Security Management Center

October 2013

Unified Network Security Management

The Security Management Center (SMC) forms the core of our security solution, providing unified network security management for the Stonesoft Next Generation Firewall, Firewall/VPN, IPS, and SSL VPN. In addition to managing Stonesoft devices, the Security Management Center also provides event management, status monitoring, and reporting capabilities for third-party devices. By collecting all this information in one centralized system, administrators can get a good overview of what is happening in their environment.

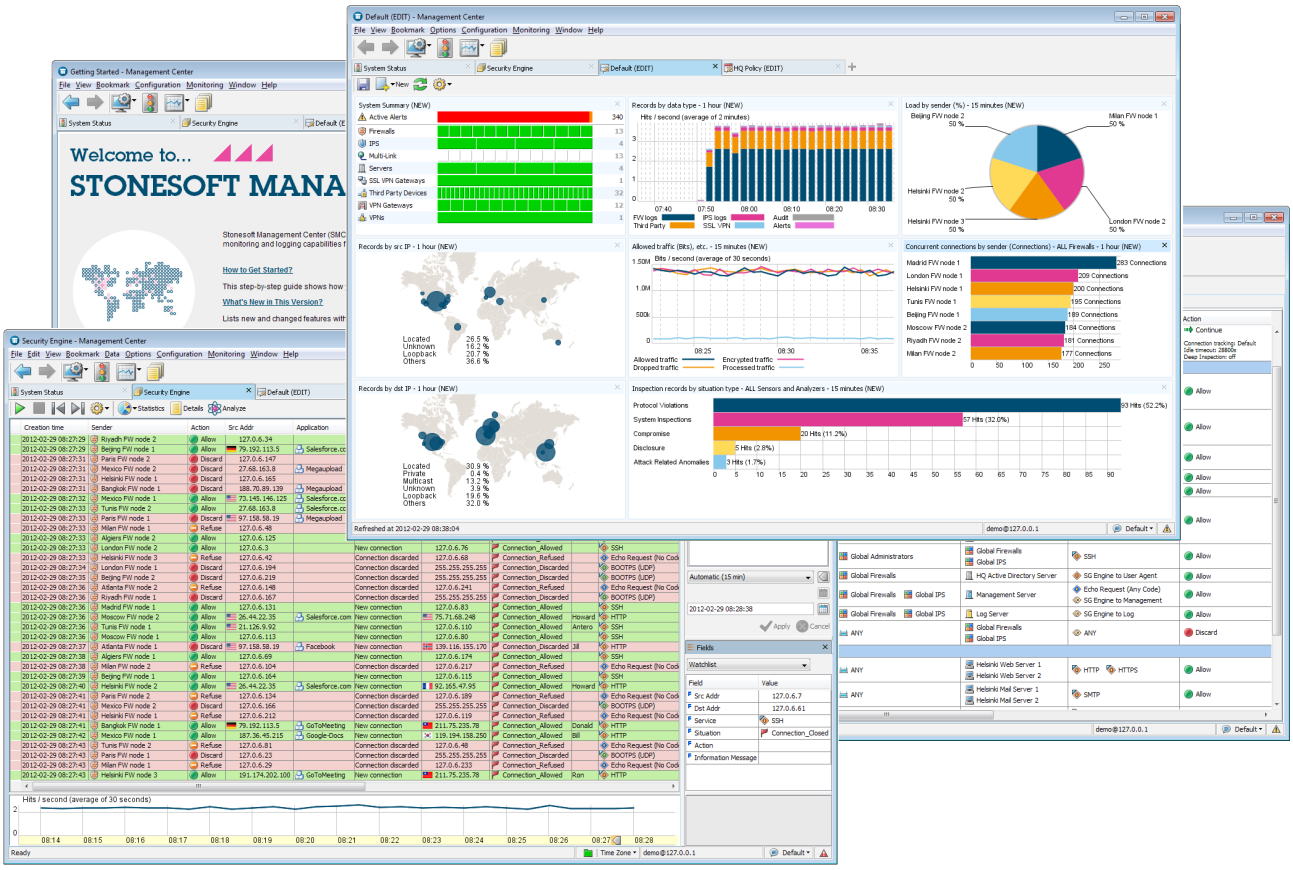
The Security Management Center includes at least one Management Server and one Log Server, which can be installed either to the same or to separate servers. The Management Client is the graphical user interface used for configuring, managing and monitoring the entire system. Optionally the Security Management Center solution can be extended by adding additional Management and Log Servers, Web Portal Servers and Authentication Servers.

The Security Management Center is designed to manage large, geographically-distributed installations. It is flexible and allows scaling up the existing components and adding new components to the system without sacrificing its ease-of-use. The larger the environment, the greater the benefits you gain through the efficient policy management, and the centralized monitoring and reporting capabilities the SMC provides. The administration workflows are optimized to make daily security management as efficient as possible.

