FAIRLINE

政府網路安全發生根本性轉變

第一步建立可視性網路架構

根據統計國內政府機關每個月平均受到 3000 萬次的境外網路攻擊

台灣因地緣政治與區域鄰近性，經常遭受各種新式資安攻擊的國際資安攻防熱區，俄烏戰爭引起網路犯罪分子利用更多的地緣政治來攻擊關鍵基礎設施，讓亞太地區國家、企業更加體認網路攻擊增添地緣政治的風險變數。

網路可視性就是網路安全

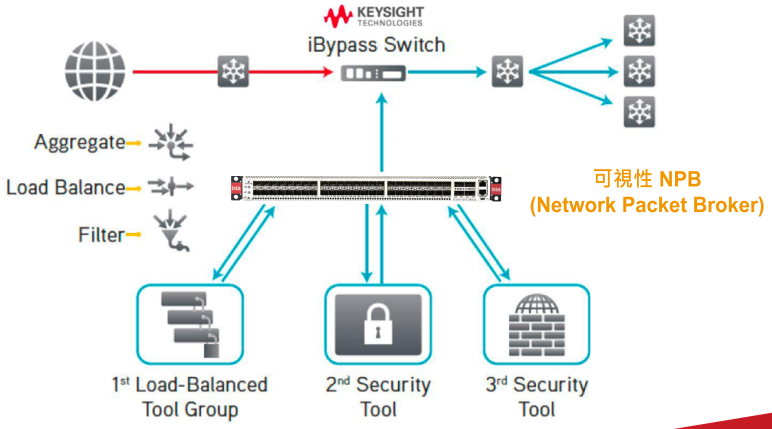
安全工具和技術的好壞最大取決於它們接收到的用於分析的網路數據。
網路數據遺失或無法辨識則....

無法識別威脅，
那麼您就無法防禦它。

無法識別入侵或破壞，
那麼您就無法阻止它
並減輕損失。

不知道哪些系統受到了影響，
無法確定是否已恢復到安全
狀態。

無可視性的網路架構，這會引發一系列問題，
例如流程故障、盲點、丟失關鍵數據以及問題解決的延遲。



▶建立一個支持您的安全計劃的可見性架構
智能地過濾必要的數據以便 IT 可以就問題做出明智的決策有效分辨和網絡改進。

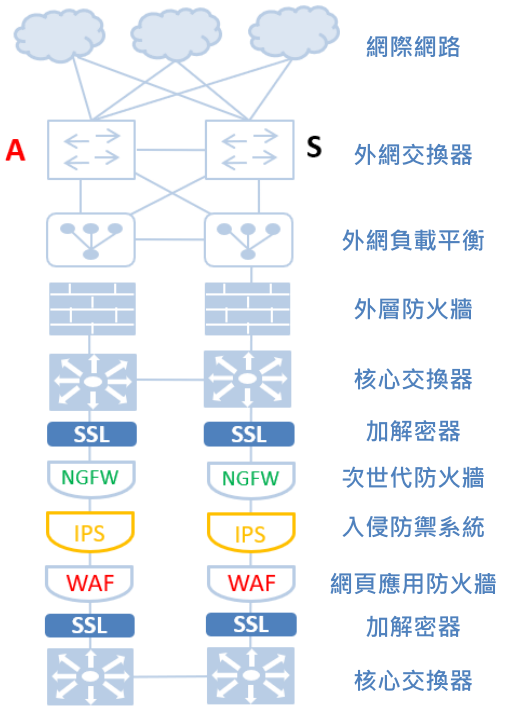
台灣政府實際案例

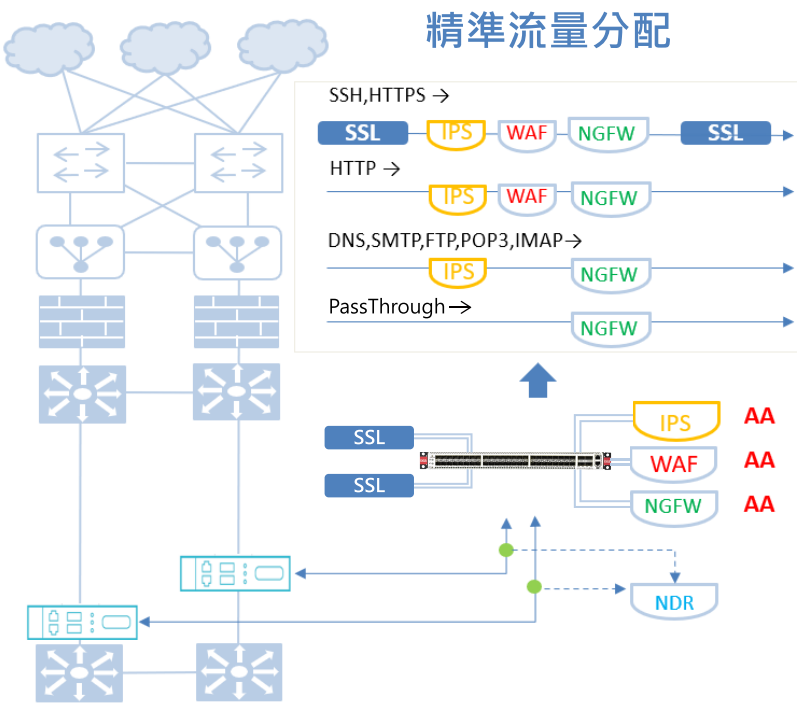
過去的架構

- 單點故障切換
- 無法達到 AA 模式
- 無精準流量分配
- 無法將流量複製給資安設備
- 資安設備升級版需安排斷線時間

採用可視性 NPB 架構後

- 單點故障不影響服務
- 資安設備 AA 模式
- 精準過濾分配流量
- 可複製多份流量至給資安設備
- 升級無需安排斷線時間
- 多個廠商可同時進行產品測試





FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市三民區民族一路80號27樓之2 A08室

KEYSIGHT TECHNOLOGIES
Authorized Distributor