基於雲端環境下智慧製造系統之安全通道實作分析

Cryptology and Information Security Conference 2022

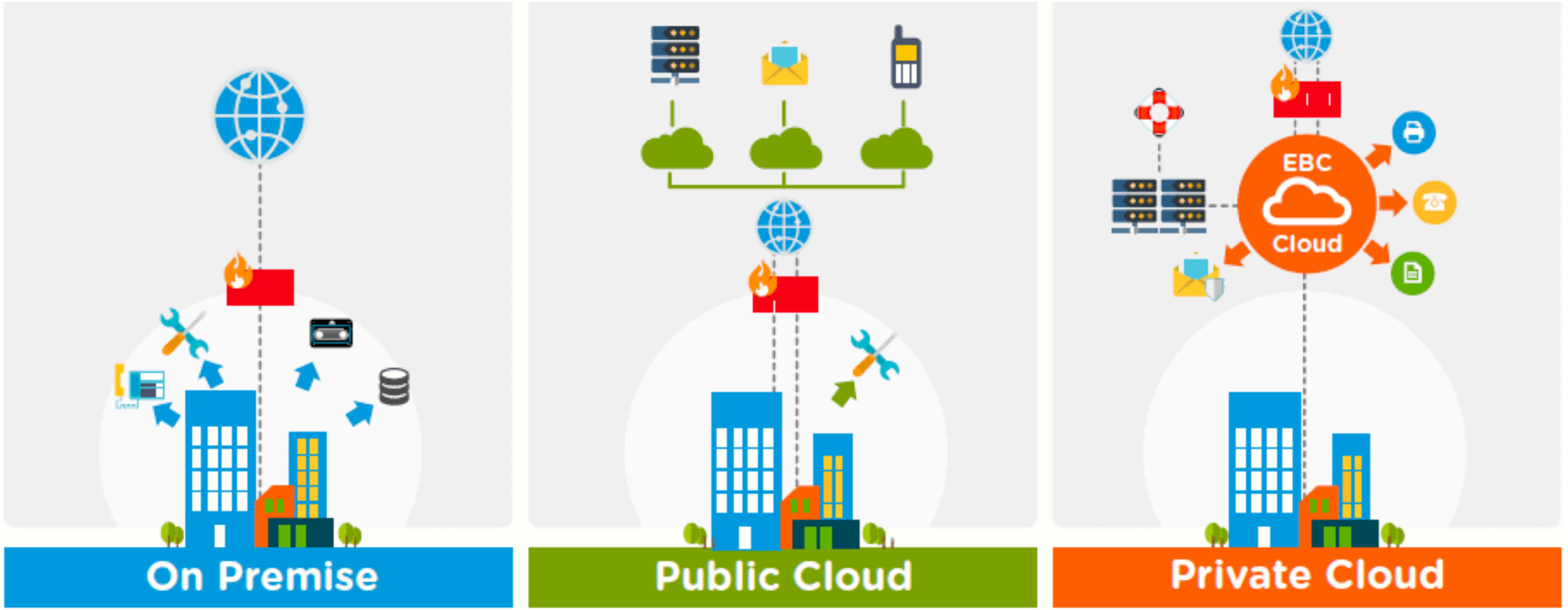
臺灣科技大學資訊管理系 江忠晏
臺灣科技大學資訊管理系 羅乃維

前言與研究動機

- 2020年全球深受新冠肺炎影響，許多產業開始採取遠距辦公，許多產業開始進行數位轉型，台灣的中小製造業也不例外。
- 所幸經濟部從2018年起籌組智慧製造輔導團，協助我國中小企業導入智慧製造，提前做好準備。
- 因此現今中小製造業實施智慧製造更是個趨勢，其中雲端技術是不可或缺的一環。

前言與研究動機

- 2019年台灣企業雲端大調查結果中，台灣的一般製造業上雲的比例達到近50%，其中最常上雲的應用多為24小時服務或非關鍵性任務的應用。
- 這項統計數據表明目前越來越多製造業接觸到雲端服務，從傳統的本地部署（On-Premises）架構，轉向雲端架構（Cloud）。



https://www.ebcgroup.co.uk/news-insights/on-premises-vs-cloud

前言與研究動機

- 對於普遍企業使用雲端服務的優點不外乎以下幾點
  - 降低IT預算及時間成本
  - 具有服務彈性（Flexibility）及擴展性（Scalability）
  - 易於系統維護
  - 易於管理控制

