

SSL Interception(SSLi)

SSL 流量的「可視化」

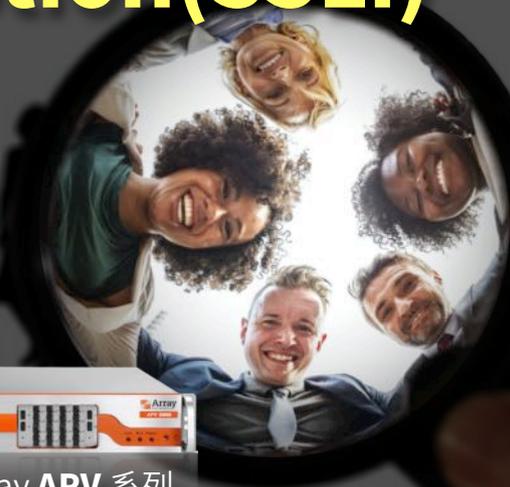
Array vAPV 系列
虛擬應用交付控制器



Array AVX 系列
網路功能平台



Array APV 系列
應用交付控制器

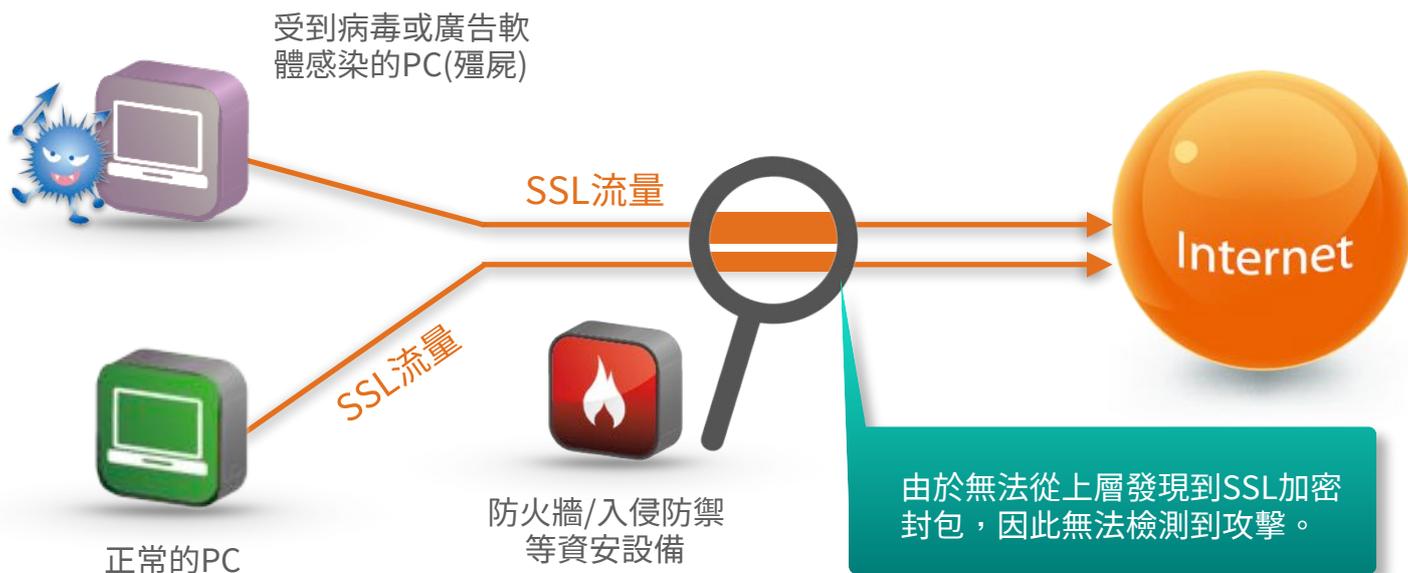


○ Always on SSL時代的「兩個課題」

網路流量使用SSL加密，能夠增強網站在搜尋引擎最佳化(SEO)方面的優勢，且其發展的速度已超越原本預期；並可確保路由上封包的隱匿性和存取目標網站的正確性，對於安全性的提升也極具成效；但是，在這二年間成為主流的SSL加密流量，從IT營運管理的角度來看，也正在產生新的挑戰。

