pwc 資誠

推動證券商導入金融零信任說明會

-網路安全

資誠智能風險諮詢管理有限公司

2025.7

Agenda

項次	內容
1	實作參考原則分級解析-網路安全
2	零信任架構導入常見問題-網路安全

1

實作參考原則分級解析-網路安全

零信任架構實作參考原則分級-5大支柱

Identity

身分

是指唯一描述特定使用者或實體（包括非個人實體）的屬性或屬性集。

Devices

設備

是指任何可連接到網路的資產（包括其硬體、軟體、韌體等），包括伺服器、桌上型電腦和筆記型電腦、印表機、行動電話、物聯網設備、網路設備等。

Networks

網路

是指開放的通訊介質，包括典型通道（例如機構內部網路、無線網路），以及其他潛在通道（例如用於蜂巢式網路和應用程式層級通道）。

Applications

應用程式

包括在本機、行動裝置和雲端環境中執行的資通系統、程式和服務。

Data

資料

包括正在訪問或曾經訪問的設備、網路、應用程式、資料庫、基礎設施和備份（包括本機和虛擬環境）中的所有結構化和非結構化檔案和片段。

金融業導入零信任架構參考指引-實作參考原則

等級 I

支柱	功能
身分	身分認證
	身分互通
設備	設備合規
	供應鏈風險
網路	網路區隔
	流量加密
應用程式	存取授權
資料	外洩防護
	資料分類
	資料可用性
	資料加密

等級 II

支柱	功能
身分	身分認證
	權限存取
設備	設備合規
	資源存取
網路	網路區隔
	流量管理
應用程式	存取授權
	程式安全
	程式部署
資料	資料存取

等級 III

支柱	功能
身分	可視性分析
設備	威脅防護
	可視性分析
網路	網路韌性
	可視性分析
應用程式	威脅防護
	可視性分析
資料	外洩防護
	可視性分析

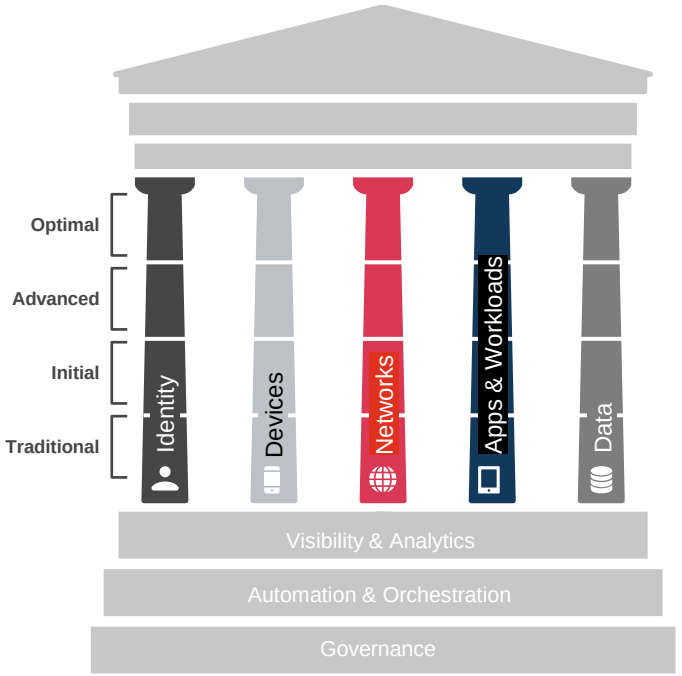
等級 IV

支柱	功能
身分	自動化治理
設備	自動化治理
網路	自動化治理
應用程式	自動化治理
資料	自動化治理

金融業導入零信任架構參考指引-實作參考原則

身分(7)
- 身分認證（I*1、II*1）
- 身分互通（I*2）
- 權限存取（II*1）
- 可視性分析（III*1）
- 自動化治理（IV*1）

設備(7)
- 設備合規（I*1、II*1）
- 供應鏈風險（I*1）
- 資源存取（II*1）
- 威脅防護（III*1）
- 可視化分析（III*1）
- 自動化治理（IV*1）



網路(7)
- 網路區隔（I*1、II*1）
- 流量管理（II*1）
- 流量加密（I*1）
- 網路韌性（III*1）
- 可視性分析（III*1）
- 自動化治理（IV*1）

資料(8)
- 外洩防護（I*1、III*1）
- 資料分類（I*1）
- 資料可用性（I*1）
- 資料存取（II*1）
- 資料加密（I*1）
- 可視化分析（III*1）
- 自動化治理（IV*1）