前言與研究動機

- 不過一體兩面，若將資料上傳雲端就容易延伸出網路傳輸安全、資料傳輸完整性、資料外洩等資通安全問題。
- 在製造業環境下，大多工具機為市售CNC或PLC，僅提供資料傳輸功能（Modbus RTU、TCP），不開放修改內部程式，或有些控制器則因運算性能等因素，無法即時的進行加密運算將資料即時上傳雲端。
- 因此本研究將著重在工廠對外路由器至雲端服務伺服器之間的站到站（Site-to-Site）網路層安全，確保封包機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）。

文獻探討

物聯網安全及架構

- Kirupakar等人提到隨著物聯網蓬勃發展，隱藏的資安疑慮是需要重視的。
- Kirupakar等人的研究為在低功率、有限的CPU及記憶體性能的邊緣節點裝置上，實作輕量化的入侵檢測系統，藉由監測任一邊緣節點的CPU使用率、記憶體使用率等重要指標，以判斷是否為DDOS攻擊。
- Sun等人提出了一個基於企業服務匯流排所延伸出的雲端服務匯流排（Cloud Service Bus）SaaS平台，其主要目的為整合生產商用軟體於他們所提出的架構平台上，例如ERP及CRM軟體。

文獻探討

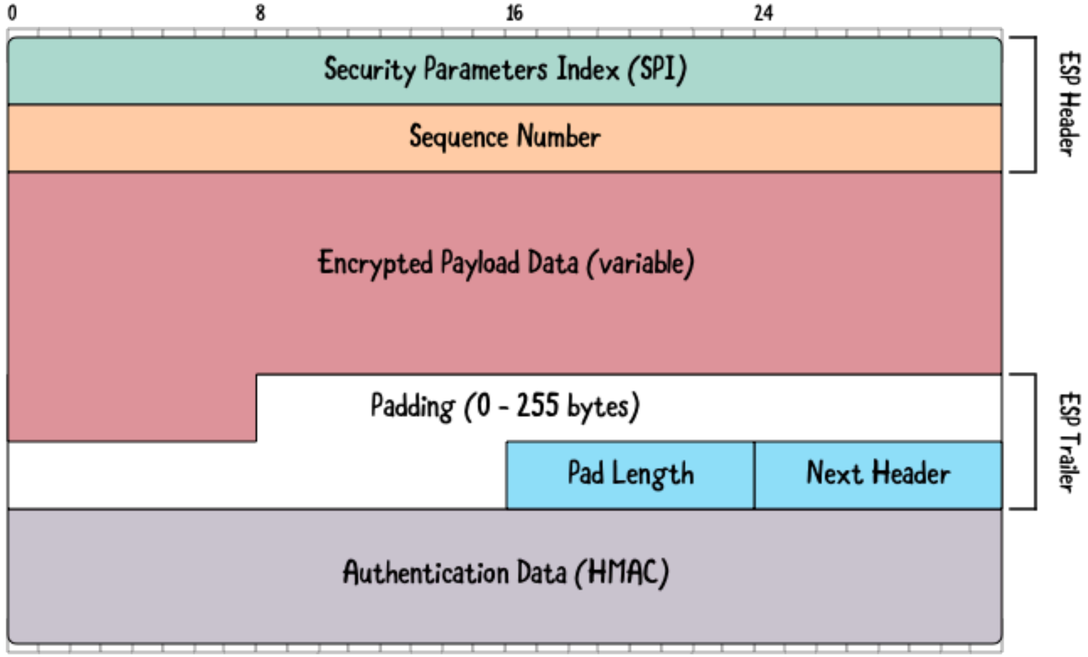
安全通道建構技術

- 使用虛擬私人網路（Virtual Private Network）不僅能以廣域網路的便宜價錢，享受到專屬線路的安全，對於建置及維護更為彈性。
- 而通常穿隧協議（Tunneling Protocol）都是基於安全通道進行實施，目前主流有通用路由封裝（Generic Routing Encapsulation）、端對端隧道協定（Point to Point Tunneling Protocol）、第二層穿隧協議（Layer 2 Tunneling Protocol）、網際網路安全協定（Internet Protocol Security）。
- Jahan等人的研究結論提到GRE適合於時間敏感的應用；IPsec適合於安全性敏感的應用；PPTP、L2TP並無加密機制，需搭配其他協議才可加密，且L2TP需設定使用者端軟體，架設較麻煩。
- 總括以上，目前企業所使用的CPE-based VPN中，鑑於其安全性，以IPsec VPN為主流。

