

# FORCEPOINT NGFW Security Management Center (SMC)

Single-pane NGFW/IPS administration for maximum visibility across the network

**Forcepoint NGFW Security Management Center (SMC) provides unified, centralized management of all models of Forcepoint Next Generation Firewalls – physical, virtual or cloud – across large, geographically distributed enterprise environments.**

With superior flexibility, scalability and ease-of-use, Forcepoint SMC makes dynamic network security environments more manageable and able to support aggressive business growth plans. Its “Smart Policies” enable business processes to be expressed in natural terms, while its optimized workflows streamline daily administrative tasks for high efficiency and low total cost of ownership (TCO).

SMC provides 360° visibility throughout enterprise networks, gathering event management and status monitoring information from Forcepoint NGFWs, endpoints and third-party devices for interactive investigation as well as detailed reports.

In addition, Forcepoint SMC can aggregate NGFW log data from multiple, geographically distributed Forcepoint NGFW Log Servers for consolidated reporting while maintaining data sovereignty.

## High Availability

Today’s businesses have zero tolerance for disruption, demanding around-the-clock access to critical resources. With Forcepoint’s SMC’s high availability option, organizations maintain continuous access to log resources for resilient incident analysis and response.

## Security Management Client

Regardless of geographic location, administrators can securely access the Forcepoint SMC through its Management Client. This client provides a powerful graphical user interface for configuration, monitoring, logging, alerts, reports, updates and upgrades to Forcepoint Next Generation Firewalls. The Forcepoint SMC client gives administrators a holistic view of the network and context- driven drill-down actions for fast, effective management of your entire security environment.

## Key Benefits

- ▶ **Centralized, single-pane management of up to 2000 physical or virtual Forcepoint NGFWs throughout distributed environments**
- ▶ **Flexibility and scalability for deployment in large enterprise networks**
- ▶ **High availability option for demanding uptime requirements**
- ▶ **Smart Policies and efficient workflow automation for fast and accurate deployment and maintenance of Forcepoint NGFW**
- ▶ **User and endpoint context, awareness and visibility across your entire network, from the data center and edge to branch sites and the cloud**
- ▶ **Choice of software deployment options or appliance**



## Forcepoint NGFW Security Management Center (SMC) Specifications

MANAGEMENT SERVER	
Number of Managed Devices	Licensed: 1 to 2,000 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, TACACS+, Client Certificate
Device Connections	SSL-encrypted
LOG SERVER	
Number of Supported Devices	Unlimited
Log Records per Second	The high-performance logging system can process more than 500,000 records per second
Device Connections	SSL-encrypted, IPv4/IPv6
Log Storage Size	Unlimited
Number of Log Forwarding per Log Server	Unlimited
FEATURES	
GENERAL	
Management Client	Java-based for Windows and Linux and Java Web Start for Mac
SMC Application Programming Interface (SMC API)	Documented API enabling easy third-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
Home Screen Dashboards	Customizable home screen dashboards for NGFWs, VPNs, users and other elements
User Behavior Correlations	User behavior-related checks and dashboards for user names and source IP addresses



## Forcepoint NGFW SMC Specifications (continued)

<b>High Availability</b>	Up to four standby management servers
<b>Upgrades</b>	Upgrades and dynamic update packages can be automatically downloaded
<b>Backups</b>	Integrated backup tool for taking backups from the whole system, including all next generation firewall configurations
<b>Navigation</b>	Intuitive browser-like navigation with browsing history, tabs and bookmarks
<b>Spotlight Search Tools</b>	Efficient element and references search tools with context-sensitive quick actions
<b>Quick Filtering</b>	Convenient type-ahead filtering in element lists, tables and policy cells
<b>Multi-Selection Support</b>	Perform actions and commit changes to hundreds of elements simultaneously
<b>System Clean-Up Tools</b>	Enables administrator to easily find which elements and rules are not used
<b>ADMINISTRATION</b>	
<b>Alert Escalations</b>	Allows administrator to forward alerts from the system using email, SMS, SNMP trap and custom scripts
<b>Alert Thresholds</b>	Automatic alert thresholds for overview statistics
<b>Audit Logs</b>	Extensive audit information about all changes in the system
<b>System Reports</b>	Inventory and audit reports about administrators' activities
<b>Plug-and-Play Installation</b>	Cloud (or USB stick)-based installation with initial policy push
<b>Automated Tasks</b>	Refresh policies, archive, export and delete logs, make backups with automated tasks
<b>Administrative Domains</b>	Allows division of the environment into isolated configuration domains
<b>Import/Export</b>	XML and CSV export and import with intelligent conflict handling between SMC installations
<b>Remote Upgrades</b>	One-click fail-safe remote upgrade
<b>Administrator Role-Based Access Control</b>	Custom roles can be defined and combined in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Super User) to control permissions flexibly and accurately
<b>License Management</b>	Automatic online license updates and maintenance contract status reports
<b>Certificates Management</b>	Consolidated view of all certificates and credentials
<b>Troubleshooting Tools</b>	Extensive remote diagnostic capabilities: integrated traffic capture tool, diagnostics, configuration snapshot download from next generation firewall and session monitoring views



