Cell Technology

Cell IPS 產 品 型 錄

網路型入侵偵測防禦系統

Key Features:

- 內建超過 2500 種的特徵資料庫
- 具備阻擋惡意程式與混合式攻擊能力
- 整合防火牆與 NAT 功能
- 三種運作模式 Bridging、Gateway 以及 Passive
- 支援多國語言版本設定介面，包括英文，繁體中文，日文等
- 即時發出告警事件，並具完整的攻擊事件記錄

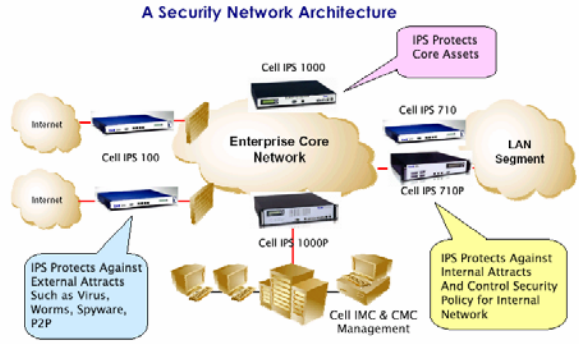
產品特色:

- 專屬 CRiOS 系統，即時偵測與防禦網路威脅
- 單一機體設計，採用專屬作業系統，安全無死角
- 隨插隨用設計，最短的導入時間
- 彈性的管理方式，支援 2-tier 與 3-tier 管理方式，
- 具備內建與外掛報表系統

簡介

自從劃時代的 CodeRed 等網路蠕蟲 (Worms)，病毒 (Virus) 出現，到現在的混合式攻擊，間諜軟體的威脅，所有的網路管理者都面對極大的挑戰，網路安全方案亦由以往的被動偵測防護技術，發展爲主動攔截技術(或稱爲入侵防禦技術)。

Cell Technology 自行研發的入侵防禦系統，採用專屬的作業系統(Custom Real-time Intelligent Operation System, CRiOS)以及 Packet Processing Engine (IPPE)系統，是一套先進可靠的系統。產品線包括提供給 SOHO 使用的系統到大型網路使用的系統。可以有效阻擋最新網路型病毒、蠕蟲攻擊與間諜程式，有效的監控 P2P 與 IM 等網路服務，甚至是 SoftEther 這類的加密應用，我們也可以有效的監控。另外，我們也開放用戶自行新增特徵檔,可以針對特定的應用進行偵測或阻擋。管理的方式相當簡單與具備彈性，操作介面採用容易上手的 GUI 介面，可以依據環境採用 2-Tier 或 3-Tier 的架構, 系統已經預設多個政策提供給用戶選用，用戶只需簡單的點選所要的政策。特徵檔可透過網路自動下載, 隨時保持在最佳防禦狀態。



系統功能

三種運作模式

Cell IPS 提供三種主要運作模式，透通橋接(Inline Bridging)、閘道(Gateway)與被動(Passive)模式。橋接模式下提供標準的內部與外部網路界接埠，可以快速部署在網路上使用，立即過濾入侵攻擊。閘道模式提供防火牆與 NAT/PAT 功能，除了內部與外部網路界接埠，可以設定 DMZ 網段，運用防火牆政策限制進出網路的網路資源，並同時提供入侵偵測防禦功能。被動模式則是在監控網段進行偵測(IDS)。