應用程式(7)
- 存取授權（I*1、II*1）
- 威脅防護（III*1）
- 程式安全（II*1）
- 程式部署（II*1）
- 可視化分析（III*1）
- 自動化治理（IV*1）

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

3. 網路

網路被切分為最小的區段，防止未授權的存取與橫向擴散

金融業導入零信任架構參考指引-實作參考原則

網路被切分為最小的區段，防止未授權的存取與橫向擴散

I 靜態指標

- **3-1 網路區隔**：具網段隔離機制，採最小需求原則限制存取資源之網路連線，並得限制同網段主機間連線及資源存取，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。
- **3-4 流量加密**：於資源存取路徑進行資料傳輸加密(如 https 等加密協定)。

II 動態指標

- **3-2 網路區隔**：具軟體定義網路(SDN)或網路微分段(Micro-Segmentation)機制，可以依據業務需求或動態屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以個別主機或個別系統為獨立網路區隔，縮小攻擊表。
- **3-3 流量管理**：呈現對系統、端點與網路間連線的相依性關係，可以單一設備為單位延伸看到相關系統、端點與網路之狀態，並具備流量異常監控及應處機制。

III 即時指標

- **3-5 網路韌性**：對網路連線紀錄具有即時偵測及回應機制(如NDR)，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。
- **3-6 可視性分析**：整合事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，並與資安監控機制整合，針對入侵指標或攻擊行為樣態進行即時的判斷與應處。

IV 整合指標

- **3-7 自動化治理**：具可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。

金融業導入零信任架構參考指引-實作參考原則

3-1 網路區隔

I 靜態指標

具**網段隔離**機制，採**最小需求原則**限制存取資源之網路連線，並**「得」限制同網段主機間連線及資源存取**，防止攻擊者利用遭入侵的主機作為跳板機進行橫向擴散。

3-2 網路區隔

II 動態指標

具**軟體定義網路(SDN)**或網路**微分段(Micro-Segmentation)機制**，可以依據業務需求或**動態**屬性(如人員身分、設備樣態及連線時間等)調整網路防護邊界；並可以**個別主機或個別系統**為獨立網路區隔，縮小攻擊表面。

金融業導入零信任架構參考指引-實作參考原則

	網路分段	網路微分段	軟體定義網路(SDN)
定義	將網路分成**多個獨立區域**(網段)，控制每個區域的連線。	將網路劃分為**更小的隔離區塊**(如個別主機、系統)，每個區域擁有**獨立的安全規則**，限制彼此之間的連線。	使用軟體來**動態**管理網路設定，根據業務需求**調整**流量路徑。
指標	*I* 靜態指標	*II* 動態指標	*II* 動態指標
主要目的	限制網路流量，保護不同網段間的資料安全	限制感染範圍，**防止橫向擴散**	提供靈活的網路配置，依需求動態調整網路配置
應用範例	辦公區域網路(LAN)劃分成內部和外部網路	金融機構將各項業務分區，防止攻擊傳播	大型企業動態控制各部門的網路流量與安全策略
技術機制	使用VLAN或傳統防火牆進行子網隔離	透過微分段技術(可在網路分段原架構下)，建立更細微隔離	使用SDN控制器管理，控制網路設備
安全優勢	將網段內部流量限制到**最小需求**，降低攻擊面	單一主機受到攻擊時，其他主機不易受影響，減少橫向移動風險	自動化管理，提供快速配置調整能力
適用場域	所有企業	安全需求高的環境，如**金融**、醫療等敏感資料系統	需要靈活配置、集中控制動態網路的企業

