

Cell CMC

Centralized security Management Centre



Overview

Security becomes a very critical issue in any corporation with connecting to intranet or internet networks either deploying by a wire or wireless network system. It would have potential exposure to the hacker's world. Many corporations have already deployed a large number of security devices such as firewalls, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to protect their valuable network assets and avoid being attacked by the hackers. However, it is not a trivial task to manage and operate those security devices efficiently. There are many different brands of network security devices in your single network infrastructure to generate huge amount of logs and events in different data format. Therefore, the security event management is really a major concern to most of the network administrators in a typical corporation. To cope with this problem, a centralized security event management platform is required to focus resources on solving the most high-risk security threats and manages different brands of network security devices more efficiently and effectively.

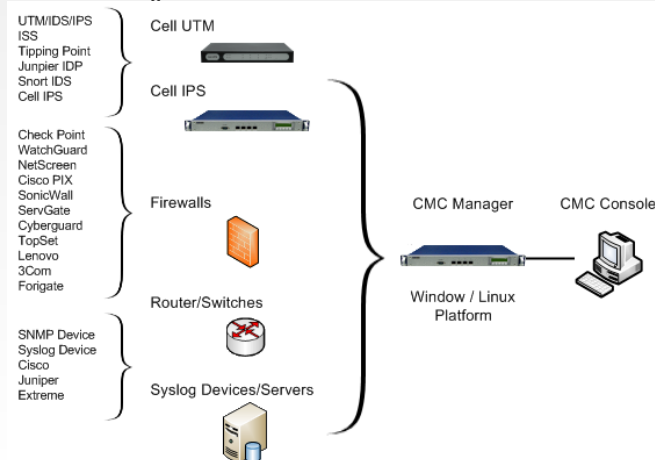
Cell CMC, is a centralized security events/logs management platform with appliance base that provides a real-time monitoring and response by a single CMC Manager console to the security threats throughout the networks. CMC Manager can monitor, manage and provide response to the security devices such as firewalls, IDS, IPS, IDP, UTM and other network devices such as routers or switches and effectively to normalize cross-product security events/logs into single normalized dataset for correlate logs analysis, and visualize in a GUI interface, determine severity levels, provide operation knowledge-base for action, tracking response activities for all security logs, events and alarms as well as incident and prioritizes them in a single console. Also, Cell CMC provides a powerful management console for logs performance and analysis, policy configuration, logs storage, database management and reporting management.

Features

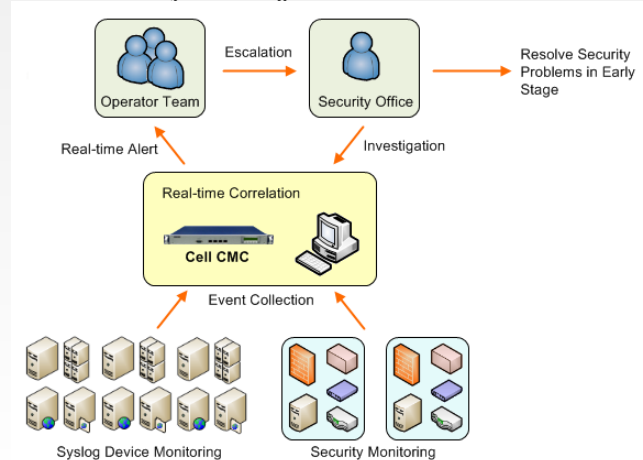
- Enterprise Platform for Centralized Security Information Management
- Visualize Incidents and Automate Investigation at a Single Console
- Scalable and Flexible Deployment Architecture
- Streamlined Operation for Security Threat Centre
- Cross-Product Analysis in Real-Time Basis
- Incident Identification and Workflow Control
- Standalone (Cell CMC Console GUI) or 3-Tier of Centralized Management (Cell NetsVision)
- Powerful System Administration and Database Management

