

# Security Management Portal

*Cost-effective, managed security*

## YOUR CHALLENGE

Outsourced security services is one of the fastest growing segments in the security market. As a result of heightened awareness and increasingly sophisticated network security threats, businesses are turning to outside expertise to secure their networks. This creates a unique opportunity for Service Providers, resellers and network integrators to generate new revenue streams by providing remotely-managed network security and Virtual Private Networks (VPNs), thus increasing loyalty, promoting brand awareness and attracting new customers.

Remote management often involves repetitive and confusing tasks, requires the purchase and maintenance of equipment, and may not be fully compatible with existing billing systems. It can be difficult to enter the managed security services market due to the high investment required and the lengthy and complicated deployment. You need a solution that supports quick and cost-effective management of multiple client offices and provides a variety of value-added subscription services, all with minimal setup and maintenance costs.

## OUR SOLUTION

### Security Management Portal

The Security Management Portal (SMP) introduces a new management model for Managed Security Service Providers (MSSPs) that target small and medium businesses (SMBs) and vertical markets. SMP offers a robust, resilient architecture that supports tens to tens of thousands of Check Point Safe@Office® gateways.

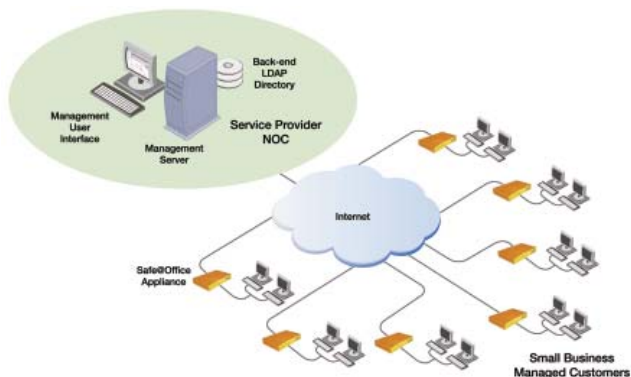
Featuring an intuitive, Web-based user interface, SMP includes a host of features for service providers and allows for quick and easy integration with existing billing and CRM systems. SMP includes a set of built-in virus and spam scanners allowing you to deliver profitable value-added services to end users.

SMP was developed by SofaWare Technologies, a Check Point company, focused on building innovative solutions to enable service providers and network integrators to deliver managed broadband security solutions to the SMB market.

By outsourcing Internet security and network management, businesses can drastically increase the efficiency of IT operations and receive enterprise-class value-added security services for their office networks.

### SMP On-Demand

With SMP On-Demand, you can enjoy the benefits of SMP, in a cost-effective Software as a Service (SaaS) solution that provides quick and easy entry into the managed network security market. Based on SMP, SMP On-Demand is a fully-hosted solution offering managed firewall and intrusion prevention services, always-on antivirus protection, VPN connectivity, and other value-added services. With SMP On-Demand, you can create your own service plans and pricing and customize customer reports with your own logo and branding.



### SMP ON-DEMAND

A fully hosted security management and service provisioning solution for MSSPs

### SECURE, RESILIENT ARCHITECTURE

Built to support tens to tens of thousands of security gateways with ease

### FIREWALL AND VPN MANAGEMENT

Remote management of firewall and intrusion prevention settings, as well as Dynamic VPN communities

### ANTIVIRUS AND ANTISPAM

Automatic signature updates for the embedded gateway antivirus and on-the-fly scanning of email for viruses and spam

### WEB FILTERING

URL-based Web Filtering protects against malicious and undesirable Web sites

### SECURITY REPORTING

Automatically generated, customizable security reports

### AUTOMATED FIRMWARE UPDATES

Up-to-date security with automatic firmware and security updates

### VULNERABILITY SCANNING

Identifies vulnerabilities in the subscriber network and demonstrates the value of the security services

### DYNAMIC DNS

Provides Dynamic DNS services, enhancing usability of dynamic IP environments

### USER-FRIENDLY MANAGEMENT

A Web-based interface increases efficiency and reduces training costs

### INTEGRATED SUBSCRIBER MANAGEMENT SYSTEM

A complete subscription management solution for security service providers

### ALL-IN-ONE

SMP integrates a wide array of managed services into a single turnkey solution:

- Network and firewall management
- VPN management
- Firmware updates
- Antivirus and antispam
- Gateway antivirus signature updates
- Logging and reporting
- Dynamic DNS
- Vulnerability scanning
- User authentication management

These features enable service providers to deliver cost-effective, comprehensive managed security services to small businesses, while lowering installation costs. SMP allows for the complete remote management of all network security aspects and eliminates the need for on-site configuration and troubleshooting. In addition, Safe@Office gateways can be pre-configured before being shipped to the customer, minimizing deployment time and costs.



