

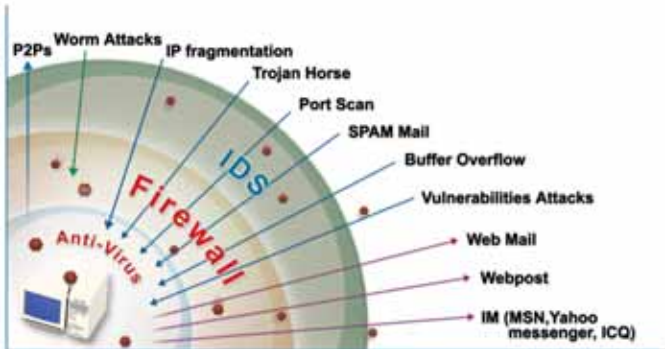
Advanced Intrusion Detection & Prevention

NetKeeper



- **Anti-Intrusion** 阻擋駭客入侵
- **Anti-DoS / DDoS** 阻擋分散式阻斷服務攻擊
- **Anti-Virus** 阻擋網路病毒
- **Anti-SPAM** 阻擋垃圾郵件
- **Anti-P2P** 阻擋 P2P 分享下載程式
- **Anti-Instant Messenger** 阻擋即時聊天程式
- **Anti-Web Mail** 防止經由 Web Mail 洩漏機密文件
- **Anti-Web Post** 防止網頁資料上傳

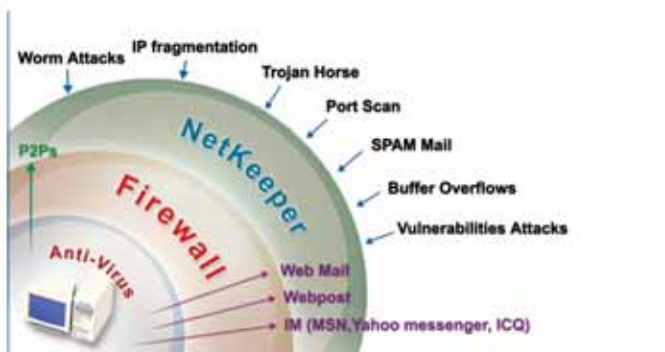
NetKeeper VS. Firewall / Anti-Virus / IDS