Application

Cell CMC Manager Platform



Cell CMC Security Monitoring Flow



Hardware Specification

Product Models

Cell CMC-05

Cell CMC-10

Hardware Appliance



Hardware System	19" 1U Rack-mount Intel based platform	19" 2U Rack-mount Intel based platform
Physical Interfaces	4 GE Interfaces	4 GE, 4 optional SFP
System Console	Serial console port RS232 (DB9)	Serial console port RS232 (DB9)
Hardware Redundancy	No	Dual power/system fan Optional RAID HDD for external storage/backup
Dimension	430 x 44 x 369 mm	430 x 88 x 515 mm
Weight	4.5 Kg	18 kg
System Performance	Support 5 security or 10 syslog devices	Support 10 security or 20 syslog devices
Power Supply Voltage	Full-range ATX 250W	1+1 Redundant 500W Each
Power Input	90-264VAC, 47/63 Hz	100-240 VAC, 50/60 Hz
Operation Temp	0 to 40 degree	0 to 40 degree
Operation Humidity	5-85%@40C	5-85%@40C
Standard Regulatory	FCC, CE, RoHS	FCC, CE, RoHS

System Specification

System Operation System

- Cell CRIOS (Custom Real-time Intelligent OS)
- Cell IPPE (Intelligent Packet Processing Engine)

CMC Manager Console Requirement

- Pentium 4/2.4G or Above
- 512MB RAM or above, 80MB hard disk
- One FE 100BT network interface, standard VGA
- Windows XP/2000 or Linux platform

Language Supported

- English, Trad & Sim Chinese, Japanese, Korean

System Administration/Diagnostic

- Cell CMC Console (via Java-based GUI)
- System diagnostic (via serial console port)
- System status (via LCD at front panel)

CMC System Configuration

- Multiple of CMC Manager consoles supported
- With automatic discovery of network topology

Alert Monitoring

- Centralize logs/alerts per system view
- User can queries on logs and alerts based on different criteria
- Can integrate with 3-party NMS by SNMP
- Notification: SNMP, mail, alarm

Database Management

- Backup, purge and restore database archive via CMC Console
- Support open-source database MySQL

Report Generation

- By signature, source IP, destination IP, time
- Schedule reporting by Email, FTP and local file spooling
- Reports can be bar or pie charts
- Reports can be exported to PDF, HTML and txt
- Reports can be accessed by web based console
- Reports can be provided by a calendar-based real-time basis

Security and Syslog Devices Supported

- Firewall : Checkpoint FW-NG, Netscreen, 3Com firewall, Cisco PIX, WatchGuard, Fortigate, SonicWALL, ServGate, Cyberguard, Topset, Lenovo and etc.
- IDS/IDP/UTM : Snort IDS, Tipping Point, Sysmantic Manhunt, ISS RealSecure, Netscreen IDP, Cell IPS/UTM
- Router/Switch : Cisco, Extreme, Juniper
- All standard syslogs devices supported

Cell CMC Centralized Management

- With Cell NetsVision iCMS-CMC platform
- 3-tier network deployment
- Support multi-iCMS Commanders in a network and managed by a single iCMS Manager
- Support Support external storage system for data storage, back up or external database

Cell NetsVision, Intelligent Cell Management System (iCMS) Specification

Cell NetsVision, an intelligent Cell Management System (iCMS) is the complete, comprehensive and centralized software management platform to monitor, control and manage for all Cell products including Cell IPS, UTM, CMC, Janus and NetsAccess in a highly performance and scalability purpose. It is designed with Cell's proprietary technology of iPlug-in integration and 3-tier system architecture design, it supports powerful capability of operating, administrating, provisioning, and maintaining all system logs/or events via a feature-rich Graphical User Interface (GUI) operated by a Java-based server and client based software platform under Linux Operation System. Please refer to Cell NetsVision Datasheet for specification and ordering information.

About Cell Technology

Cell Technology headquartered at Hong Kong SAR, a network & security technology provider specializes in design, develop and deliver innovative and intelligent IP packet processing platform into software and hardware appliances. Cell product solutions including Cell IPS, UTM, CMC, Janus, TMS, NetsVision and NetsAccess address the business needs that optimize the IP network performance, secure the network security and resiliency, and manage the quality of IP services. For more information, please visit www.cell-technology.net.