### ARCHITECTURE

SMP's primary elements are a management server and an intuitive, Web-based user interface. SMP's Web-based user interface provides an easy conduit to view, edit, and navigate between service plans, customers, gateways, and VPN/security policies. The interface also provides a single, centralized snapshot of all rules, objects, logs, statuses, and alerts for Safe@Office gateways. SMP also offers the option of enabling a Web-based Self-Provisioning Portal that allows managed customers to edit some of their own settings. This further simplifies security provisioning and monitoring while increasing customer participation.

### SIMPLE PROVISIONING AND MAINTENANCE

SMP simplifies the deployment and maintenance of Safe@Office gateways by using group-based management tools. Administrators can create a single service plan consisting of a template that defines gateway properties, an associated VPN and security policy, and additional services such as antivirus protection and content filtering. Once a service plan has been defined, the service provider can associate it with an unlimited number of Safe@Office gateways. Each gateway that is assigned a particular service plan inherits all of that plan's properties, including its VPN and security policy.

When the policy needs to be updated, an administrator simply updates the plan via SMP's Web-based user interface, and then watch as the updates are automatically applied to the appropriate

Safe@Office gateways. By eliminating the need to make repetitive policy changes to thousands of individual devices, SMP delivers unparalleled scalability and time-savings.

### VIRUS AND SPAM SCANNING

SMP offers support for Check Point Embedded NGX gateway antivirus updates. It also features a centralized, network-based email antivirus and antispam scanning solution. By scanning email traffic for security threats before they ever reach the customer's network, SMP ensures that the content entering the network is free of malicious code and no bandwidth is wasted on downloading infected files. SMP has built-in support for SpamAssassin and ClamAV scanners and supports external OPSEC CVP-based scanners.

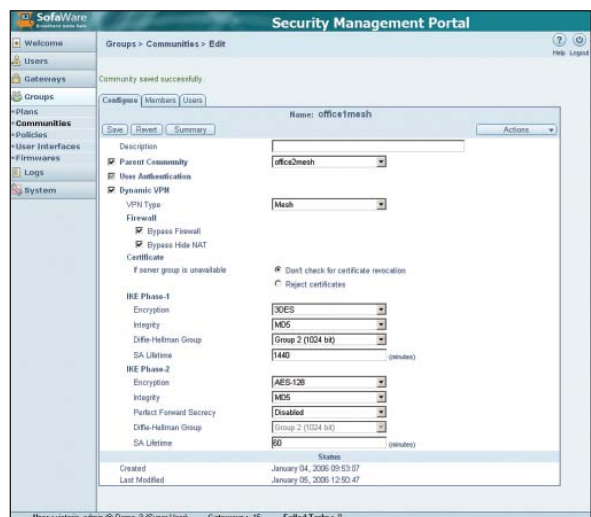
### WEB CONTENT FILTERING

SMP supports a URL-based Web Filtering add-on that allows users to protect their employees and families from up to 32 categories of objectionable or malicious Web sites. Users can define gateway-specific or global white and black lists to allow or block access to specific URLs. By providing two ways of filtering content, SMP provides business owners with flexibility to customize their Web Filtering policies, and block access to categories of objectionable sites such as for adult entertainment or on-line gaming.

### INSTANT MANAGED VPN DEPLOYMENT

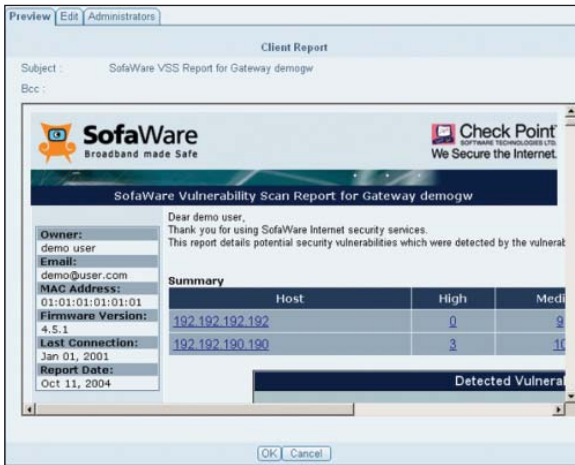
Many businesses use VPNs to secure traffic between headquarters and branch offices and to connect remote users. Managing a VPN can be a time-consuming and complex task. SMP simplifies it by enabling administrators to create VPNs in a single operation, using the Dynamic VPN (DVPN) module.