金融業導入零信任架構參考指引–問答

Question:
零信任在實施網路區隔時，建議採用什麼原則來限制網路連線？

選項A

最高效能原則

→ X 不適用

選項B

最大連接數原則

→ X 不適用

選項C

最小需求原則

→ ✓ 依需求限制存取資源之網路連線

金融業導入零信任架構參考指引–問答

Question:
根據零信任參考指引，為防止攻擊橫向擴散，建議採用什麼技術？

選項A

強化VPN通道

→ X 不適用

選項B

隨機調整內部IP

→ X 不適用

選項C

採微分段與網路區隔

→ ✓ **將主機或個別系統為獨立網路區，縮小攻擊表面**

金融業導入零信任架構參考指引-問答

Question:
零信任網路區隔強調「軟體定義網路」的主要目的為？

選項A

緩解網管人力負擔

→ ✗ 不適用

選項B

動態調整網路邊界

→ ✓ 可依需求或動態屬性變更路網拓樸

選項C

加速網路連線速度

→ ✗ 不適用

3-3 流量管理

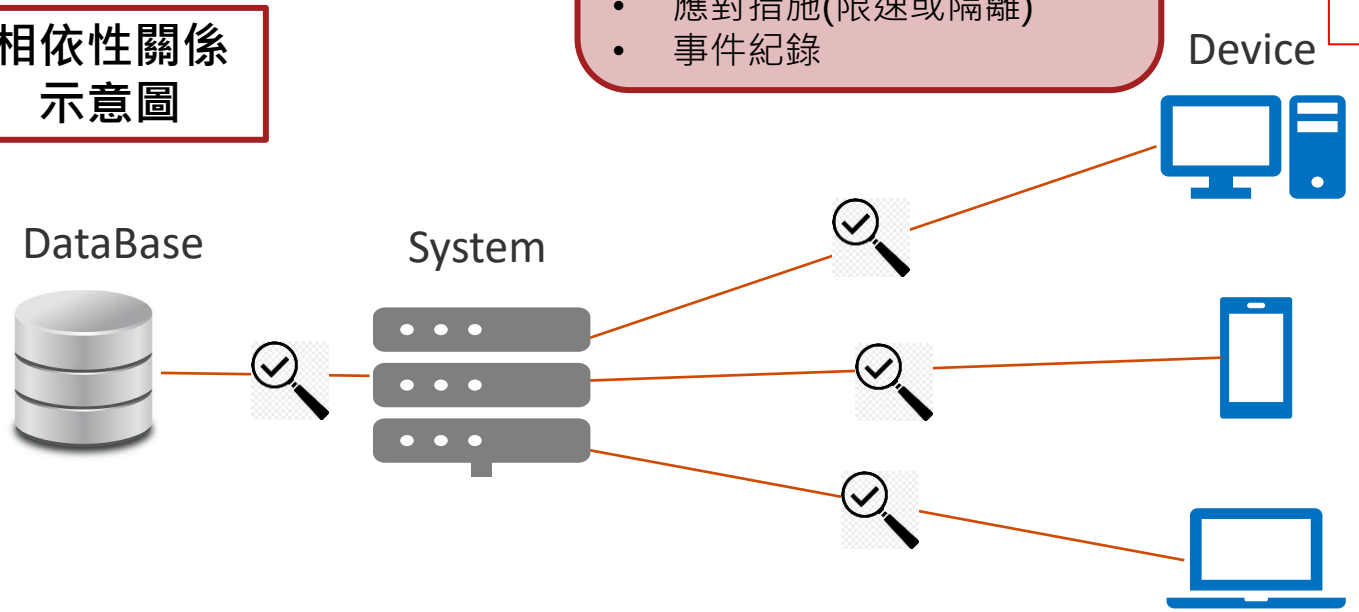
呈現對系統、端點與網路間連線的相依性關係，可以**單一設備為單位延伸看到相關系統、端點與網路之狀態**，並具備流量異常監控及應處機制。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

流量監控
- 近期流量趨勢圖，識別瓶頸
- 異常警示 以期更快速地回應
- 應對措施(限速或隔離)
- 事件紀錄

⚠ 異常嘗試行為
⚠ 高流量警示
⚠ 敏感資料訪問
⚠ 訪問頻率過高

相依性關係示意圖



單一設備檢視
- 設備名稱、IP位置
- 裝置狀態(上線、離線)
- 連接的系統與伺服器
- 防火牆設定

金融業導入零信任架構參考指引-問答

Question:
零信任流量管理對設備的狀態監控，建議應包含哪些面向？

選項A

監控單一設備

→ X 不適用

選項B

監控網路狀態、相關系統

→ X 不適用

選項C

監控設備及相關系統、端點與網路

→ ✓ 可監控流量之網路拓樸

金融業導入零信任架構參考指引-問答

Question:
根據網路流量管理原則，以下哪項功能是正確的？

選項A

監控端點設備，不考慮系統間的連接

→ X 不適用

選項B

監控網路流量，但無法處理異常

→ X 不適用

選項C

可以從單一設備延伸查看相關系統、端點與網路的狀態，並具備異常監控及應處機制

→ ✓ 適用

3-4 流量加密

於資源存取路徑之資料傳輸加密(如採 https 等加密協定)。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

加密流量概念：

- **保密性**：確保資料僅供授權方存取。
- **完整性**：防止資料被修改。

兩種加密方式：

- 通道加密：針對傳送的路徑。(Https/VPN/FTPS/SSH...)
- 訊息加密：端到端訊息加密。(E2E Encryption/電文加密 ...)

