Enhancing Security through Continuous Threat Assessment

EdgeGuard

網路威脅偵測與防禦裝置

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

簡介

EdgeGuard 是一套偵測外部與內部惡意網路攻擊系統，能夠快速的判斷出網路惡意攻擊與阻擋來源/目的連線，在基礎網路後端即時建立出第一層防禦來確保公司既有營運服務的安全性。

除了針對惡意連線能夠進行阻擋外，同時能夠捕捉嘗試傳入企業內部的惡意程式，進一步防止惡意程式在內部系統進行感染。

提供簡易的 UI 方便使用者管理惡意連線告警與匯出資料，顯示情資的數量與更新紀錄確保系統擁有最新的比對黑名單，且能定期產生報告與即時通報緊急資安事件給使用者。

另外，EdgeGuard 硬體層面則是提供多組 Inline 網路埠，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

- 採用工業主機的安全設備，內部與外部佈署方式提供企業網路第一線防護

  提供最多 1 組 1GbE 旁路(Bypass)網路埠，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)技術讓設備服務更穩固，不因軟硬體問題造成網路服務中斷。

  阻擋惡意連線的方式提供企業第一線防護
  設備能夠進行快速的佈署，一旦將設備連線至企業網路後，能夠形成惡意連線與惡意程式的防護網。

- 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，確保在裝置失效時，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。

- 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 供其他設備進行整合。

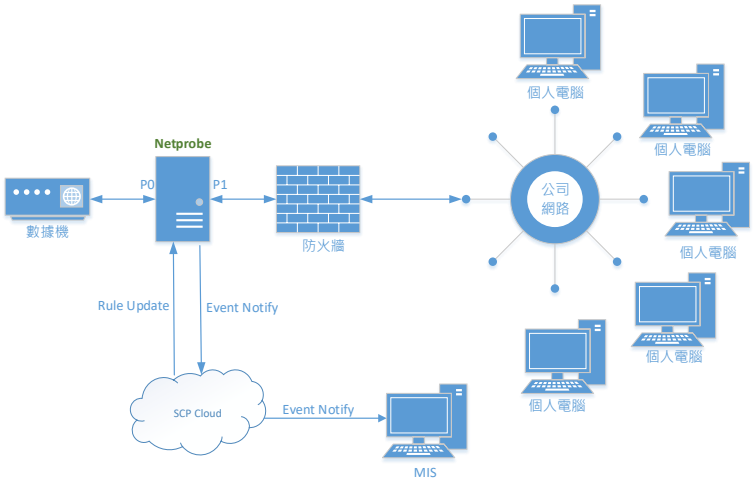
  - 誘捕系統：可模擬多種網路通訊協定與服務。依其功能可分為常見管理服務協定、常見網頁服務協定及常見資料庫服務等 3 大類。一旦駭客或惡意程式踏入陷阱時，便將其來源 IP 新增至 IP 黑名單內。各類協定分別如下所示：
    - 常見管理服務 SSH、Telnet、RTSP 及 RDP
    - 常見網頁服務 HTTP 與 HTTPS
    - 常見資料庫服務 MSSQL、MySQL、Oracle Database 及 MongoDB
  - 行為分析：

- 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。

應用場景

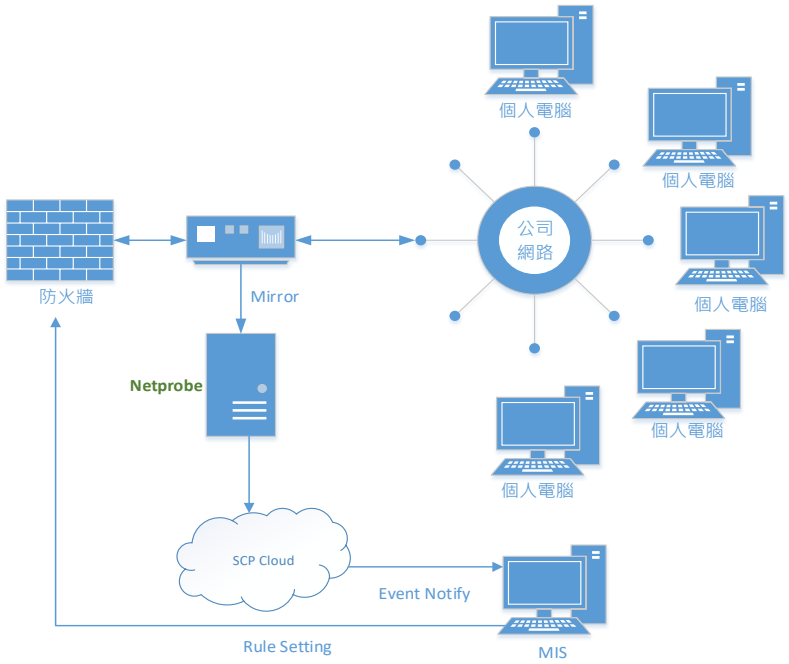
- 外網環境佈署

  EdgeGuard 置放於防火牆外部，監測每個封包進出，如發現惡意 IP 隨即阻擋且隨即發送通報。



- 內部環境佈署

  EdgeGuard 置放公司環境，透由橋接器(Switch)將出入封包複製一份給 EdgeGuard，此時 EdgeGuard 會被動的察看每個封包，如發現惡意 IP 隨即發出通報，一旦將設備連線至企業網路後，能夠形成惡意連線與惡意程式的防護網。



系統需求

系統規格	
Network Bypass Interface	1GbE 2
Storage	2.5" 500GB * 1
RAM	8GB
OS	Ubuntu 16.04

NSGUARD

NSGUARD Technology, Inc.