In one step, administrators can define VPN communities and set security parameters for the entire VPN. By grouping a customer's VPN endpoints in a community, the administrator can automatically create a fully meshed VPN, establishing site-to-site tunnels between each pair of sites. New users and sites that are added to a community automatically inherit the appropriate properties and immediately establish secure IPsec sessions with the rest of the community. In addition, the Dynamic VPN module fully supports dynamically-addressed IP gateways and automatically updates all VPN endpoints with the most recent IP addresses of the gateways in their community. This further reduces administrators' burdens.



### VULNERABILITY SCANNING SERVICE

SMP features an integrated vulnerability scanning service (VSS) that scans subscriber networks for security vulnerabilities. Vulnerability scanning reports can be generated automatically at user-defined intervals and automatically emailed to customers. The security reports include information about identified security vulnerabilities and information obtained by port scanning. Vulnerability scanning is an excellent tool for a service provider to demonstrate the security services' value to customers, using customizable, HTML-based reports.



### STRONG AUTHENTICATION

Service providers that want to implement strong authentication can do so by using the internal Certificate Authority (CA) that is included with SMP's Dynamic VPN module. SMP issues X.509 digital certificates to all Safe@Office gateways that are part of a VPN community, in order to ensure secure Site-to-Site VPN communications.

This feature provides industry-standard, two-factor authentication without the additional complexity and expense of separate Public Key Infrastructure (PKI) systems.

### AUTOMATIC FIRMWARE UPDATES

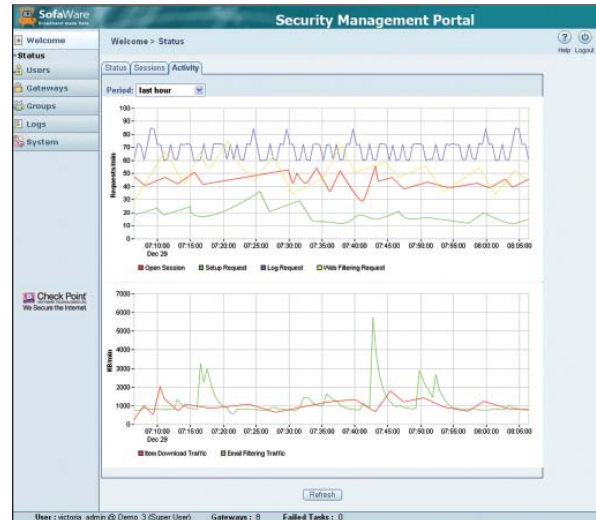
Ensuring thousands of security gateways are all enforcing the highest level of security can be a daunting administrative task. To alleviate this problem, SMP uses "pull" technology for automatic firmware updates: Gateways automatically detect and download new firmware whenever it becomes available on the management server, rather than the management server having to spend time initiating communications with each gateway individually. This reduces the administrative load on the management server. Administrators also have the option of overriding the group settings and pushing unique firmware and settings to specific gateways.

### INTEGRATED LOGGING, REPORTING, AND MONITORING

SMP turns the vast amount of data collected from security devices into understandable information that can be used to demonstrate the effectiveness of security services. Security reports are automatically generated and emailed to customers at user-defined intervals. In addition, these reports can be viewed directly from the SMP management interface. They include information about blocked attacks, detected viruses, filtered Web sites and more.

In addition, SMP offers powerful real-time monitoring tools that let you see the status of the SMP server and its connected devices at

a single glance. This includes real-time load visualization graphs, status displays, customizable alerts and connectivity events. Using event alerts, you can proactively support your customers and notify them about connection outages, a VPN tunnel drop, or an attack.



### EFFORTLESS SUPPORT FOR DYNAMICALLY ADDRESSED GATEWAYS

Tracking and monitoring customer gateways that use dynamic IP addresses can be difficult, since their IP addresses change each time they connect to the Internet. SMP alleviates this issue by fully supporting the management and monitoring of dynamically addressed gateways.

SMP can act as a secure Dynamic Domain Name Service (Dynamic DNS or DDNS) server, which constantly checks and updates the mapping of a domain name to a gateway's corresponding IP address. Each time the gateway's IP address changes, Dynamic DNS maps the DNS name to the new IP address. Dynamic DNS allows service providers to appeal to a larger customer base by enabling customers to use lower cost dynamic IP connectivity.