金融業導入零信任架構參考指引–問答

Question:
零信任在實施流量加密時，建議採用何種方式？

選項A

資料只允許在VPN內傳送

→ X 不適用

選項B

傳輸過程採用HTTPS或其他加密協定

→ ✓ 適用

金融業導入零信任架構參考指引-實作參考原則

3-5 網路韌性

對網路連線紀錄**具有即時偵測及回應機制(如NDR)**，可因應業務需求、偵測到入侵指標(IOC)或遭受攻擊時，動態調整網路設定(如調整網路防護邊界即時隔離、切換備援路由或資源配置等)或即時告警，以維持網路服務，將對業務影響最小化。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

NDR(網路偵測回應)

- **功能**：即時監控網路和設備間流量，偵測並回應潛在威脅指標(IOC)
- **操作**：發現異常活動時，NDR自動
  - (1) 發出告警
  - (2) 發出事件單
  - (3) 調整網路防護
  - (4) 消除橫向移動

名詞解釋

- IOC(威脅指標)：潛在威脅的資料點，如可疑IP地址、異常文件、可疑URL

金融業導入零信任架構參考指引–問答

Question:
根據網路韌性管理原則，以下哪項不屬於動態調整網路設定的方式？

選項A
切換備援路由
→ ✓ 適用

選項B
調整資源配置
→ ✓ 適用

選項C
調整網路防護邊界即時隔離
→ ✓ 適用

金融業導入零信任架構參考指引-實作參考原則

3-6 可視性分析

整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於SIEM 平台並與資安監控機制(SOC)整合，針對入侵指標(IOC)或攻擊行為樣態(Mitre ATT&CKTTP)進行即時的判斷與回應(如事件單、SOARPlaybook 等)。

I 靜態指標

II 動態指標

III 即時指標

IV 整合指標

1. **集中收容日誌資料至同一平台**(如SIEM)
   - 確保安全事件有完整、可查的紀錄
2. **異常偵測與警告機制**
   - 定期審查並監控日誌，偵測異常行為
   - 發現可疑活動，立刻觸發警示採取應對
3. **資安監控與即時回應**
   - 與資安監控中心(SOC)整合，快速分析入侵指標(IOC)或攻擊行為模式(Mitre ATT&CK TTP)
   - 根據事件自動執行回應動作(如生成事件單或啟動SOAR Playbook)

名詞解釋

- SIEM：安全資訊事件管理系統，集中收集和分析資安日誌，即時偵測異常，協助快速應對安全威脅。
- Mitre ATT&CK TTP：Mitre建立的框架，描述攻擊的戰術、技術、程序(TTP)，幫助團隊識別攻擊行為。
- SOAR Playbook：敘述如何驗證及回應安全事件的文件。若SOAR(資安協作自動化應變系統)失效，可作為人工處理的備案。

