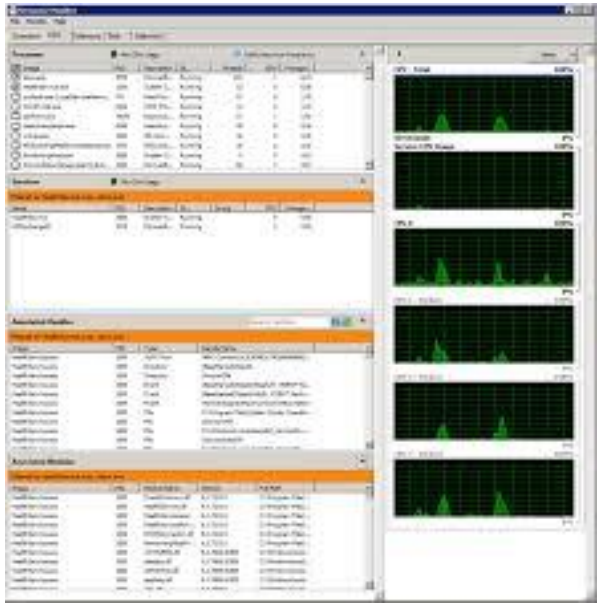
DoS / DDoS 演練方式

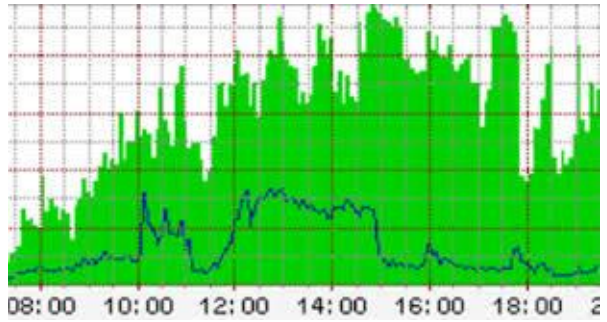
消耗網路資源

- 消耗**網路頻寬**為主，讓使用者無法使用受攻擊之系統，達到癱瘓網路的目的
- 主要使用**網路流量**作為攻擊

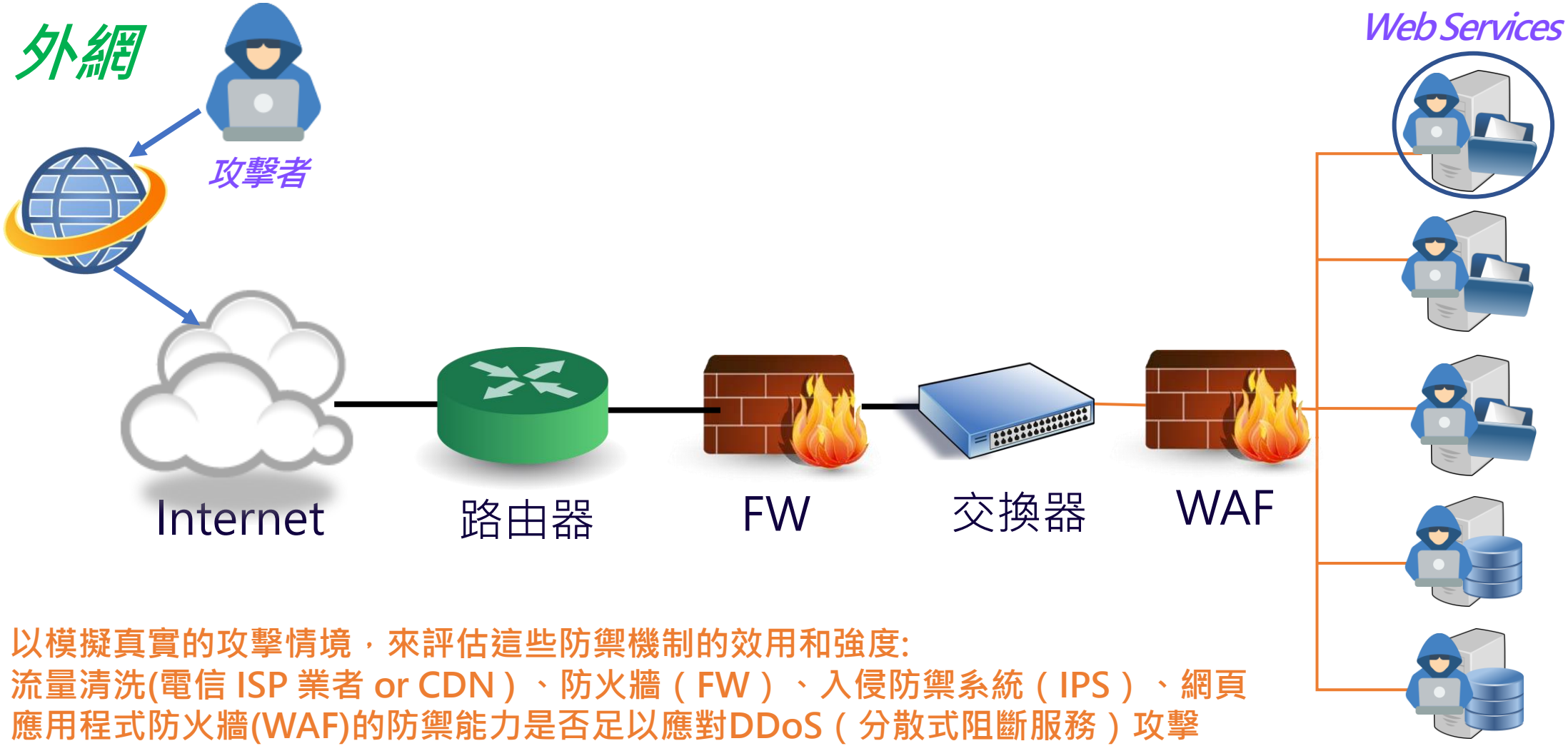
消耗系統資源

- 消耗**系統的資源**如記憶體及CPU，讓系統無法正常運作，達到癱瘓系統的目的
- 大部分使用**大量連線**行為作為攻擊





DoS / DDoS 演練規劃



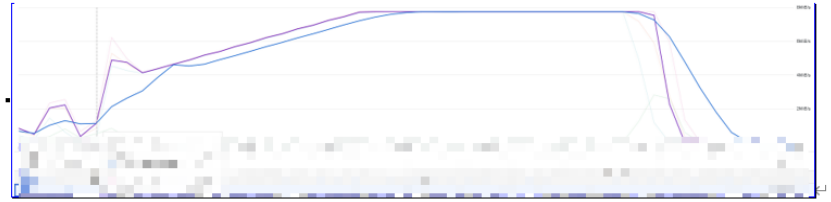
以模擬真實的攻擊情境，來評估這些防禦機制的效用和強度:
流量清洗(電信 ISP 業者 or CDN）、防火牆（FW）、入侵防禦系統（IPS）、網頁應用程式防火牆(WAF)的防禦能力是否足以應對DDoS（分散式阻斷服務）攻擊

