following section describes a simplified enterprise network architecture and illustrates some of the more sophisticated features that come from combining high-quality servers like the Sun Fire V60x/V65x server with best-of-breed software like Check Point's VPN-1/FireWall-1 software.

Example Perimeter Security Architecture

Figure 3-1 illustrates the basic components of a typical enterprise network:

- Dual redundant Internet connections enable the organization to provide services to its Web site customers independent of the failure of a single connection.
- A DMZ is used to host publicly-accessible servers like the organization's Web, mail and DNS servers. An organization concerned with high availability would have multiple servers for each function, not shown in this example diagram.
- A content network stores catalog, order, and customer profile information for controlled use by the Web server. Many Web server configurations use an additional tier for an application server, illustrated fully in Figure 4-1 on page 18.
- An internal network represents one of many such networks used to host internal workstations and workgroup servers used by employees.

Figure 3-1: Example enterprise network architecture.



©2003 Sun Microsystems, Inc.

- A separate network for the IT organization hosts business-critical servers like the company's payroll and Enterprise Resource Planning (ERP) systems, as well as a central console used to manage firewalls throughout the organization. These systems are maintained on a separate, network that even employees on the internal network cannot access.

VPN/Firewall Appliance Deployment

There are a total of four iForce VPN/Firewall Appliances deployed in the example perimeter security architecture: two that form a high-availability Internet gateway for the organization; one that protects layers within the Web application infrastructure; and one that protects systems in the IT organization from intrusion even from internal sources. These systems can be managed using a single SmartCenter management console.

High-Availability Internet Gateway (a)

The enterprise Internet gateway is configured with two iForce VPN/Firewall Appliances in a high-availability, load-sharing configuration. Check Point ClusterXL technology distributes traffic between redundant gateways so that computing capacity may be combined to increase maximum throughput — thus utilizing the total throughput possible for the organization's multiple Internet connections. In the event that any VPN/firewall appliance becomes unreachable, all connections are re-directed to a the second server without interruption. For organizations with geographically-distributed operations, a Multiple Entry Point (MEP) configuration can be established using State Synchronization technology to allow client connections to fail-over from one site to another in the event that one location becomes inaccessible.

The Internet gateway filters all traffic that passes between the Internet and the organization's multiple internal networks. Using Check Point's patented Stateful Inspection technology, protocol-based attacks are prevented because the state of each network connection is maintained and any invalid packets are dropped. If the gateway detects an attack-in-progress, Check Point's SmartDefense software can take automatic, pre-programmed countermeasures.

In addition to Check Point's own client software, organizations wishing to provide clientless, secure, remote access to Web-based applications, for example Web-based e-mail, Check Point's SSL proxy can be configured as the end-point for secure Web browser connections to the mail server, handling user authentication and freeing the mail server from the heavy encryption workload that SSL connections impose.

Check Point's Open Platform for Security (OPSEC) defines protocols and interfaces that enable third-party software developers to integrate their services into the perimeter security packet flow. The example network architecture illustrates the use of OPSEC's Content Vectoring Protocol (CVP) to pass incoming mail messages through a virus scanning server before delivering them to the mail server. Sophisticated systems like Trend Micro's InterScan VirusWall can be used to detect viruses and worms hidden in e-mail attachments, removing them before they can do damage to an organization's internal systems. Trend Micro's product is installed as part of Sun's iForce Perimeter Security Solution, which can also integrate the iForce VPN/Firewall Appliance into enterprise networks.

For more information on using virus scanning technology with Check Point software-powered firewalls, please refer to the Sun White paper entitled: Secure on Sun: the iForce Perimeter Security Solution.

Protecting Valuable Assets (b)

Most Web-based applications like e-commerce sites are implemented using multiple architectural layers, including front-end Web servers, application servers, and database servers. The back-end database often contains a company's crown jewels, including product catalogs, photographs,

pricing, customer information such as names, addresses, and credit card information, and order status and contents. Many companies realize that some of their most valuable information is contained in these databases yet fail to adequately protect them — a fact testified to by the unexpected success of the Sapphire/SQL Slammer worm in January 2003.

Figure 4-1 on page 18 illustrates a more fully-populated Web application infrastructure.

The simplified Web services infrastructure illustrated in Figure 3-1(b) shows how the iForce VPN/Firewall Appliance can be interposed between layers to enable only authorized traffic between them, preventing any successful intrusion into one layer from penetrating to the layers underneath. In the example shown, Web and application server software is hosted on a single front-end server, with the back-end database protected by a firewall appliance. In production settings, Web and application servers are separated and horizontally scaled for performance and availability, with database servers clustered so that data services don't become unavailable. Fully-developed sites like these beg for the performance and high-availability features of the iForce VPN/Firewall Appliance to protect the various layers from intrusion, and the company's crown jewels from compromise.

Protecting Sensitive Internal Systems (c)

It has been long known that the majority of successful security compromises actually come from internal sources, whether they are intentional (for example, a disgruntled employee), or unintentional (a well-meaning employee connects a virus-infected laptop into the internal network). Regardless of the source, organizations understand the need to separate security domains into multiple subnets, each with their own access rules. For example, an organization with sales, marketing, and engineering networks might allow traffic between the marketing and sales organization, but significantly limit access to the engineering network where secret new product designs are stored.

The example architecture shows an access-restricted network for the IT organization, where sensitive applications like payroll and ERP are hosted. A separate iForce VPN/Firewall Appliance is used to protect this network, allowing limited outbound traffic, and only allowing authorized clients of the payroll and ERP systems to access them.