文獻探討

IPsec機制

- IPsec具有兩種安全協議，分別為AH（Authentication Header）及ESP（Encapsulating Security Payload）。這兩種協議都具備資料完整性、資料來源驗證，然而AH不支持資料加密，故本研究著重於ESP封裝協議。



https://comp38411.jtang.dev/docs/ip-security/encapsulating-security-payload/

文獻探討

IPsec機制

- IPsec中最重要的便是安全關聯（Security Association），因為它定義雙方要如何協商，並儲存了雙方各種參數，例如要使用何種加密演算法？要使用何種封裝協議？SA的生命週期多久？而這些安全關聯會放在主機或路由器的安全關聯資料庫 SAD（Security Association Database）中。

文獻探討

IPsec機制

- 網際網路金鑰交換能夠使雙方自主協調，產生ISAKMP SA及IPsec SA，ISAKMP SA是用以保護私鑰安全，其中參數包括認證方式、加密演算法、雜湊函式等，而IPsec SA如上安全關聯所述為進行通訊時所規範的參數。

- IKE分作為Phase 1 （ISAKMP）及Phase 2（IPsec），Phase 1為雙方互相認證，Phase 2是基於Phase 1，可以執行多次，產生出多組的IPsec SA，假設IPsec SA的生命週期為3600秒，代表著每一個小時就會更新一筆IPsec SA，而沒有Phase 1便不會有Phase 2，換句話說Phase 2是基於Phase 1確保的安全所進行的。

文獻探討

IPsec機制

- IPsec分作為kernel space及user space實作，Linux 3.6+ Kernel的虛擬通道介面VTI（Virtual Tunnel Interface）及Linux 4.19+ Kernel的XFRM框架皆屬於kernel space，而OpenVPN（Analogy with IPsec）及strongSwan中的libipsec則是user space。

- user space實作模式為在kernel space產生出一個虛擬tun device，封包在傳出時，必須從kernel space進行memcopy至user space，再藉由VPN engine進行封包處理，再從user space進行memcopy回kernel space，因此大量的來回處理會使memcopy達到效能瓶頸，不適合於路由器上實作，僅適合於host上實作。

文獻探討

XFRM框架

- XFRM為實作IPsec的kernel框架，在傳送封包前會先經過xfrm4_lookup()，其作用為查詢是否有對應的Outbound SA，若符合，則進入XFRM框架內根據模式及協議進行處理，最後執行ip_output()，完成封包發送。

- 在接受封包後會偵測封包類型，如果封包類型為AH、ESP，則會進入XFRM框架內查詢對應的Inbound SA，再透過安全關聯中的模式及協議進行處理，處理完後將原始封包擷取出來重回到ip_local_deliver()，再經過udp_rcv()或tcp_rcv()，最終將封包傳送至上層。

研究方法與步驟

工業物聯網架構流程

- 本研究使用TP-Link Archer C7 AC1750模擬工廠端路由器、MediaTek LinkIt 7688單晶片以模擬工業控制器，進行簡單的定時獲取系統時間，並上傳資料至雲端服務中的資料存取伺服器，模擬工業物聯網中將資料定時上傳之模式。此外，在路由器上實作安全通道並分析其吞吐率、延遲及驗證安全性。

研究方法與步驟

雲端服務架構流程

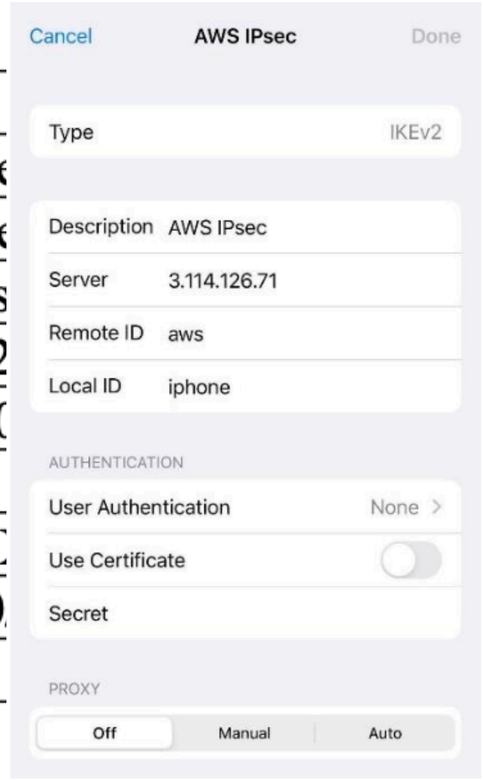
- 本研究採用Amazon Web Services以作為雲端服務架構的模擬。
- 首先建立VPC雲端環境，並在VPC中配置Internet Gateway以連通內外雙向網路，再分別建立兩個Subnet。在Public Subnet中建立EC2 Instance作為NAT Instance，在IT Subent中建立EC2 Instance作為虛擬化資料存取伺服器（Docker、Flask、MongoDB）。
- 最後透過Route Table將外部流量導至NAT Instance上，經由NAT Instance轉發給其他子網路，或是子網路流量經由NAT Instance導至Internet Gateway上。

