

# Thunder SSLi® 硬體設備規格表 (入門款)

	Thunder 1040 CFW	Thunder 3350-E CFW	Thunder 3350S CFW
<b>Firewall Performance</b>			
Throughput	20 Gbps	30 Gbps	50 Gbps
Layer 4 CPS	450K	550K	1.4 Million
Concurrent Sessions	24 Million	32 Million	64 Million
FW Rules	12K	16K	64K
<b>Secure Web Gateway Performance<sup>*1+2</sup></b>			
SSLi Throughput	1.5 Gbps	3 Gbps	5.5 Gbps
SSLi CPS	RSA: 4K ECDHE: 3K	RSA: 8K ECDHE: 4.5K	RSA: 20K ECDHE: 10K
<b>IPsec Performance<sup>*2</sup></b>			
IPsec Throughput	8 Gbps	10 Gbps	24 Gbps
IPsec Tunnels	2K/5K <sup>*2</sup>	5K	20K
IKE Gateways	2K/5K <sup>*2</sup>	5K	20K
<b>Network Interface</b> <span style="float:right">Hardware Bypass Model</span>			
1 GE (BASE-T)	5	1 + 4 (Bypass)	6
1 GE Fiber (SFP)	0	0	2
1/10 GE Fiber (SFP+)	4 <sup>*5</sup>	4 <sup>*5</sup>	8 + 4 <sup>*5</sup>
25 GE Fiber (SFP28)	0	2 (Optical Bypass) <sup>*6</sup>	0
40 GE Fiber (QSFP+)		0	0
Management Ports	Ethernet Mgmt. Port, RJ-45 Console Port		
<b>Hardware Specifications</b>			
Processor	Intel Communications Processor	Intel Xeon 8-core	Intel Xeon 14-core
Memory (ECC RAM)	8 GB <sup>3</sup> / 16 GB	16 GB	64 GB
Storage	SSD	SSD	SSD
Hardware Acceleration	Software	Software	Software
TLS/SSL Security Processor	Hardware on S models (2 options) <sup>*7</sup>	Hardware	Hardware
Dimensions (inches)	1.75(H) x 17.5(W) x 17.25(D)	1.75 (H) x 17.5 (W) x 18 (D)	1.75 (H) x 17.5 (W) x 18 (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	15 lbs/17 lbs (RPS)	18 lbs	18 lbs
Power Supply (DC option available)	Single 750W <sup>*4</sup>	Dual 750W RPS	Dual 750W RPS
	80 Plus Platinum Efficiency, 100 - 240 VAC, 50 - 60 Hz		
Power Consumption (Typical/Max) <sup>*3</sup>	80W / 110W	151W / 205W	175W / 222W
Heat in BTU/hour (Typical/Max) <sup>*3</sup>	273 / 376	516 / 700	598 / 758
Cooling Fan	Removable Fans	Hot Swap Smart Fans	
Operating Ranges	Temperature 0° - 40° C   Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC <sup>7</sup> , BSMI, RCM <sup>7</sup>   RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM   RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC <sup>7</sup> , KCC, BSMI, RCM   RoHS
Standard Warranty	90-Day Hardware and Software		

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions. As for network interface, it's highly recommended to use A10 Networks qualified optics/transceivers to ensure network reliability and stability.

\*1 Tested in single appliance SSLi deployment with maximum SSL option. Cipher "TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA" with RSA 2K keys are used for RSA cases. "TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256" with EC P-256 and RSA 2K keys are used for PFS case.  
 \*2 With maximum SSL  
 \*3 With base model. Number varies by SSL model  
 \*4 Optional RPS available  
 \*5 10Gbps speed only  
 \*6 Fixed SFP+ optical ports with dual rate (10GBASE-SR and 1000BASE-SX)  
 \*7 Hardware Bypass model comes equipped with the hardware TLS acceleration  
 7 Certification in process  
 + FIPS model must be purchased



