FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint NGFW Security Management Center

EFFICIENT, CENTRALIZED MANAGEMENT OF FORCEPOINT NGFWS THROUGHOUT DISTRIBUTED ENTERPRISE ENVIRONMENTS

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

With superior flexibility, scalability, and ease-of-use, 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 and optimized workflows streamline daily administrative tasks for high efficiency and low TCO.

SMC provides 360° visibility throughout enterprise networks, gathering event management and status monitoring information from both Forcepoint 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 24/7/365 access to critical resources. With Forcepoint's SMC High Availability option, organizations can deploy extremely resilient management infrastructure and maintain continuous access to log resources.

SECURITY MANAGEMENT CLIENT

Regardless of geographic location, administrators can securely access the Forcepoint SMC with the Management Client. The 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-of-glass management of up to 2000 Forcepoint NGFWs in distributed environments.
- Flexibility and scalability for deployment in large distributed enterprise environments.
- High availability option for demanding uptime requirements.
- Smart Policies and efficient workflow automation for fast and accurate deployment and maintenance of Forcepoint NGFW.
- Situational awareness and visibility across your entire network, from the data center and edge to branch sites and the cloud.

FORCEPOINT NGFW SECURITY MANAGEMENT CENTER SPECIFICATIONS

MANAGEMENT SERVER	
Number of Managed Devices	Licensed: 2 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+
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 Forwardings 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
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 at the same time
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	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	Cloud (or USB stick)-based installation with initial policy push
Automated Tasks	Refresh policies; archive, export, and delete logs; make backups with automated tasks
Administrative Domains	Allows division of the environment into isolated configuration domains
Import/Export	XML and CSV export and import with intelligent conflict handling between SMC installations

FORCEPOINT NGFW SECURITY MANAGEMENT CENTER SPECIFICATIONS CONTINUED

Remote Upgrades	One-click fail-safe remote upgrade
Administrator Role-Based Access Control	Custom roles can be defined and combined in addition to predefined roles like Owner, Viewer, Operator, Editor and Superuser, to control permissions flexibly and accurately
License Management	Automatic online license updates and maintenance contract status reports
Troubleshooting Tools	Extensive remote diagnostic capabilities: integrated traffic capture tool, diagnostics, configuration snapshot download from next-generation firewall, and session monitoring views
POLICY MANAGEMENT	
Virtual Contexts	Share same master context across several SMC Administrative Domains — up to 250 virtual contexts, and each has 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 client applications: • Identify applications by payload, and restrict access accordingly • Use client application information from McAfee Endpoint Intelligence 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
User Identification	Create user-based rules either with or without authentication
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
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 users

FORCEPOINT NGFW SECURITY MANAGEMENT CENTER SPECIFICATIONS CONTINUED

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 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	Lightweight web access to policies, logs, and reports
THIRD-PARTY MANAGEMENT	
Third-Party Device Monitoring	Allows administrator to monitor and view status changes in third-party device availability
Third-Party Device Log Injestion	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 and consolidate data in NetFlow v9 and IPFIX formats
Third-Party Device Statistics	Graphical statistics and reports based on third-party log data and simple network management protocol (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-and-Drop Filtering	Interactive log filtering—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 filterable log visualizations
Log Aggregations	Summarize the 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, LEEF, and McAfee Enterprise Security Manager log exporting; logs can also be exported to PDF and ZIP files directly from the log browser
Log 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
Log Data Contexts	Shortcuts to browse different types of logs with dedicated column sets
High Availability	Support for backup Log Server

FORCEPOINT ADMINISTRATIVE DOMAIN LICENSE PROVIDES 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 of Domains	200
Number of Administrators	Unlimited
Number of Managed Devices per Domain	Unlimited
Number of Elements per Domain	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	View log event visualizations and other log details in a separate HTML page
PDF Export	Print reports and logs to PDF documents
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

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[DATASHEET_FORCEPOINT_NGFW_SECURITY_MANAGEMENT_CENTER_EN] 100030.032417