## Forcepoint NGFW SMC Specifications (continued)

POLICY MANAGEMENT	
<b>Virtual Contexts</b>	Share same master context across several SMC Administrative Domains; up to 250 virtual contexts, each with its own policies and routing tables
<b>Hierarchical Policy Management</b>	Policy templates, sub-policies, aliases and rule comment sections keep the policy organized and understandable
<b>Application Identification</b>	<ul style="list-style-type: none"><li>▶ Restrict access based on network and/or client applications</li><li>▶ Identify applications by payload and restrict access accordingly</li><li>▶ Whitelist/blacklist by application name and version from Forcepoint Endpoint Context Agent</li></ul>
<b>Change Management</b>	Require review and approval by a second administrator before changes are deployed
<b>URL Filtering</b>	Restrict access by URL categories
<b>Domain Names</b>	Restrict access dynamically by using domain names
<b>User Identification</b>	Create user-based rules either with or without authentication
<b>Zones</b>	Physical interfaces can be tagged with zones and referred to in the policies
<b>Geoprotection</b>	Restrict access by countries or geographical regions
<b>Inspection Policies</b>	Granular control for deep packet inspection and easy ways to toggle off false positives
<b>Quality of Service (QoS) Policies</b>	QoS class-based policy configuration
<b>Policy-Based File Filtering</b>	Define how files are inspected using McAfee Global Threat Intelligence file reputation, Anti-Malware Scan and McAfee Advanced Threat Defense
<b>Network Address Translation (NAT)</b>	<ul style="list-style-type: none"><li>• Default NAT</li><li>• Element-based NAT</li><li>• NAT policies</li></ul>
<b>Policy Validation Tool</b>	Helps administrator find configuration mistakes before policy activation
<b>Policy Snapshots</b>	Allows for exploration and comparison of Forcepoint Next Generation Firewall configuration history
<b>Policy Restoration</b>	A previous policy version can be recovered and uploaded to the next generation firewall
<b>Rule Usage Optimization Tool</b>	Enables administrators to see how many times each rule has matched within a specified time period
<b>Rule Search Tool</b>	Integrated tool for searching rules in policies
<b>Rule Names</b>	Ability to create rule names that are visible in logs, statistics and reports
<b>Fail-Safe Policy Uploads</b>	System automatically restores the previous policy version if the new version fails



## Forcepoint NGFW SMC Specifications (continued)

CONFIGURATION	
<b>Routing</b>	Drag-and-drop routing configuration for the firewalls and specific widgets to add routes and default routes
<b>Dynamic Routing</b>	Advanced OSPF and BGP configuration via intuitive graphical user interface
<b>Automatic Anti-spoofing</b>	Anti-spoofing configuration is created automatically based on routing
<b>Site-to-site VPNs</b>	<ul style="list-style-type: none"><li>▶ Policy-based IPsec VPN</li><li>▶ Route-based IPsec VPN and tunneling (GRE)</li></ul>
<b>Remote access VPNs</b>	<ul style="list-style-type: none"><li>▶ IPsec VPN client (iOS and Windows)</li><li>▶ SSL VPN client (Android, Mac and Windows)</li><li>▶ Clientless SSL VPN Portal</li></ul>
<b>Endpoint Context Agent Management</b>	Extend access control and visibility to the applications running on endpoints
<b>Incident Case Management</b>	Integrated tools for collaborative network incident management
<b>Firewall Element Creation Wizard</b>	Create hundreds of firewall elements through a firewall creation wizard
<b>Browser-Based User Authentication</b>	Configure and customize an easy browser-based authentication service for users
STATUS, STATISTICS AND REPORTING	
<b>System Status Monitoring</b>	Real-time status information about network devices and their connections
<b>Appliance Status Monitoring</b>	Graphical view on the hardware status of the appliances
<b>Networks Diagrams</b>	Visualize configurations, topologies and status connectivity
<b>Session Monitoring</b>	Dedicated views to monitor connections, VPN security associations (SAs), authenticated users, active alerts and dynamic and static routes
<b>Overviews</b>	Customize dashboards of user and network statistics for real-time monitoring
<b>Geolocations</b>	Show the country information for all IP addresses with the help of country flags and geolocation statistics. Show where network attacks come from
<b>Reporting</b>	Customize and schedule reports that provide detailed information about network statistics. Detailed Advanced Malware Detection reports
<b>Web Portal</b>	Lightweight web access to policies, logs and reports



