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

Data Sheet

Provider-1

Centralized security management for large enterprises

YOUR CHALLENGE

Large-scale businesses like conglomerates or holding companies, face security policy challenges due to the diverse nature of their subsidiaries' businesses. In these complex environments, security managers need the right tools to efficiently manage multiple policies. Large-scale enterprises often have security policies that must be tailored to geographically distributed branches with independent network management. At the same time, security personnel must support a corporate-wide security policy with rules enforcing appropriate user access, preventing attacks, and enabling secure communication and fail-over capabilities.

OUR SOLUTION

Check Point's Provider-1® is a unique security management solution designed to meet the scalability requirements and security challenges of large enterprises. By simultaneously supporting central management for many distinct security policies, Provider-1 dramatically improves the operational efficiency of managing large security deployments. Provider-1 consolidates management for Check Point perimeter, internal, Web, and endpoint security gateways, delivering a robust mechanism for creating and enforcing security policies and automatically distributing them to multiple enforcement points.

Provider-1 is supported by SmartDefense Services, which maintain the most current preemptive security for the Check Point security infrastructure. To help companies stay ahead of new threats and attacks, SmartDefense Services provide real-time updates and configuration advisories for defenses and security policies.

Multi-Policy Management

With Provider-1, security policies can be customized. For example, enterprises can tailor a security policy to enable vendor applications that tie into corporate financial networks to communicate safely and securely, yet without having access to confidential corporate data. Or a security policy can enable franchise companies to communicate with regional and international headquarters, yet safeguard the franchise's internal network integrity. An administrator can create policies for branches that are geographically distributed and have independent network management or create high-level global policies that manage all networks. This ability to centrally create and deploy multi-level policies delivers unparalleled scalability by eliminating the need to make repetitive policy changes to thousands of individual devices.

NGX

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

PRODUCT DESCRIPTION

The Provider-1® centralized security management solution is designed to meet the unique challenges of large-scale enterprises. Provider-1 easily scales to enable security managers to efficiently manage multiple policies for a wide-spread system, thereby ensuring the entire corporate IT architecture is adequately protected.

PRODUCT FEATURES

- Multi-domain, multi-policy management
- Central network and security management
- Granular, role-based administration
- Management high availability
- Centralized SmartDefense Services updates against new threats