研究方法與步驟

安全通道建置及分析

- 本研究透過strongSwan建置工廠本地端至雲端服務Site-to-Site安全通道（kernel space），以及雲端服務端至行動裝置端的Roadwarriror安全通道。

conn cloud configuration	
ike	aes-sha1-curve
esp	aes-sha1-curve
leftid	on-premis
left	192.168.2
leftsubnet	192.168.2.0
rightid	cloud
right	3.114.X.X
rightsubnet	172.16.0.0
auto	route

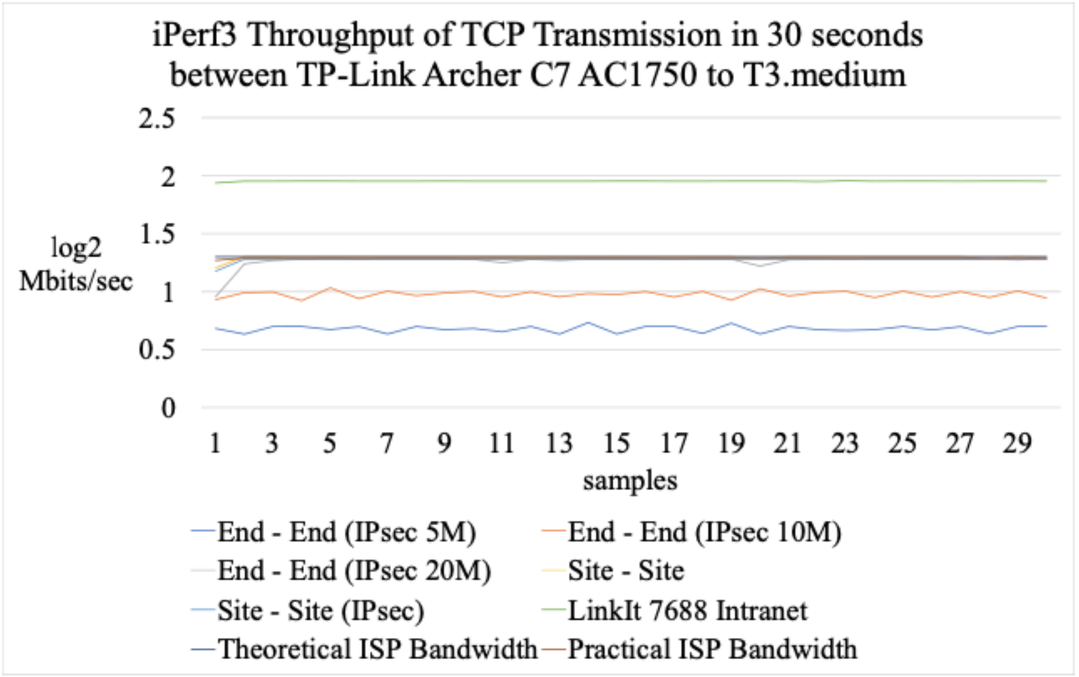


conn mobile configuration	
ike	aes-sha1-modp1024
esp	aes-sha1-modp2048
leftid	cloud
left	172.16.1.52
leftsubnet	172.16.0.0/16
right	%any
rightsourceip	172.15.0.0/16
auto	route
conn on-premises configuration	
ike	aes-sha1-curve25519
esp	aes-sha1-curve25519
leftid	cloud
left	172.16.1.52
leftsubnet	172.16.0.0/16
rightid	on-premises
right	106.104.X.X
rightsubnet	192.168.1.0/24
auto	route

實驗分析

工廠本地端至雲端架構安全通道

- 本研究成功地建立與雲端架構端的安全通道，並透過iPerf隨機抽樣10天不同時間（早、中、晚），共30個樣本的廣域網路、無安全通道、安全通道站到站及點到點、LinkIt 7688乙太網路介面30秒平均吞吐率。