## Forcepoint NGFW SMC Specifications (continued)

THIRD-PARTY MANAGEMENT	
<b>Device Monitoring</b>	Allows administrator to monitor and view status changes in third-party device availability
<b>Device Log Injection</b>	Log parsing and reception in syslog format for third-party devices and out-of-the box support for CEF, LEEF, CLF and WELF format
<b>NetFlow/IPFIX Reception</b>	Ability to receive and consolidate data in NetFlow v9 and IPFIX formats
<b>Device Statistics</b>	Graphical statistics and reports based on third-party log data and simple network management protocol (SNMP) counters
<b>Number of Supported Devices</b>	200 per Log Server
<b>Licensing</b>	Each third-party device consumes 0.2 from Management Server license device count
LOGS	
<b>Browser</b>	Granular view for separate log types such as VPN, file filtering and endpoint in addition to common log browsing view for all log data
<b>Drag-and-Drop Filtering</b>	Interactive log filtering—drag and drop any log data cell to the Query Panel
<b>Statistics</b>	Create log statistics on the fly and see the top trends
<b>Visualizations</b>	Find the anomalies in logged traffic in filterable log visualizations
<b>Aggregations</b>	Summarize the large amount of filtered log data by any columns
<b>Archiving</b>	Archive logs in multiple directories by using filtering
<b>Backups</b>	Integrated backup mechanism for Log Server configuration and log data
<b>Exports</b>	CSV, XML, CEF, LEEF and McAfee Enterprise Security Manager log exporting; logs can also be exported to PDF and ZIP files directly from the log browser
<b>Forwarding</b>	Real-time log redirection in syslog; CEF, LEEF, XML, CSV, IPFIX, NetFlow and McAfee Enterprise Security Manager formats; configuration for filtering, data type; and log field selection available
<b>Data Contexts</b>	Shortcuts to browse different types of logs with dedicated column sets
<b>High Availability</b>	Support for backup Log Server



## Centralized Management of Multiple Customer Environments

Managed Security Service Providers (MSSPs) need to reduce the high administrative costs associated with managing multiple servers across multiple domains. Forcepoint Administrative Domain License enables multiple customer environments to be managed through a single management server. Configurations can be reused and shared across domains for rapid and efficient distribution of changes. The unique architecture of the

Forcepoint Administrative Domain License solution simplifies enterprise and MSSP environments, making them easier to maintain. Role-based access control (RBAC) ensures accurate definition of administrator responsibilities and domain access limitations. Domain-based customers can access reports, policy configurations and logs easily via a secure, lightweight web portal.

## Forcepoint Administrative Domain License Specifications

DOMAINS	
Maximum Number	200
Number of Administrators	Unlimited
Number of Managed Devices	Unlimited
Number of Elements	Unlimited
FEATURES	
Configuration Separation	Isolate customer environments to different domains, and make sure that customers' network elements never get mixed up
Configuration Sharing	Share elements such as policy templates for all domains
Access Control	Configure the administrators' visibility and responsibilities with the help of domains
Monitoring	Monitor the status of all granted domains with the help of the domain overview
Customization	Customize the PDF style templates
Migration Tools	Move elements between domains with the integrated "move-to" tool
Import/Export	Import and export elements between different SMC installations and domains
Virtual Contexts	Share the same master context across domain boundaries of up to 250 virtual contexts, which can each have their own policies and routing tables



## Forcepoint Web Portal Server

Forcepoint Web Portal Server provides MSSPs' customers, administrators and management with a lightweight web-based portal for viewing logs, scheduled reports, current policies and policy change history. MSSP administrators can configure the amount of information displayed on the portal based on customer needs or to reduce support requests.

