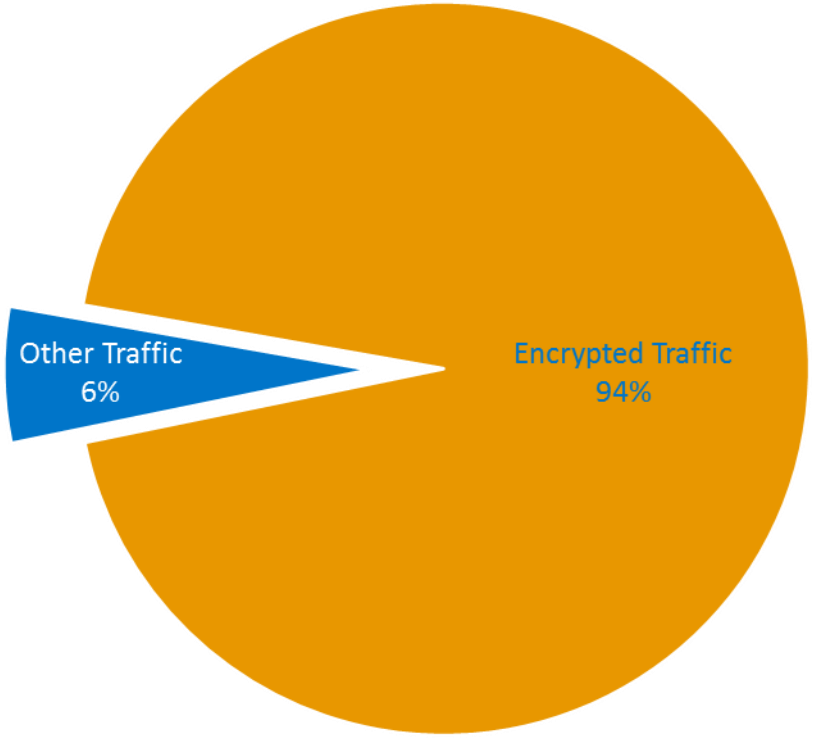
隱藏在加密流量的威脅

A10

Always Secure. Always Available.