The Security Management Center High Availability (HA) enables the creation of an extremely resilient management infrastructure, ensuring continuous access to the management and log resources. When using Management Server HA, administrators have full control of the security devices even if the primary Management Server is unavailable. Log Server HA ensures that logs and alerts are received even if the primary Log Server is unavailable. With HA licenses, it is possible to ensure that maintenance of the Management or Log Server does not cause any interruptions in business traffic.

STONESOFT
A McAfee Group Company

Security Management Center Specifications



The Security Management Client provides all relevant security management tools and functions in the same unified graphical user interface. Configuration, monitoring, logging, status information, alerts, reports, updates, and upgrades can be managed centrally for all devices, regardless of their physical location. All these tools have been designed to work seamlessly together from day one. The Management Client provides administrators with useful shortcuts and drill-down actions for effective management of the whole security environment.

Security Management Center Specifications

MANAGEMENT SERVER	
Number of Managed Engines	License limited. 2-2000 nodes with one Management Server.
Number of Administrators	Unlimited
Number of Elements	Unlimited
Number of Policies	Unlimited
Number of Log Servers	Unlimited
Number of Web Portal Servers	Unlimited
Administrator Authentication	Local database, RADIUS
Device Connections	SSL encrypted

LOG SERVER	
Number of Supported Engines	Unlimited
Log Records per Second	The high performance logging system is able to process more than 100 000 records/s
Device Connections	SSL encrypted
Log Storage Size	Unlimited
Number of Log Forwardings per Log Server	Unlimited

STONESOFT
A McAfee Group Company

Security Management Center Specifications

FEATURES

General	
Management Client	Java based client program with Webstart support
SMC API	Documented API enabling easy 3rd party product and service integration. Uses REST architecture where data can be XML or JSON coded.
Simultaneous Administrators	Several administrators can perform changes at the same time. Critical elements like policies are locked for editing
High Availability	Support for up to four standby management servers
Automatic Updates and Upgrades	Management downloads automatically the latest engine upgrades and dynamic updates
Backups	Integrated backup tool for taking backups from the whole system including all engine configurations
Navigation	Intuitive browser-like navigation with browsing history, tabs and bookmarks
Search Tools	Efficient element and references search tools
Quick Filtering	Convenient type-ahead filtering in element lists, tables and policy cells.
Multi-Selection support	Perform actions and commit changes to hundreds of elements at the same time
System Clean Up Tools	Enables administrator to find easily which elements and rules are not used

Administration	
Alert Escalations	Allows administrator to forward alerts from the system using Email, SMS, SNMP trap and custom scripts
Alert Thresholds	Automatic alert thresholds for Overview Statistics
Audit Logs	Extensive audit information about all changes in the system
System Reports	Inventory and audit reports about administrators´ activities
Plug and Play Installation	Automatic installation cloud (or USB stick) based installation with initial policy push
Automated tasks	Refresh policies, archive/export/delete logs, take backups etc. with automated tasks
Domains	Allows to divide environment to isolated configuration domains (see separate datasheet for more details)
Import/Export	XML and CSV export and import with intelligent conflict handling between SMC installations
Messenger Tool	Integrated administrator messaging tool
Remote Upgrades	One-click fail-safe remote upgrade
Role Based Access Control	Flexible and accurate administrators´ permission control
License Management	Automatic license online updates and maintenance contract status reports
Troubleshooting Tools	Extensive remote diagnostic capabilities: integrated traffic capture tool, diagnostics, configuration snapshot download from engines, session monitoring views, etc.

Configuration	
Authentication Server	SMC Server that provides 4 RADIUS based strong authentication methods and automatic user linking capabilities for existing AD/LDAP Server (see separate datasheet for more details)
Routing	Drag & drop Routing configuration for the Firewalls
Automatic Antispoofing	Antispoofing configuration is created automatically based on Routing
VPN Management	Easy-to-use VPN editor and VPN diagrams that reveal the underlying topology
Incident Case Management	Integrated tools for collaborative network incident management
Firewall Element Creation Wizard	Create hundreds of Firewall Elements through a Firewall Creation Wizard
Browser Based User Authentication	Configure and customize an easy browser based authentication service for your end users
Anti-Spam	Flexible Anti-Spam configuration for Firewalls
Multi-Link Configuration	Configure Stonesoft patented Multi-Link solution graphically from SMC