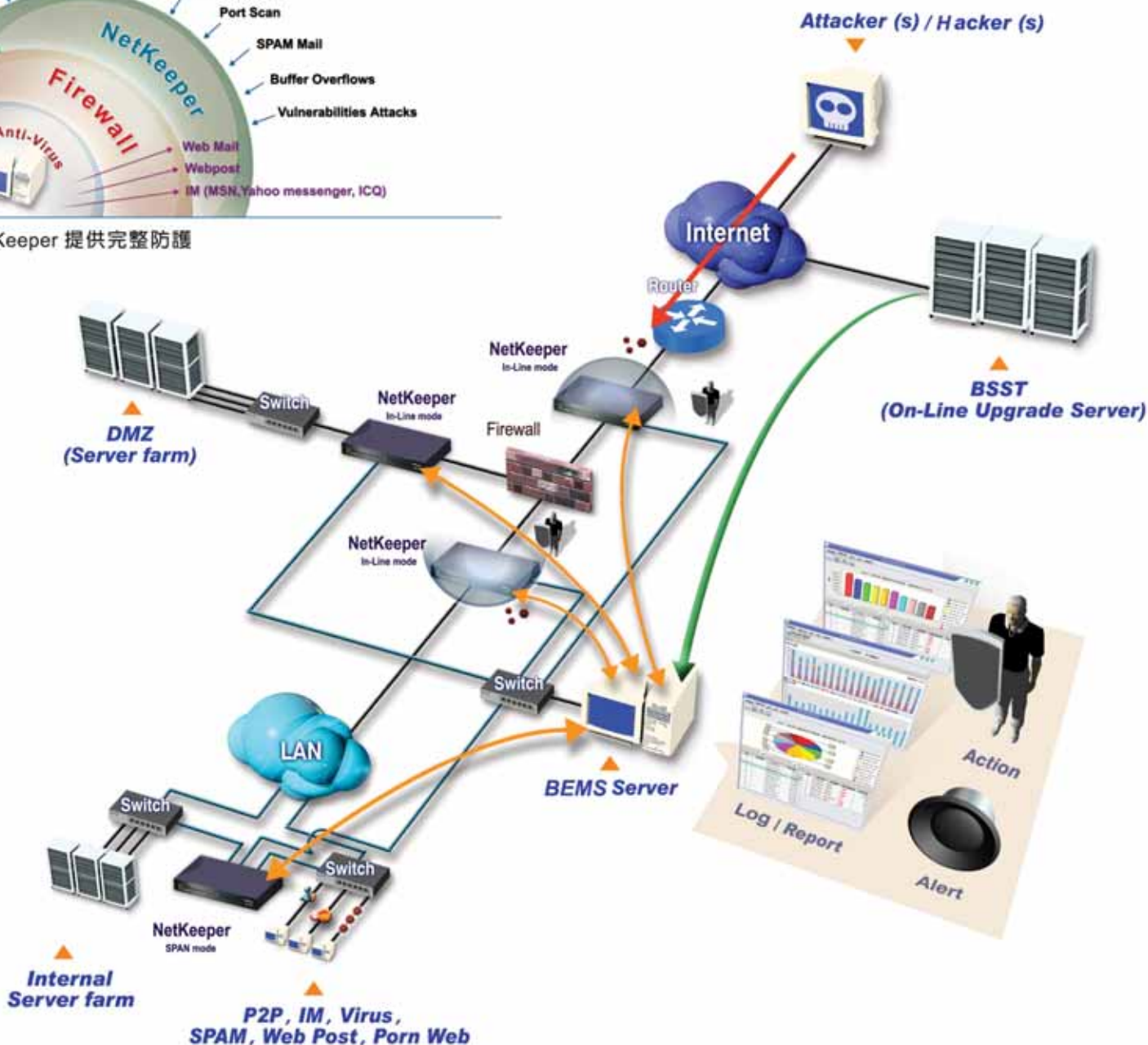
防火牆 / 防毒軟體無法有效防護

NetKeeper 可阻擋

- ▶ 緩衝區溢位 (Buffer Overflow) 攻擊
- ▶ 通訊埠掃描 (Port Scan) 攻擊
- ▶ 木馬程式 (Trojan Horse) 攻擊
- ▶ 碎片封包 (IP Fragmentation) 攻擊
- ▶ 蠕蟲 (Worm) 攻擊
- ▶ 系統與應用程式漏洞 (System & Application Vulnerabilities) 攻擊
- ▶ 阻斷服務與分散式阻斷服務 (DoS / DDoS) 攻擊
- ▶ P2P · IM · Virus · SPAM · Web Post · Web Mail 等等



NetKeeper 提供完整防護





NetKeeper
Advanced Intrusion Detection & Prevention

NetKeeper 軟體規格

- 即時分析網路傳輸封包，以偵測是否有非法入侵或攔截服務之攻擊
- 支援多種網路操作模式
 - In-Line
 - Tap
 - SPAN
 - Monitor
 - Bypass
- 具 2,300 條以上的攻擊特徵碼資料庫
 - Anti-Intrusion 阻擋駭客入侵
 - Anti-DoS / DDoS 阻擋分散式阻斷服務
 - Anti-P2P 阻擋 P2P 分享下載程式
 - Anti-Instant Messenger 阻擋即時聊天程式
 - Anti-Virus 阻擋網路病毒
 - Anti-SPAM 阻擋垃圾郵件
 - Anti-Web Mail 防止經由 Web Mail 洩漏機密文件
 - Anti-Web Post 防止網頁資料上傳
- 採用高安全性之嵌入式即時作業系統 (Embedded Real-Time OS)
 - 具隱藏模式，外界無法偵知此設備的存在
 - 支援 SNMP V2
 - 支援 Unlimited VLAN tagging
- Maximum IDP engine throughput: 200Mbps
- 最佳化之偵測 / 過濾引擎，整合了攻擊辨識碼資料庫比對及異常行為模型分析之雙重功能
- 異常行為模型分析，可偵測各種異常行為，如 Protocol 異常及流量異常等
- 不需其他設備支援下，可主動過濾非法 TCP、UDP、IP 等封包並中斷其連線，且保證正常網路存取
- 對 DoS、DDoS 攻擊行為具高度辨識能力，可在攻擊發生之初，即時過濾攻擊封包，保護網路安全
- 使用者可對攻擊事件認定之參數，根據本身網路環境進行微調，以符合實際環境
- 使用者可自定增加攻擊特徵資料庫及自定增修偵測 / 過濾事件之回應功能達成
 - Layer 7 Access Control List
 - Keyword / Phrase Filtering
 - URL Filtering
 - Application Filtering
- 具即時警報系統，並可透過 E-mail 通知管理者
- 定時自動更新攻擊特徵碼
- 定時自動更新硬體核心版本
- 具安全加密之遠端管理介面
- 支援軟體旁路功能設計 (Fail open software bypass)

NetKeeper 硬體規格

- 提供三個 10/100Based-TX 高速乙太網路介面
- 標準 Rack Mount 1U 高度機箱，可直接安裝於 19 吋機架
- 提供一個九針 RS-232 serial port
- 自動故障旁路功能設計 (Fail open hardware bypass)
- 機台尺寸: Standard 19 inches 1U Chassis ,
445 mm (Length) x 265 mm (Width) x 45 mm (Height)
- 電源規格: AC Line 90-264 VAC , 50-60HZ IA MAX

BroadWeb Extensible Management System

Hardware Requirements ▶

	Minimum	Recommended
CPU	P4-1.8G	P4-2.4G or above
Memory	512MB	1GB or above
Hard Drive	20G	40G or above
OS	Windows XP	

- Java-Based 介面，使用者可利用 Web 瀏覽器操作管理
- 集中式管理介面，可同時控管多台 NetKeeper
- 利用三層式遠端管理確保架構之安全性
- 可由圖形模式監測 / 分析即時攻擊事件與網路流量
- Rule-based 的政策管理機制
- Role-based 的系統管理存取權限機制
- 即時攻擊事件與政策管理直接連結，管理者可由即時監控畫面修改政策管理方式，即時阻止攻擊來源
- 政策可根據 IP 或群組的方式管理特定對象
- 使用者可根據網路狀況自行定義政策
- 可利用 SQL 指令擷取報表資訊，根據使用者的需要自訂報表格式
- 可利用 Email 或 FTP 定時寄送攻擊分析報表
- 可啟動攻擊事件封包擷取功能，詳細列出封包內容
- 定時自動更新硬體核心版本及攻擊辨識碼
- 支援 Syslog
- 可選擇輸出之報表格式，CSV 及 HTML 格式



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

<http://www.broadweb.com.tw> E-mail: sales@broadweb.com.tw



ISO 9001:2000