Exploiting The Growing Encrypted Blind Spot



94% of all internet traffic is encrypted

Source: *Google Transparency Report | Dark Reading*

NG Firewall Report

Browser-based
Encrypted traffic is over ***90%***

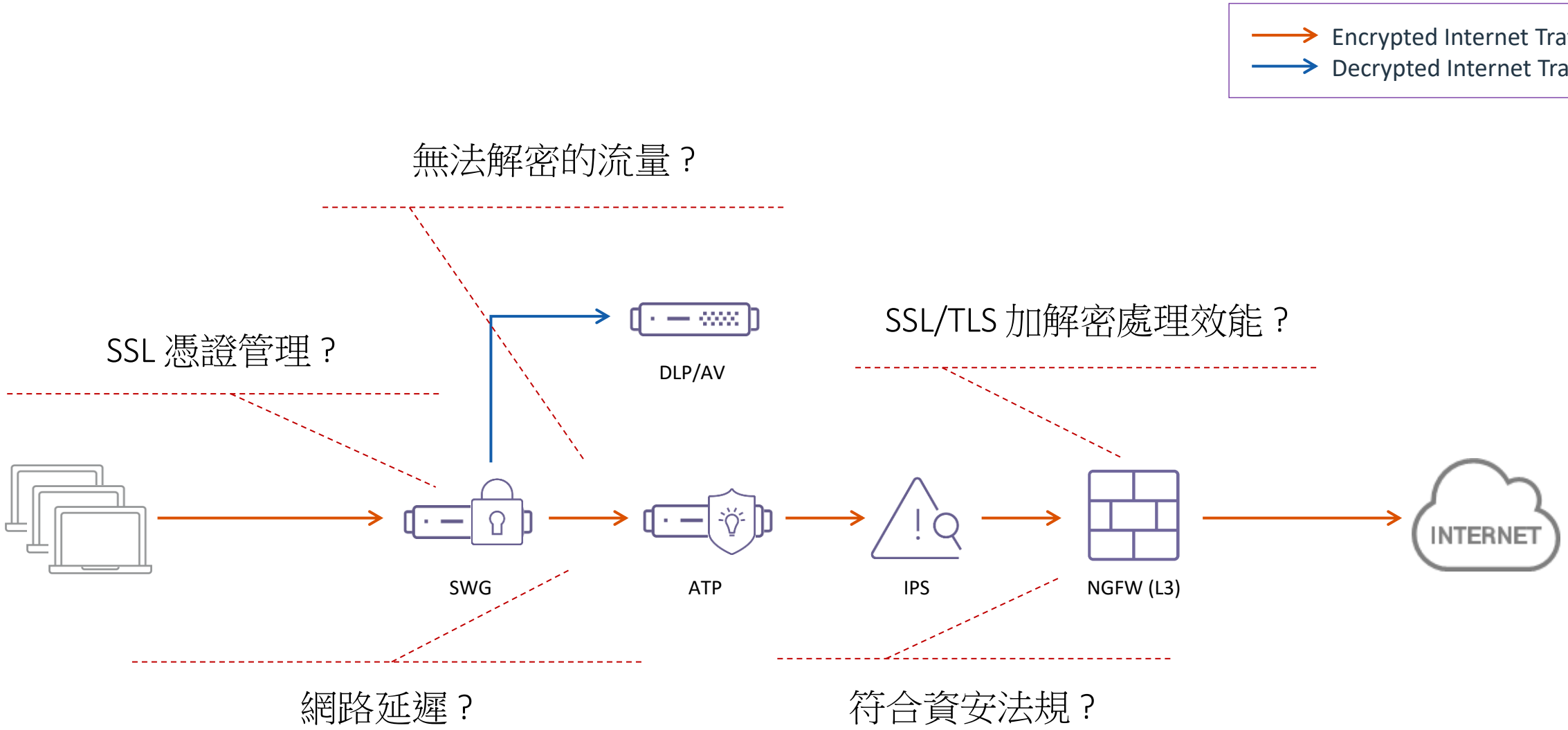
導致風險的應用程式 - 詳細資料

6/9 ~ 6/16 資料收集傳輸量約260G

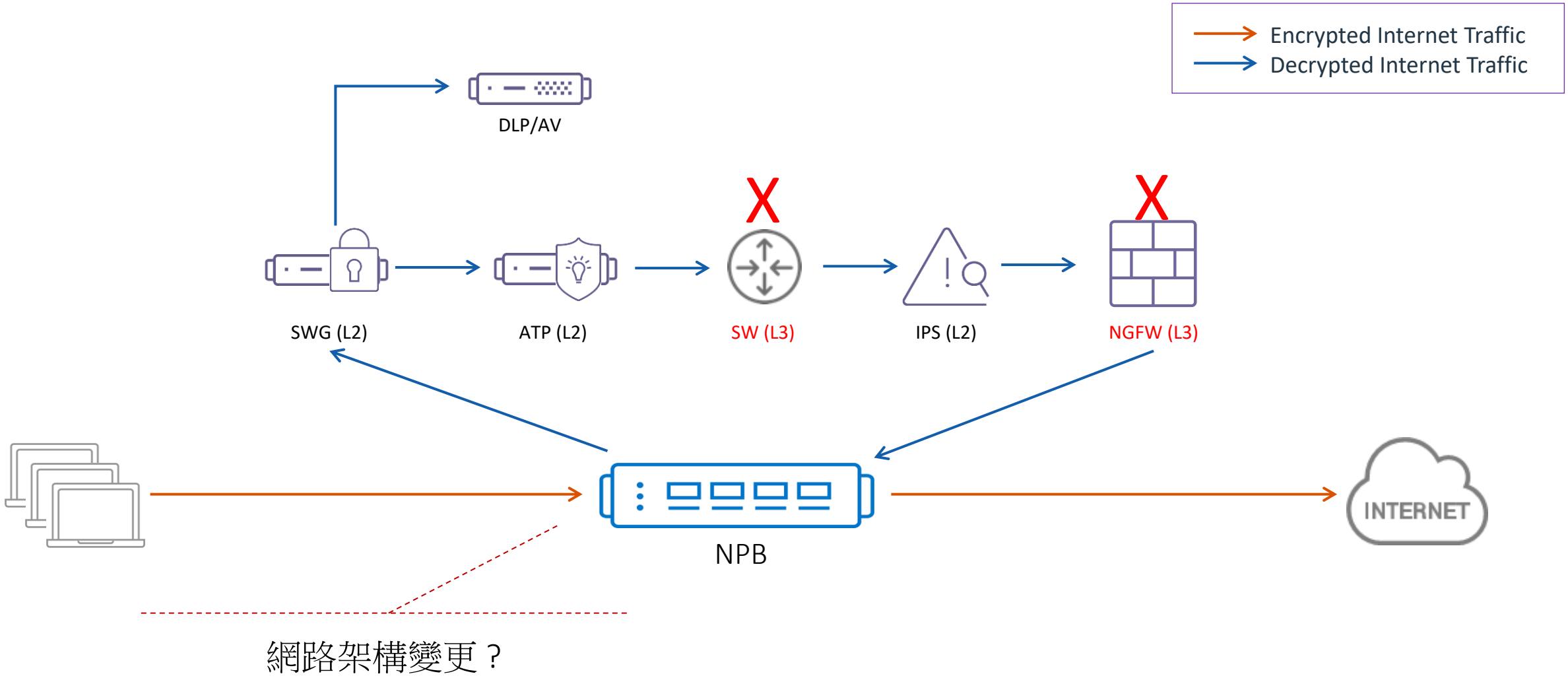
Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	24.03GB	133220
4	pop3	collaboration	email	client-server	2.49GB	14431
4	gmail-base	collaboration	email	browser-based	1.87GB	20934
4	hotmail	collaboration	email	browser-based	341.44MB	4895
3	outlook-web-online	collaboration	email	browser-based	33.84MB	373
3	hinet-webmail	collaboration	email	browser-based	7.99MB	105
4	outlook-web	collaboration	email	browser-based	122.03KB	49
3	yahoo-mail	collaboration	email	browser-based	99.4KB	22
4	ssl	networking	encrypted-tunnel	browser-based	131.94GB	2205755
4	ssh	networking	encrypted-tunnel	client-server	1.23GB	2240
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	862Bytes	1
2	ike	networking	encrypted-tunnel	client-server	212Bytes	2
5	ftp	general-internet	file-sharing	client-server	1.6GB	18506