DoS / DDoS 演練規劃_報告範例 - 演練過程記錄

（二） 階段 1.1：發送發起值 [redacted] Mbps UDP Traffic

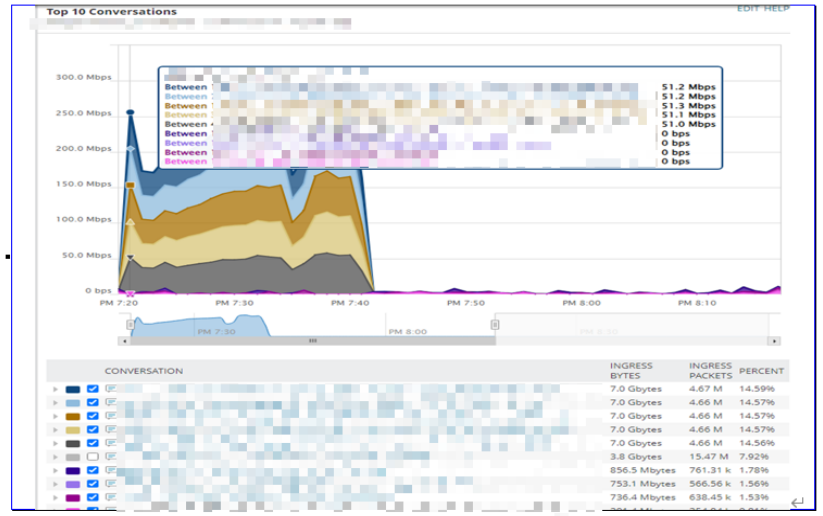
1. 時間：[redacted]
2. 標的狀態：服務正常
3. 演練測試紀錄：

(1) DDoS 廠商



【圖 3】DDoS UDP traffic-01

(2) 受測方對外防火牆流量

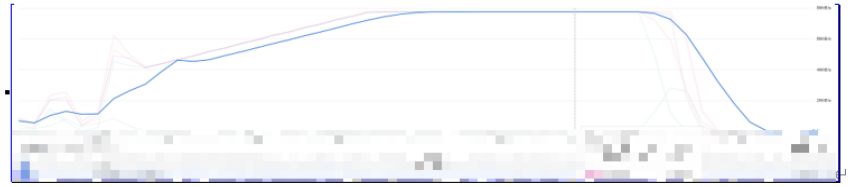


【圖 4】演練中-受測方對外防火牆流量([redacted])

（六） 階段 1.5：發送 [redacted] Mbps UDP Traffic 持續 [redacted] 分鐘

1. 時間：[redacted]
2. 標的狀態：服務正常，並已啟動中華電信流量清洗。
3. 演練測試紀錄：

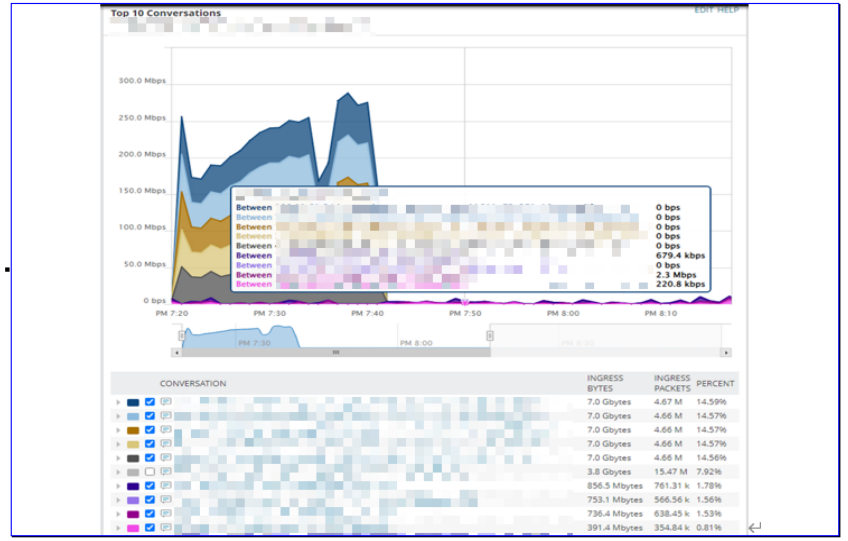
(1) DDoS 廠商



【圖 11】DDoS UDP traffic-05

(2) 受測方對外防火牆流量

DDOS 後查詢 19:43:33 後無流量紀錄(防火牆)。



【圖 12】受測方對外防火牆流量([redacted])