Forcepoint Web Portal Server supports English, Spanish and French natively, with the ability to add new languages.

### Key Benefits

- ▶ **Clientless, read-only access to logs, reports, policies and policy change history**
- ▶ **Real-time network status available for defined users**
- ▶ **Support for mobile devices**

## Forcepoint Web Portal Server Specifications

SPECIFICATIONS	
Maximum Number of Concurrent Users	250 per license
Number of Administrators	Unlimited
Number of Web Portal Users	Unlimited
User Authentication	Management Server database, RADIUS, TACACS+
Device Connections	SSL-encrypted
FEATURES	
Security Policies	View next generation firewalls' latest configurations in HTML format
Reports	View reports that are scheduled to be published in the web portal in HTML format
Log Browsing	Browse and filter the logs in HTML format
Log Details	Monitor the status of all granted domains with the help of the domain overview
PDF Export	View log event visualizations and other log details in a separate HTML page
Announcements	Administrators can specify announcements to be shown in the web portal
Policy Comparison	Compare the different next-generation firewall configuration versions to see if the change request has been implemented
Localization	Web portal supports English, Spanish and French, and can be easily translated to support other languages
Customization	Customize the look and feel of web portals





### Forcepoint SMC Appliance

Forcepoint Security Management Center (SMC) Appliance is an all-in-one dedicated device for configuring, managing and monitoring Forcepoint Next Generation Firewalls — physical, virtual and cloud-based. Forcepoint SMC provides ease of deployment to get you up and running quickly, combining Forcepoint’s NGFW management server and log server into a single plug-and-play package running on optimized 1U hardware.

### Forcepoint NGFW SMC Deployment Options

There are three ways to deploy Forcepoint SMC: on your systems, on your bare hardware or hypervisor, or as an all-in-one appliance.<sup>1</sup>

### Forcepoint SMC Appliance Specifications

COMPONENTS	FORCEPOINT NGFW SMC DEPLOYMENT OPTIONS		
	SOFTWARE	ISO IMAGE	APPLIANCE
SMC Software	✓	✓	✓
Operating System	Customer-supplied	✓	✓
Hardware	Customer-supplied	Customer-supplied	✓

### Forcepoint SMC Appliance Specifications

PERFORMANCE	
Managed Firewalls	2,000
Maximum Domains	200
Indexed Logs per sec.	80,000
Events per day	6,912,000,000
Log Size per day (GB)	690

<sup>1</sup> An SMC software license has to be purchased separately for all 3 deployment options. An appliance alone does not include any licenses.



## Forcepoint SMC Appliance Specifications

PHYSICAL	
Form Factor	1U
Processor	2 x Intel Xeon
Memory	32 GB
Storage (HDD)	Capacity 900 GB (4 X 300 GB, RAID-5), Hot Swappable
Power Supply	2 x 550W (100V~240V) Hot Swappable
Dimensions	23.9" D x 17.09" W x 1.68" H (60.7cm D x 43.42cm W x 4.28cm H)
Weight	28.26 lbs. (12.82 kg)
Regulatory & Compliance	FCC / ICES / EN55022 / VCCI/BSMI / C-Tick / SABS / CCC / MIC Class A and UL60950-1 / Verified to comply with RoHS Directive

## Forcepoint SMC Ordering

ORDERING	PART #
Forcepoint NGFW Security Management Center (software)	SMC
Forcepoint NGFW Security Management Center 1000 Appliance	SMCAP
Forcepoint NGFW Security Management Center High Availability (only available for software and ISO image deployments)	SMCHA
Forcepoint SMC Additional Log Server	ALS
Forcepoint SMC Domains (Up to 200 Domains)	ODFSMC
Forcepoint SMC Web Portal	OWPS

**CONTACT**  
[www.forcepoint.com/contact](http://www.forcepoint.com/contact)

© 2018 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[DATASHEET\_FORCEPOINT\_NGFWSECURITYMANAGEMENTCENTER\_EN] 100082.021218