金融業導入零信任架構參考指引-實作參考原則

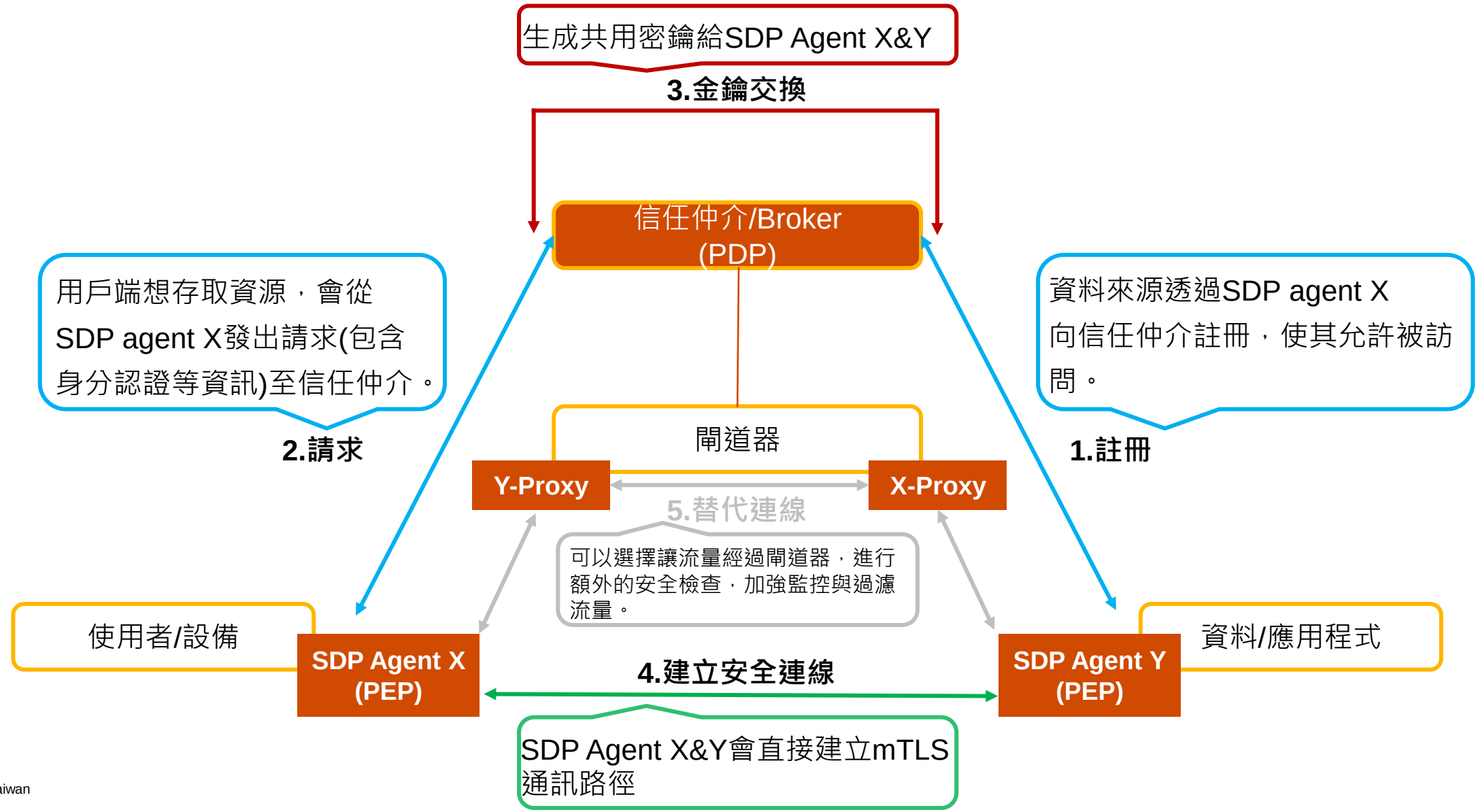
3-7 自動化治理

可依資安政策、工作流程情境及網路態勢快速調適之網路管理機制。

- *I* 靜態指標
- *II* 動態指標
- *III* 即時指標
- *IV* 整合指標

階段	說明
手動管理	•手動進行網路環境設置，定期整合政策及情勢變化。
部分自動	•使用部分自動化管理，根據政策與監控資料進行設置。
全面自動	•自動化變更管理方法，自動化所有網路環境配置；並自動評估風險，執行政策和安全措施。
最佳化	**•網路與環境通過程式碼定義，並由自動化變更管理工具管理，實現全自動化，且能因應需求快速變動。 ***網路存取控制NAC、軟體定義網路SDN、軟體定義邊界SDP*****

網路支柱之應用-軟體定義邊界 Software Defined Perimeter(釋例)



網路支柱之應用-軟體定義邊界 Software Defined Perimeter(應用案例)

SDP Agent X&Y

- **SDP Agent X:**位於設備，包含用戶的身分認證資料，讓系統知道這個用戶是誰。
- **SDP Agent Y:**位於伺服器端/雲端，保護公司的資料的或應用程式。