Policy Management	
Virtual Engines	Share same Master Engine across several SMC Domain to up to 250 Virtual Engines that can each have their own policies and routing tables
Hierarchical Policy Management	Policy templates, Sub-Policies, Aliases and Rule Comment Sections keep the policy organized and understandable
Application Identification	Ability to identify applications by payload and restrict access accordingly
URL Filtering	Restrict access by URL categories
Domain Names	Restrict access dynamically by using Domain Names
User Identification	Create user-based rules either with or without authentication
Zones	Physical interfaces can be tagged with Zones and referred in the policies
QoS Policies	Quality of Service class based policy configuration
Policy Validation Tool	Helps administrator to find configuration mistakes before policy activation
Policy Snapshots	Allows to explore and compare engines´ configuration history.
Policy Restoration	A previous policy version can be recovered and uploaded to the engine
Rule Usage Optimization Tool	Enables administrator to see how many times each rule has matched within a specified time period
Rule Search Tool	Integrated tool for searching rules in policies
Rule Names	Ability to create rule names which are visible in logs, statistics and reports
Fail-Safe Policy Uploads	System automatically restores the previous policy version in case the new version fails

Status, Statistics and Reporting	
System Status Monitoring	Real-time status information about network devices and their connections
Appliance Status Monitoring	Graphically follow the hardware status of the appliances
Networks Diagrams	Visualize configurations, topologies and status connectivity with drawings
Session Monitoring	Dedicated views to monitor connections, VPN SAs, authenticated users, active alerts and dynamic and static routes
Overviews	Customizeable dashboards of network statistics for real-time monitoring
Geolocations	See the country information for all IP addresses with the help of country flags and geolocation statistics. See where the network attacks come from
Reporting	Customizable and schedulable reports that provide detailed information about the network statistics
Web Portal	Light-weight web access to policies, logs and reports (see separate datasheet for more details)

Third Party Event Management	
Third Party Device Monitoring	Allows administrator to monitor and view status changes in third party device availability
Third Party Device Log Reception	Log parsing and reception in syslog format for third party devices. Out of box support for CEF, LEEF, CLF and WELF format
NetFlow/IPFIX Reception	Ability to receive and consolidate data in NetFlow v9 and IPFIX formats
Third Party Device Statistics	Graphical statistics and reports based on third party log data and SNMP counters
Number of Supported Third Party Devices	200 per log server
Licensing	Each third party device consumes 0.2 from management server license device count

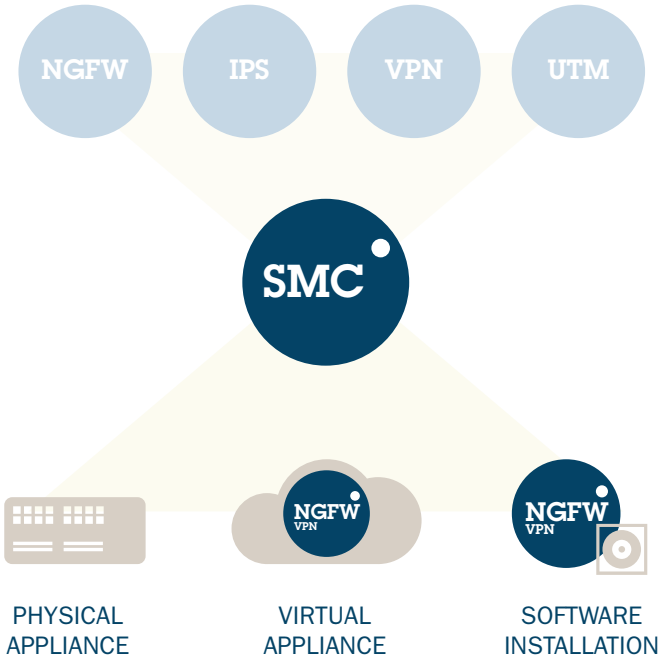
Logs	
Log Browser	Common log browsing view for all log data
Drag & Drop Filtering	Efficient log filtering - just drag and drop any log data cell to the Query panel
Log Statistics	Create log statistics on the fly and see the top trends
Log Visualizations	Find the anomalies in logged traffic in filtrable log visualizations
Log Aggregations	Summarize large amount of filtered log data by any columns
Archiving	Archive logs in multiple directories by using filtering
Backups	Integrated backup mechanism for Log Server configuration and log data
Log Exports	CSV, XML, CEF and LEEF log exporting. Logs can be also exported to PDF and ZIP files directly from log browser
Log Forwarding	Real-time log redirection in syslog, CEF, LEEF, XML, CSV, IPFIX and NetFlow formats. Configuration for filtering, data type and log field selection available
Log Data Contexts	Shortcuts to browse different types of logs with dedicated column sets.
High Availability	Support for backup log servers

PRODUCT CODES

LIC-SG-SMC-X	Security Management Center (SMC) for 2-2000 managed devices
LIC-SG-SMC-XX-HA2	Two Management Servers in active-standby mode for 2-2000 managed devices
LIC-SG-LOG	Additional Stonesoft Log server

SUPPORT

Premium Support	24/7-call logging via web, email and phone, two hour response time, software updates
Basic Support	8/5-call logging via web, email and phone, next business day response time, software updates



Unified management for different installation types and roles.

Stonesoft Corporation International Headquarters
Itälahdenkatu 22A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
A McAfee Group Company

Stonesoft Inc Americas Headquarters
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131