Centralized Management (c)

One of the key benefits of the iForce VPN/Firewall Appliance is that any number of appliances can be configured, managed, and monitored from one central point, along with any existing implementations of Check Point VPN-1/FireWall-1 software on Sun servers or even those from Sun's competitors. SmartCenter is Check Point's flagship management solution and is comprised of an intuitive dashboard that enables administrators to centrally define VPN, firewall, and Quality-of-Service (QoS) policies, and a management server that stores and distributes these different elements of a company's security policy. It provides administrators with an enhanced understanding of distributed security deployments. This is combined with automatic policy distribution to deliver greater control, improved security, and enhanced ease of use.

In the example architecture, the Security Management Console (c) hosts Check Point SmartCenter software, and can configure, manage, and monitor iForce VPN/Firewall Appliances throughout the organization, regardless of their location. Check Point's management software connects to the various appliances through SSL connections that are authenticated using standard X.509 certificates for virtually impenetrable security.

©2003 Sun Microsystems, Inc.

Virtual Private Networks

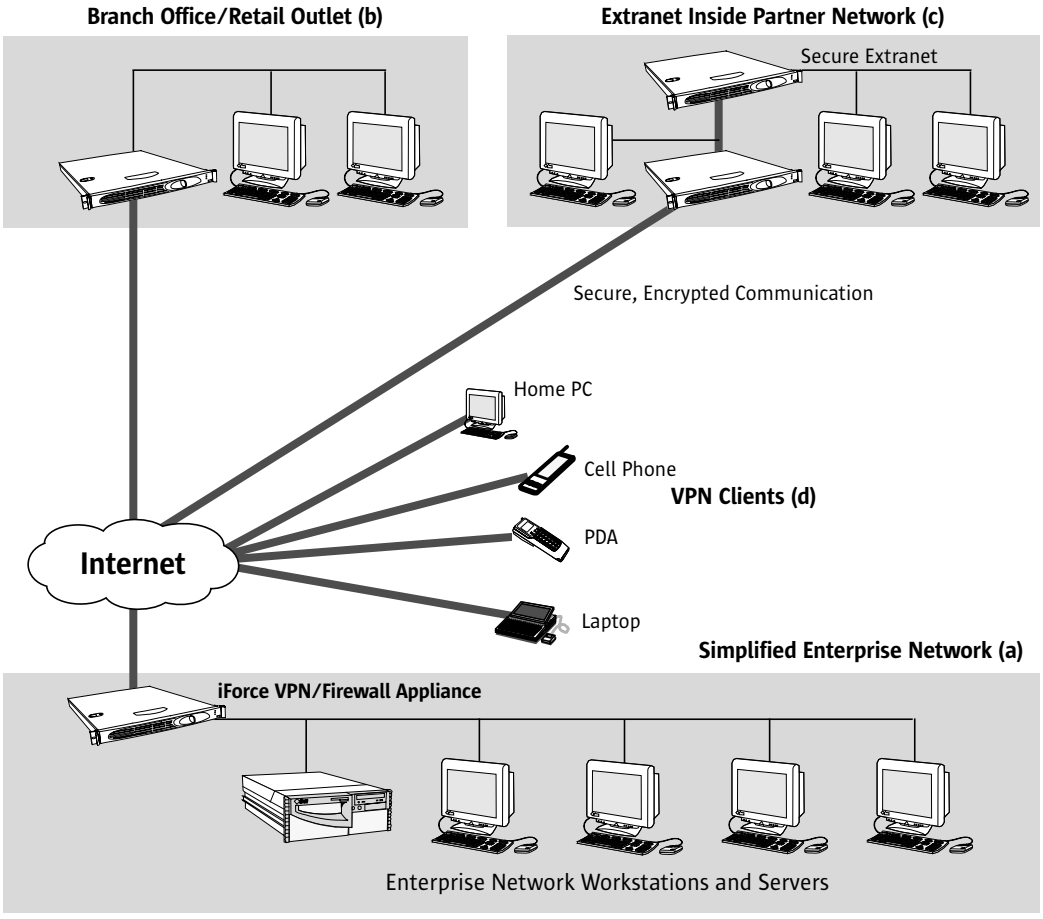
Virtual private networks make it possible for organizations to interconnect with geographically dispersed networks and individual clients using secure, encrypted communication over the Internet. In addition to saving the cost of maintaining modem pools or leased-line connections, it could be argued that VPNs are even more secure because even if the packet stream is intercepted, an intruder would have to break strong encryption in order to view packet contents.

The iForce VPN/Firewall Appliance integrates access control, authentication, and encryption to guarantee the security of network connections, the authenticity of local an remote users, and the privacy and integrity of data communications. The appliance supports Rijndael Advanced Encryption Standard (AES), DES, 3DES, DES-40, and CAST-40 algorithms, and can support both Site-to-Site VPNs and Client-to-Site VPNs.

The use of strong authentication techniques is important to prevent unauthorized clients from connecting to an enterprise network, and the iForce VPN/Firewall Appliance supports authentication through X.509 certificates, pre-shared secrets, Internet Key Exchange (IKE), RADIUS, TACACS/TACACS+, two-factor tokens, user name and password, and S/Keys.

Figure 3-2 illustrates how virtual private networks can be used to connect a simplified enterprise network (a) with branch offices and retail outlets (b), create extranets within partner companies (c), and connect VPN client systems anywhere on the Internet (d).

Figure 3-2: Example VPNs including Site-to-Site and Client-to-SIte configurations



Site-to-Site VPNs

Site-to-Site VPNs can be used to extend an enterprise network to remote offices, branch offices, retail outlets, and to secure, private networks within client companies. Terminating VPNs at the firewall is an optimal solution because the security and privacy of encrypted communication can be combined with the packet-filtering capabilities of the firewall to allow branch offices or partners to access only specific internal servers. For example, a branch office might be allowed to access internal Web and mail servers, and an order-entry system, but not the workstations in the marketing department. Likewise, clients within a partner company might be able to access an ERP system giving them sales projections so that they can plan their production appropriately, but deny access to all other internal servers.

