Gorilla Technology Group

網路威脅偵測與防禦裝置

NetProbe 2.2

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，具備 NDR (Network Detection and Response)功能，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。

NetProbe 同時支援正規表示(Regular Expression)功能來達到封包第七層內容的快速比對，情資來源包含第三方 Snort Rule 或使用者自行定義方式，豐富化惡意封包判斷方式。

另外，NetProbe 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 1U 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

  1U 輕量級設備，提供最多 2 組 1GbE 或 10GbE 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。

- 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。

- 封包內容快速比對，加強惡意偵測

  支援特徵比對功能，對於封包深層內容進行快速比對並同時進行封包阻擋、儲存與告警的相對應處理，惡意特徵來源情資透過雲端機制隨時更新，以達到更即時與最新的防護。

- 封包錄製，保存原始資料

  支援封包錄製功能，可利用 IP、Port 與 Protocol 為條件將特定的封包儲存至 PCAP 檔案，提供後端管理者分析。

- 封包複製轉發，提供後端即時收錄

  支援封包轉發功能，透過設定可達到封包單一或多份複製，並再透由閒置的網路埠將其封包轉發出去，其中還可搭配規則功能，透過規則中的 IP、Port 與 Protocol 的設定來做為轉發條件。

- NetFlow 資料產出

  支援 IP Session 產出功能，提供即時網路流量資訊，監測網路現今所承載流量大小、流向之情況，提供後端管理者資源分析依據。

- 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。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。

- 封包內容比對模組(DPI)

  - 支援正規表示比對功能，針對封包第七層內容進行快速特徵碼比對，達到深層防護功能。

- 比對到的特徵同時還可搭配其它模組進行封包錄製、拋棄與告警相對應功能，達到更多的附加應用。
- 目前可支援 50 萬筆特徵規則。
- 特徵情資來源包含第三方 Snort Rule 與透過管理頁面自行定義操作。

- 封包錄製模組
  - 支援特定封包錄製功能，其觸發條件包含特定 IP、Port 與 Protocol，封包將儲存成 PCAP 檔案後提供後台管理人員下載。
  - 透過管理頁面即時操作，採用不中斷服務方式進行設定。
- 封包複製轉發模組
  - 支援封包複製，可透過設定將封包複製單份或多份。
  - 支援複製封包轉發，搭配規則中的 IP、Port 與 Protocol 條件將複製封包透過指定的網路埠轉發出去。
  - 透過管理頁面即時操作，採用不中斷服務方式進行設定。
- 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。

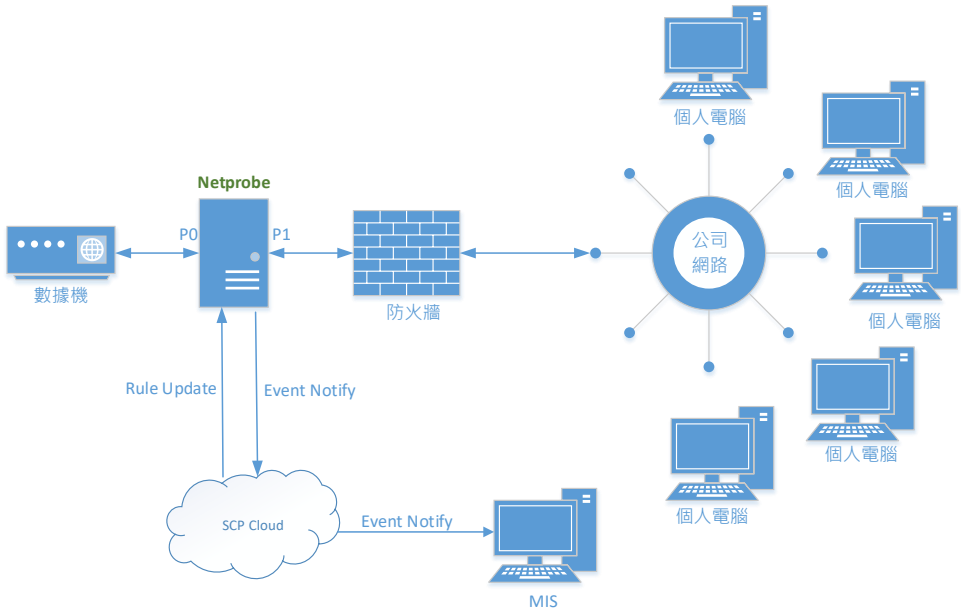
  - 誘捕系統：可模擬多種網路通訊協定與服務。依其功能可分為常見管理服務協定、常見網頁服務協定及常見資料庫服務等 3 大類。一旦駭客或惡意程式踏入陷阱時，便將其來源 IP 新增至 IP 黑名單內。各類協定分別如下所示：
    - 常見管理服務 SSH、Telnet、RTSP 及 RDP
    - 常見網頁服務 HTTP 與 HTTPS
    - 常見資料庫服務 MSSQL、MySQL、Oracle Database 及 MongoDB
  - 行為分析：
    - 係指透過分析誘捕系統捕獲的駭客互動行為的方式，篩選出最符合駭客攻擊特徵的來源 IP，並搭配自製演算法，參考其發生頻率、發生時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