Part Number: A10-DS-15113-TW-23 MAR 2021

睿科網路科技有限公司  
 www.a10networks.com

115 台北市南港區三重路66號6F  
 apac@a10networks.com

Tel: +886 2 2785 2729  
 M: +886 910 212 628

# A10

## Thunder SSLi®

### 即時可視化 隱藏在加密流量中的威脅



A10 Thunder SSLi® (SSL Insight) 可協助企業分析包括加密資料的所有內容，攔截 SSL 通訊，解密及傳送明碼流量至協力廠商資安設備（例如防火牆、威脅預防平台及鑑識工具等）進行深度封包檢測(DPI)，使得第三方安全設備能夠在不影響效能的情況下分析所有流量，進而消除 SSL 加密流量產生的資安盲點。

#### 關於 A10 Networks

A10 Networks (睿科網路) 是全球應用網路技術領導廠商，提供一系列高性能應用網路解決方案，協助數以千計的大企業、服務供應商和超大型網路營運商確保其資料中心的應用程式與網路保持高可用性、加速性和安全性。A10成立於2004年，總部位於美國加州聖荷西市，並在世界各地設有辦事處為客戶提供服務。詳細資訊請瀏覽：[www.a10networks.com](http://www.a10networks.com) and @A10Networks.

# Thunder<sup>®</sup> SSLi<sup>®</sup>

## 即時可視化隱藏在加密流量中的威脅

A10 Thunder<sup>®</sup> SSLi<sup>®</sup> (SSL Insight) 可協助企業分析包括加密資料的所有內容，攔截 SSL 通訊，解密及傳送明碼流量至協力廠商資安設備（例如防火牆、威脅預防平台及鑑識工具等）進行深度封包檢測 (DPI)，使得第三方安全設備能夠在不影響效能的情況下分析所有流量，進而消除 SSL 加密流量產生的資安盲點。

### 功能與優點

#### 在不變更網路架構下 單點解密及分析

企業通常部署多個安全解決方案，以分析及過濾應用程式流量。Thunder<sup>®</sup> SSLi<sup>®</sup> 可在不變更網路架構下集中解密 SSL 流量，並以明碼將其傳送至各種設備同時追蹤各個連線，確保將需求及回應引導至檢查流量的相同設備。單一台 Thunder<sup>®</sup> SSLi<sup>®</sup> 設備可提供 SSL 可見度至整個安全堆疊架構。

Thunder<sup>®</sup> SSLi<sup>®</sup> 能夠與下列項目互通：

- 防火牆
- 安全 Web 閘道
- 入侵防禦系統 (IPS)
- 統一威脅管理 (UTM) 平台
- 資料遺失預防 (DLP) 產品
- 威脅預防平台
- 網路鑑識及 Web 監控工具

#### 依據流量選擇性管理 確保合規和隱私性

Thunder<sup>®</sup> SSLi<sup>®</sup> 使用 ICAP 通訊協定，能夠與協力廠商資安設備互動，決定流量是否應受 SSL Insight 控制。此外，URL 分類服務可強制執行隱私政策，略過受信任通訊或避免檢查醫療或金融記錄等資料，以符合法規遵循標準及確保資料隱私。

#### 消除盲點 完全掌握 SSL 流量

雖然專屬資安設備提供網路流量的深度檢測及分析，但很少能夠高速解密及重新加密 SSL 流量。事實上，部分資安設備完全無法檢測 SSL 流量，Thunder<sup>®</sup> SSLi<sup>®</sup> 可支援解密多種資安產品的流量，包括內嵌、非內嵌（被動 /TAP）及 ICAP 功能設備，讓企業完全掌控、檢查以前不可見的流量，檢測隱藏的威脅並加以防禦。

#### 安全存儲金鑰 通過 FIPS 140-2 認證

將加密金鑰儲存在網路設備可能引入嚴重的資安漏洞，威脅者可能從脆弱點獲取金鑰並進一步竊取數據或進行加密攻擊。Thunder<sup>®</sup> SSLi<sup>®</sup> 採用硬體加密模組 HSM（硬體亂碼化設備）並通過 FIPS140-2 第 3 級的認證，因此可在高效能的加解密環境中安全地存儲金鑰。