VPNs provide a superior solution not only because of the cost savings compared to leased-line charges; deployment can take place quickly and easily, without the logistical issues of setting up dedicated lines, for example between a manufacturer in China and a home office in Europe. Performance is often an issue with VPNS, as encryption overhead can significantly reduce throughput — this is not an issue with the iForce VPN/Firewall Appliance. Capable of handling between 212 Mbps and 640 Mbps of VPN traffic using AES encryption, the appliance can be outfitted with features to optimize VPN performance for the task at hand, delivering needed performance at minimal cost. The iForce VPN/Firewall Appliance can be configured with options including Check Point's Performance Pack, up to two Intel Pentium III processors, and a hardware VPN accelerator card.

Figure 3-2 illustrates two configurations for client-to-site VPNs, each of which interconnect with the simplified enterprise network shown in Figure 3-2(a).

Branch Office/Retail Outlet (b)

For businesses with branch offices or retail outlets placed around the country or around the world, a single iForce VPN/Firewall Appliance can be used to support VPN traffic to the enterprise network and also to control network traffic to/from the Internet. With both functions incorporated into a single easy-to-deploy and easy-to-manage appliance, organizations can minimize their cost of ownership while providing maximum protection to systems within their remote offices.

Figure 3-2(b) illustrates a branch office or retail outlet with a single iForce VPN/Firewall Appliance acting as both an Internet gateway and the end-point for VPN connections. All network traffic bound for the enterprise network is encapsulated into an encrypted VPN tunnel, while network traffic bound for the Internet is controlled by the appliance's firewall capabilities, as described in "VPN/Firewall Appliance Deployment" on page 10.

This architecture makes the branch office operate as if it were part of the enterprise network. Subject to filtering rules, workstations at the branch office/retail outlet can access services in the enterprise network securely and privately. In addition, the appliance can be configured, managed, and monitored from a central location, reducing, and sometimes eliminating the need for on-site security administration.

Extranet Inside Partner Network (c)

In some cases, a company might want to have only a specific set of workstations or servers connected to the enterprise network through a VPN. This can be the case where some workstations in a partner or supplier company need to be able to access the enterprise network, but where other systems should have no access. It can also be the case in a retail outlet, for

©2003 Sun Microsystems, Inc.

example where networked point-of-sale terminals should have no access to the enterprise network, but where the manager's office should. Placing a VPN/firewall appliance inside the remote network provides additional security, and can be used to more strictly limit access.

Figure 3-2(c) illustrates a secure extranet supporting two workstations within a partner network. A single workstation not able to use the VPN is illustrated, and typically would represent the majority of systems in the remote network.

The iForce VPN/Firewall Appliance is an excellent tool for implementing such a secure network within a remote office or a partner's corporate network. Because it is secure out-of-the-box, an appliance can be configured at the company's home office and simply shipped to the partner or supplier for installation on their internal network. Once access is established for authorized workstations, the appliance can continue to be configured, managed, and monitored from the enterprise network, establishing a trusted, and secure extranet.

Client-to-Site VPNs

The need for secure remote access is not limited to networks; remote IP-enabled devices ranging from home PCs to cell phones and PDAs need to have secure access to resources in the enterprise network:

- Companies need to provide secure remote access for partners, suppliers, and consultants where only a single workstation is required to have access, and where traffic volume and required performance does not justify the use of a dedicated VPN/firewall appliance.
- Organizations with many small branch offices — a coffee shop chain, for example — need to allow remote access to specific internal systems, but from only a single remote workstation in each outlet.
- With home broadband connections on the rise, telecommuting employees can be even more productive with secure remote access to their company networks, accessing e-mail, Web, and file servers as if they were in the home office.
- Travelling employees often need to access internal systems from whatever IP-enabled device they have, whether it's a PDA, hand-held computer, laptop, or even a PDA software-enabled cell phone.

A set of potential VPN clients are illustrated in Figure 3-2(d). VPN access for devices anywhere on the network can be established a choice of several client software packages that are compatible with the iForce VPN/Firewall Appliance.

Check Point VPN-1 SecuRemote Clients

Check Point VPN-1 SecuRemote software is included with the iForce VPN/Firewall Appliance at no extra cost. VPN-1 SecuRemote software establishes an IPSec-based VPN tunnel between Microsoft Windows systems and a iForce VPN/Firewall Appliance using the same strong encryption capabilities as Check Point's Site-to-Site VPN technology. VPN-1 Client for Macintosh provides the same level of security for Apple Macintosh clients.

Check Point VPN-1 SecureClient Software

Check Point VPN-1 SecureClient software extends VPN-1 SecuRemote features with a centrally-managed personal firewall, Secure Configuration Verification and advanced management. Available at additional cost, VPN-1 SecureClient helps IT organizations to lock down systems

attached to their networks via VPN so that they cannot be used as a means to compromise security of the enterprise network itself.

In addition to supporting Microsoft Windows, Apple Macintosh, and Linux clients, VPN-1 SecureClient software also supports Microsoft Pocket PC 2002 and Handheld PC 2000-based handheld computers and PDAs.

Client-less VPNs

For individual client systems requiring access only to Web applications like Web-based e-mail, internal Web sites, or Web-based interfaces to enterprise applications, 'client-less' VPNs can be established between an SSL-enabled Web browser and a iForce VPN/Firewall Appliance.

©2003 Sun Microsystems, Inc.

Chapter 4

Wide Industry Demand

Every organization recognizes the need for both perimeter security and VPNS that support secure communication across the Internet. Financial, government, communication, manufacturing, retail — all of these market segments can benefit from the high price/performance and low cost of ownership available with the iForce VPN/Firewall Appliance. This chapter reviews some of the innovative ways in which Sun's appliance can help specific industries.