分析流量特徵，自動調整各項 DoS / DDoS 觸發規則。

應用場景

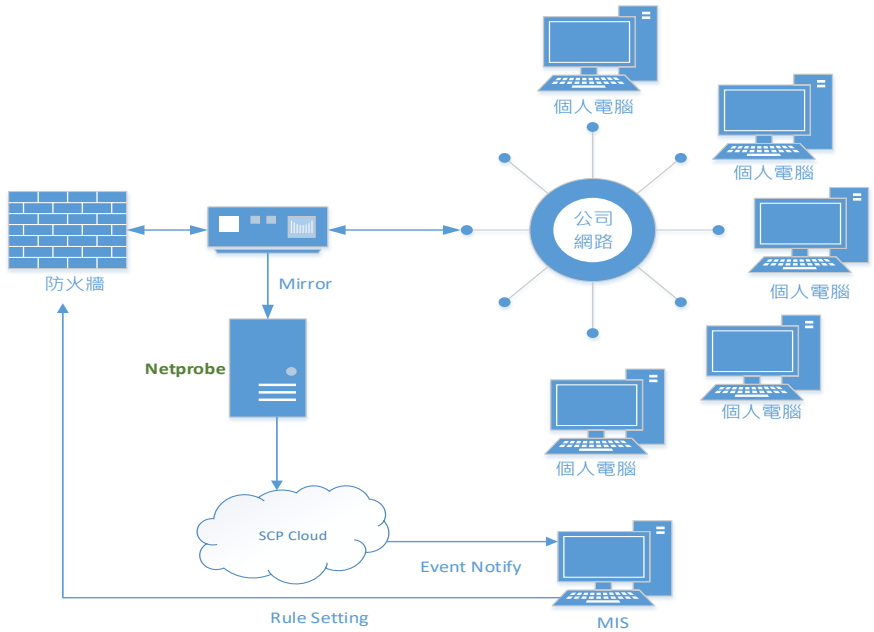
- 外網環境佈署

  NetProbe 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。



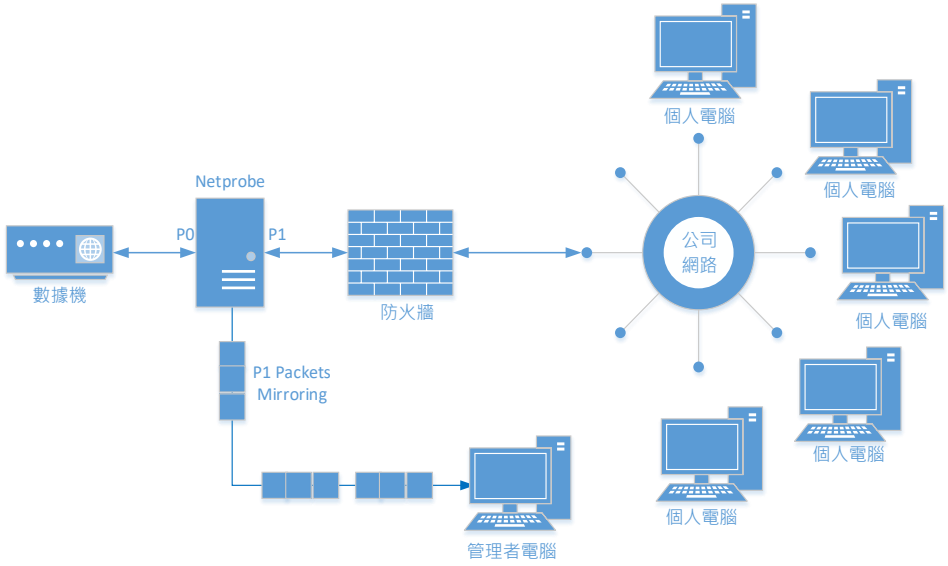
- 內部環境佈署

  NetProbe 置放公司環境，透由橋接器(Switch)將出入封包複製一份給 NetProbe，此時 NetProbe 會被動的察看每個封包，如發現惡意 IP 隨即發出通報。



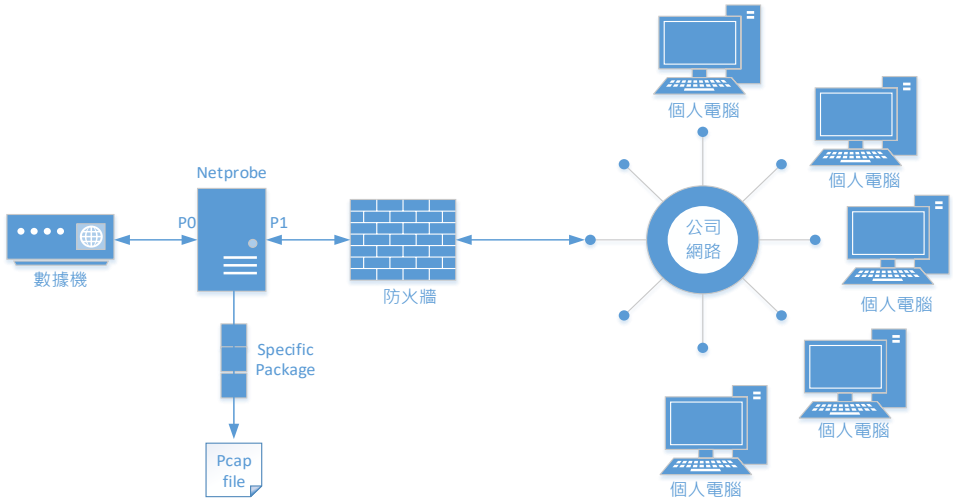
- 封包複製轉發佈署

  透過封包轉發功能，可佈署於公司網路任何地方，進行特定封包複製轉發，不影響既有封包進出。



- 封包儲存佈署

  透過封包儲存功能，可佈署於公司網路任何地方，可針對設備特定的埠或封包中的 IP、Port 與 Protocol 內容進行封包儲存。



系統規格

系統規格	
Network	
Bypass Interface	1GbE or 10 GbE * 4 or 8
IDS / IPS througput	10 Gbps
Dos / DDoS throughput	10 Gbps
Latency	≤ 60 μ sec
Storage	2.5" 500GB * 1
Memory	64G
Power	220W ATX PSU Power redundancy
Chassis Dimension	16.93" x 18.7" x1.73"(430mm x 475mm x 44mm) 19" 1U Rack-mount
I/O Interfaces	
Front Panel	Power LED x 1 HDD Active LED x 1 RJ-45 Console x 1 Parallel LCM display and 4 keypad

Gorilla Technology

Follow Us