加密資料共133G

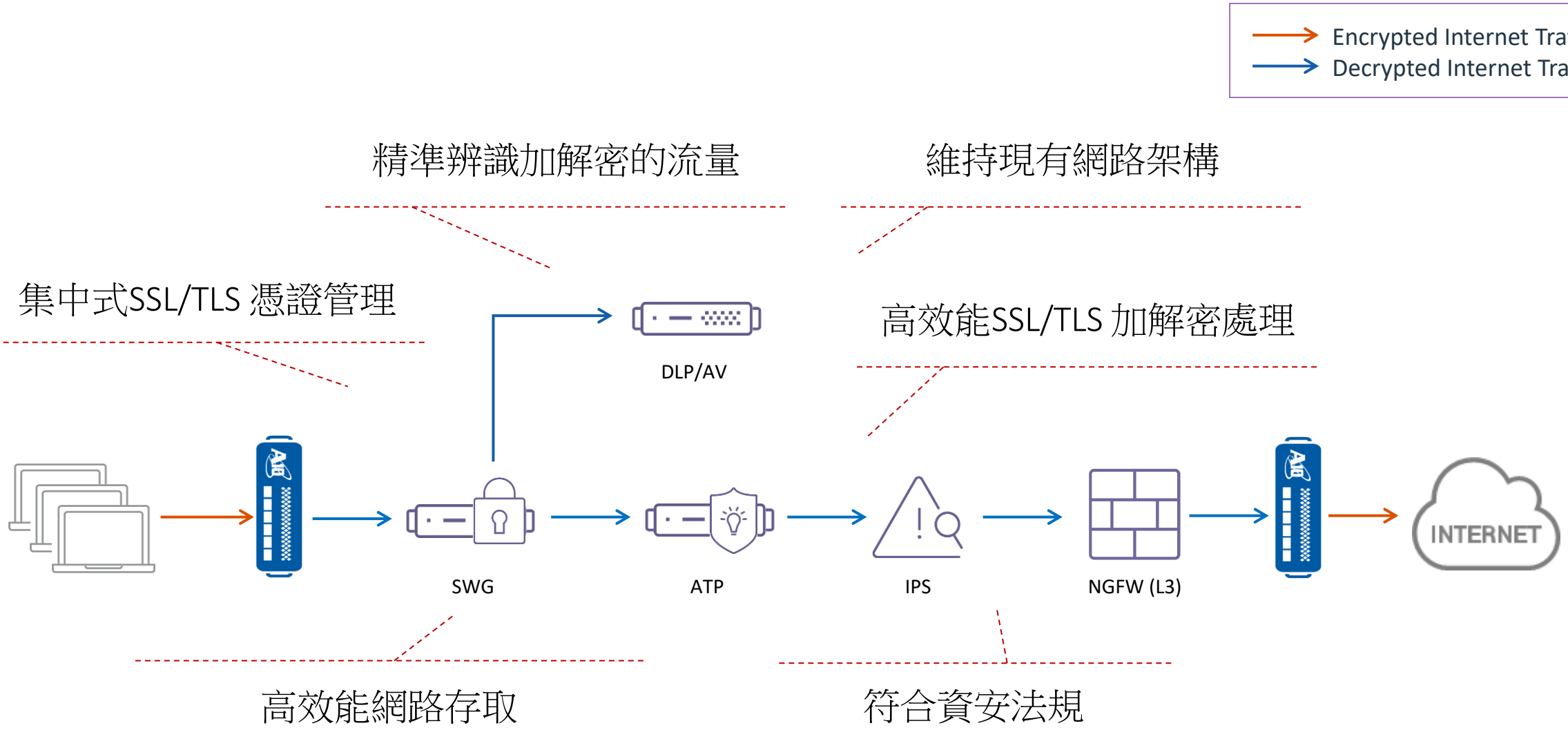
傳統解決方案 1


Encrypted Internet Traffic
Decrypted Internet Traffic
無法解密的流量？
SSL 憑證管理？
DLP/AV
SSL/TLS 加解密處理效能？
SWG
ATP
IPS
NGFW (L3)
INTERNET
網路延遲？
符合資安法規？

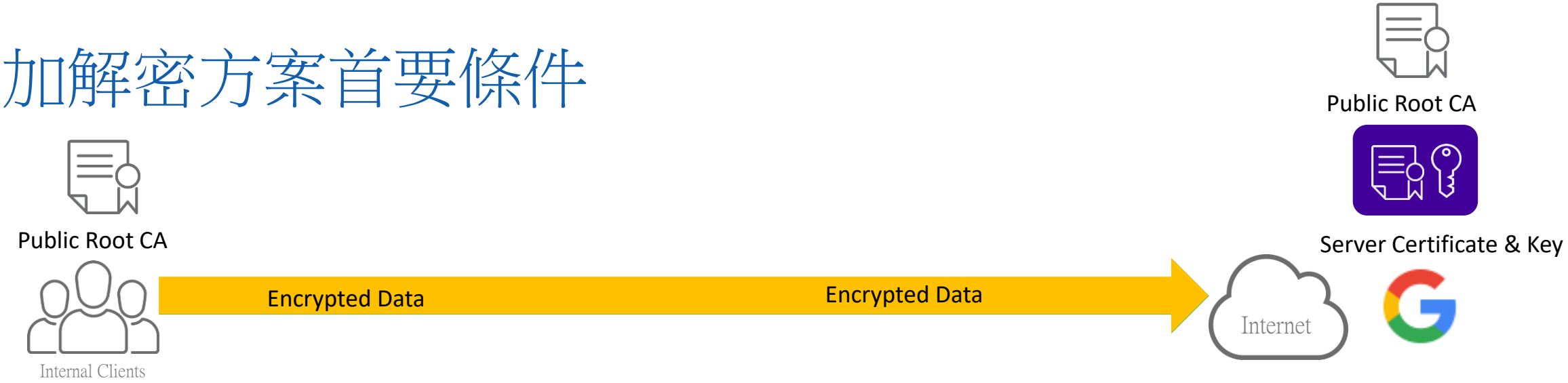
傳統解決方案 2


Encrypted Internet Traffic
Decrypted Internet Traffic
DLP/AV
X
X
SWG (L2)
ATP (L2)
SW (L3)
IPS (L2)
NGFW (L3)
NPB
INTERNET
網路架構變更？