實驗分析

工廠本地端至雲端架構安全通道

- 在這個實驗中，從實驗數據觀察到廣域網路的吞吐率在20 MBits/s上下，而無安全通道站到站也在 20 MBits/s 上下，故確保在無安全通道的情況下，從台灣至東京可達到ISP所提供的頻寬。

- 礙於實驗環境之網路頻寬限制，綜括以上實驗數據而言，在頻寬超過 20 MBits/s 時，首先必須探討廣域網路是否能夠達到ISP的理論頻寬，再探討在此頻寬下安全通道的吞吐率是否成為瓶頸，最後在頻寬超過90 MBits/s時，LinkIt 7688的乙太網路吞吐率則為瓶頸，需考慮更換控制器或網路實體介面。

實驗分析

工廠本地端至雲端架構安全通道

- 本研究亦透過Netperf實驗無安全通道、安全通道站到站及點到點延遲時間。

平均延遲時間	最小值	平均值	最大值	標準差
無安全通道	39.32 毫秒	40.17 毫秒	83.20 毫秒	27.50 毫秒
安全通道	40.10 毫秒	43.30 毫秒	87.38 毫秒	32.77 毫秒
點到點	40.97 毫秒	744.14 毫秒	87.61 毫秒	29.24 毫秒

實驗分析

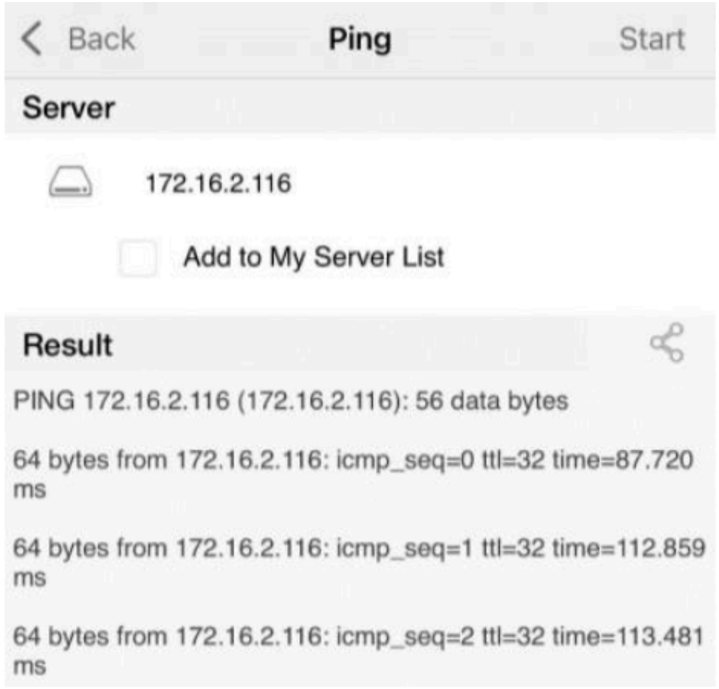
工廠本地端至雲端架構安全通道

- 在這實驗觀察到無安全通道的平均延遲為40.17毫秒，安全通道站到站平均延遲為43.30毫秒，而點到點的平均延遲為44.14毫秒，意味著安全通道的處理時間（Encryption/Decryption Processing Delay）約莫3毫秒。

實驗分析

iPhone 13至雲端架構安全通道

- 本研究亦成功地於iPhone 13上使用iNetTools進行端對端ICMP測試，並在雲端架構端透過Wireshark截取封包，觀察到封包確實為ESP，並解密成ICMP，以達到傳輸安全目的。



249	28.476529	172.16.1.52	49.217.141.249	ESP
269	29.493975	49.217.141.249	172.16.1.52	ESP
270	29.493975	172.15.0.1	172.16.2.116	ICMP
271	29.494024	172.15.0.1	172.16.2.116	ICMP
272	29.494438	172.16.2.116	172.15.0.1	ICMP

結論

- 本研究利用TP-Link Archer C7 1750 及MediaTek LinkIt 7688開發版建立簡易工業物聯網環境、Amazon Web Services作為雲端服務伺服器環境及Docker、Flask、MongoDB作為資料存取伺服器，以模擬中小製造業上雲環境。接著使用iPerf3和Netperf分別分析安全通道吞吐率及延遲，觀察到在ISP頻寬20 Mbits/s情況下，安全通道不會造成吞吐率瓶頸，處理延遲時間約莫3毫秒，同時使用Wireshark以驗證安全通道之安全性。