Financial Institutions

The very structure of financial institutions impose stringent security requirements that must be met by their IT organizations. In order to reach more customers, most financial institutions have a large number of branch offices, all of which must securely interconnect with the main office. Trading systems that support the very purpose of many institutions are attractive targets for hackers, and must protected with highly-secure and also highly-available firewalls.

Branch offices can be efficiently supported with an iForce VPN/Firewall Appliance that acts as an Internet gateway and which also transmits authorized traffic over a secure, encrypted VPN back to the home office. When internal trading systems are accessed at the home office through a VPN, performance is key, and the iForce VPN/Firewall Appliance can be tuned with the right set of options to deliver needed performance— up to 640 Mbps using AES encryption — by licensing only the software that is needed. Costs can be controlled further with the remote management capabilities of the appliance, reducing the need for on-site security personnel at each branch office.

Trading systems must support high transaction rates and must also meet availability levels that in some cases are mandated by law. A financial institution's reputation is on the line for each

©2003 Sun Microsystems, Inc.

transaction that it handles, making both performance and security a business-critical issue. Figure 4-1 illustrates the use of iForce VPN/Firewall Appliances in a firewall sandwich configuration to support high transaction rates with high levels of availability. Enormous amounts of network throughput can be supported by load-balancing incoming and outgoing traffic through a set of horizontally-scaled appliances. Internal to the site, each functional layer is separated by firewalls that not only validate traffic entering the layer below, but also help prevent any unauthorized activity in one layer from accessing the layer above. These firewalls are configured using Check Point ClusterXL technology for high availability.

The same highly-secure, high-performance and high-availability Web application infrastructure can be applied not only in the financial industry, but in government, retail, and service-provider market segments as well.

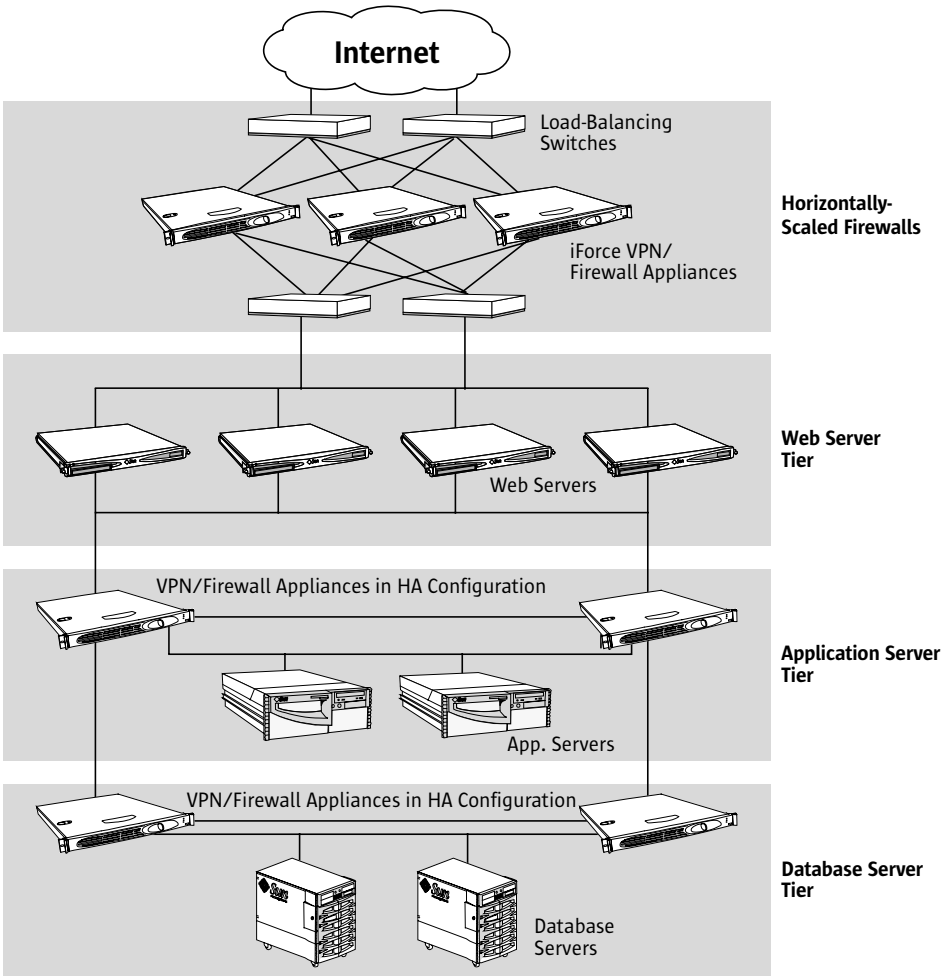


Figure 4-1: Example Web application infrastructure with firewall sandwich and HA firewall configurations protecting each tier.

Government Organizations

Because of their sheer size, government organizations tend to have multiple network entry points, a large number of subnets in buildings distributed across the country, and multiple organizational layers that must be protected. In these environments it's important to have a single security policy consistently applied across the organization —a feat made easy with central configuration, management, and monitoring using Check Point SmartCenter management software.

Government organizations can use iForce VPN/Firewall Appliances to consistently manage multiple Internet entry points. They can also use them to partition off their different subnets so that any worm, virus, or malicious activity can be confined to a limited subset of the network rather than left to propagate from network to network. With government organizations usually having some firewall infrastructure already in place, it's a bonus that the iForce VPN/Firewall Appliance can be managed exactly like existing Check Point VPN-1/FireWall-1 installations on Sun servers and platforms from other vendors.