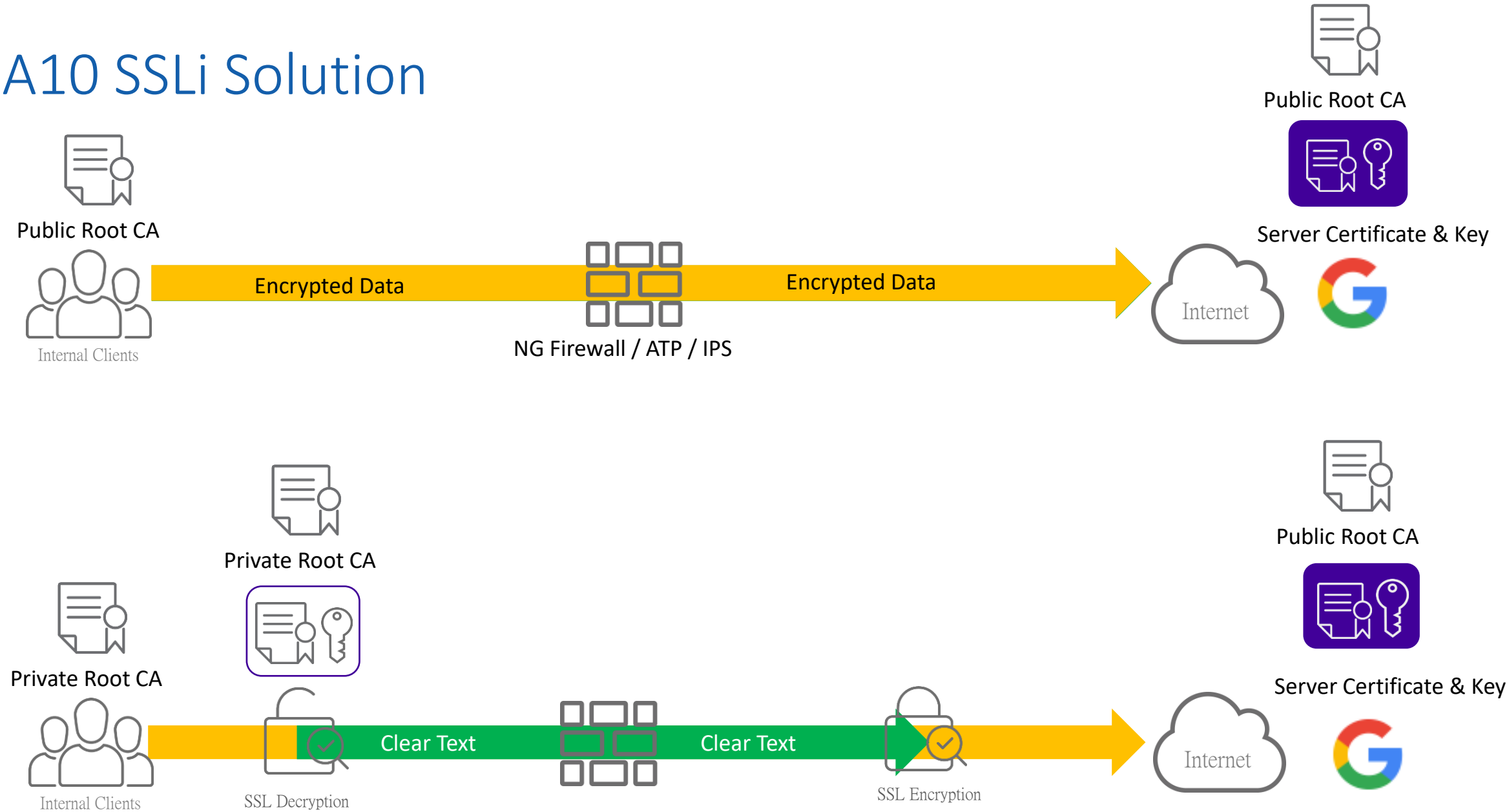
全方位解決方案 – A10 SSL Insight



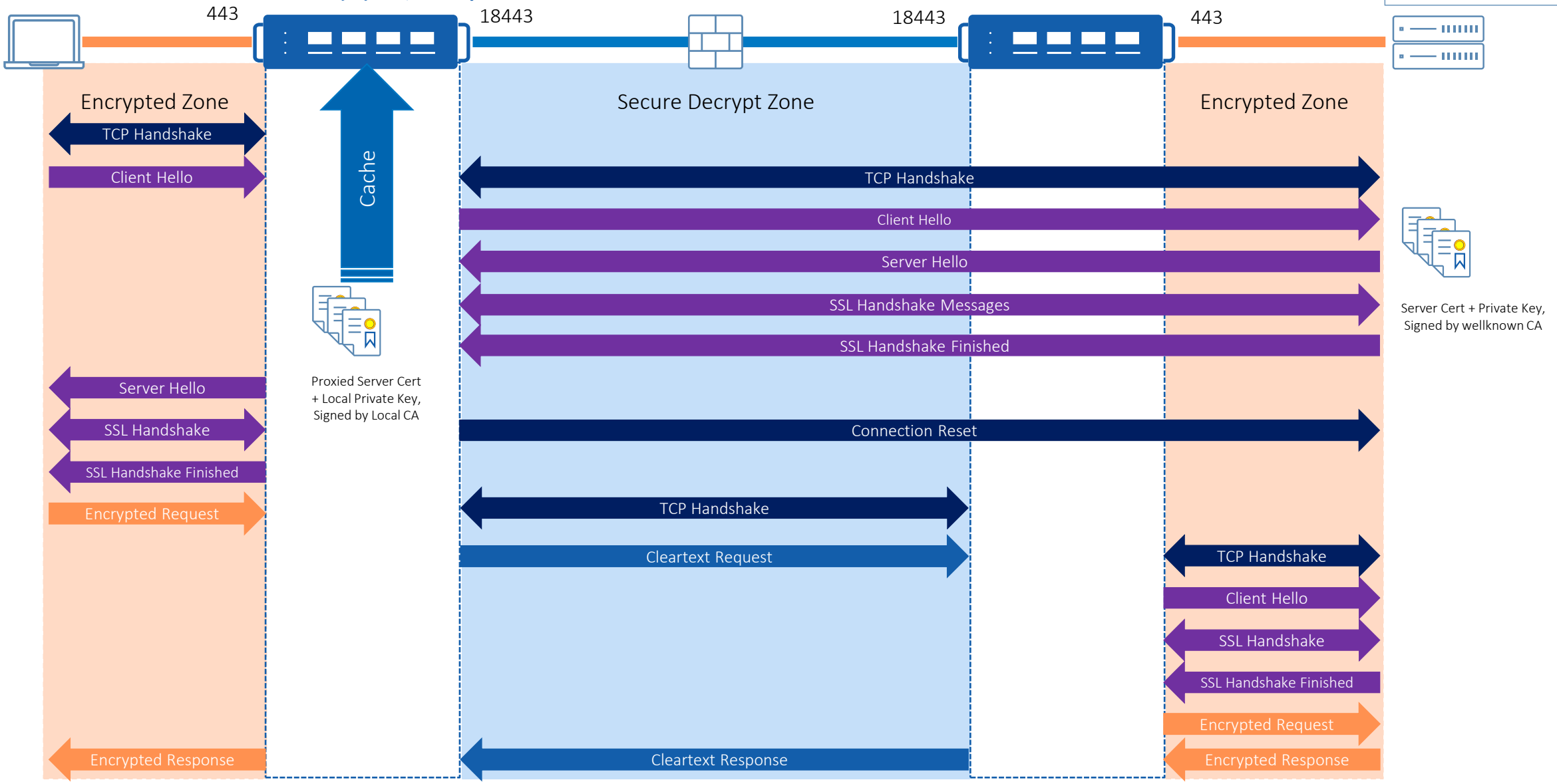
加解密方案首要條件


Public Root CA
Public Root CA
Server Certificate & Key
Encrypted Data
Encrypted Data
Internet
Internal Clients

A10 SSLi Solution



A10 SSLi 運作流程



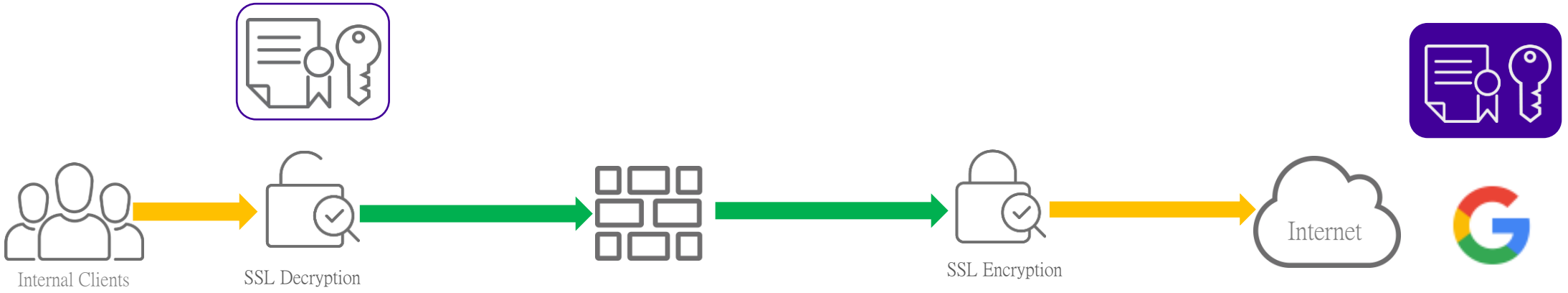
無法解密的流量：Certificate Pinning

Problem

- Certificate Pinning validates against a key embedded in the certificate chain for a domain name
- Some Apps (ex. Twitter, Skype, Windows update ….) contain a predefined list of ‘pinned certificates’, specifically designed to defeat SSLi type solutions

Solution

- Apply SSLi-Bypass for Pinned-Cert Apps. There is no standard technique to decrypt such apps
- Bypass by SNI in client SSL hello or SAN/Issuer/subject in server certificate (server hello).



