



Security Assurance Center
安 保 中 心 安 全 管 理 方 案
SAC Centralized Security Management Solution

- 四階式 (4-Tier) 分散建置集中控管安全方案
- 彈性擴充 IPS 設備佈建規模
- 異常處理決策管理機制
- 政策統一修改/特徵碼集中自動更新
- 用戶自訂多套政策模組 (Rule-Set)
- 整合式統計報表系統與即時監視系統
- 多層次分層管理

SAC 威播安保中心安全管理方案，是一套分散式建置，四階式 (4-Tier) 集中管理之安全管理方案。SAC 採用政策群組技術 (Rule-Set)，使管理者除可集中更新所有 IPS 之安全政策外，並可依用戶需求為特定之 IPS 提供差異化政策。此外，SAC 的四階式管理技術，也提供了企業在佈建大型 IPS 防禦網路時所需要的可擴充性 (Scalability) 及整合性報表 (Report Aggregation) 能力。SAC 主要組成包括：SAC Console、SAC Commander、SAC Controller 以及 IPS 入侵防禦設備。

- SAC Console 是網路安全管理者直接使用的操作介面，是利用 Java 開發而成的直覺式多國語言圖形化操作介面，透過此介面使用者可輕易的設定設備參數，訂定安全防禦政策，即時監視網路安全事件情形與封包流量狀態，以達成安全設備防護的目的
- SAC Controller 提供了用戶即時監視介面、安全政策設定介面以及中央控管網路安全設備群組的能力，並可產出整合性的安全事件報告或個別報告
- SAC Commander 負責蒐集、整合 SAC Controller 傳來的安全報告資料，提供整合性企業網路安全趨勢分析的能力
- IPS 入侵防禦設備是全功能的入侵防禦系統硬體設備，可以建置在企業網路系統的任何地方，負責執行安全防禦政策，偵測網路封包正常與否，以及阻絕不正當的網路攻擊行為，確保網路系統的正常運作並防範企業機密外洩。IPS 設備建議可安佈建受保護的設備或網段的出入口處，例如大型企業當中的分公司的網路出口，或是大型工廠的生產機具網路出入口，或是晶圓廠的生產機台前端等等。

特色

Console ▶

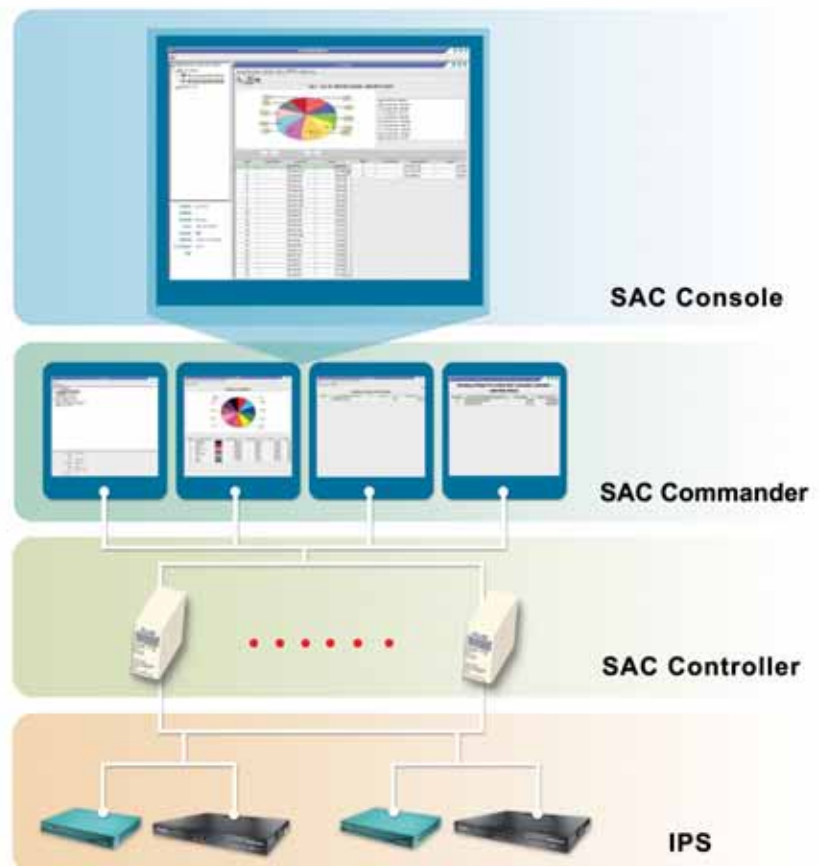
- Java-Based 圖形化使用者操作管理介面
- 登入連線具備加密功能
- 可直接連結 SAC Commander 或 SAC Controller