○ 看不見的威脅

某些安全設備例如「防火牆和入侵防禦」，對於SSL加密流量的處理呈現性能不佳。在SSL/TLS通訊中，原則上在伺服器與客戶端之間進行密鑰交換後，將會以加密的狀態發送或接收封包的上層資料，這意味著在路由上的安全系統，僅能直接在TCP層級上截取通訊；而病毒或廣告等惡意軟體的行為，也可能會因為加密而變得難以發現，這對於IT人員而言，可說是「全新的威脅」。



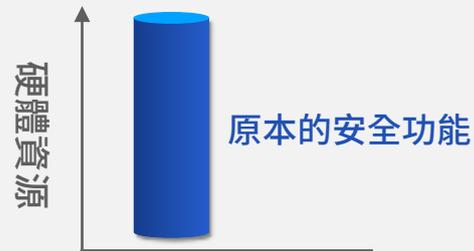
○ 既有系統過度負載

另一方面，雖然有一些安全設備本機就支援SSL流量的解密/重新加密，但是，即使在那樣的情況下，添加SSL處理對安全設備而言是一個沈重的負擔；既有系統所能夠承受的限度為何呢？系統性能的劣化也會影響到商業效率，但如果以「安全為代價」，這樣的付出也未免太大了……。



防火牆/入侵防禦
等資安設備

現況...
安全功能專享資源



SSL支援後...
SSL處理所消耗的資源



但是有時候...設備SSL模組成為瓶頸



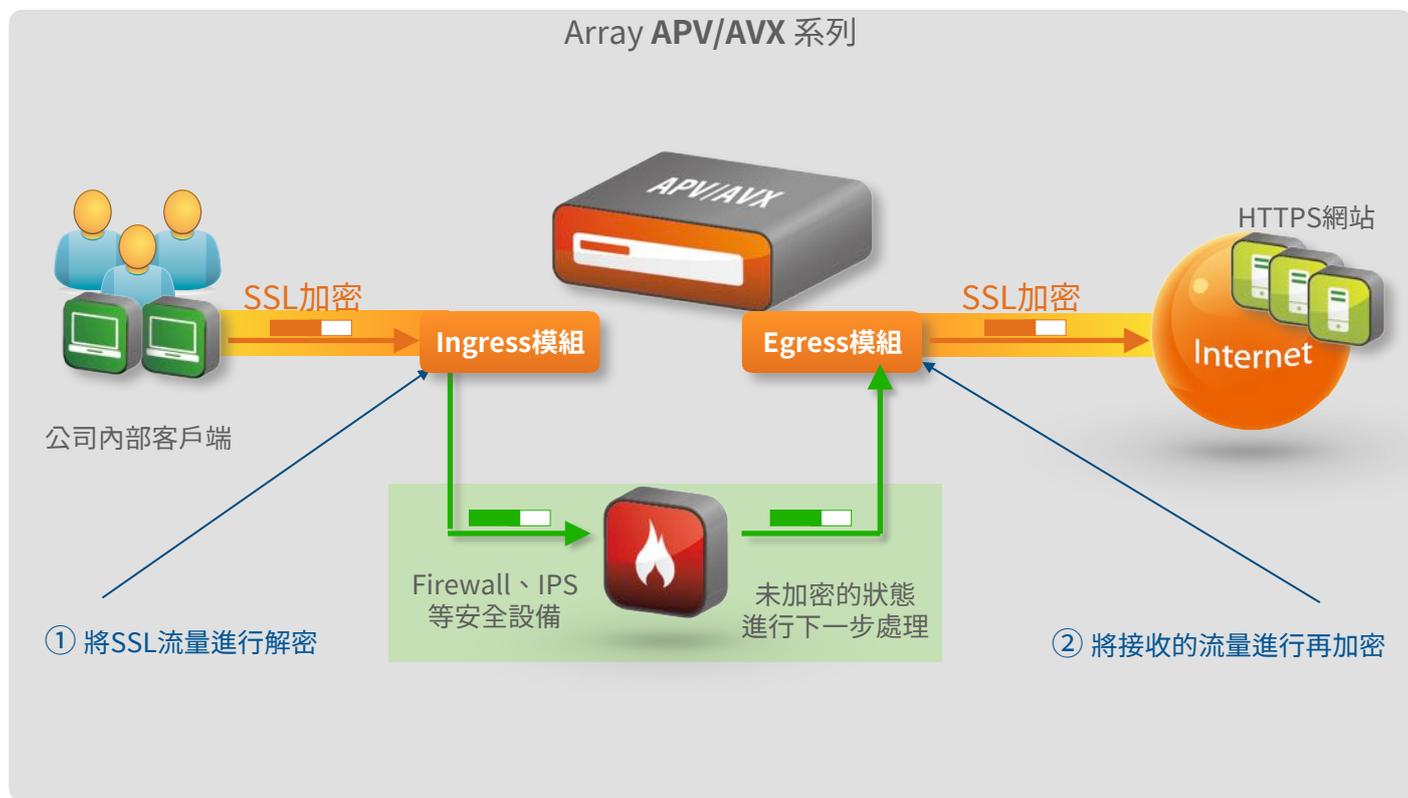
SSL流量再增加的話
情況會是如何？

多台設備組合連動時
情況會是如何？



○ Array SSL Interception