Manufacturing Companies

For manufacturing companies, a key factor influencing profitability is the degree to which supply chains are integrated. In today's competitive marketplace, manufacturing companies must keep inventory to a minimum while maintaining the agility to quickly ramp up production to meet changes in customer demand. Manufacturing companies manage this balancing act not only by Electronic Data Interchange (EDI) of orders to suppliers, but also by disclosing predictions of future demand — helping suppliers be better prepared for future production requirements.

Disclosing sensitive data to partners and suppliers must be done with security that virtually guarantees privacy of data, and this can be accomplished using VPNs configured using the iForce VPN/Firewall Appliance. As illustrated in Figure 3-2(c), suppliers can establish private, secure remote subnets that provide controlled access to internal systems. Where only a single workstation at a supplier site needs to be provided access to internal systems, VPN client software like Check Point VPN-1 SecureClient can be used as illustrated in Figure 3-2(d). In either scenario, a manufacturing company can significantly reduce costs using VPNs over the Internet rather than configuring, maintaining, and paying high monthly fees for leased-line connections, particularly when integrating a supplier in a foreign county.

Retail Concerns

Retailers have similar concerns to manufacturing companies. They of course must secure their perimeters with state-of-the-art firewall technology, but where manufacturing companies must securely send orders to suppliers around the world, retailers must securely accept orders from their retail stores and outlets. In addition to the exchange of orders, retail companies need to provide employees with e-mail regarding company business, provide on-line catalogs that display products, and obtain up-to-the-minute information from their point-of-sale systems at each outlet.

As Figure 3-2(b) illustrates, the iForce VPN/Firewall Appliance can help make retail outlets more secure, but they can also support secure VPNs that support secure communication back to the home office. Using VPNs rather than leased lines saves on monthly telecommunication costs, and central VPN/firewall administration helps increase IT staff productivity.

Communication Companies and Service Providers

Communication companies including telephone companies and service providers have unique security concerns for the different areas of their business:

- As the Internet and telephony continue to converge, communication companies have an increasing amount of equipment that can be accessed using Internet protocols, and hence must be secured from outside intrusion. For example, systems routing incoming toll-free calls to different call centers depending on call load and time of day are software-based, and must be available to those who are authorized to operate them, and securely closed to those who are not. The iForce VPN/Firewall Appliance can be used throughout a communication company's

©2003 Sun Microsystems, Inc.

infrastructure so that access is well controlled, and the effect of any inadvertent intrusion localized and minimized.

- Internet Service Providers (ISPs) have paradoxical security requirements. They must be secured from outside intrusion, while providing services to their dial-up, broadband, and roaming customers. Security policies enforced by carefully-crafted firewall rules are the norm in ISPs, and central management of local, regional, and national ISP infrastructure and points-of-presence is an absolute requirement. ISPs can deploy iForce VPN/Firewall Appliances to protect the various layers of their services architecture, including their DMZ, services network, storage network, and administration/billing networks.
- Web hosting providers need to use firewalls to protect even the most low-end Web hosting services from unauthorized intrusion, and the Stateful Inspection of the iForce VPN/Firewall Appliance gives these service providers confidence that they are providing the best protection for their customer sites. For high-end, multi-tier sites, Web hosting providers that protect each services layer as illustrated in Figure 4-1 have the edge on providers that don't.
- Managed Service Providers (MSPs) often handle network infrastructure and security services for their corporate clients, making it easy for customers to outsource everything from e-mail and Web services to basic network connectivity and security. The iForce VPN/Firewall Appliance can play a key role for MSPs needing low-cost, high-performance, and easy-to-managed customer-premises equipment. Where MSPs need to install and manage customer-site equipment, the iForce VPN/Firewall Appliance can be configured in the MSP's data center, deployed to the customer premises, and managed remotely. Administration costs can be minimized by using standard configurations that are created and maintained on a Check Point Provider-1 management system and deployed to tens and even hundreds of customer firewalls.

Chapter 5

Product Configurations and Features

The iForce VPN/Firewall Appliance is a pre-integrated package that includes the Sun V60x/V65x server, network interface and optional VPN accelerator PCI cards, Check Point SecurePlatform software, and Check Point VPN-1/FireWall-1 software. Customers purchase the appliance directly from Sun re-sellers, and license the desired Check Point software features as needed — making it easy for customers to configure the system for their specific purposes.

Sun Fire V60x/V65x Server Configurations

The foundation for the iForce VPN/Firewall Appliance is the low-cost, high-performance, reliable, rack-mount Sun V60x/V65x server. Depending on the appliance configuration purchased, the server is equipped with up to two 2.8 GHz Intel Pentium III processors, 512 KB Level 2 ECC cache, either 512 MB or 1 GB of main memory, and an redundant power supply option for those requiring higher availability. The Sun Fire V60x/V65x server has two on-board 10/100/1000 Mbps Ethernet ports. Depending on the desired configuration, the additional PCI slots can be equipped with additional dual 10/100/1000 Mbps Ethernet interface card.These servers are data center ready with its rack-mount form factor, and both front and rear status LEDs.

Of the possible interface card and CPU/memory combinations, Sun offers five different server configurations (Table 5-1). The selection ranges from a total of four to fourteen network interfaces, and performance speeded by up to two CPUs, 1 GB of main memory, and a VPN accelerator card.

©2003 Sun Microsystems, Inc.

Table 5-1: Five different server configurations are offered, supporting from four to eight network interfaces

Configuration	Number of CPUs	Total Memory	Total Number of Interfaces	Dual 10/100/1000 Mbps Interfaces	Total Number of Power Supplies
1	1	512 MB	4	1	1
2	1	512 MB	6	2	1
3	2	1 GB	6	2	1
4	2	1 GB	10	4	2
5	2	1 GB	14	6	2

Performance

Performance of the iForce VPN/Firewall Appliance varies depending on the number of CPUs and amount of memory installed, the number and type of network interfaces, and whether or not the Check Point Performance Pack feature is licensed.

