NGFW Security Management Center

Single-pane 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.

Key Benefits

- Centralized, single-pane management of up to 6,000 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

With superior flexibility, scalability and ease-of-use, Forcepoint Security Management Center (SMC) makes dynamic network security environments more manageable and able to support aggressive business growth plans. 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 degree 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.

Forcepoint NGFW SMC Specifications

MANAGEMENT SERVER	
Number of Managed Devices	Licensed: 1 to 6,000 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 and Microsoft Active Directory (LDAP)
Device Connections	TLS-encrypted
LOG SERVER	
Number of Supported Devices	Unlimited
Log Records per Second	The high-performance logging system can receive up to 500,000 records per second
Device Connections	TLS 1.2 Encrypted and authenticated using X.509v3 Keys and Certificates
Log Storage Size	Unlimited
Number of Log Forwarding per Log Server	Unlimited
GENERAL	
Management Client	HTML5 based UI
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 Monitoring	In addition to the user behavior-related correlations and checks, it provides endpoint security status information and endpoint application statistics

High Availability	Up to four standby management servers
Upgrades	Upgrades and dynamic update packages can be automatically downloaded
Backups	Integrated backup tool for taking backups from the whole system, including all next generation firewall configurations
Navigation	Intuitive browser-like navigation with browsing history, tabs and bookmarks
Spotlight Search Tools	Efficient element and references search tools with context-sensitive quick actions
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 simultaneously
System Clean-Up Tools	Enables administrator to easily find 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	Easy alert thresholds for overview statistics
Audit Logs	All changes to the system are recorded in audit logs
System Reports	Inventory and compliance audit reports about administrators' accounts and activities
Zero Touch Provisioning	Cloud (or USB stick)-based installation with initial policy push
Automated Tasks	Automated log data management, archive and retention, backups, upgrades and policy refresh tasks
Administrative Domains	Allows division of the environment into isolated configuration domains
Import/Export	XML and CSV export and import all times, rather than just between installations
Remote Upgrades	One-click fail-safe remote upgrade of the managed NGFWs
Administrator Role-Based Access Control	Custom roles can be defined and combined in addition to predefined roles (e.g., Owner, Viewer, Operator, Editor, Superuser) to control permissions flexibly and accurately
License Management	Automatic online license updates and maintenance contract status reports
Certificates Management	Consolidated view of all certificates and credentials
Troubleshooting Tools	Extensive remote diagnostic capabilities: integrated traffic capture tool, configuration snapshot download from next generation firewall and session monitoring views
Incident Case Management	Integrated tools for collaborative network incident management

POLICY MANAGEMENT	
Virtual NGFW Engine	Share same master context across several SMC Administrative Domains; up to 250 virtual contexts, each with its 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	→ Restrict access based on network and/or endpoint applications → Restrict access from/to applications by payload → Allow list/block list by application name and version from Forcepoint Endpoint Context Agent
Change Management	Require review and approval by a second administrator before changes are deployed
URL Filtering	Restrict access by URL categories
Domain Names	Restrict access dynamically by using domain names that can be translated to IP-addresses
User Identification	Match user-based rules via transparent user identification or enforcing strong authentication methods
Zones	Physical interfaces can be tagged with zones and referred to in the policies
Geoprotection	Restrict access by countries or geographical regions
Inspection Policies	Granular control for deep packet inspection and easy ways to toggle off false positives
Quality of Service (QoS) Policies	QoS class-based policy configuration
Policy-Based File Filtering	Define how files are inspected using McAfee Global Threat Intelligence file reputation, Anti-Malware Scan and McAfee Advanced Threat Defense
Network Address Translation (NAT)	→ Default NAT → Element-based NAT → NAT policies
Policy Validation Tool	Helps administrator find configuration mistakes before policy activation
Policy Snapshots	Allows for exploration and comparison of Forcepoint Next Generation Firewall configuration history
Policy Restoration	A previous policy version can be recovered and uploaded to the next generation firewall
Rule Usage Optimization Tool	Enables administrators 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 that are visible in logs, statistics and reports
Fail-Safe Policy Uploads	System automatically restores the previous policy version if the new version fails

