

Security Management Portal

Cost-effective, managed security

YOUR CHALLENGE

Outsourced security services is one of the fastest growing market segments in the security marketplace. As a result of growing awareness and increasingly sophisticated network security threats, small businesses are turning to outside expertise in securing their office networks. This creates a unique opportunity for service providers and network integrators to increase customer loyalty and generate new revenue streams by providing remotely managed network security and VPNs.

However, remote management can often involve repetitive and confusing tasks, a multitude of equipment, provide insufficient compatibility with existing billing systems, and require a large financial investment. You need a solution that allows quick and cost-effective management of multiple client offices and multiple clients and that supplies a variety of value-added services to the subscriber.

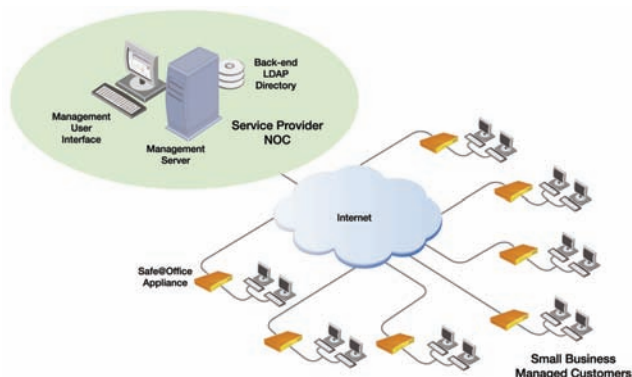
OUR SOLUTION

Security Management Portal (SMP) introduces a new management model for MSSPs (Managed Security Service Providers) that target the small business and vertical markets. SMP offers a robust, resilient architecture that supports from tens to tens of thousands of Safe@Office® gateways. SMP has an intuitive, Web-based user interface, which includes a host of service-provider-oriented capabilities and allows easy and quick integration with existing systems, such as billing systems.

SMP includes a set of built-in virus and spam scanners that make it possible for you to deliver value-added services to end users with more revenue potential than ever before.

The Security Management Portal was developed by SofaWare Technologies, a Check Point company focusing on building innovative solutions that allow service providers and network integrators to deliver managed broadband security solutions to small businesses.

Security Management Portal enables the delivery of cost-effective, comprehensive managed security services to small businesses. By outsourcing Internet security and network management, small businesses can lower costs and receive value-added services as well as enterprise-class security for their office networks.



SECURE, RESILIENT ARCHITECTURE

Built to easily support from tens to tens of thousands of small business security gateways.

FIREWALL AND VPN MANAGEMENT

Remote management of firewall and intrusion prevention settings as well as dynamic VPN communities.

ANTIVIRUS AND ANTI-SPAM

Automatic signature updates and on-the-fly scanning of email for viruses and spam.

WEB FILTERING

Highly customizable URL based Web filtering.

SECURITY REPORTING

Automatically generated security reports demonstrate the performance and effectiveness of the security services.

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

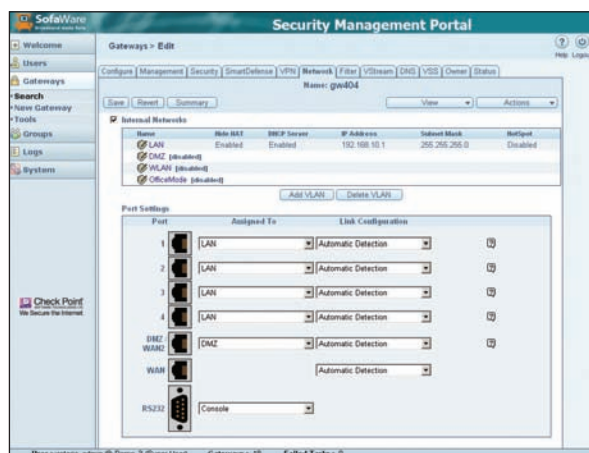
A complete subscription management solution for security service providers.

ALL-IN-ONE

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

- Network and firewall management
- VPN management
- Firmware updates
- Email antivirus and anti-spam
- Gateway antivirus signature updates
- Web content filtering
- Logging and reporting
- Dynamic DNS
- Vulnerability scanning

These features enable service providers and network integrators to deliver cost-effective, comprehensive managed security services to small businesses while lowering installation costs by letting you manage everything remotely and eliminating the need for on-site configuration and troubleshooting.



ARCHITECTURE

SMP's primary elements are a management server and an intuitive, Web-based user interface.