PRODUCT BENEFITS

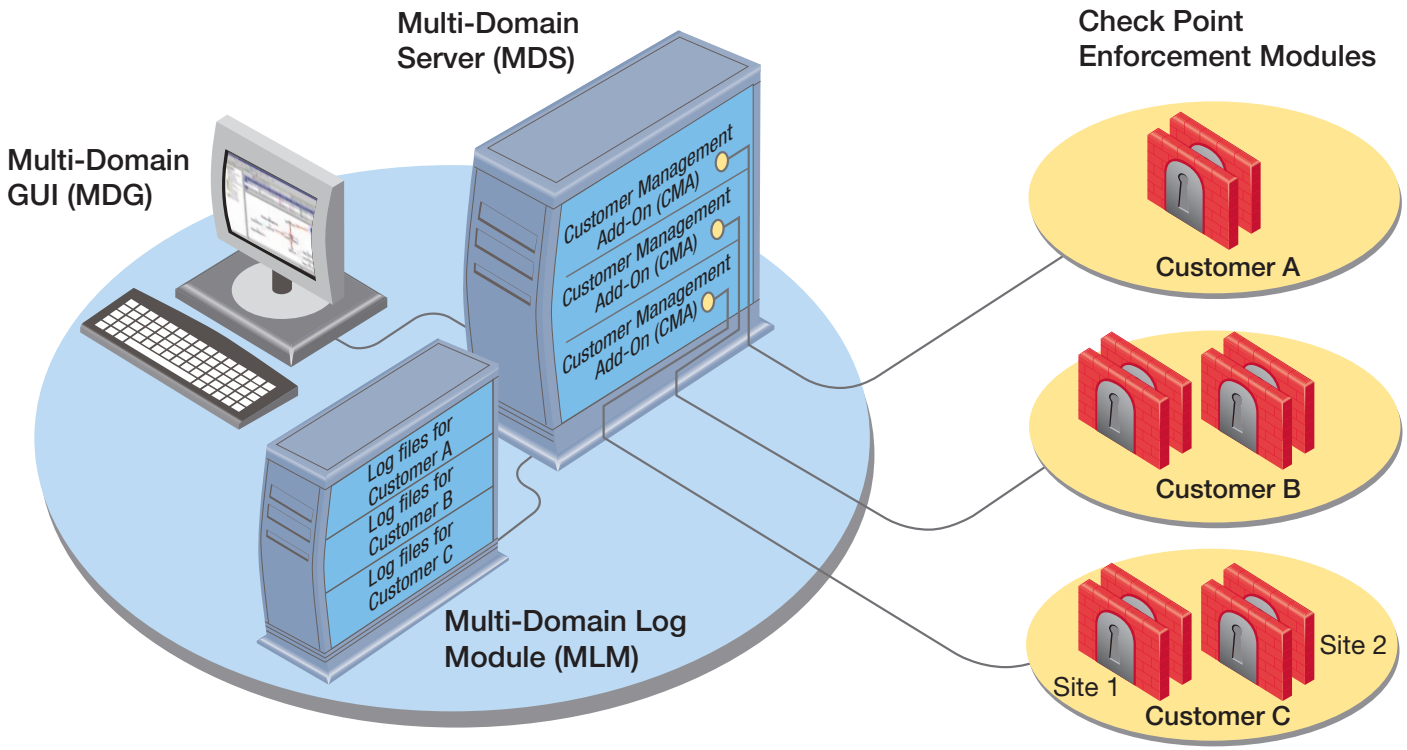
- Simplify security policy provisioning
- Reduce administrative overhead and capital investment
- Deeper insight into enterprise security
- Full visibility over your entire security environment

NGX HIGHLIGHTS

- Integrated management for Check Point Integrity™
- Support for Eventia Reporter™ and Eventia Analyzer™
- Extended administration support for third-party authentication methods

Intelligent Security

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



Provider-1 aggregates multiple, distinct security policies on a single platform.

Provider-1 is now integrated with the VPN-1® line of solutions—including VPN-1 VSX™—Check Point Integrity™, Connectra™, and InterSpect™, allowing for centralized management and monitoring of all security enforcement points.

The components of the Provider-1 architecture that enable efficient management of multiple Check Point gateways include the Customer Management Add-On (CMA), the Multi-Domain Server (MDS), the Multi-Domain GUI (MDG), the Multi-Domain Log Module (MLM), and the Customer Log Module (CLM).

Customer Management Add-On

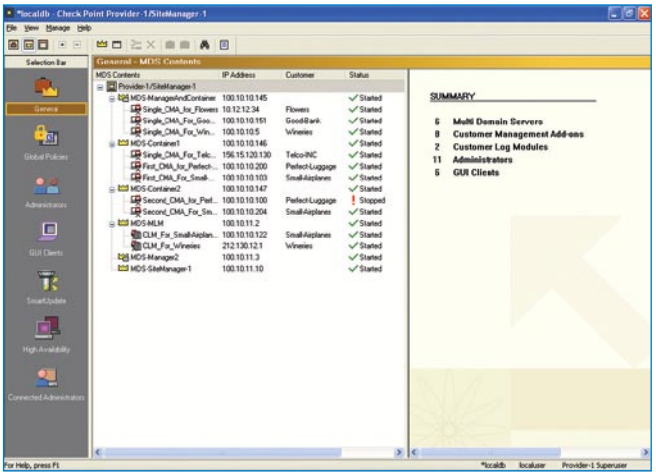
Via a CMA, an administrator defines, edits, and installs security policies applicable to a specific network or gateway. Multiple CMAs can be deployed where the secondary CMA is automatically synchronized with the primary CMA for high availability.

Multi-Domain Server

The MDS houses the CMAs, as well as Provider-1 system information. Although multiple CMAs can be stored on the same MDS, each CMA is completely isolated, providing absolute data privacy. Multiple MDSs can be linked in the Provider-1 system to manage thousands of policies in a single environment and to provide fail-over capabilities.

