



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

PRODUCT DESCRIPTION

SecurePlatform™ Pro enables administrators to turn an off-the-shelf Intel- or AMD-based open server into a prehardened, high-performance VPN-1 gateway within five minutes. It also includes extensive dynamic routing, multicast protocol support, and central management of administrator support.

PRODUCT FEATURES

- Prehardened, preconfigured security installation on open servers within five minutes
- Integrated routing and multicast protocol support
- Centralized administrative rights provisioning

PRODUCT BENEFITS

- Enhances security infrastructure reliability
- Increases security for popular multicast application traffic
- Simplifies deployment of enterprise-class security on open servers
- Reduces need for routers at branch offices

SecurePlatform Pro

Prehardened operating system for Check Point intelligent security solutions

YOUR CHALLENGE

When choosing a security platform, organizations usually choose between two distinct choices: simplicity or flexibility. If they go with the simplicity of a security appliance, they lose the flexibility to change technologies as their needs change. Or they can deploy their security solution on an inexpensive, flexible open server that must be modified, or “hardened,” to make it secure, a process that can be less than simple. Unfortunately, with limited financial and IT personnel resources, organizations frequently feel they must choose between simplicity and flexibility.

OUR SOLUTION

The Check Point SecurePlatform™ Pro prehardened operating system combines the simplicity and built-in security of an appliance with the flexibility of an open server running a prehardened operating system. With Check Point’s market-leading security solutions—VPN-1® Pro™ and VPN-1® Express™—running on the SecurePlatform Pro prehardened operating system, time-pressed IT administrators can deploy enterprise-class security on inexpensive Intel- or AMD-based open servers anywhere in the network.

EASY TO DEPLOY, SIMPLE TO SECURE

The SecurePlatform Pro prehardened operating system enables administrators to install Check Point’s market-leading VPN-1® gateways and SmartCenter™ management servers within five minutes on Intel- or AMD-based open servers. It eliminates the need for administrators to uninstall or reconfigure portions of the operating system or to apply fixes manually whenever a new vulnerability is found. Instead, SecurePlatform Pro provides a preconfigured, prehardened operating system that meets the requirements of the most-demanding network environments.

A SecurePlatform Pro-based VPN-1 gateway is as easy to deploy as a purpose-built appliance and offers superior investment protection. As organizations face new attacks, like application-layer worms, or adopt new protocols, such as Voice over IP, VPN-1 gateways running on SecurePlatform Pro can scale to face new demands. With extensive hardware and driver support, organizations can easily change their hardware configurations as their security needs evolve.



Intelligent Security

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

Advanced routing and deployment scenarios

For organizations looking to implement scalable, fault-tolerant, secure networks, SecurePlatform Pro enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on VPN-1 gateways. By integrating advanced routing protocols with a company's VPN-1 gateway deployment, SecurePlatform Pro enables the creation of redundant, highly available security gateway clusters. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

SecurePlatform Pro also integrates multicast protocol support, including IGMP, PIM-DM, and PIM-SM. By incorporating multicast protocols, SecurePlatform Pro enables VPN-1 gateways efficiently and effectively to manage which multicast sessions, such as stock tickers or videoconferencing, to forward into their networks.

In addition, SecurePlatform Pro supports load sharing in a dynamic routing environment and immediate failover for dynamic routing protocols, increasing the resilience of the network. Immediate failover to other VPN-1 gateways—a feature unique to Check Point products—prevents networks from becoming victim to a “ripple effect.” That’s where having a single security gateway in a cluster fail will cause other routers in the network to communicate with each other—attempting to find an alternate route to the cluster even though the original route is still valid.

Dynamic Routing Protocols	Multicast Protocols
BGP	IGMP
OSPF	PIM-DM
RIPv1	PIM-SM
RIPv2	

Straightforward security management

SecurePlatform Pro options are managed from either a Web interface or an industry-standard command line interface (CLI). The Web interface provides administrators a simple, easy-to-use point to change networking configurations, install new product licenses to add functionality, or upgrade to new versions of SecurePlatform Pro. To reduce training costs of network administrators responsible for routing, SecurePlatform Pro includes standard CLI commands for configuring and managing routing and multicast protocols.

To simplify the management of multiple administrators across a distributed network, SecurePlatform Pro enables organizations to use a central RADIUS server to provision administrative rights for configuring and managing SecurePlatform Pro options. Centralized management of administrative rights not only reduces the configuration burden but also ensures a consistent provisioning of rights across all SecurePlatform Pro deployments.

©2003-2005 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 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 12, 2005 P/N 501782