No.	Active	Src Netw	Ne	Dst Net	Ne	Signature Group	Severity	Action	Notification
1	☑	Default	☐	Default	☐	P2P_AND_FILESHARE	Critical	Drop Packet By IPS	Default
2	☑	Default	☐	Default	☐	EMAIL_IMAP_EXPLOIT	Medium	Drop Packet By IPS	Default
3	☑	Default	☐	Default	☐	WEB_CGI_EXPLOIT	High	Drop Packet By IPS	Default
4	☑	Default	☐	Default	☐	SCANNING	Medium	Drop Packet By IPS	Default
5	☑	Default	☐	Default	☐	ORACLE_TRAFFIC	Info	Alert Only	Default
6	☑	Default	☐	Default	☐	WEB_CGI_SCAN	Medium	Drop Packet By IPS	Default
7	☑	Default	☐	Default	☐	ORACLE_EXPLOIT	High	Drop Packet By IPS	Default
8	☑	Default	☐	Default	☐	BACKDOOR_ACCESS	Critical	Drop Packet By IPS	Default
9	☑	Default	☐	Default	☐	ANTISPYWARE	Critical	Drop Packet By IPS	Default
10	☑	Default	☐	Default	☐	EMAIL_SMTP_EXPLOIT	High	Drop Packet By IPS	Default
11	☑	Default	☐	Default	☐	WEB_MISC_EXPLOIT	Low	Alert Only	Default
12	☑	Default	☐	Default	☐	WEB_UNIX_SCAN	Low	Alert Only	Default
13	☑	Default	☐	Default	☐	ICMP_ACCESS	Medium	Drop Packet By IPS	Default
14	☑	Default	☐	Default	☐	DENIAL_OF_SERVICE	Critical	Drop Packet By IPS	Default
15	☑	Default	☐	Default	☐	GENERIC_PROTOCOL_DECODE	Info	Alert Only	Default
16	☑	Default	☐	Default	☐	FINGER_TRAFFIC	Info	Alert Only	Default
17	☑	Default	☐	Default	☐	WEB_FRONTPAGE_EXPLOIT	Medium	Drop Packet By IPS	Default
18	☑	Default	☐	Default	☐	FTP_TRAFFIC	Info	Alert Only	Default
19	☑	Default	☐	Default	☐	VIRUS_AND_WORMS	Critical	Drop Packet By IPS	Default

2500 種預設攻擊特徵檔與政策範本

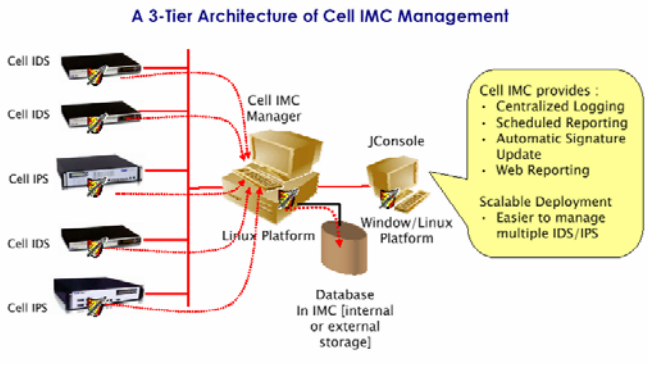
Cell IPS 提供超過 2500 種預先定義好的攻擊特徵檔，可從網路下載更新，防禦最新攻擊，並提供政策範本，可以迅速做好設定。提供客製攻擊特徵檔能力，並可依據環境修改防火牆與 IPS 政策。

系統管理與報表分析

Cell IPS 提供兩個管理介面。用戶可以透過 serial console 進行基本設定與檢視系統資訊。在本機使用 Java based GUI(Cell Console)管理 IPS，設定政策，更新特徵檔，監看 IPS 使用狀態，檢視事件，產生多種報表，如 PDF, Excel, HTML 等等，用以進行分析，並提供簡易資料庫管理工具。

網管中心(IMC)

Cell IMC 採用 3-Tier 管理架構，是一個集中的網管系統，適合在多個 Cell IPS 應用環境中。集中監看 IPS 運作狀態，統一制定與派送政策，定期自動下載特徵檔，集中收集與分析資安事件。



Cell Technology

產品規格

Cell IPS 20	Cell IPS 100	Cell IPS 710	Cell IPS 710P	Cell IPS 1000
				

產品名稱	Cell IPS 20	Cell IPS 100	Cell IPS 710/710P	Cell IPS 1000
適用環境	小型企業/分公司	中型企業/分公司	中大型企業	中大型企業
硬體	桌上型	19" 1U Rack-mount	710-19" 1U Rack-mount 710P-19" 2U Rack-mount	1000-19" 1U Rack-mount
系統效能	Max 20Mbps 12,000 sessions	Max 100Mbps 250,000 sessions	Max 800Mbps 800,000 sessions	Max 1.2Gbps 1,000,000 sessions
網路介面	3 FE Interfaces No buit-in hardware by-pass	4 FE Interfaces Built-in 2 FE Hardware by-pass	710: 4 GE Interface 710P: 4 GBIC and 3 GE Interfaces Built-in 2 GE Hardware by-pass	2 GE, 2 Fiber, 1 FE ports Built-in 2 GE Hardware by-pass
管理主控台	Via serial console port RS232 (DB9)	Via serial console port RS232 (DB9)	Via serial console port RS232 (DB9)	Via serial console port RS232 (DB9)
容錯能力	N/A	System HA	System HA 710P: System HA,Dual power supply, Dual system fan	System HA
內建旁路功能	N/A	Yes	Yes	Yes
中信局項次	LP5-950060 第六組第 2 項	LP5-950060 第六組第 5 項	710:LP5-950060 第六組第 7 項 710P:LP5-950060 第六組第 7,8 項	LP5-950060 第六組第 10,11 項