### EFFICIENT ROLE-BASED ADMINISTRATION

SMP provides a flexible way of distributing management responsibility among a group of security administrators, dividing that responsibility by type of service plan, customer, or specific functional tasks. All administrator activity is logged and reported, improving security by providing information that can identify unauthorized policy changes.

### EASY INTEGRATION

SMP includes a comprehensive SOAP/XML standards-compliant API that allows easy integration of third-party billing systems and customer service applications with SMP, as well as creation of custom Self-Provisioning Portals.

### RESILIENT MANAGEMENT INFRASTRUCTURE

SMP provides a fully redundant management infrastructure that enables round-the-clock control of customer security. Service providers can deploy more than one management server in a NOC, with full load balancing and automatic failover, thereby enabling carrier-grade service, fault tolerance, and scalability. Security reports include information about identified security vulnerabilities and information obtained by port scanning. Vulnerability scanning is an excellent tool for a service provider to demonstrate the security services' value to customers. The vulnerability scanning reports are HTML-based and can be extensively customized by editing a report template.

Security Management Portal (SMP)		SMP On-Demand		
Delivery Method	Locally installed software	Hosted service		
<b>Supported Services</b>	<ul style="list-style-type: none"> <li>• Firewall Management</li> <li>• VPN Management</li> <li>• Gateway Management</li> <li>• VStream Antivirus Updates</li> <li>• Real-Time Monitoring</li> <li>• Automated Firmware Updates</li> <li>• Dynamic DNS</li> <li>• Role-Based Permissions</li> <li>• Logging and Reporting</li> <li>• Web Filtering</li> <li>• Vulnerability Scanning (Nessus Required)</li> <li>• Built-in Customer Database</li> <li>• Customer Emailing</li> <li>• Self-Provisioning Portal</li> </ul>	<ul style="list-style-type: none"> <li>• Firewall Management</li> <li>• VPN Management</li> <li>• Gateway Management</li> <li>• VStream Antivirus Updates</li> <li>• Real-Time Monitoring</li> <li>• Automated Firmware Updates</li> <li>• Dynamic DNS</li> <li>• Role-Based Permissions</li> <li>• Logging and Reporting</li> <li>• Web Filtering</li> <li>• Built-in Customer Database</li> <li>• Customer Emailing</li> </ul>		
<b>Integration</b>	<ul style="list-style-type: none"> <li>• SOAP/XML API</li> <li>• XML Import/Export</li> <li>• LDAP Integration</li> </ul>	<ul style="list-style-type: none"> <li>• SOAP/XML API</li> <li>• XML Import/Export</li> </ul>		
<b>Operating Systems</b>	Microsoft Windows 2000/2003 Server	-		
<b>Directory Servers</b>	<ul style="list-style-type: none"> <li>• Microsoft Active Directory</li> <li>• Sun iPlanet Directory Server</li> </ul>	-		
<b>SKUS</b>	Security Management Portal (SMP) – 10 Gateways	SMP-10	SMP On-Demand Annual Pack for 50 Gateways	SMP-OD-BASE-50
			SMP On-Demand Annual Extension Pack for 10 Gateways	SMP-OD-EXT-10
	Security Management Portal (SMP) – 50 Gateways	SMP-50	1 Year of Web Filtering – 5 nodes	SMP-UFP-5USR
	Security Management Portal (SMP) – 250 Gateways	SMP-250		
	Security Management Portal (SMP) – 500 Gateways	SMP-500		
	Security Management Portal (SMP) – 1000 Gateways	SMP-1000		
	Security Management Portal (SMP) – 5000 Gateways	SMP-5000		
	1 Year of Software Updates – 5 nodes	SMP-FIRM-UPD-5USR		
	1 Year of VStream Antivirus Signature Updates – 5 nodes	SMP-VSTREAM-UPD-5USR		
1 Year of Web Filtering – 5 nodes	SMP-UFP-5USR			

### SCALABILITY

- Scalable to 100,000 plus devices
- Automated server load balancing
- Automated server failover
- Profile-based management
- Batch updates

### MANAGED DEVICES

- Check Point Safe@Office
- ZoneAlarm Secure Wireless Router Z100G
- Check Point UTM-1 Edge
- Nokia IP30 / IP40 / IP60
- NEC SecureBlade



**CONTACT US:** For more information on SMP, contact us at <http://www.sofaware.com/contactus.aspx>.

©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, DynamicShielding 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, INSPECT XL, 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, SmartView Tracker, 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.

March 13, 2007 P/N 502588

**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](mailto: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](http://www.checkpoint.com)



**Check Point**  
 SOFTWARE TECHNOLOGIES LTD.