Commander ▶

- 蒐集並整合 Controller 的安全入侵事件資料
- 整體網路安全事件監控分析

Controller ▶

- 事件處理決策管理機制
- 安全政策模組 (Rule-Set) 技術
- 使用者可自定安全政策模組及安全政策
- 整合性即時封包流量監測
- 整合性即時安全事件監視
- 安全事件詳細記錄
- 整合性安全事件趨勢分析
- 彈性化整合性報表系統，支援 TOP N 客制化報表查詢功能
- 整合性安全事件記錄報表
- 定期安全事件定期報表輸出
- 支援 Syslog 格式之事件記錄輸出
- 多層次分層管理權限
- 自動化遠端特徵碼集中更新機制



SAC Commander 主機軟硬體建議規格

- 作業系統：Windows XP Professional (SP1 以上)
- 中央處理器：Pentium-4 2.8G 以上
- 記憶體：最少需求為 512M DDR RAM，建議使用 1G DDR2 RAM 以上
- 硬碟空間：60GB 以上

SAC Controller 主機軟硬體建議規格

- 作業系統：Windows XP Professional (SP1 以上)
- 資料庫系統：MySQL v4.0.18 以上
- 中央處理器：Pentium-4 2.8G 以上
- 記憶體：最少需求為 1G DDR RAM，建議使用 2G DDR2 RAM 以上
- 硬碟空間：60GB 以上

(建議此主機為 SAC Controller 專用，請勿與其他軟體系統混合使用。)

功能規格

Commander ▶

- 最多可支援接收 20 部 SAC Controller 的資料
- 可顯示所管理之 Controller/IPS 的詳細資料，如連線與否，啟動時間，核心版本 ... 等相關資料
- 提供安全事件分類趨勢圖
- 提供整合性安全事件分析