Multi-Domain GUI

The MDG is designed to simplify multi-policy security management. Via the MDG, administrators manage the entire Provider-1 environment, easily incorporating new networks into the Provider-1 system. Using the MDG, administrators can provision and monitor security via a single console and oversee rules, policies, logs, statuses, and alerts for thousands of users.



Multi-Domain GUI presents a comprehensive view of all networks or policies under management.

Multi-Domain Log Module

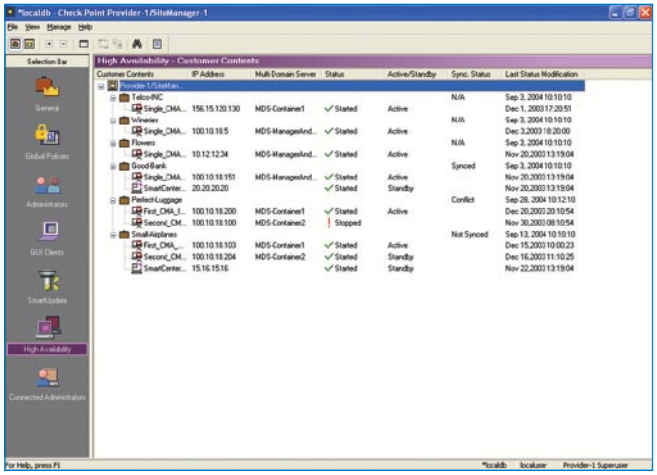
The MLM is an optional component that improves performance for large deployments by offloading log processing activities from the MDS. Redundant log management can be created by designating an MLM as a primary log server and the MDS as a backup server. In the event that the MLM cannot be reached, logs are automatically redirected to the MDS. Multiple discrete logs can be stored separately on a single MLM.

Customer Log Module

A CLM is a single log server that is housed within an MLM. Service Providers may deploy CLMs to monitor specific branch activity.

Total Availability Management

Provider-1 delivers a fully redundant management architecture for rapid disaster recovery. High availability is supported at multiple levels—from the enforcement point (Check Point gateways), where the customer is protected in the event of a gateway computer failure, to the CMA, where multiple CMAs can be set up to guarantee management fail-over for the associated network. Alternately, a SmartCenter™ can also serve as a backup server at the CMA level. Multiple MDSs deployed in a Service Provider environment also provide mutually redundant fail-over capabilities and can be configured to automatically synchronize global policy data. For enterprises with local and remote branches, centralized fail-over security management is another critical success factor in achieving efficient, comprehensive system security.



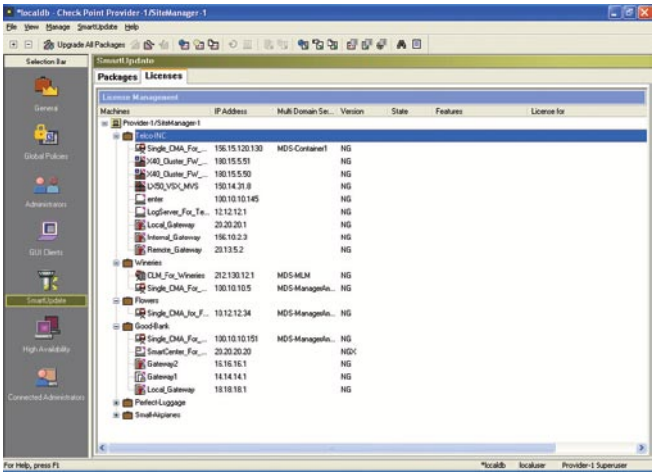
High availability for multiple CMAs is managed centrally via the MDG.

Role-based administration and auditing

IT departments must often delegate levels of authority among administrators so that there is a hierarchy of access even within systems support. Whereas some administrators will have global authorities to maintain the system backbone, others may handle specialized activities and only require permissions for certain parts of the system. Differentiating between levels of access permissions is critical not only for securing user transactions, but also for monitoring for attacks, abuse, and load management.

