



# VPN-1 Power

*Comprehensive security for  
the most demanding environments*

## YOUR CHALLENGE

Business evolves quickly, and your IT infrastructure is evolving with it. In fact, business change is happening faster than many security organizations are capable of adapting to it. New applications such as Voice over Internet Protocol (VoIP) and instant messaging (IM) are forcing change. Also, new business requirements such as regulatory compliance and obstacles to business continuity must be dealt with—not to mention the new attacks that threaten your network. Your choices? Slow down business until security can catch up or expose your network to the risk and liability of attack.

## OUR SOLUTION

VPN-1® Power security gateways provide an active defense that enables you to secure your most demanding sites—such as core networks and data centers. A central element of the Check Point unified security architecture, VPN-1 Power adapts as new applications are introduced and new threats appear—delivering proactive protection for new technologies such as IM or VoIP as well as against whole classes of attacks. With advanced security acceleration technology, VPN-1 Power ensures that your business information flows efficiently without compromising security. The result is an integrated firewall, VPN, and intrusion prevention solution that keeps your business safe and your information available.

### PROVIDING AN ACTIVE DEFENSE AGAINST THREATS

VPN-1 Power protects against next-generation threats and attacks by providing truly integrated security based on FireWall-1® and SmartDefense™ intrusion prevention technologies. FireWall-1 and SmartDefense cooperate as if they were a single application—the level of effort needed to combat today's blended threats.

FireWall-1 is based on Check Point-patented Stateful Inspection, the de facto standard for Internet security. It understands the context of network traffic and provides out-of-the box support for more than 150 predefined applications, protocols, and services such as Citrix, Oracle, Web conferencing, and more. Because it is extensible, FireWall-1 quickly adapts as new applications, which need to be secured, appear on your network.

SmartDefense intrusion prevention uses Application Intelligence™ technologies to understand how applications and protocols should work. With this information, SmartDefense intrusion prevention can preemptively block entire classes of attacks based on suspicious behavior. You stay protected as new variants appear—without the need for signature updates that do not appear until after the threat has done its damage. And Check Point SecureXL™ security acceleration technology enables you to provide preemptive intrusion prevention protection at throughput of more than 5 Gbps—with all default protections active on an open server.

## PRODUCT DESCRIPTION

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

## PRODUCT FEATURES

- Integrated firewall, VPN, and intrusion prevention
- Accelerated security for throughput up to 12 Gbps
- Centralized, policy-based security management

## PRODUCT BENEFITS

- Ensures consistent, proven security across a distributed network
- Increases security performance to support high-demand environments
- Enhances the ability to deploy new applications quickly without security concerns
- Protects against new threats through SmartDefense™ Services
- Simplifies management of complex security infrastructures

# NGX™

*The NGX platform delivers a unified  
security architecture for Check Point.*

This intelligence also means companies can deploy advanced applications such as video and voice with the confidence that unknown vulnerabilities cannot endanger the network. As IT security departments deploy VoIP throughout a distributed network, VPN-1 Power prevents disruptive attacks by ensuring that VoIP sessions adhere to standards and to specific vendor implementations. It also prevents denial-of-service (DoS) attacks against your communications system by recognizing suspiciously high numbers of call attempts that would signal a possible attack.

Likewise, you can stop potentially vulnerable applications such as IM clients that do not adhere to corporate standards or peer-to-peer file trading that crosses your VPN-1 Power security gateway. A common vector for spyware and malware to enter the network, these applications can be difficult to stop because of built-in masquerading techniques. VPN-1 Power security gateways recognize these attempts and provide the means to establish control over potentially harmful applications.

To reduce the risk of internal endpoint security violations, VPN-1 gateways integrate with Integrity™ endpoint enforcement. As internal hosts attempt to access resources beyond a VPN-1 gateway, it will check for the presence of an Integrity endpoint security client and determine whether the host complies with your security policy. Administrators either can deny noncompliant hosts access or log them as noncompliant for later action.