Array SSL流量可視化(SSL Interception)，會在完成SSL流量的解密後(未加密)傳送到安全設備(Ingress模組)，此外，通過安全設備的流量將會暫時回到Array的設備中，並於再次加密後往目的地前進(Egress模組)；返回方向的通訊將會以相反方式進行(Egress→解密、Ingress→加密)



● 維持系統產出量(Throughput)

Array APV/AVX系列配置了專用的硬體模組以進行SSL封包的解密/重新加密處理；由於安全設備不再需要處理SSL流量，因此能夠更確實可靠地配置系統產出量。而AVX系列網路功能平台所配備CPU核心指派至特定的虛擬設備，因此也不會發生超量使用(Overcommit)的情形。

● 既有設備有效利用

由於安全設備僅需對解密後的流量進行檢查即可，因此能夠發揮原本的功能與性能並足以接管營運流程，這樣可以提供全面性的投資保護。

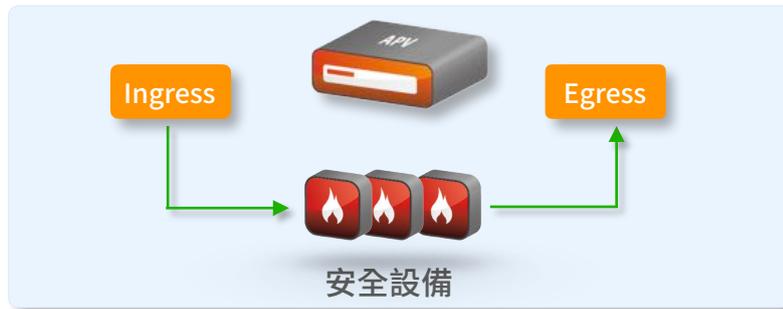
● 線性而高度彈性的擴充能力

由於Array APV/AVX除原有的負載平衡功能外，還能夠進行流量分配，因此能夠以線性追加安全設備，藉此提高系統的產出量。此外，在更換安全設備時，您可以靈活選擇適合的機型與建置模型，而無需考慮安全設備的SSL處理性能所造成的影響。



