

SP-4060 Secure Appliance

Gigabit Security Solution for Mid-tier Enterprise

Features and Benefits

- Purposely-built hardware for Check Point FireWall-1/VPN-1.
- Cluster technology ensures high availability
- Proprietary ISP link redundancy
- Pre-installed Check Point for plug-and-play deployment
- Tightly integrating Check Point and i-Security SEC to deliver high performance
- Built-in 3 Fast Ethernet, 3 Gigabit Ethernet deliver 1.5Gbps firewall throughput
- Intuitive web-based interface to manage system configurations

As a medium-scale enterprise security requirement, you may be connecting to gigabit switches and routers, you need high firewall processing power, you need high availability with hot standby redundancy. i-Security SP-4060 Secure Appliance, tightly integrated with Check Point Firewall-1/VPN-1 is just the right choice for you.

Fully Integrated Solution

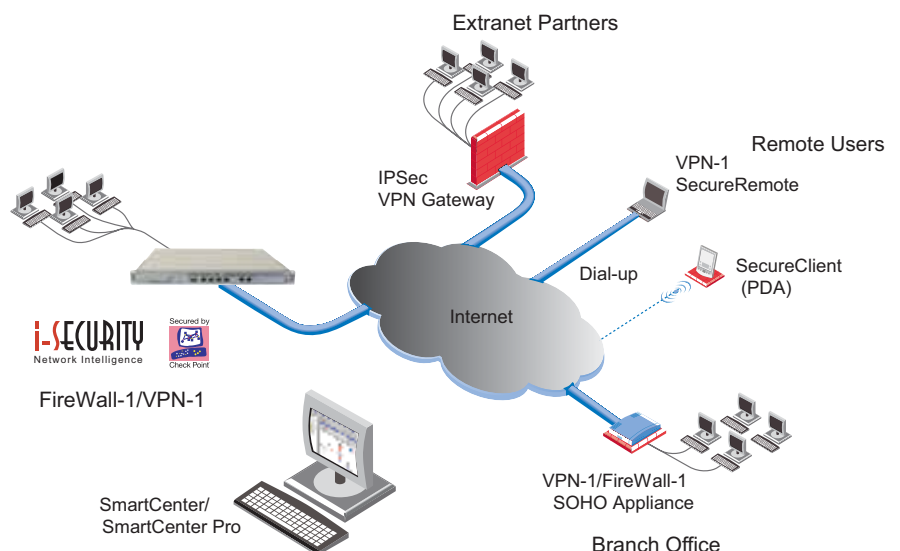
SP-4060 equipped with what you need for your enterprise connectivity: 3 auto-sensing Fast Ethernet, 3 auto-sensing Gigabit Ethernet, pre-installed with Check Point Firewall-1/VPN-1 and hardened SecurePlatform Operating System, SP-4060 is a full stateful-inspection firewall, customers are free from the hassles of hardware compatibility issues, installation efforts and hardware specification defining. It is also equipped with Security Enhancement Chip (SEC) to deliver 1.5Gbps firewall throughput. SP-4060 comes with a web-based system administration allows easy first-time setup, device connectivity configuration, as well as product installation and licensing control.

ISP Link Redundancy

High availability device such as i-Security SP-4060 is still prone to downtime if the link to Internet is broken by any means. The proprietary technology from i-Security and Check Point SecurePlatform can easily handle the case by having more than one ISP links connected to the Internet, ensures your Internet connectivity as well as your business operations.

Security Enhancement Chip

With i-Security's proprietary Security Enhancement Chip (SEC), the performance of inspecting application layer data could be enhanced greatly because of its state-of-art software-hardware fused technology on inspection engine, connection status table matching. In the meantime, the system status monitoring technology in SEC makes high-availability options for Check Point Firewall even more reliable, the hardware signaling system communicates through TCP/IP network, seamlessly merge two systems into a single high available system.



Leading Technology from Check Point

Check Point FireWall-1 delivers comprehensive attack protection and network security. Using INSPECT, the most adaptive and intelligent inspection technology, FireWall-1 integrates both network-level and application-level protection. As the industry's leading Internet security solution, Check Point FireWall-1 provides the highest level of security, with access control, attack content security, protection, authentication, and integrated Network Address Translation (NAT). FireWall-1 leverages Check Point SMART Management, enabling you to intelligently manage security infrastructure with maximum efficiency.

One-Click VPNs

With One-Click VPNs, large-scale VPNs can be created with a single operation. By defining VPN communities, organizations can set the security parameters for an entire VPN, such as an intranet, Extranet or remote access deployment in one step. By simply defining all VPN-1 end points in a community VPNs are automatically enabled among all gateways or between a gateway and a remote user. As new sites are added to the community, they automatically inherit the appropriate properties and can immediately establish secure IPSec sessions with the rest of the VPN community.

Protection Against Network and Application Threats

In today's environment, centralized protection from known and new threats is increasingly important. FireWall-1 includes SmartDefense and Application Intelligence capabilities to protect your company against all types of network and application-level attacks. For example, SmartDefense automatically blocks and logs oversized packets, SYN floods and fragmentation attacks. It also defends against such well-known attacks as Nimda, Code Red and Cross Site Scripting. Real-time attack information and protection updates through the online Check Point SmartDefense attack center are optionally available.



SP-4060 Specification

LAN ports	3 built-in 10/100/1000 Mbps Ethernet ports 3 built-in 10/100 Mbps Ethernet ports
Memory	1GB, Max.2GB
Hard disk drive	40GB
Operating system	Check Point SecurePlatform
Firewall application	Check Point FireWall-1, VPN-1
Firewall performance	Max. 1.5Gbps
VPN throughput	Max. 240 Mbps
Concurrent sessions	Max. 850,000
System management	Web, SSH command line , serial port
HA Capability	Hot standby redundancy
Form factor	1 RU rack-mountable
Operating temperature	5°C to 40°C
Operating humidity	20% to 80% Non-condensing
Power supply	110/240 Auto switch

For further information, please contact us

North America

2880 Zanker Road,
San Jose, California 95134,
United States
Tel: +1 (408) 834-7449
Fax: +1 (408) 432-7235
Enquiry: sales@i-security.us
Support: support@i-security.us

Asia Pacific

Hong Kong
Room 1003, World-wide House,
19 Des Voeux Road, Central,
Hong Kong.
Tel: +852 3656-7895
Fax: +852 3656-7788
Enquiry: asiapac@i-security.us

China Beijing

Unit 601, Tower W2, Oriental Plaza
1 East Chang An Avenue,
Dong Cheng District Beijing
100738, CHINA.
Tel: +86 (10) 8520 0338
Fax: +86 (10) 8520 0337
Enquiry: sales@i-security.com.cn
Support: support@i-security.com.cn

China Shanghai

Level 23, Citigroup Tower33,
Huayuanshiqiao Road, Shanghai
Pudong 200120, CHINA.
Tel: +86 (21) 6101 0402
Fax: +86 (21) 6101 0220