SMP's Web-based user interface simplifies security management for deployments of tens to tens of thousands of customers. It provides an easy way 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 to enable a Web-based self-provisioning portal that lets managed customers directly edit some of their own settings. This further simplifies security provisioning and monitoring while increasing customer participation.

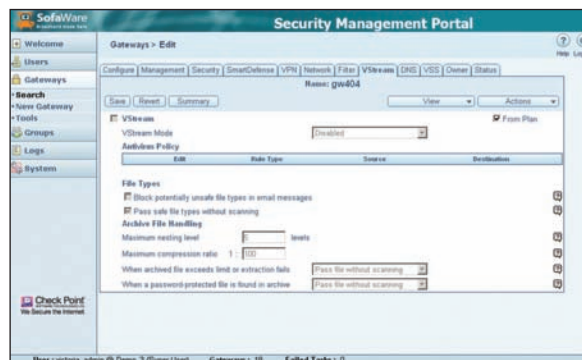
SIMPLE PROVISIONING AND MAINTENANCE

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, administrators simply update the plans via SMP's Web-based user interface and then watch as the updates are being applied automatically to the appropriate Safe@Office gateways with no further effort required by the administrators.

This delivers unparalleled scalability and time-savings by eliminating the need to make repetitive policy changes to thousands of devices individually.



VIRUS AND SPAM SCANNING

By offering a centralized, network-based email antivirus and anti-spam solution, SMP blocks security threats before they ever reach the customer's network. The antivirus signatures are automatically updated, keeping the security up-to-date with no need for any user or network administrator intervention.

SMP owners can choose between built-in virus and spam scanners and third-party OPSEC CVP based scanners.

SMP offers support for gateway antivirus updates. Signatures are automatically fetched from the SofaWare online update center and then efficiently delivered by SMP to gateways subscribed to the gateway antivirus updates service.

WEB CONTENT FILTERING

SMP supports URL based Web filtering, allowing users to protect their employees and families from up to 32 categories of objectionable or malicious Web sites. In addition, gateway-specific or global white and black lists can be defined to allow or block access to specific URLs.

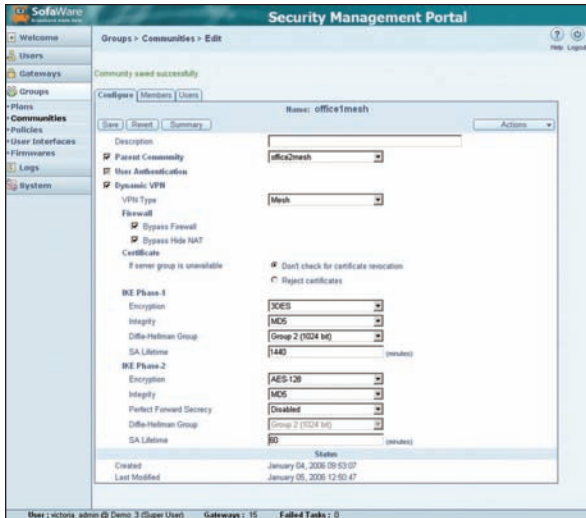
This feature allows small business owners to block access to objectionable sites from their entire network (using categories that cover content such as pornography and fraud sites), as well as block access to sites which they just don't want their employees to access during work time, such as shopping or gambling.

INSTANT MANAGED VPN DEPLOYMENT

SMP enables administrators to create VPNs in a single operation by using the Dynamic VPN (DVPN) module.

Administrators can define VPN communities and set security parameters for the entire VPN in one step. By grouping a customer's VPN endpoints in a community, a fully meshed VPN is automatically enabled among those points (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. Additionally, the Dynamic VPN module fully supports dynamically addressed IP gateways and takes care of automatically updating all VPN end

points with the most recent IP addresses of the gateways in their community. This further reduces administrators' burdens.

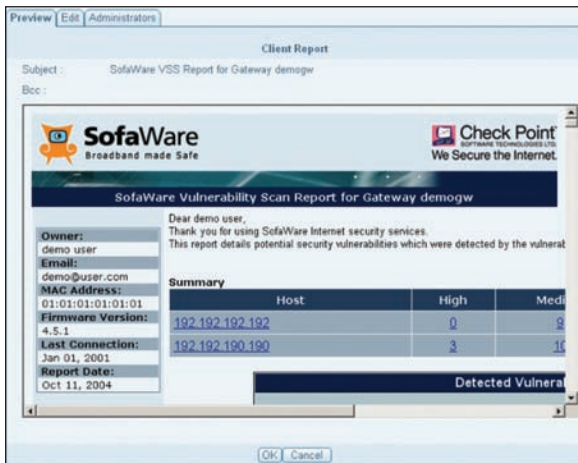


VULNERABILITY SCANNING SERVICE

By offering an integrated vulnerability scanning service (VSS), SMP offers the ability to scan subscriber networks for security vulnerabilities.