#### 確認憑證狀態 降低不必要的風險

如攻擊者使用無效憑證滲透網路，用戶可能會面臨多重被攻擊的風險。Thunder<sup>®</sup> SSLi<sup>®</sup> 通過支持從服務器接收憑證撤銷列表 (CRL)、線上憑證狀態協定 (Online Certificate Status Protocol, OCSP) 即時檢查憑證撤銷狀態的協定，有助於即時驗證、確保憑證有效。

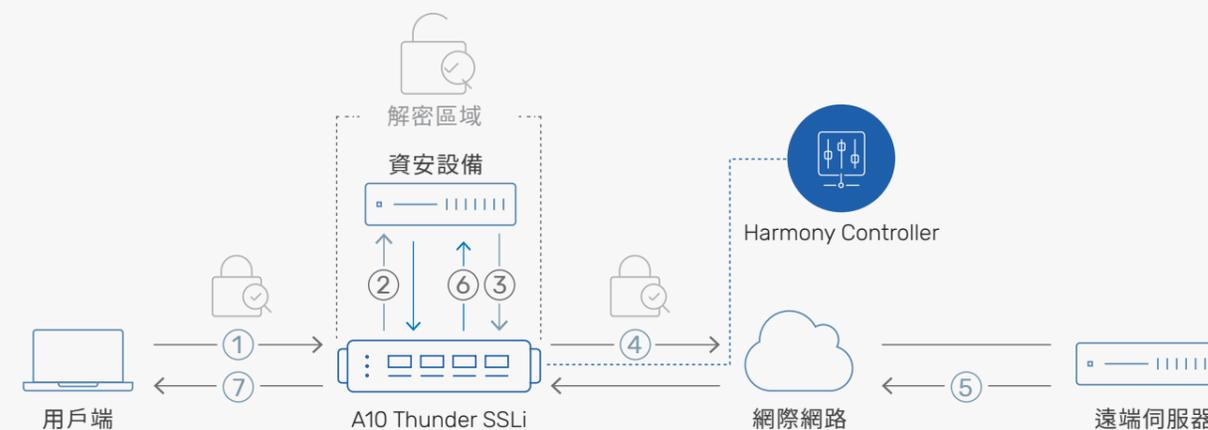
#### 減少營運成本 降低網路延遲率

Thunder<sup>®</sup> SSLi<sup>®</sup> 提供一個集中點來解密網路流量，將解密後的流量轉發到許多內聯 (in-line) 和非內聯 (non-inline) 網路安全設備，不必在每個安全設備上執行重複解密及重新加密作業，可幫助這些資安設備卸載需要大量 CPU 運算的工作，大幅提升整體效能、同時也減少針對不同資安設備重複投資的營運成本。

#### 全方位且可擴充的 管理功能

為了簡化及自動化管理，Thunder<sup>®</sup> SSLi<sup>®</sup> 除了提供業界標準 CLI、Web 圖形化者介面之外，更支援全功能 RESTful API (aXAPI<sup>®</sup>)，能夠與協力廠商或自訂管理主控台整合。對於較大規模的部署需求，客戶還可使用 A10 Harmony<sup>™</sup> 集中管理系統，進行大規模、跨地理位置、多設備的日常維運。

### 架構及關鍵元件



- ① 用戶端加密流量由用戶端傳送至 Thunder<sup>®</sup> SSLi<sup>®</sup> 設備進行解密。
- ② Thunder<sup>®</sup> SSLi<sup>®</sup> 設備將解密後的資料傳送至資安設備來檢測明碼資料。
- ③ 安全設備在檢查後將流量發送回 Thunder<sup>®</sup> SSLi<sup>®</sup>，進行重新加密。
- ④ Thunder<sup>®</sup> SSLi<sup>®</sup> 設備將重新加密的流量傳送至伺服器。

- ⑤ 外部伺服器回傳加密流量至 Thunder<sup>®</sup> SSLi<sup>®</sup> 設備。
- ⑥ Thunder<sup>®</sup> SSLi<sup>®</sup> 設備解密外部流量，並將其轉送至資安設備進行檢測。
- ⑦ Thunder<sup>®</sup> SSLi<sup>®</sup> 設備從資安設備接收流量，重新加密後傳送至用戶端。