VPN-1 gateways also work with computers that have the integrated Intel vPro system to provide an extra layer of internal security. If a computer with a vPro-enabled network interface card (NIC) attempts to violate security policy, VPN-1 can lock it down, preventing further network access.

### Integrated protection for Web servers

Organizations can deploy Web Intelligence™, an optional Web application firewall, on VPN-1 Power security gateways to provide 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 patent-pending technology that prevents buffer-overflow attacks. Malicious Code Protector uses a unique detection mechanism that analyzes the behavior of executable code, catching malicious attacks without the aid of signatures, stopping both known and unknown attacks.

### VPN-1 UTM Power: Accelerated security with content inspection

Because some organizations desire the content inspection capability found in unified threat management solutions, customers have the option of purchasing VPN-1 UTM Power. VPN-1 UTM Power provides the accelerated security found in VPN-1 Power but complements it with integrated antivirus and Web filtering. Updated through SmartDefense Services, these features enable a higher level of security for email, Web, and other content-driven traffic.

### SmartDefense Services

VPN-1 Power security gateways are supported by SmartDefense Services, which maintain the most current preemptive security for the Check Point security infrastructure. To help you stay ahead of new threats and attacks, SmartDefense Services provide real-time updates and configuration advisories for defenses and security policies. SmartDefense Services, a subscription-based solution for all Check Point products, enable your defenses to evolve with or ahead of threats by enhancing existing defenses and adding new defense techniques between regularly scheduled product upgrades.

### TOTAL CONTROL, TOTAL VISIBILITY

Key to your security objectives' success is having strong management, auditing, and analysis tools for your overall security environment. As part of a Check Point unified security architecture, VPN-1 Power provides unified control over security policy and unified visibility into security information across a distributed security infrastructure. Using SmartCenter™ Power, you can define one policy that is enforced across all VPN-1 Power, VPN-1 UTM, and VPN-1 UTM Edge™ security gateways. By working on a single policy, you reduce the risk of configuration error and the time required to manage your security.

SmartCenter Power increases your organizational efficiency by providing control and visibility over other Check Point solutions within your network. Connectra™ Web security gateways, InterSpect™ internal security gateways, and Check Point Integrity™ endpoint enforcement all integrate with SmartCenter Power so that you can easily view your complete security infrastructure's security events from a single console.

As new security features like content inspection are added to VPN-1 gateways, organizations can update SmartCenter without doing a full upgrade by using plug-in management updates. Updating other Check Point security solutions from a central location with SmartUpdate™ lowers the cost and complexity of keeping security up-to-date and shortens the time needed to ensure all gateways have the latest security protections—decreasing your exposure to attack.

The Check Point SmartViewTracker™ integrated log viewer unifies the logs from Check Point solutions distributed throughout your network. You gain immediate awareness of important security events through a single information view for logs and can take appropriate action instantly.

### VPN CONNECTIVITY WITH TOTAL SECURITY

Because organizations are dealing with increasingly complex virtual private networks, VPN-1 Power contains a comprehensive set of technologies to build remote access and site-to-site VPNs that simplify configuration while still maintaining flexibility for different deployment scenarios.

### Simplifying complex site-to-site VPNs

With the increased complexity of linking sites together for video, voice, and other applications, organizations need tools to lay out complicated topologies with minimal effort. VPN-1 Power meets that need by providing a unified method to create and manage complex VPNs. The SmartDashboard™ enables administrators to define participants—including third-party VPN gateways—in large-scale VPNs. VPN gateways can be configured for both star and mesh topologies in minutes with minimal management overhead for shared secrets through an integrated certificate authority. Providing even more flexibility, VPN-1 Power includes two methods to define and create VPNs:

