



VPN-1 Power

Comprehensive security for the most demanding environments

YOUR CHALLENGE

With its worldwide reach, the Internet provides a flexible and cost-effective infrastructure for extending the corporate network to all employees and key business partners. However, the Internet also conceals constantly changing threats to corporate resources. Hackers continually invent new ways to attack enterprise applications. At the same time, application requirements are growing more complex and more performance intensive. To take full advantage of the Internet, enterprises must be able to guarantee both the security of business communications and the protection of internal resources, while addressing the challenges of availability, performance, and scalability for mission-critical applications.

OUR SOLUTION

Check Point's VPN-1® Power™ delivers comprehensive, accelerated security for today's demanding environments, with tightly integrated firewall, VPN, and intrusion prevention technologies that provide comprehensive security and remote connectivity for corporate applications and network resources. It accelerates the industry's most intelligent security inspection technologies, Stateful Inspection and Application Intelligence™, providing preemptive attack prevention against both network- and application-layer attacks for high-performance networks. VPN-1 Power solutions are available on the industry's broadest range of open platforms and security appliances—meeting the price/performance requirements of any size organization.

COMPREHENSIVE NETWORK AND APPLICATION SECURITY

VPN-1 Power integrates access control, authentication, and encryption to guarantee the security of network connections, the authenticity of local and remote users, and the privacy and integrity of data communications. In addition, it is tightly integrated with intrusion prevention capabilities, offering advanced application protection. VPN-1 Power also includes an optional Web application firewall, providing unsurpassed protection for the Web environment.

FireWall-1 integration

For effective enterprise perimeter, internal, and Web security and efficient administration, VPNs must include integrated firewall capabilities. VPN-1 Power includes market-leading FireWall-1® software to secure all popular Internet services with Check Point-patented Stateful Inspection technologies. VPN-1 Power supports more than 150 predefined applications, services, and protocols out of the box, including instant messaging, multimedia services, Oracle SQL, peer-to-peer applications, RealAudio, and Web applications.



The NGX platform delivers a unified security architecture for Check Point perimeter, internal, and Web security.

PRODUCT DESCRIPTION

VPN-1® Power™ is an integrated firewall, VPN, and intrusion prevention gateway providing comprehensive, accelerated security and remote connectivity for applications and network resources.

PRODUCT FEATURES

- Accelerated security
- Secure VPN connectivity with FireWall-1® integration
- Comprehensive network and application security
- Secure communications with IPSec, L2TP, SSL, and strong authentication
- Centralized, integrated, policy-based security management