系統功能

專屬系統
- Cell CRiOS (Custom Real-time Intelligent Operating System)
- Cell IPPE (Intelligent Packet Processing Engine)

運作模式
- Gateway 與 In-line Bridging
- Passive (IDS)

外部防火牆整合阻斷能力
- Checkpoint, NetScreen, Cisco PIX

狀態檢查防火牆與 NAT
- Standard stateful firewall inspection
- 阻斷攻擊
- Network/Port Address Translation

系統管理
- Cell Console (via Java-based GUI)
- System Diagnostic (via serial console port)
- System Status (via LCD at front panel)

偵測能力
- Stateful Pattern matching (signature detection),DoS and DDoD detection, L7 application detection
- HTTP protocol flow analyzer
- Multi-rule search by protocol, generic content, packet anomaly, protocol anomaly, traffic anomaly and keywords
- Real-time TCP sessions and packet loggings
- TCP Segment Reassembler
- Support 802.1q VLAN detection
- IP Fragmentation
- SYN Flooding
- UDP and ICMP Flooding control

語言版本
- 繁體中文
- 日文
- 英文

特徵檔更新
- 手動,自動,設定排程

SIM/SEM 平台整合
- Snort SNMP v2 Trap
- UDP syslog messages
- Cell Centralized security Management Centre (CMC) SIM Platform

IPS Sensor 設定
- 單獨運作/或 多個 sensors
- 單一 IPS 可支援多個 Cell IMC/Cell CMC

報表系統
- 內建報表與分析工具
- 頻寬報表
- 輸出格式包括 PDF, Excel, HTML 等

資料庫管理
- 內建資料庫 - backup, purge 與 restore
- 外部資料庫(IMC)
- 政策備份

IMC (Intrusion Management Centre)規格

IMC 硬體需求
- Pentium 4 (2.8G)或以上, 2GB RAM
- 120G 硬碟空間或以上
- FE/GE 介面
- Linux OS , Redhat 8/9 或 Fedora Core 1/2

Cell Console 硬體需求
- Pentium 4 或以上, 512MB RAM
- 60MB 硬碟空間或以上
- FE/GE 介面
- Windows 2000, Windows XP

特徵檔更新
手動,自動,設定排程

系統平台架構
- 3-tier 網路架構
- 單一 Cell Console 支援多個 IMC
- 單一 IMC 支援多個 IPS

Sensor 管理
- 可同時下載政策到多個 IPS
- 標準 IPS 主控台
- 可自行定義攻擊特徵檔
- 網路與物件導向

資料庫管理
- 定期備份(backup)與清除(purge)資料庫
- 支援開放源碼資料庫 MySQL,提供 database schema

報表系統
- 可以據特徵檔,來源 IP,目標 IP 產生報表
- 定即報表,支援 Email, FTP 或是本機儲存
- 輸出格式包括 Excel, CSV, PDF, HTML 以及 Text file 等
- 支援網頁瀏覽報表(IMC)

告警事件監看
- 集中儲存事件
- 可設定不同條件搜尋特定事件
- 經由 SNMP,Syslog 與其他廠牌網管系統整合
- 告警方是: SNMP, Syslog, Email

About Cell Technology
Founded in 2000 with headquartered at Hong Kong SAR, Cell Technology is a new generation of technology startup to design, develop and market innovative and competitive broadband network product solutions from the convergence of Information Technology (IT) and Telecommunications technologies for worldwide market. The networking products are included Cell IPS, Cell SPM, Cell CMC, Janus and others. Please visit www.cell-technology.net Sales : sales@cell-technology.net

Headquarter : 2/F Shui On Centre, 8 Harbour Road, Wanchai, Hong Kong. Tel : (852) 2824 8910 Fax : (852) 2824 8365
Taiwan Office : 8F-2,No.51,Jhengsin St., Zuoying District, Kaohsiung City 813, Taiwan (R.O.C)

Cell IPS Datasheet ver 3.0E-CTC/Rev1/2007-03