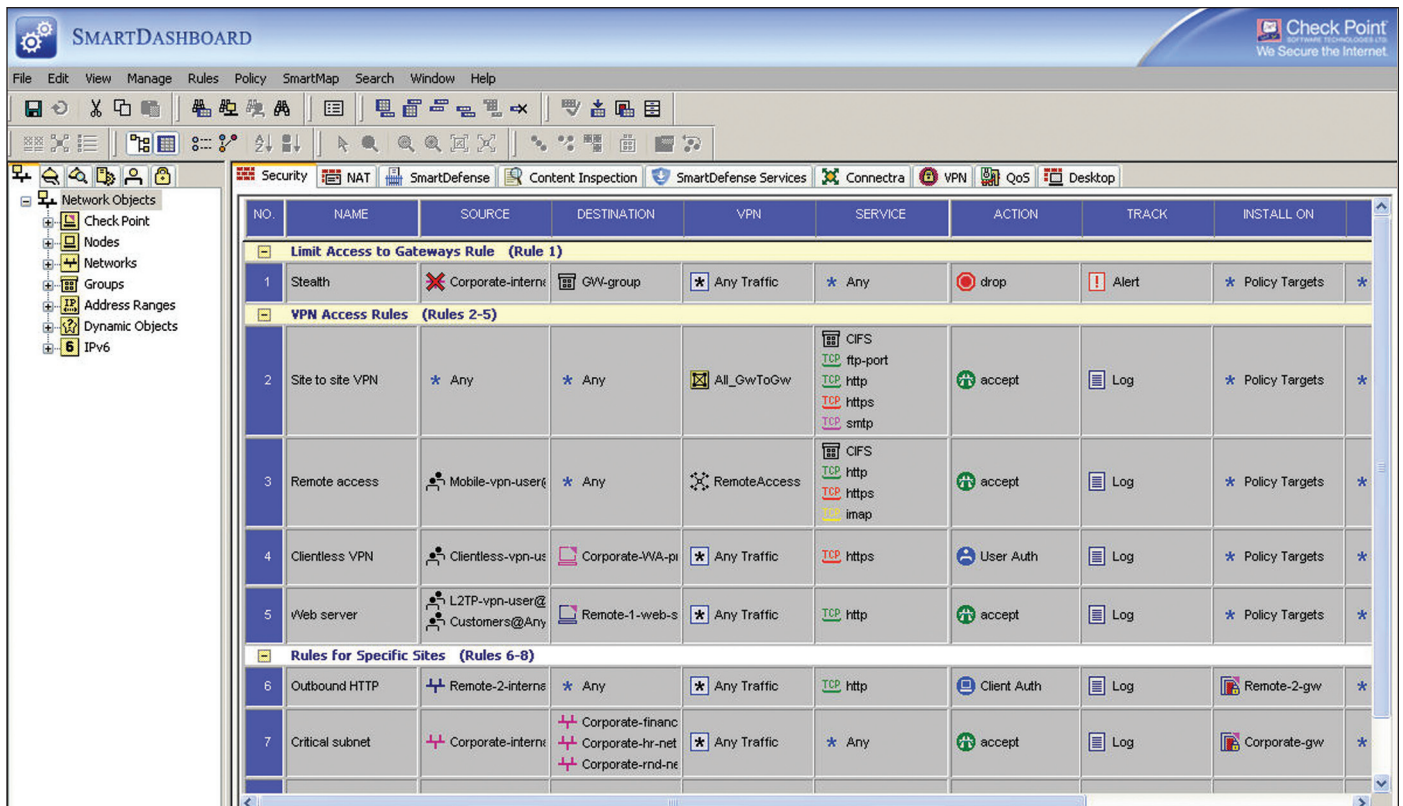
**Route-based VPNs**—administrators define what traffic should be encrypted by VPN rules, enabling the creation of complex large-scale site-to-site VPNs in dynamic environments. Route-based VPNs also support the extension of dynamic routing and multicast communities across VPNs