PRODUCT BENEFITS

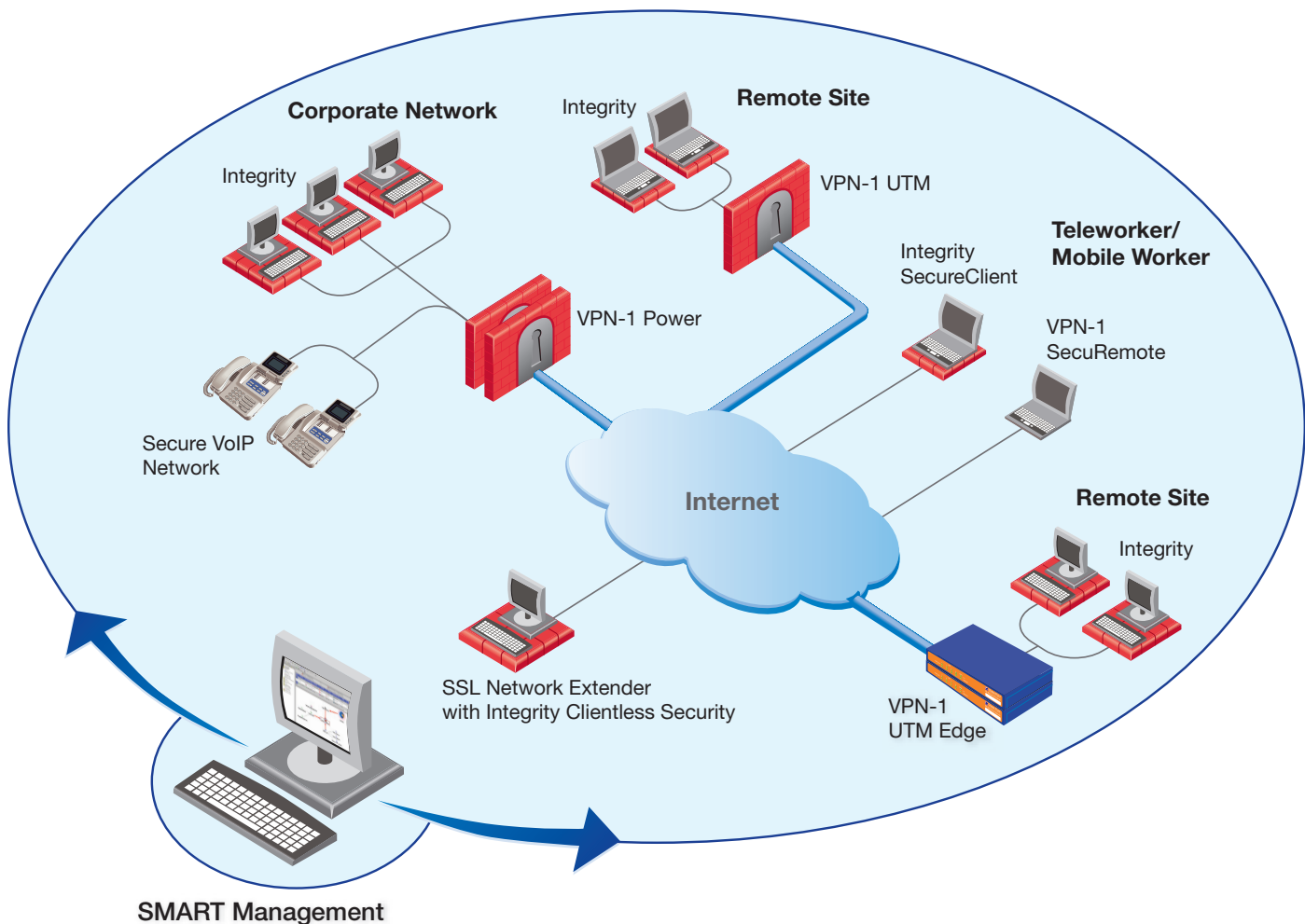
- Delivers reliable performance for demanding environments
- Provides advanced application protection for changing threats
- Streamlines security administration and lowers management cost

NGX HIGHLIGHTS

- Intelligent VoIP security
- Advanced network/routing capabilities
- Route-based VPNs
- Support for multicast security



Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.



VPN-1 Power is the most proven security and connectivity solution for the extended enterprise.

Secure applications

Application Intelligence is a set of advanced capabilities, integrated into VPN-1 that detect and prevent application-layer attacks. Application Intelligence redefines the network security landscape by evolving VPN-1 into an advanced security gateway solution that integrates both network- and application-layer capabilities to deliver comprehensive attack protection. Enterprises benefit from superior intrusion prevention capabilities without the complexity of managing additional devices.

Secure Web applications

Web Intelligence™ is an optional advanced Web application firewall that is tightly integrated into VPN-1, providing advanced Web application security. Web Intelligence protects Web applications from common hacking techniques such as command injection, cross-site scripting, directory traversal, LDAP injection, and SQL injection. Web Intelligence also includes Malicious Code Protector™, a patented technology

that prevents buffer overflow attacks. Malicious Code Protector uses a unique detection mechanism that analyzes the behavior of malicious code, catching attacks without the aid of signatures and stopping both known and unknown attacks.