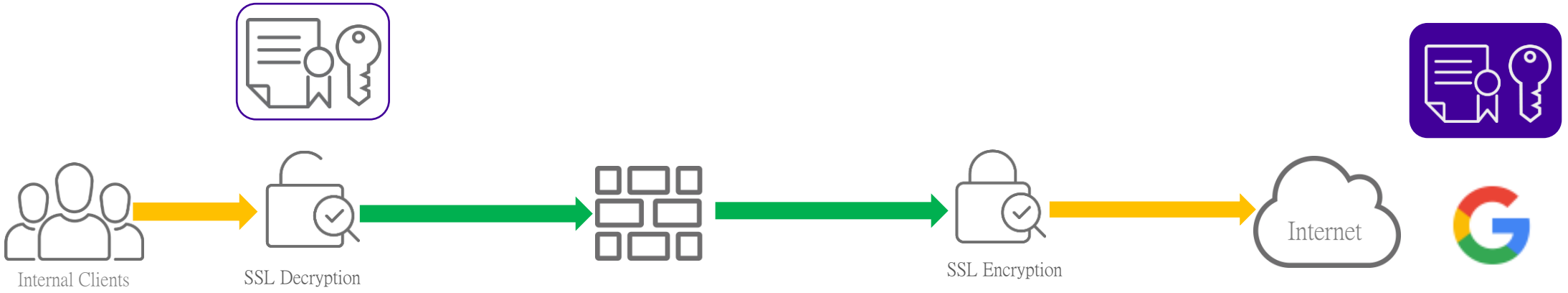
無法解密的流量：CAC Authentication (自然人憑證/數位簽章)

Problem

- SSLi is not supported for applications requiring client authentication, ex. using a Common Access Card (CAC) or a Smart Card

Solution

- SSLi is bypassed for a specified remote server(SNI) only if it requests CAC.



符合資安法規

Selective bypass option to

- Preserve privacy and compliance
- Meet data privacy regulations (HIPAA, PHI, PCI/DSS etc..) by keeping sensitive data encrypted

Traffic can be bypass based on

- A10 Web Classification
- Server Name Indication (SNI)/ Certificate Issuer/ Certificate Subject
- Source & Destination IP Addresses

WEB CLASSIFICATION SERVICE

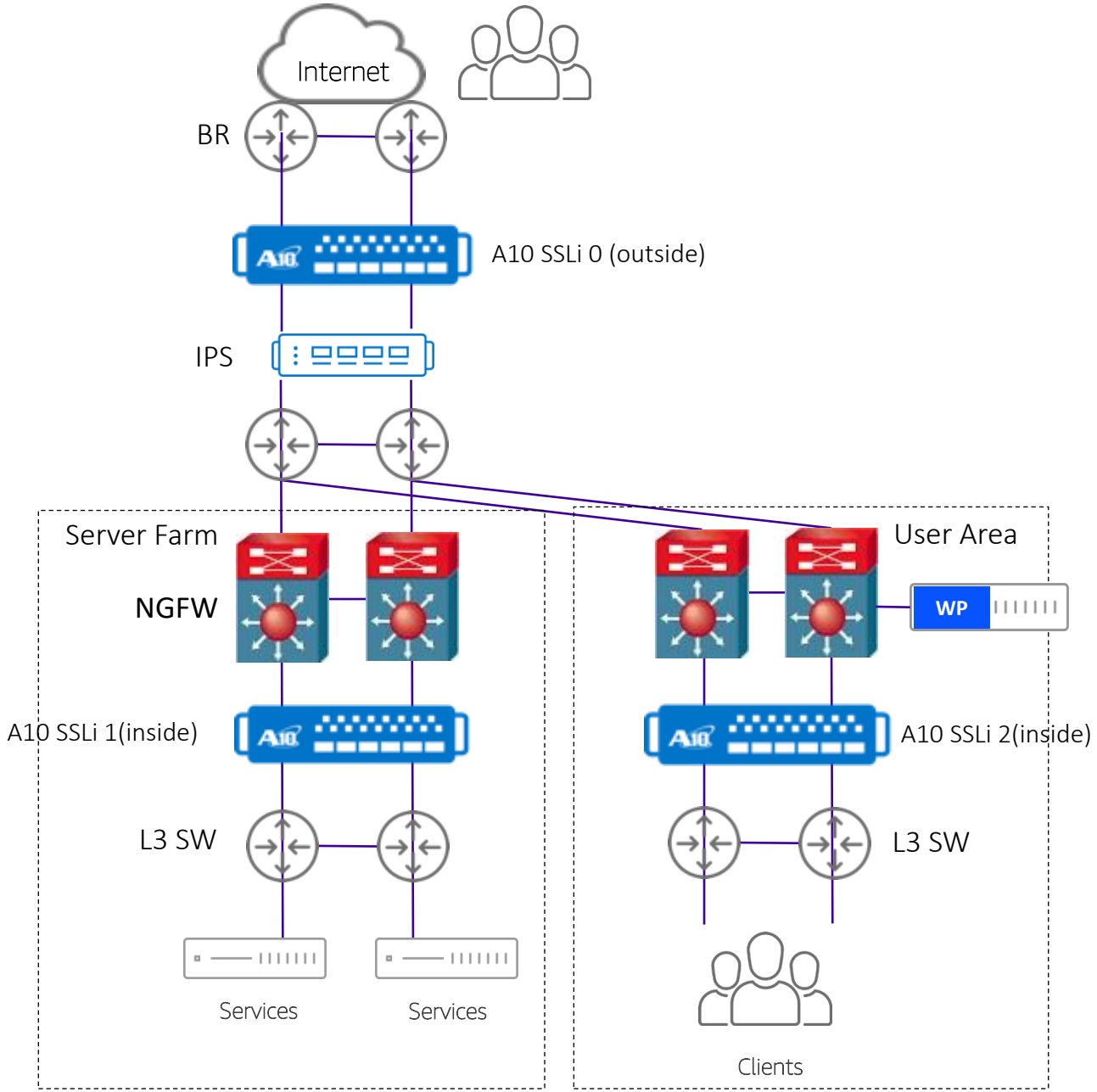
- ✓ 82 site categories
- ✓ 27+ billion URLs
- ✓ 600+ million domains
- ✓ 45+ languages
- ✓ 12 million Dynamic URL correlations