Performance Pack accelerates security functions on Linux platforms. By implementing access control, NAT, accounting, and anti-spoofing at the hardware-interrupt level, it greatly reduces the overhead associated with processing packets.

Overall firewall throughput ranges from 1.4 Gbps to 3.1 Gbps as illustrated in Table 5-2, as measured with 1500 byte packets. VPN performance with 128-bit AES encryption ranges from 390 Mbps to 1.02 Mbps as illustrated in Table 5-3. VPN performance with 168-bit triple-DES encryption ranges from 99 Mbps to 254 Mbps as illustrated in Table 5-4. Adding Check Point's SecureXL Turbocard can improve unencrypted firewall traffic throughput by up to 700% and 3DES VPN traffic throughput by up to 900%.

Maximum packet rates in kilo-packets per second (Kpps) were measured with 64 byte packets in order to provide another point of reference.

Table 5-2: Firewall network throughput with and without Check Point Performance Pack.

	Firewall Network Throughput	
Server Configuration from Table 5-1	**With Performance Pack**	**Without Performance Pack**
Configuration 1, 2 (1 CPU)	2.9 Gbps	1.95 Gbps
Configuration 3, 4, 5 (2 CPUs)	**3.1 Gbps**	1.4 Gbps

Table 5-3: VPN throughput with 128-bit AES encryption.

	VPN Throughput, 128-bit AES Encryption	
Server Configuration from Table 5-1	**With Performance Pack**	**Without Performance Pack**
Configurations 1, 2 (1 CPU)	563 Mbps/189 Kpps	390 Mbps/67 Kpps
Configurations 3, 4, 5(2 CPUs)	**1.02 Gbps/247 Kpps**	402 Mbps/63 Kpps

Table 5-4: VPN throughput with 3DES encryption.

Server Configuration from Table 5-1	VPN Throughput, 3DES Encryption	
	With Performance Pack	Without Performance Pack
Configurations 1, 2 (1 CPU)	116 Mbps/127 Kpps	102 Mbps/47 Kpps
Configurations 3, 4, 5 (2 CPUs)	**254 Mbps/197 Kpps**	99 Mbps/53 Kpps

Platform Selection Guidelines

A combination of performance and number of network interfaces can be used to guide customer purchasing decisions:

- For most applications, a single CPU with 1 or 2 dual 10/100/1000 Mbps network interface cards provides an optimal combination of throughput and flexibility (configurations 1 and 2). The dual 10/100/1000 Mbps interface cards deliver higher throughput than configurations using the quad 10/100 Mbps interface card, however the quad Ethernet card must be used if more than six interfaces are needed.
- The addition of a second CPU in configurations 3-5 works best in conjunction with Check Point Performance Pack, significantly raising throughput for both heavy firewall traffic and VPNs using AES encryption.
- For optimal performance with heavy 3DES encryption traffic, the VPN accelerator card delivers the best throughput, however higher packet rates are supported by Check Point Performance Pack on 2 CPU systems.

The iForce VPN/Firewall Appliance comes with Check Point SecurePlatform and VPN-1/FireWall-1 software pre-installed. Using the SecurePlatform hardware configuration GUI, administrators can perform initial setup (including IP addresses, netmasks, router, DNS addresses, and license keys) over the network without the need for a serial console. With initial addresses set up, Check Point SmartCenter software can be used to configure, manage, and monitor the appliance.

With all software pre-installed, customers only need to obtain the license keys for the specific features they wish to enable. For example, customers can license only FireWall-1 features if no VPN functionality is needed, saving costs by paying only for software that is used.

Product Architecture

Check Point VPN-1/FireWall-1 software is built using a modular, three-tier architecture that gives customers maximum flexibility in deploying and managing firewall appliances (Table 5-1):

- The VPN-1/FireWall-1 enforcement modules are responsible for actual rule enforcement and VPN management, and are always loaded on the server platform itself.
- The SmartCenter management console may be used on the server platform itself or on a separate system, depending on whether SmartCenter Enterprise Management Console is licensed. One of SmartCenter software's functions is to create VPN/firewall rule sets and securely load them into the enforcement module. If multiple firewalls are deployed, Smart Center Enterprise Management Console allows administrators to manage all rule sets on one console and push them to VPN/firewall appliances around the network, simplifying management of complex networks (Table 5-1(b)).

©2003 Sun Microsystems, Inc.

- The Graphical User Interface (GUI) module provides an intuitive, easy-to-use access to Check Point's SmartDashboard, enabling administrators to centrally define VPN, firewall, and QoS policies. Advanced features such as Check Point's SmartMap can be licensed as desired. The GUI module can be installed on any Solaris Operating System or Microsoft Windows platforms, including the platform on which SmartCenter Enterprise Management Console is installed.

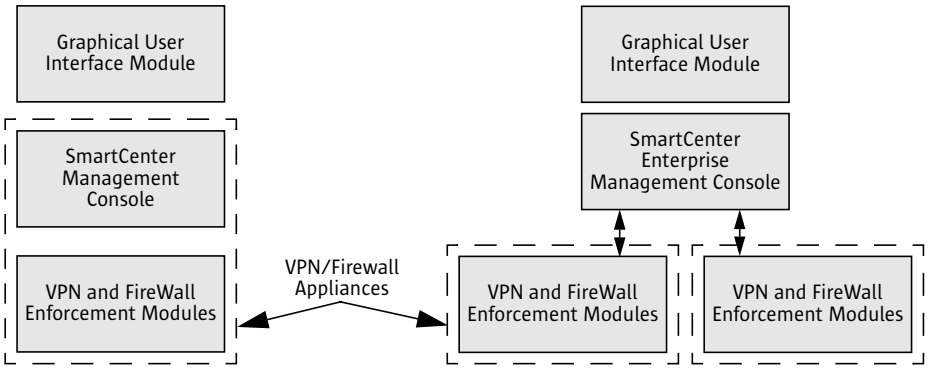


Figure 5-1: Check Point's modular software architecture supports flexible management options, including managing VPN-1/FireWall-1 software loaded on Sun server platforms.