Vulnerability scanning reports can be automatically generated 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. The vulnerability scanning reports are HTML-based and can be extensively customized by editing a report template.



STRONG AUTHENTICATION OUT-OF-THE-BOX

Service providers that want to implement strong authentication can do so by using the Internal Certificate Authority 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 community 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

Making sure that tens of thousands of managed 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.

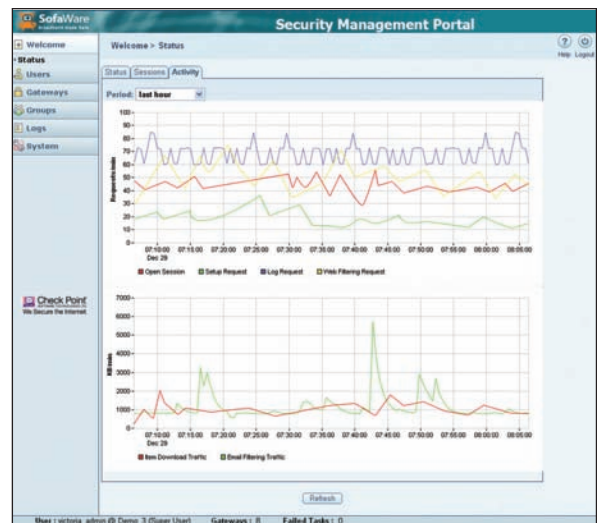
The SMP administrator also has the option to override the group settings and push unique firmware and settings to specific gateways.

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, the security reports can be viewed directly from the Security Management Portal. The security reports 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 the devices connected at a single glance, including real-time load visualization graphs, real time status displays, and customizable alerts on security and connectivity events.



EFFORTLESS SUPPORT FOR DYNAMICALLY ADDRESSED GATEWAYS

If customer gateways are assigned dynamic IP addresses, tracking and monitoring them can become a concern since their IP addresses change each time they connect to the Internet.

SMP alleviates this concern by fully supporting management and monitoring of dynamically addressed gateways.

In addition, SMP can act as a Dynamic Domain Name Service (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, DDNS 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 to distribute 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 on, improving security by providing information than can identify unauthorized policy changes.

RESILIENT MANAGEMENT INFRASTRUCTURE

Security Management Portal provides a fully redundant management infrastructure that enables around-the-clock control of customer security. Service providers may deploy more than one management server in a NOC, with full load

balancing and automatic failover, enabling carrier grade service, fault tolerance and scalability.

EASY INTEGRATION

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

VIRTUAL PORTALS

SMP allows the creation of virtual portals, or multiple instances of SMP on the same server, each one acting as a standalone "virtual SMP." For example, a service provider with multiple resellers can configure a private instance for each reseller. This allows saving on hardware, software, and ongoing maintenance, while allowing resellers to manage their own customers with minimal initial capital investment.

CENTRALIZED MANAGEMENT

- Firewall management
- Network management
- Public hot spot management
- Gateway antivirus definition updates
- Real-time monitoring
- Automated firmware updates
- Dynamic DNS
- Role-based permissions

VIRTUAL PRIVATE NETWORKING

- Complete dynamic IP support
- Built-in Certificate Authority (CA)

CONTENT FILTERING

- Antivirus service
- Anti-spam service
- Web filtering service

LOGGING AND REPORTING

- Centralized logging
- Security reporting
- Automatic report mailing
- Customizable report templates
- Status monitoring and alerting

SUBSCRIBER MANAGEMENT

- Built-in customer database
- Customer emailing
- Self Provisioning Portal (SPP)

SCALABILITY

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

INTEGRATION

- LDAP
- Built-in syslog server
- SOAP/XML protocol support and XML import/export

OPERATING SYSTEMS

- Microsoft Windows 2000/2003 Server
- Sun Solaris 8.0/9.0

DIRECTORY SERVERS

- Microsoft Active directory
- Sun iPlanet Directory Server

MANAGED DEVICES

- Check Point Safe@Office, ZoneAlarm Z100G Secure Wireless Router
- Check Point VPN-1® UTM Edge™
- Nokia IP40/IP45/IP60
- NEC SecureBlade

CONTACT US

For more information on SMP, contact us at smp@sofaware.com.



©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, 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, 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.

March 13, 2007 P/N 502451

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.