Enhancing Security through Continuous Threat Assessment

NetProbe

網路威脅偵測與防禦系統

NSGUARD
NSGUARD Technology, Inc.
捷睿智能股份有限公司

簡介

NetProbe 是一套網路威脅偵測與防禦系統，能夠快速的判斷出網路惡意攻擊並進行阻擋，在基礎網路前端即時建立出第一層防禦來確保公司既有營運服務的連續性與可用性。

NetProbe 透過判斷惡意 IP 快速比對的方式運作，這將大大降低異常的誤報與傳輸因深入判斷而造成速率下降的問題，規則筆數高達 400 萬筆且支援定時更新服務，情資範圍包含惡意來源主機 IP、惡意網域 IPs 與特定國家一般或加密惡意伺服器 IP。

另外，NetProbe 支援旁路(Bypass) 技術達到即時切換，讓進出的封包可直接穿過而不加以檢測，進而達到服務不中斷。

產品效益

- 內部與外部佈署方式提供企業網路第一線防護

  佈署方式可選擇偵測 (Detection) / 防禦(Prevention) 模式於第一線偵測網路狀況，旁路(Bypass)技術讓服務更穩固，不因軟硬體問題造成網路服務中斷。

- 400 萬筆黑名單設定，建立完整資安防禦

  支援 400 萬筆黑名單設定，範圍包含來源惡意主機 IP、惡意網域 IPs 與特定國家一般或加密的惡意伺服器 IP，達到最高等級的防護。

- DoS / DDoS 偵測與防禦

  支援 Layer 3 與 Layer 4 DoS / DDoS 偵測與防禦功能。系統預設 DoS / DDoS 偵測觸發規則，亦可學習客戶網路流量特徵，自動調整最佳觸發規則。

- 惡意告警通知

  當偵測到惡意攻擊時，會發送告警資訊至雲端後隨即通知網路管理人員，其內容包含時間、來源/目的 IP、觸發規則等資訊。

- 模組化設計

  客戶可以依自身需求，選擇最符合組織網路環境的功能模組與網路介面配置。

功能說明

- 威脅偵測/防禦與管理模組

  可以支援威脅偵測模式(IDS)以及威脅防禦模式(IPS)。當以 Inline 布署方式啟用 IPS 模式時，可以同時啟用 Bypass 功能，確保在系統失效時，不致影響網路傳輸。管理模組主要用以呈現偵測阻擋資訊、管理資訊以及網路流量資訊等。包含：

  - 偵測阻擋資訊：呈現目前偵測、阻擋網路威脅數量、網路流量分析等資訊。
  - 管理資訊：提供帳號管理介面，提供新增、修改、刪除帳號等功能以及系統狀態資訊。

- 威脅情資管理模組

  可支援雲端威脅情資同步或手動匯入威脅情資，如：全球性公開威脅情資、行政院技術服務中心或區域聯防平台提供之威脅情資、商用付費威脅情資等。目前可支援可設定超過 400 萬個 IP 黑名單，並即時進行異常網路連線偵測。

- DoS / DDoS 偵測與防禦模組

  - 支援來源/目的 IP 同時連線數量偵測、同一時間 TCP Sync / UDP / ICMP / SCTP 封包數量等 Layer 3 與 Layer 4 的 DoS / DDoS 偵測與防禦功能。
  - 支援 DNS 清洗功能，可透過命令列指令或 API 方式設定 IP 與 Domain Name 黑白名單功能。
  - DoS / DDoS 偵測到自動防禦之間的反應時間小於 2 秒。

- 自我學習模組

  本系統之自我學習模組採用系統誘捕與行為分析等方法，自動偵測惡意 IP 並將其加入黑名單，並可提供 API 供其他系統進行整合。

- 誘捕系統：可模擬多種網路通訊協定與服務。依其功能可分為常見管理服務協定、常見網頁服務協定及常見資料庫服務等 3 大類。一旦駭客或惡意程式踏入陷阱時，便將其來源 IP 新增至 IP 黑名單內。各類協定分別如下所示：
  - 常見管理服務 SSH、Telnet、RTSP 及 RDP
  - 常見網頁服務 HTTP 與 HTTPS
  - 常見資料庫服務 MSSQL、MySQL、Oracle Database 及 MongoDB
- 行為分析：
  - 係指透過分析誘捕系統捕獲的駭客互動行為的方式，篩選出最符合駭客攻擊特徵的來源 IP，並搭配自製演算法，參考其發生頻率、發生時間、攻擊範圍等資訊，賦予來源 IP 不同威脅等級，再將威脅 IP 更新至 IP 黑名單內。
  - 分析流量特徵，自動調整各項 DoS / DDoS 觸發規則。

系統需求

建議硬體規格	
CPU	**16-core and above**
RAM	**64GB DDR3 and above**
Hard Drive	**1TB and above**
Other	**Network Interface X4 (Optional Bypass)**

NSGUARD

NSGUARD Technology, Inc.