Option for ssli exception list to intercept traffic for bypass category

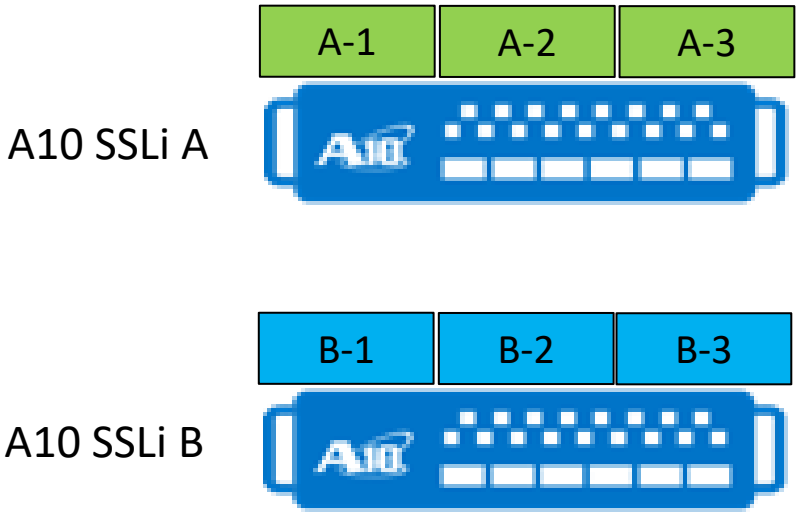
- Allow to intercept a domain under a category even if that category is set to bypass