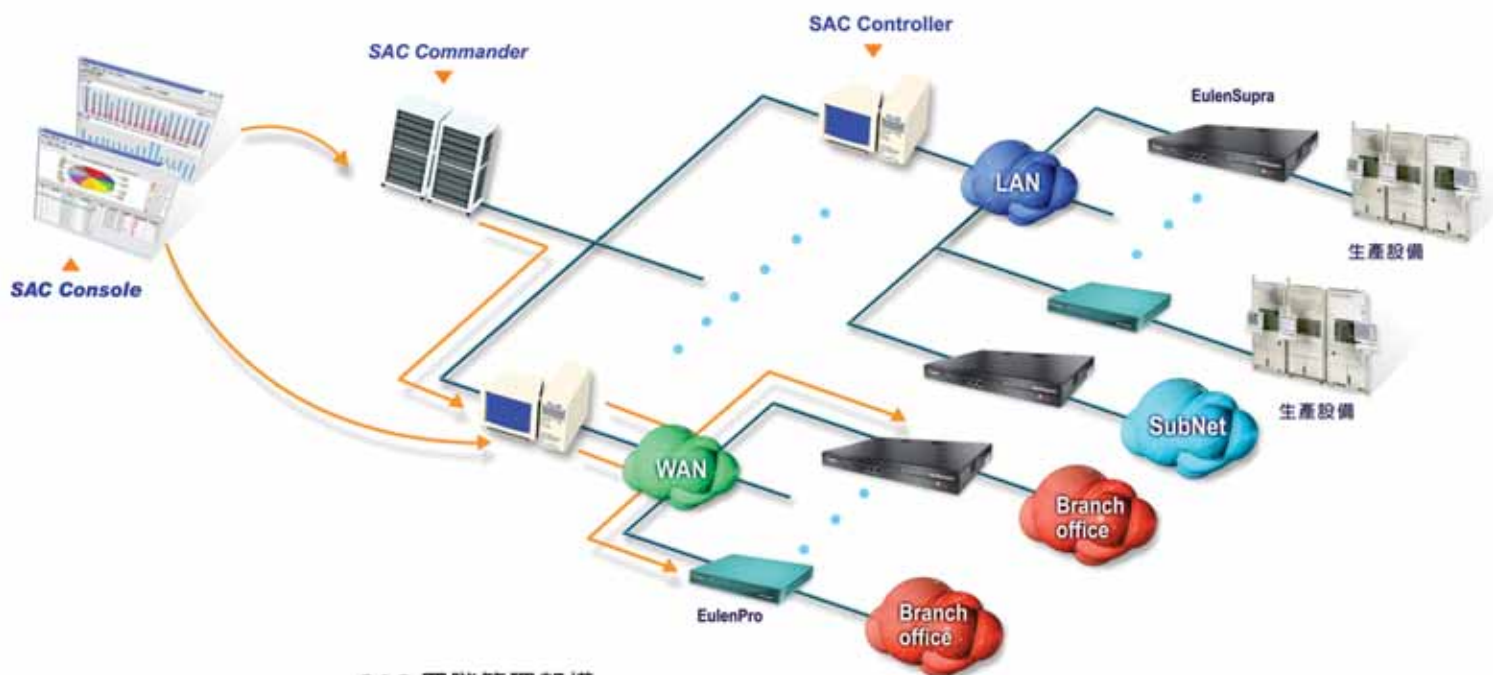


SAC 決策機制流程圖

功能規格

Controller ▶

- 最多可管理 50 台 IPS 設備
- 提供事件處理決策管理機制
- 可觀看所管轄的 IPS 核心及特徵碼更新狀況
- 能指定個別 IPS 名稱
- 具備觀察每一個所控管 IPS 是否正常運作之能力
- 可調整個別 IPS 之設備參數，包括運作模式，隱藏模式，連線模式，時間，SNMP 參數與存取控制等設定
- 採用 Rule-set 模組化政策設定技術
 - 可採用原廠預設政策模組或制定多套使用者自訂政策模組
 - 政策模組包括 2300 條以上 IPS 防禦政策與防火牆 ACL 政策
 - 使用者可任意指定每台個別之 IPS 所採用之政策模組
 - 透過修改政策模組可達成集中更新 IPS 防禦政策之目的
- 防禦政策及防火牆 ACL 可定義其啟動的時間
- 防禦政策可設定 IP/Mask 群組，以指定政策生效之群組範圍
- IPS 防禦政策的反應有：丟棄封包，中斷連線，事件監視，以及事件紀錄
- 防火牆 ACL 政策的反應有：通過，不通過，通過但需經過 IPS 檢查，事件監視及事件紀錄
- 具有彈性選擇觀看單一、多個或是所管轄之全部 IPS 之即時監測與報表
- 提供防火牆 ACL 及 IPS 即時事件與即時流量監視系統
- 提供防火牆 ACL 及 IPS 之 TOP N 報表系統
 - 提供搜尋個別 IPS 所記錄之詳細事件記錄之能力
 - 提供 TOP 10 預設統計報表
 - 提供各類事件趨勢報表
 - 提供嚴重等級趨勢報表
 - 提供 TOP N 的客製化 (Query on Demand) 報表
 - 可依照事先定義之範本提供定期報表，並具預覽功能
 - 定期報表可採 HTML、PDF 或 CVS 格式透過 E-mail 或 FTP 輸出
- 支援 Syslog 事件記錄輸出
- 具多國語言(英, 繁中, 簡中等)操作介面



SAC 四階管理架構

IPS 設備功能

	Eulen Pro	Eulen Supra / Supra+
系統基本規格		
效能	30Mbps	200Mbps
同時連線數	10,000	10,000/256,000
IPS 系統介面	10/100Mbps x 2	10/100Mbps x 2
系統管理介面	10/100Mbps x 1	10/100Mbps x 1
軟/硬體旁路	Yes	Yes
支援隱藏模式	Yes	Yes
SNMP Trap	Yes	Yes
運作模式	In-Line Mode Monitor Mode Bypass Mode	In-Line Mode Monitor Mode Bypass Mode
Layer 4/7 防護		
Firewall ACL	Yes	Yes
Intrusion Attack(s)	Yes	Yes
IM (Instant Message)	Yes	Yes
P2P Application	Yes	Yes
URL Filtering	Yes	Yes
Content Filtering	Yes	Yes
異常狀態防護		
Anti-Evasion	Yes	Yes
Protocol Anomaly	Yes	Yes
Statistical Anomaly	Yes	Yes
IP Reassembly	Yes	Yes
TCP Session Reassembly	Yes	Yes
DoS/DDoS 防護		
TCP SYN Flooding	Yes	Yes
TCP Flooding	Yes	Yes
UDP Flooding	Yes	Yes
UDP Smurfing	Yes	Yes
IGMP Flooding	Yes	Yes
IP Flooding	Yes	Yes
特徵碼偵測		
多重模式偵測	Yes	Yes
特徵碼個數	> 2,300 stateful signatures	> 2,300 stateful signatures
User Define Signature	Yes	Yes
更新		
遠端線上更新/升級	Yes, 核心 + 特徵碼	Yes, 核心 + 特徵碼
更新頻率	自動每日檢查/不定期即時更新	自動每日檢查/不定期即時更新



BroadWeb

Empower Your Network Security

新竹市 300 科學工業園區新安路 8 號 4 樓

Tel: +886-3-578-7068

Fax: +886-3-563-5659 / +886-3-578-7059



[http:// www.broadweb.com](http://www.broadweb.com) E-mail: sales@broadweb.com