Secure VoIP

VPN-1 Power offers comprehensive security for VoIP applications, including Stateful Inspection of H.323, MGCP, SCCP (Skinny), and SIP. In addition, VPN-1 is capable of addressing complex VoIP deployments, such as hiding gatekeepers behind a Network Address Translation (NAT) device. In addition, ClusterXL®, FloodGate-1®, and SecureXL™ can help enterprises build a high-performance, fault-tolerant, and prioritized voice network.

CONNECTIVITY WITH SECURITY

VPN-1 Power contains the most comprehensive set of products and technologies for remote-access, intranet, and extranet VPNs. Check Point offers a broad range of VPN products from which organizations can choose to design the configuration that best meets their requirements.

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. The security administrator simply defines all VPN-1 endpoints in a community, and 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.

Advanced site-to-site VPN capabilities

VPN-1 Power is designed to extend company resources to remote locations, no matter how complex the environment is. VPN-1 supports VPN domains, the traditional method of defining VPN boundaries with a static group of IP addresses. In addition, VPN-1 supports route-based VPNs, in which the VPN topology is delegated to network routing decisions. Such flexibility gives enterprises a powerful mechanism for providing connectivity in complex and dynamic networks. Route-based VPNs allow administrators to extend dynamic routing protocols from headquarters to remote locations over VPN tunnels, improving network and VPN management efficiency for large networks. Route-based VPNs also enable directional VPNs, allowing administrators to enforce security policy over VPN tunnels without static IP addresses. For constantly changing networks, route-based VPNs are an ideal solution. Organizations can make frequent changes to the network topology, such as adding an internal network, without having to repeatedly reconfigure static VPN domains.

Flexible authentication

Check Point-secured VPN solutions offer a multitude of authentication options, including RADIUS, TACACS/TACACS+, and token cards. In addition, OpenPKI ensures that Check Point-secured VPN solutions are compatible with leading PKI solutions from vendors such as Baltimore Technologies, Entrust, and VeriSign, enabling organizations to manage very large IPSec VPN deployments. VPN-1 Power features a unique hybrid mode authentication that allows organizations to deploy IPSec VPNs while leveraging existing authentication schemes such as SecurID tokens.

Organizations that want to implement strong authentication out of the box can use Check Point One-Click Certificates. With an Internal Certificate Authority included with VPN-1 Power, X.509 digital certificates can be issued to VPN-1 gateways and VPN-1 SecureClient™ users. One-Click Certificates provide industry-standard, two-factor authentication without the complexity and expense of PKI systems.

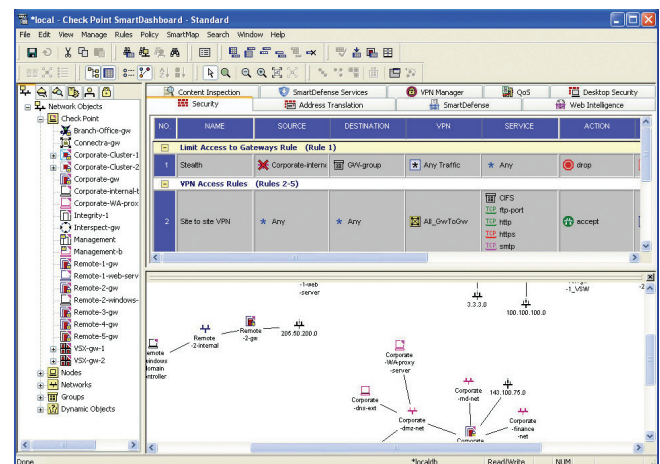
Support for multiple remote-access technologies

Every enterprise has a unique blend of requirements for remote access, depending on the types of users, the mix of applications to be accessed, and the level of endpoint security and management control demanded. VPN-1 Power provides flexibility, supporting multiple client options. SecuRemote™ provides basic connectivity that is easy for users requiring occasional remote access to IP applications.

SecureClient provides a higher level of security by adding a centrally managed personal firewall. Check Point Integrity™ SecureClient offers complete remote access protection with integrated VPN client and fully managed endpoint security. SSL Network Extender™, a Web-browser-based applet, conveniently provides complete access to IP-based applications from any Internet device. VPN-1 Power also supports Microsoft L2TP and Symbian VPN clients.