Product Features

The iForce VPN/Firewall Appliance offers Check Point VPN-1/FireWall-1 product features to provide a secure-out-of the box solution that includes stateful packet inspection, network address translation, content filtering, application proxies, SmartDefense, VPNs, easy management, and high-availability and load-sharing configurations.

Patented Stateful Inspection

FireWall-1 helps enterprises to define and enforce a single, comprehensive security policy that protects all network resources against attacks and unauthorized access. Its architecture delivers a highly scalable solution that integrates all aspects of network security. Access control through Check Point's patented Stateful Inspection technology provides application-layer awareness without the need for performance-degrading proxies. It supports more than 150 pre-defined applications, services, and protocols including commonly-used HTTP, SMTP, FTP, and telnet.

Network Address Translation

Network Address Translation (NAT) conceals internal network addresses from the Internet, helping avoid disclosure of internal addresses and obscuring the details of internal networks from hackers. NAT is managed through a robust, easy-to-managed SecureNAT function in VPN-1/FireWall-1 software.

The VPN/firewall appliance's advanced NAT capabilities supports all applications and services, including Microsoft NetMeeting, Intel Internet VideoPhone, and VXtreme.

Both dynamic and static NAT modes are supported, providing a significant amount of control and flexibility in setting up an organization's network:

- Dynamic mode uses a single IP address behind which all internal network resources are hidden. This conserves registered IP addresses and hides the actual internal addresses used. Because the IP address used in dynamic mode is used only for outbound communication, and is not actually used by any internal server or user, hacking and spoofing are ineffective.

- Static mode allows administrators to set up a one-to-one assignment between published IP addresses and internal IP addresses. This mode is typically used when an organization wishes to published IP addresses for external servers such as Web and mail servers, but does not wish to expose the real IP addresses of those servers.

Content Filtering

Content-filtering capabilities can be used to protect users from worm attacks, malicious ActiveX components, and undesirable Web content. Access can be controlled to specific Web pages, to specific FTP functions like PUT and GET, and even to specific SMTP header fields.

VPN-1/FireWall-1 has built-in content-filtering capabilities which can be augmented by even more sophisticated tools by referring content to external filtering servers through both the OPSEC framework and Check Point's Content Vectoring Protocol (CVP). For example, Sun's iForce Perimeter Security Solution integrates Trend Micro's Interscan VirusWall with a VPN-1/FireWall-1 firewall using CVP.

Application Proxies

For organizations wishing to implement security policies using traditional application proxies, Check Point VPN-1/FireWall-1 software includes proxies for dozens of applications.

Of particular note is Check Point's SSL proxy, which allows encryption for secure Web communications to be handled by the firewall, enabling any Web-based application to be securely accessed over the Internet with no client VPN software required. This, combined with the many authentication methods available with FireWall-1/VPN-1 software, offers a high level of security through standard Web browser interfaces.

SmartDefense

Included with FireWall-1, SmartDefense actively protects organizations from known types of attacks using intelligent security technology. It blocks attacks by type and class using Check Point's patented Stateful Inspection technology and provides a single, centralized console for real-time information on attacks as well as attack detection, blocking, logging, auditing and alerting.

SmartDefense software can detect activity like port scanning and denial-of-service attacks, alerting administrators, logging suspicious activity, and even automatically blocking access from the offending IP address. For example, denial-of-service attacks that use SYN flooding techniques on Web servers can be averted with the VPN-1/FireWall-1 acknowledging connection requests to the Web servers, reducing the likelihood of operating system queues overflowing.

Customers may subscribe to automated SmartDefense updates from Check Point that incorporate new rules when new exploits are uncovered; in addition customers may define their own organization-specific rules.

Virtual Private Networks

Many of the VPN configurations discussed in this paper illustrate branch offices and extranets connected securely to the main office through VPNs. With VPN-1 software, a company's entire VPN configuration can be centrally managed using SmartCenter management software. When configured properly, VPNs can securely transmit sensitive information such as credit card information between internal systems.

One-click VPNs can be created with a single administrator operation. In one step, organizations can set the security parameters for an entire VPN deployment by defining VPN

 ©2003 Sun Microsystems, Inc.

communities. By simply defining all VPN gateways in a community, VPNs can be automatically configured between all offices. As new sites are added to the community, the automatically inherit appropriate properties and can immediately establish secure IPSec sessions with the rest of the VPN community. When used with one-click VPNs, One-Click Certificates establishes standard X.509 certificates published by Check Point's internal certificate authority, providing the strongest available authentication between VPN-1 gateways.

VPNs must protect the privacy of data being transmitted, and by adhering to the IPSec standard, VPN-1 software automatically negotiates the strongest possible encryption and data authentication algorithms between VPN endpoints. This includes the new Advanced Encryption Standard (AES) Rijndael and triple-DES algorithms:

- Rijndael Advanced Encryption Standard (AES), 128- and 256-bit keys
- Triple-DES, 168-bit keys
- DES, 56-bit keys
- DES-40, 40-bit keys
- CAST-40, 40-bit keys

For maximum security and flexibility, VPN-1 software provides integrated support for multiple user authentication methods. Mobile VPN users can be authenticated using smart cards, token-based products like SecurID, LDAP-stored passwords, RADIUS or TACACS+ servers, pre-shared secrets, X.509 digital certificates, and even biometric techniques.