信任仲介

定義：

- 控制中心，負責管理存取請求的審查與授權。

功能：

- 管理身分認證與授權
- 生成和分配密鑰
- 中樞管理與監控
- 控制Gateway的使用

應用案例：

證券分析師或交易員須從外部網路連線至內部交易平台或市場即時資料庫。

傳統風險：

VPN全域開放，裝置一旦連線就能看見整個內部網路。

SDP解決方案：

使用者透過SDP閘道發起連線，系統同時驗證使用者身分、設備健康度、存取情境，並透過信賴等級授予連線僅開啟授權的資源(其餘完全隱藏)，封鎖不合規裝置。

網路支柱之應用-信任仲介 Broker Integration 參考架構

ZT Broker Integration

- **信任仲介（Broker）：**隱藏應用程式，所有存取請求必須通過仲介來驗證，包括身份驗證、行為分析、設備狀態檢查。

架構

1. 使用者 / 設備（User / Device）

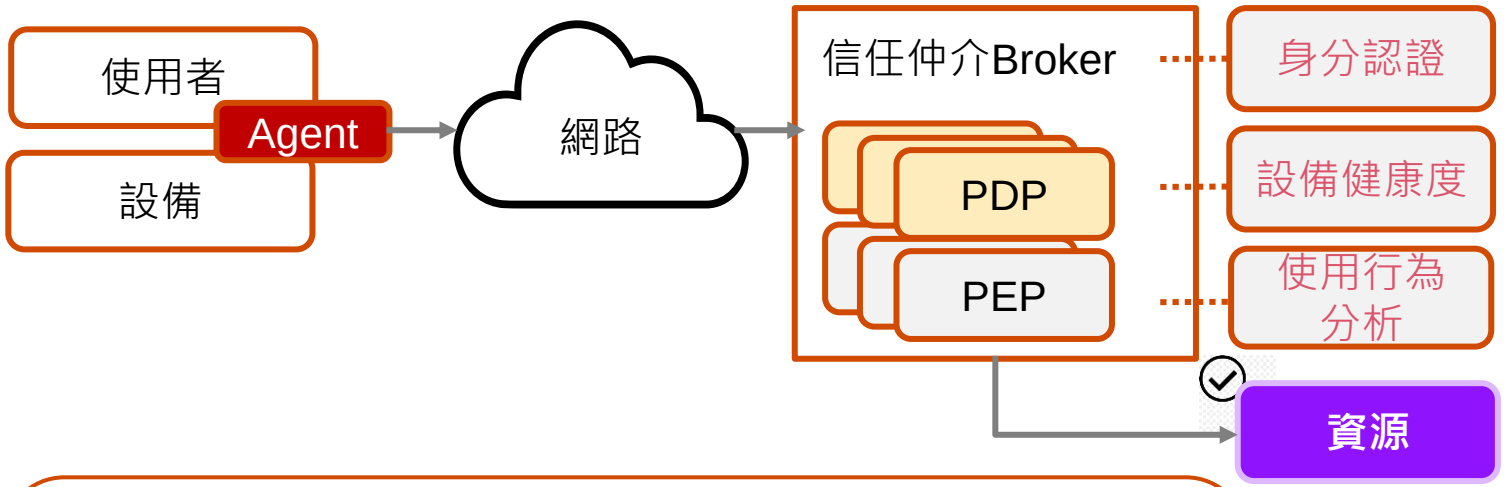
- 透過 Agent（代理程式）連接網路，提交身份與設備狀態。

2. 信任仲介（Broker）

- 內含 PDP（決策點）與 PEP（執行點），確保存取符合安全政策。
- 整合身份服務、行為分析 AI、設備健康狀態監測。

3. 資源存取（Resource Access）

- 當流量經過仲介，將根據安全策略允許或拒絕



作用

1. 應用程式隱藏，避免直接暴露在公共網路，降低攻擊風險。
2. 所有流量經過仲介強制驗證，確保存取受控。
3. 根據即時風險評估動態授權，提升安全性。

應用案例：員工登入雲端報表系統

- Broker 驗證為公司筆電 + MFA 通過
- PDP 判定「允許登入但僅開啟查閱功能」
- PEP 執行 → 封鎖下載功能