CONFIGURATION	
Routing	Drag-and-drop routing configuration for the firewalls and specific widgets to add routes and default routes
Dynamic Routing	Advanced OSPF and BGP configuration via intuitive graphical user interface
Automatic Anti-spoofing	Anti-spoofing configuration is created automatically based on routing
Site-to-site VPNs	→ Policy-based IPsec VPN → Route-based IPsec VPN and tunneling (GRE)
Remote access VPNs	→ IPsec VPN client (iOS and Windows) → SSL VPN client (Android, Mac and Windows) → Clientless SSL VPN Portal
Endpoint Context Agent Management	Extend access control and visibility to the applications running on endpoints
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 users
STATUS, STATISTICS, AND REPORTING	
System Status Monitoring	Real-time status information about network devices and their connections
Appliance Status Monitoring	Graphical view on the hardware status of the appliances
Networks Diagrams	Visualize configurations, topologies and status connectivity
Session Monitoring	Dedicated views to monitor connections, VPN security associations (SAs), authenticated users, active alerts and dynamic and static routes
Overviews	Customize dashboards of user and network statistics for real-time monitoring
Geolocations	Show the country information for all IP addresses with the help of country flags and geolocation statistics. Show where network attacks come from
Reporting	Customize and schedule reports that provide detailed information about network statistics
Web Portal	Read-only access to see policies and logs and scheduled reports

THIRD-PARTY MANAGEMENT	
Device Monitoring	Allows administrator to monitor and view status changes in third-party device availability
Device Log Injection	Log parsing and reception in syslog format for third-party devices and out-of-the box support for CEF, LEEF, CLF and WELF format
NetFlow/IPFIX Reception	Ability to receive, forward, and consolidate data in NetFlow v9 and IPFIX formats
Device Statistics	Graphical statistics and reports based on third-party log data and simple network management protocol (SNMP) counters
Number of Supported Devices	200 per Log Server
Licensing	Each third-party device consumes 0.2 from Management Server license device count
LOGS	
Browser	Granular view for separate log types in addition to common log browsing view for all log data
Drag-and-Drop Filtering	Interactive log filtering—drag and drop any log data cell to the Query Panel
Statistics	Create built-in log-based counters and on-demand statistics for reporting, monitoring and alerting
Visualizations	Find the anomalies in logged traffic in filterable log visualizations
Log Analyzer	Aggregate freely on the large amount of filtered log data by any columns
Archiving	Duplicate or archive logs to directories by log data type, time, or filters
Backups	Integrated backup scheduler for Log Server configuration and log data
Exports	CSV, XML, LEEF and log exporting; logs can also be snapshot reports
Forwarding	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
Data Contexts	Shortcuts to browse different types of logs with contextual column sets that are customizable
High Availability	Support for assigning primary and backup Log Servers for each log source

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	1,000
Number of Administrators	Unlimited
Number of Managed Devices	6,000
Number of Elements	Unlimited
FEATURES	
Configuration Separation	Isolate managed environments to different admnistrative 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	Grant or limit the administrators' access rights to configuration and visibility with the help of separate administrative domains
Monitoring	Monitor the status of all granted domains with the help of the domain overview
Branding	Brand PDF reports with custom 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 NGFW Engine	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 UI 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 web portal server
Number of Administrators	Unlimited
Number of Web Portal Users	Unlimited
User Authentication	Management Server database, RADIUS, TACACS+
Device Connections	TLS-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	PDF export allows downloading report in PDF format
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 NGFW—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[1].

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

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

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 / VCCIBSMI / 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)	SMCX
Forcepoint NGFW Security Management Center 1000 Appliance	SMCAP
Forcepoint NGFW Security Management Center High Availability (only available for software and ISO image deployments)	SMCHAX
Forcepoint SMC Additional Log Server	ALSX
Forcepoint SMC Domains (Up to 200 Domains)	ODFSMCX
Forcepoint SMC Web Portal	OWPSX

Forcepoint

[FP-NGFW-Security-Management-Center-Datasheet-EN] 05Oct2021