WATERFALL®
One Way to Connect

單向網路安全閘道

完全阻絕外來的網路攻擊!!!

- 讓一般網路區段也能和機敏網路區段進行資料交換且不降低安全防護層級
- 協助企業符合NERC, NIST, CFATS等法規的要求
- 透過硬體的物理架構讓資料僅能單向傳遞，絕無反向傳輸的可能性
- 不須改變既有工作流程即可消除網路威脅，大幅降低企業風險
- 減少防火牆設定、管理及稽核的成本
- 可佈署在任何網路區段

當前問題

企業組織的機密文件、敏感資料需要保護，但卻又擔心資料遭到竊取？或是企業組織的營運中心（Operation Center）、網路安控中心（SOC,NOC）等維運作業需要資料即時的交換，卻又害怕遭到網路攻擊而影響企業營運？

面對上述問題，現有的做法不外是：

- Plan A：利用防火牆將該網路區域劃分成為一個隔離的網路環境，並以防火牆規則限制存取。

> 問題：以防火牆來管理兩個網路區段，其網路實體層仍然相通，不是100%安全，且防火牆規則常有人為設定疏忽（Misconfiguration）之虞。

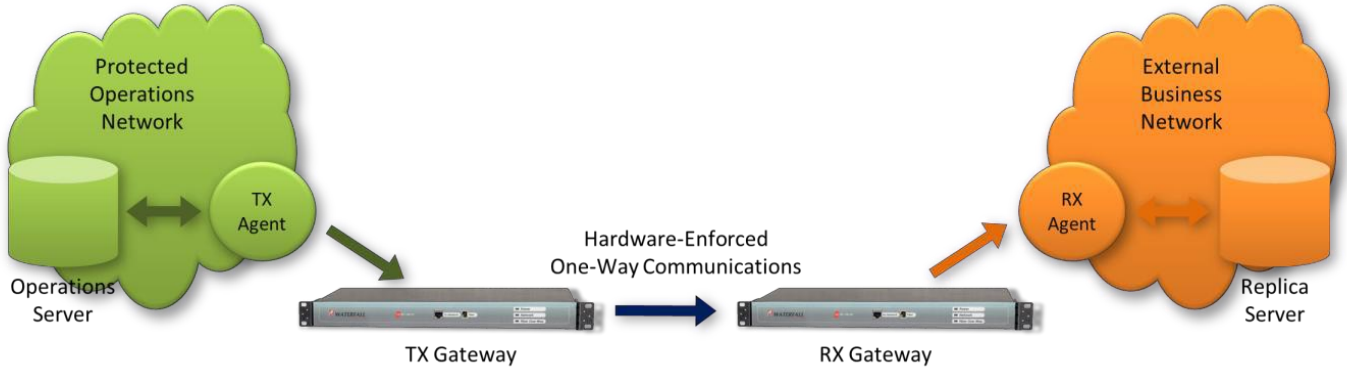
- Plan B：或是直接以實體隔離的方式來切斷機敏網路區段對外的通訊，完全沒有任何外來網路的連接。

> 問題：實體隔離無法解決內外網常需資料交換的問題，若是透過可攜式儲存裝置來交換資料，更會衍生出種種追蹤與稽核上的問題。

" Waterfall 的單向網路安全閘道（Unidirectional Security Gateway）不但完全解決上述問題，且能充分滿足企業資料交換與安控的需求！"

解決方案

Waterfall的單向網路安全閘道系統利用光纖（Fibre-Optic）傳輸的特性，也就是光的不可逆性。一般的光纖傳輸會有兩組線路：一組負責正向傳輸（TX->RX）、一組負責反向傳輸（RX<-TX），而 Waterfall 則將其中的一組線路移除。因此，資料將只能藉由 Waterfall 的TX Agent 將資料從 TX Gateway 複寫（Replicate）至 RX Gateway，完全杜絕任何反向通訊的可能性。



一般資料傳輸必須透過兩端的三向交握（3-Way Handshaking）機制來避免資料的錯誤或是封包遺失，而 Waterfall 獨特的專利技術能夠在實體的單向網路（僅 TX 端至 RX 端）架構下，無須三向交握即可達到資料傳輸的完整性以及正確性。

美國國土安全部以及 Idaho National Lab 已驗證 Waterfall 確實能夠做到百分之百不遺漏的單向網路資料傳輸，且 Waterfall 單向網路安全閘道亦通過 Common Criteria EAL 4+的認證。

Waterfall 所支援的網路協定

常見的工業應用軟體

- OSIsoft PI, GE iHistorian, GE iFIX
- Scientech R*Time, Instep eDNA, GE OSM
- Siemens: WinCC, SINAUT/Spectrum
- Emerson Ovation, SQLServer
- Matrikon Alert Manager, Wonderware Historian

常見的 IT 網管通訊協定

- Log Transfer, SNMP, SYSLOG
- CA Unicenter, CA SIM, HP OpenView
- McAfee NitroView SIEM, HP ArcSight SIEM

檔案/資料夾傳輸應用

- Folder, tree mirroring, remote folders (CIFS)
- FTP/FTFP/SFTP/TFPS/RCP

常見的工業通訊協定

- Modbus, OPC (DA, HDA, A&E)
- DNP3, ICCP

遠端存取

- Remote Screen View™
- Secure Manual Uplink

其他連接器

- UDP, TCP/IP
- NTP, Multicast Ethernet
- Video/Audio stream transfer
- Mail server/mail box replication
- IBM WebSphere MQ series
- Anti-Virus updater, patch (WSUS) updater
- Remote print server