**Domain-based VPNs**—administrators define which resources behind the gateway should have encrypted VPN traffic

### Flexible remote access support

Every enterprise has unique requirements for remote access, depending on the types of users, the applications, and the level of endpoint security needed. You gain the flexibility to meet the different needs of remote users with both IPsec and SSL VPN technologies for remote access supported within VPN-1 Power:

- VPN-1 SecuRemote®—VPN-1 SecuRemote offers basic IPsec connectivity for remote users
- VPN-1 SecureClient™—VPN-1 SecureClient offers complete IPsec connectivity with an integrated, centrally managed desktop firewall
- Integrity SecureClient—Integrity SecureClient extends the security found in VPN-1 SecureClient with Integrity endpoint security, based on the award-winning ZoneAlarm® personal firewall
- SecureClient Mobile—SecureClient Mobile delivers firewall protection and secure, uninterrupted remote access for wireless devices such as mobile phones



SmartDashboard enables centralized control over not only VPN-1 Power but also an entire security infrastructure.

- **SSL Network Extender**—SSL Network Extender™ is an on-demand client that provides full network-layer secure access through a browser plug-in, enabling remote users to access email or other network applications in their native interfaces
- **Integrity Clientless Security**—Integrity Clientless Security mitigates risks from unmanaged PCs connecting to Web-facing resources, enforcing prelogin security policy, blocking spyware, enabling on-demand, end-to-end session confidentiality, without preinstalled clients

### Building a secure VPN

A key element in Check Point's philosophy is that VPN connectivity must be matched with a high level of security. By truly integrating FireWall-1 and SmartDefense with VPN technologies, VPN-1 Power enables you to connect remote users, sites, and partners without worrying that your VPN will become a network backdoor. At your discretion, VPN-1 Power can apply the entire security policy to encrypted traffic, a subset of traffic, or allow VPN traffic to enter uninspected.

In addition, it provides strong security for the VPN against DoS attacks such as those directed against the Internet Key Exchange (IKE) mechanism. VPN-1 Power implements a unique solution for IKE DoS, asking unknown gateways attempting to connect to solve a computationally intensive problem before allocating resources.

### HIGH PERFORMANCE AND AVAILABILITY

VPN-1 Power delivers accelerated security of more than 12 Gbps on an open server, guaranteeing the availability of information without compromising security. Using Check Point-patented SecureXL™ security acceleration, VPN-1 Power security gateways enable you to get maximum performance from open servers and appliances even during DoS attacks.

VPN-1 Power uses advanced streaming technologies that allow packet processing to be performed at the kernel level, significantly improving network- and application-layer inspection, typically a computing-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 where performance is important and congestion on the Internet link may occur. FloodGate-1® ensures optimum performance for mission-critical VPN-1 traffic, enabling customers to migrate critical business traffic from private WANs 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. By adding an optional ClusterXL module, near-linear performance gains can be achieved by adding cluster members.

### Nonstop forwarding

Combined with dynamic routing protocols 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. Ripple effects are caused by changes in routing tables when VPN-1 Power gateways become unavailable, which can disrupt traffic forwarding for more than 10 minutes.

	VPN-1 Power SmartCenter Server or enforcement module	SmartConsole™
<b>Platforms</b>	Linux, SecurePlatform™, Solaris, Windows, "Secured by Check Point" appliances	Solaris, Windows
<b>Processor (minimum)</b>	Intel Pentium II or UltraSPARC II (Intel Pentium III for SecurePlatform)	Intel Pentium II or UltraSPARC II
<b>CPU speed (minimum)</b>	300 MHz or equivalent for Intel	300 MHz or equivalent for Intel
<b>Free disk space</b>	300 MB 4 GB for SecurePlatform	100 MB
<b>Memory</b>	Linux: 128 MB (256 MB recommended) SecurePlatform: 256 MB (512 recommended) Solaris: 128 MB (256 MB recommended) Windows: 256 MB	Solaris: 128 MB Windows: 256 MB

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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.

February 27, 2007 P/N 502344

### 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.