SMART MANAGEMENT

VPN-1 Power includes SmartCenter™, based on Check Point's Security Management Architecture (SMART)—the industry's most consistent and powerful management architecture. SmartCenter enables enterprises to centrally define perimeter, internal, and Web security policies, correlate and prioritize security events, and perform advanced monitoring and reporting, all via a single console. This unified architecture enables easy distribution of security policy updates across all gateways, ensuring consistent policy enforcement and improving operational efficiency.



SmartCenter provides powerful security and VPN policy management, reducing the cost and complexity of administration.

HIGH PERFORMANCE AND AVAILABILITY

As firewall and VPN deployments become larger and more mission-critical, performance is a key concern. VPN-1 Power delivers accelerated security of more than 5 Gbps on an open server, guaranteeing the availability of information without compromising on security. VPN-1 Power also uses advanced streaming technologies that allow packet processing to be performed at the kernel level, significantly improving application-layer inspection, typically a computer-intensive task. Combining the SecureXL framework and streaming technology with Check Point's commitment to open systems delivers industry-leading performance at the lowest possible cost.

Integrated VPN Quality of Service (QoS)

QoS is a requirement for any VPN deployment where performance is important and congestion on the Internet link may occur. FloodGate-1 ensures optimal performance for mission-critical VPN-1 traffic, enabling customers to migrate critical business traffic from private wide area networks to the Internet.

High availability and load sharing

ClusterXL distributes traffic of all types across a cluster of VPN-1 Power gateways. If a gateway becomes unreachable, all connections are seamlessly redirected to the remaining cluster members. Near-linear performance gains are achieved when additional cluster members are added.

Nonstop forwarding

Combined with dynamic routing protocol such as BGP or OSPF, ClusterXL delivers the industry's only High-Availability enforcement point with "graceful restart." VPN-1 Power significantly improves the availability of mission-critical applications, eliminating unnecessary "ripple effects." These ripple effects are caused by the changes in routing tables when VPN-1 Power gateways become unavailable and can disrupt traffic forwarding for up to tens of minutes.

VPN load distribution

VPN load distribution is a High-Availability and load-sharing solution for remote access VPN connections. Inbound VPN connections are distributed across multiple VPN-1 gateways than can be geographically distributed. If a gateway becomes unreachable, VPN clients are automatically connected through another member.

Multiple entry points

If multiple data centers are available, remote users can be assured continued access through the multiple entry point feature. If a primary VPN-1 gateway becomes unavailable, VPN-1 gateways at other locations are automatically engaged to establish VPN connectivity to the corporation.

SYSTEM REQUIREMENTS

VPN-1 Power gateways and SmartCenter	
Platforms	Nokia IPSO, Red Hat Enterprise Linux, SecurePlatform™, SecurePlatform Pro, Solaris 8 (32/64 bit), Solaris 9 (64 bit), Windows 2000 Server/2003 Server
Disk space	300 MB
Memory	256 MB
SmartDashboard	
Platforms	Solaris, Windows 2000/2003/XP/ME/98
Disk space	100 MB
Memory	256 MB
Remote access clients*	
Platforms	Linux, Macintosh, Windows 2000/XP/2003/Pocket PC 2003 2nd Edition/Handheld PC 2000
Disk space	20 MB
Memory	64 MB
Check Point SecurePlatform	
CPU	Intel Pentium II 300+ MHz or equivalent
Disk space	4 GB hard drive, supported NICS
Memory	256 MB minimum, 512 MB recommended

* Integrity SecureClient, VPN-1 SecureClient, and VPN-1 SecuRemote.

For detailed information on supported platforms and system requirements, please refer to http://www.checkpoint.com/products/supported_platforms/platforms_appint.html.

©2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 UTM, VPN-1 Power, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

May 3, 2006 P/N 502124

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
www.checkpoint.com

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.