網路支柱之應用-次世代防火牆NGFW 參考架構

NGFW Micro Segmentation

（次世代防火牆微分段）

- **次世代防火牆（NGFW, Next-Generation Firewall）：**透過資安策略強制執行網路存取控制與網路分段管理。

架構

1.網路流量控制（Traffic Control）

- 資安網域控制 NGFW 來執行存取策略。

2.工作負載保護（Workload Protection）

- 虛擬交換機（vSwitch）+ NGFW 控制內部網路存取權限，確保不同應用或資料之間的隔離。

3.雲端 & 資料中心（Cloud & Data Center）

- 確保所有資源受到相同安全策略保護，適用於本地與雲端環境。

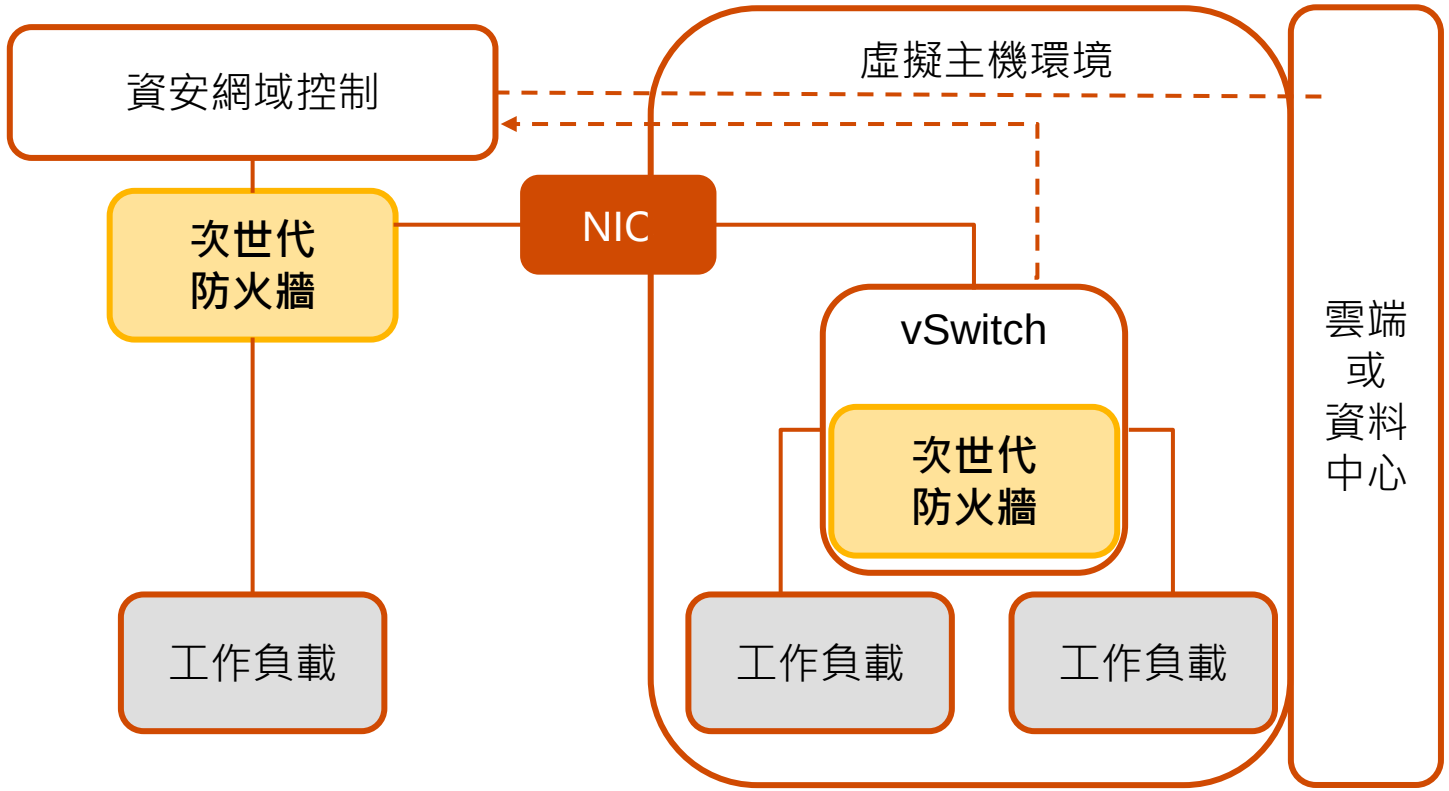
差異

1. 應用程式預判

- 透過封包流量分析，可封鎖有潛在風險的應用程式。

2. 入侵預防

- 分析傳入流量，識別已知威脅和潛在威脅。



作用

1.防止內部攻擊擴散，阻止惡意應用程式在內部網路橫向移動。

2.細緻化存取控制，確保只有授權使用者能夠訪問特定資源。

3.集中策略管理，所有存取規則由次世代防火牆（NGFW）統一控制，減少設定錯誤，提高安全性。

網路支柱之應用-網路微分段 Micro-Segmentation 參考架構

Hypervisor Micro Segmentation

（虛擬層級微分段）

- 微分段（Micro Segmentation）: 在虛擬層級（Hypervisor Level）透過微型防火牆（Micro Firewalls） 來加強安全控制。
- 將網路細分為更小的區塊，防止攻擊者在內部網路中橫向移動。