As discussed in "Virtual Private Networks" on page 12, Site-to-Site VPNs can be terminated at any Check Point VPN-1/FireWall-1 software installation, and Client–to-Site VPNs can be terminated with Check Point VPN-1 SecuRemote or VPN-1 SecureClient software. Check Point VPN-1 Pro software supports connections from Microsoft L2TP or IPSec clients, Movian for PalmOS devices, and Equinux for Apple Macintosh systems. In addition, client-less VPNs can use SSL connections for spontaneous remote access from systems without VPN client software installed.

Management and Logging

Check Point's SmartCenter software offers various levels of management functionality to deliver integrated and cost-effective solutions to enable the highest levels of security and control in a single management console. SmartCenter software consists of the SmartDashboard GUI and the SmartCenter management console module:

- SmartDashboard is a powerful, yet simple user interface for defining and managing multiple elements of a security policy, including firewall, VPN, NAT, QoS, content filtering, and VPN security. All object definitions, including users, hosts, networks, and services, are shared among all elements for efficient policy creation and security management.
- SmartCenter management console is the server that stores and distributes security policies defined using SmartDashboard. It also stores the common database that stores network object definitions, user definitions, and log files for any number of enforcement points.

The SmartCenter enterprise management module, licensed separately, allows the management console to be separated from the enforcement module, and empowered to distribute firewall policies across the enterprise. SmartCenter Pro provides all of the capabilities of SmartCenter software plus:

- Visual management of network security through SmartMap
- Enterprise-scale management

- Ability to manage, distribute, and inventory software centrally
- Real-time security and VPN performance monitoring
- Powerful integration with LDAP-based directories
- Redundant management consoles.

SmartCenter server provides real-time tracking, monitoring, and accounting information for all connections logged by the firewall. In addition, it logs administrator activity such as rule changes to speed troubleshooting in the event of a configuration error. Through its OPSEC interface, SmartCenter server can be used as a central login point for many third-party, OPSEC-certified security components, facilitating correlation of events reported by each of the different software products.

High Availability with ClusterXL

ClusterXL software can be licensed on the iForce VPN/Firewall Appliance, enabling software-based load-sharing and high availability for network gateways. ClusterXL software distributes traffic between redundant gateways so that the computing capacity of multiple appliances can be combined to increase total network throughput. In the event that any individual gateway becomes unreachable, all connections are re-directed to a designated backup without interruption.

ClusterXL software maintains all connections, including VPNs, during a fail-over using Check Point StateSync technology. There is no need for users to re-connect or re-authenticate, and they will not even notice that an alternate gateway has taken over. A key benefit to many organizations, high-value business transactions and large file transfers continue without the need to re-start.

In addition to high availability, ClusterXl software expands the performance capability of VPN deployments by using horizontal scaling to distribute traffic between multiple gateways. Up to six gateways may be configured in a cluster.

©2003 Sun Microsystems, Inc.

Chapter 6

Conclusion

Both Sun Microsystems and Check Point Software Technologies are two companies that customers trust for meeting their security needs. The iForce VPN/Firewall Appliance combines the best-of-breed products from both companies — the best of Sun server technology with Check Point's VPN-1/FireWall-1 software combined in an easy-to-configure, easy-to-manage, and easy-to-deploy appliance solution. The appliance is pre-integrated with all hardware and software provided in a single bundle. The solution is secure out-of-the box with a secure, hardened operating system pre-loaded, "Secured by Check Point" certification for the appliance, and Sun Tone certification for the Check Point VPN-1/FireWall-1 software.

The iForce VPN/Firewall Appliance provides price/performance leadership for financial institutions, government organizations, manufacturing companies, retail concerns, communication companies, and service providers. Every VPN/firewall appliance configuration includes a four or more Gigabit Ethernet ports, with peak performance of 3.1 Gbps available on a six-interface dual-processor configuration. Virtual private networks can be created with one-click configuration using Check Point's SmartDashboard, with peak throughput using 128-bit AES encryption of 1.02 Gbps. High availability and load sharing is available with ClusterXL software, and one of beauties of Sun's appliance model is that customers need only license the software they intend to use.

The VPN/Firewall appliance lowers total cost of ownership by delivering a solution using a standard, rack-optimized form factor that's data center ready, with status LEDs front and back. By using a standard Sun server platform, organizations protect their investment because if needs change, the appliance can be re-provisioned as a powerful Sun Fire V60x/V65x server running either Linux or the Solaris Operating System. Costs are lowered because the same console can

©2003 Sun Microsystems, Inc.

manage any Check Point software installation, whether on multiple appliances or on other Sun server platforms. Finally, maintenance is simplified with the operating system and the firewall software provided from a single source.

With best-of-breed solutions pre-integrated and delivered in an easy-to-configure, easy-to-manage, and easy-to-deploy solution, the iForce VPN/Firewall Appliance is one the best tools for IT organizations to have in their arsenals to help them make the most of their stretched staff and reduced capital budgets.

For more information on the iForce VPN/Firewall Appliance, visit www.sun.com/checkpoint.

Chapter 7

References

Sun Microsystems posts complete information on Sun's hardware and software products and service offerings in the form of data sheets, specifications, and white papers on its Web page at *http://www.sun.com*.

For more information on the iForce VPN/Firewall Appliance, please refer to *www.sun.com/checkpoint*.

For more information on Check Point VPN-1/FireWall-1 software, please refer to *www.checkpoint.com*.

©2003 Sun Microsystems, Inc.

SUN™ Copyright 2003 Sun Microsystems, Inc.,4150 Network Circle, Santa Clara, CA 95054, U.S.A. All rights reserved.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

TRADEMARKS
Sun, Sun Microsystems, the Sun logo, Sun Tone, Solaris, and iForce are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-800-555-9786 or 1-800-555-9SUN **Web** sun.com

We make the net work.

Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, 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, 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