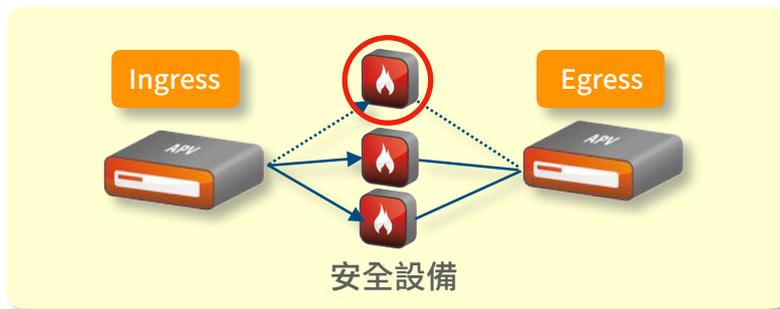
○ 單台APV實現靈活的配置

可以在單台APV設備中組合Ingress/Egress兩個模組，此時兩個模組的性能會是竭盡全力(Best Effort)的方式。



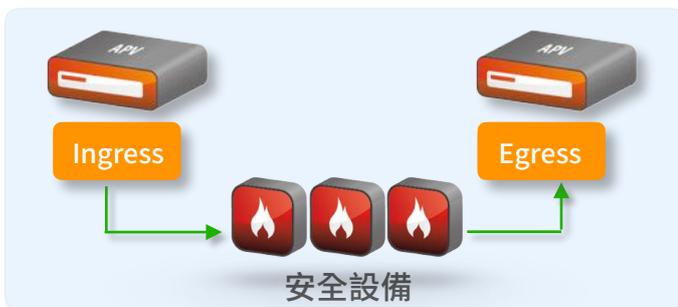
○ 搭配負載平衡進行線性擴充

除APV所具備的負載平衡功能外，安全設備的追加也能夠帶來性能上的提升。



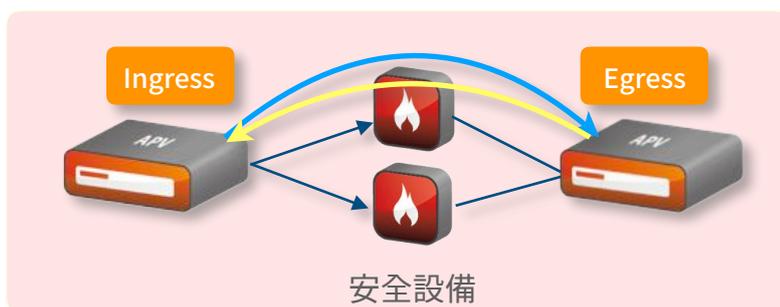
○ 需求更高性能的配置

Ingress/Egress兩種模組，亦可分別配置於2台APV，藉此發揮更高的性能，AVX系列則能夠以單台實現此組合。



○ 返回的路線與前進方向相同

透過(RTS (Return-to-Sender))功能，返回方向的封包將會通過安全設備，與前進方向相同。



○ Array SSL Interception 結合 Bypass Module 應用規劃

- 充分了解流量內容
- 降低資安設備的負載
- 提高資安設備的利用率
- 事前的預防
- 事後的分析
- 高性能SSL處理能力
- 支援硬體解密(RSA/ECC)
- 支援多種應用服務：包括Google Driver、Office365、SSH、SMTPs、POP3s.....
- 支援一萬組以上的憑證
- 支援硬體/軟體 Bypass
- 可在任一設備故障時，自動動態切換
- 支援百萬組IP/Domain過濾清單



○ Array SSL Interception 支援產品



APV-1800
7 Gbps SSL TPUT
20K TPS RSA
14K TPS ECC



APV-2800
10 Gbps SSL TPUT
20K TPS RSA
14K TPS ECC



APV-5800
25 Gbps SSL TPUT
40K TPS RSA
28K TPS ECC



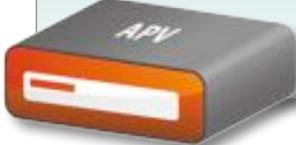
APV-7800
45 Gbps SSL TPUT
53K TPS RSA
38K TPS ECC



APV-9800
90 Gbps SSL TPUT
110K TPS RSA
76K TPS ECC



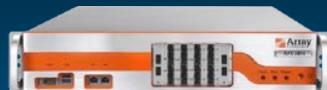
Interop Tokyo 2018 Best of show Award
安全類特別評審團獎項



AVX-5800
20 Gbps SSL TPUT
40K TPS RSA
28K TPS ECC



AVX-7800
40 Gbps SSL TPUT
55K TPS RSA
38K TPS ECC



AVX-9800
90 Gbps SSL TPUT
110K TPS RSA
76K TPS ECC