Provider-1 provides a flexible way to distribute administrative management responsibility to different teams based on their level of administration authority. It also enables enterprises to provide around-the-clock administrative network and security support for their networks. Provider-1 automatically records detailed activities of all administrators for easy auditing. In addition, policy versions can be saved as changes are made and restored, as needed.

Multiple administrative levels can be set within Provider-1. Administrators can be given authority to manage the entire Provider-1 system or just to manage customer networks. Local departmental administrators who operate outside of the Provider-1 system can be given access to their own security policies.



SmartUpdate provides centralized updates and distribution of software, licences, and policies.

Centralized software management

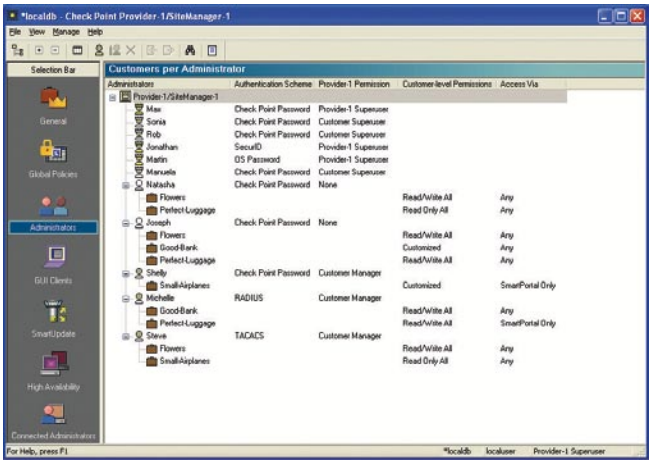
For enterprises managing thousands of enforcement points, updating and maintaining software can pose a challenge. Provider-1 enables centralized, remote software installations and licensing updates of Check Point and third-party (OPSEC™) products.

Global SmartDefense Updates

With the integrated SmartDefense Services console, administrators can centrally update security configurations and defenses, ensuring security systems are always up-to-date to defend against new and evolving threats. Enterprises will have the flexibility to define SmartDefense Services settings at the global level as well as specific to their sub-networks.

The Provider-1 trust model

The Provider-1 system ensures secure, trusted, and private communication between its components and Check Point gateways while ensuring data integrity. Each CMA has its own internal certificate authority that issues certificates for secure communication between the CMA, log servers, and its own network. Because each CMA has a unique certificate authority, different CMAs cannot penetrate each other's internal networks or establish connections with each other's gateways. All communication between MDSs is authenticated and secured, and every MDS communicates securely with the CMAs that it houses.



Provider-1 enables granular control of administrative authority.

Multiple authentication methods are supported for administrator access to the MDS and CMA. These include PKI certificates, as well as third-party authentication methods like RADIUS, TACACS, and TACACS+.

Tight integration with Check Point SMART management

Provider-1 is tightly integrated with Check Point SMART management solutions, a suite of powerful applications for centrally configuring, managing, and monitoring Check Point perimeter, internal, and Web security gateways.

This integration means that administrators can access all SmartCenter applications for a specific CMA via the MDG to centrally configure, manage, and monitor customer gateways. SmartCenter applications include:

- *SmartDashboard*™, which enables administrators to define and manage security and VPN policies
- *SmartView Tracker*™ for managing and tracking logs throughout the system
- *SmartPortal*™ for extending browser-based access to Provider-1
- *SmartMap*™ visual management for at-a-glance appraisal of security policies
- *SmartView Monitor*™ monitoring for real-time network, VPN, and user monitoring
- *Eventia Reporter*™ report generation for different aspects of network activity for specified customers and modules
- *SmartUpdate*™ to manage and maintain a license repository, as well as facilitate upgrading of Check Point software
- *SmartLSM*™ for managing large numbers of remote gateways

SUPPORTED OPERATING SYSTEMS
Multi-Domain Server SecurePlatform™, Solaris 8/9/10, RedHat Linux Enterprise 3.0
Multi-Domain GUI Windows 2000/2003/XP, Solaris 8/9/10

October 04, 2006 P/N 502256

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.