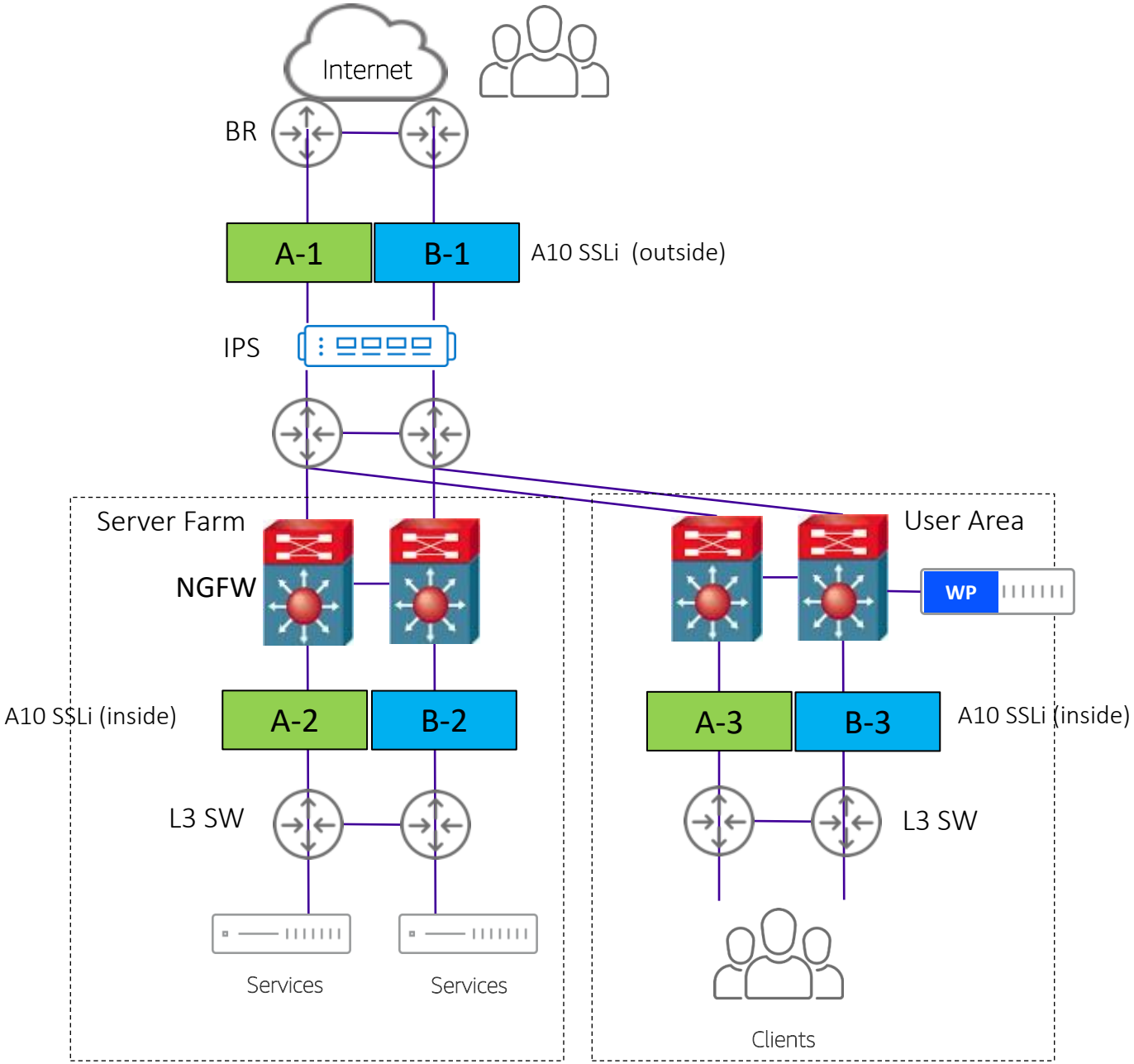
Customer A

- 功能需求
  - 提供 Server Farm 服務加解密 (外對內)
  - 提供 User Area 流量加解密 (內對外)
  - 維持客戶現有架構
  - 提供 URL Filtering
  - 漸進式流量導入機制

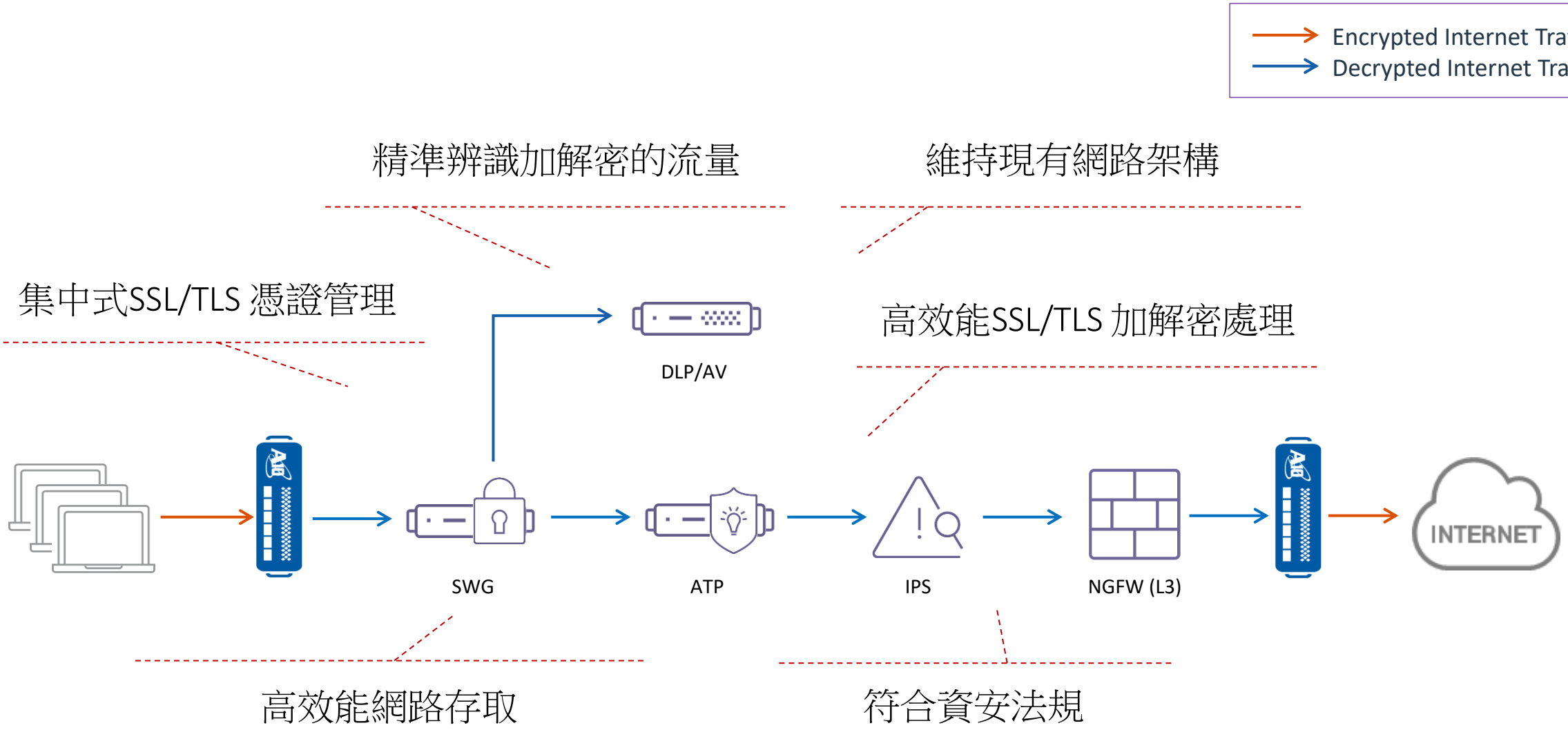


Customer A


A-1
A-2
A-3
A10 SSLi A
B-1
B-2
B-3
A10 SSLi B


Internet
BR
A-1
B-1
A10 SSLi (outside)
IPS
Server Farm
NGFW
User Area
WP
A10 SSLi (inside)
A-2
B-2
A-3
B-3
A10 SSLi (inside)
L3 SW
L3 SW
Services
Services
Clients

全方位解決方案 – A10 SSL Insight



活動期間於攤位(S26)或技術論壇**有效填寫**QRCode**問券**
現場即可獲得A10 Networks**精美贈品**
並有機會抽到Foodpanda 250**元即食券**

台灣區代理商 Unicomp 聯達資訊


Thank You
A10
Always Secure. Always Available.