架構

1. 網路交換機（Physical Switch & vSwitch）

- 物理交換機（Physical Switch）與 **NIC（網卡）**連接到虛擬交換機（vSwitch），管理虛擬環境中的流量。

2. 微型防火牆（Micro Firewall）

- 每個 工作負載（Workload） 皆有獨立的 微型防火牆，作為策略執行點（PEP），過濾進出流量。

應用場景

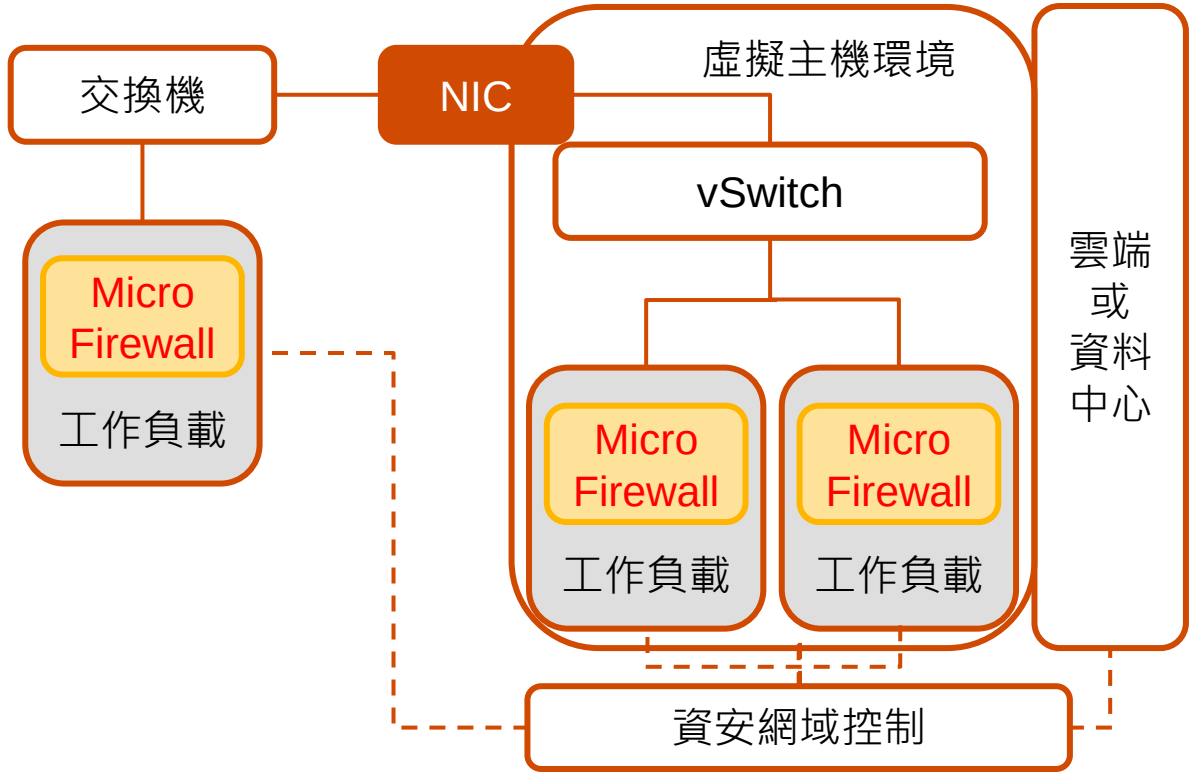
場景一：防止橫向移動攻擊

• 駭客取得某台分行電腦存取權後，嘗試掃描財務報表系統，微分段防火牆直接封鎖這種非授權橫向流量

場景二：限制系統跨部門存取

• 客服系統僅能連至帳務查詢模組，不可存取投資核心系統

• 即使帳號權限一致，不在授權路徑即封鎖



作用

1. **強化安全性**：所有流量在進入 VM 之前就會受到微型防火牆的過濾，減少內部攻擊風險。
2. **阻擋橫向移動攻擊**：防止惡意軟體或攻擊者在內部環境內部傳播。
3. **自訂安全性管理**：所有微型防火牆的策略由 **ZT Policy Controller（零信任策略控制器）**為每個工作負載自訂安全性原則。

2

零信任架構導入常見問題-網路安全

零信任架構導入常見問題一覽表-網路安全(1/2)

PwC 整理常見導入零信任架構之網路安全時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
舊系統不支援SDN無法重塑，如何因應「同網段隔離」要求?	• 透過自動化或人工方式盤點各系統關聯設備，使用VLAN/PVLAN將關聯設備分組，搭配ACL 設定禁止非相關系統的互通連線。 • 或可選擇透過開啟本機防火牆設定規則進行控管。
目前已有網路流量監控機制，但尚未呈現對系統、端點與網路間連線的相依性關係，有什麼建議落實措施？	旨在可即時透過任一設備掌握系統與網路的運作狀態，建議可考量: • 網路微分段機制，透過使用可視化分析模組收集傳送流量資訊及工作負載背景資訊，繪製應用系統相依性圖。 • 非微分段機制，透過網路流量分析(NTA)及追蹤端點與服務間之流量，搭配可視化工具實踐、ITOM/CMDB先建立「應用系統與組件」的 CI（Configuration Items），然後紀錄CI之間關聯性。

零信任架構導入常見問題一覽表-網路安全(2/2)

PwC 整理常見導入零信任架構之網路安全時，所遭遇挑戰及因應做法，供導入機關參考

常見問題	建議做法
舊應用、裝置或瀏覽器不支援HTTPS，建議如何調整以達到傳輸加密？	可優先更新瀏覽器或升級應用。若不可行時，可暫時採用技術性替代方案使用反向代理/應用層代理，或是透過VPN/VDI、遠端桌面登入支援HTTPS環境訪問內/外網系統。未來可擬定計劃逐步淘汰不安全的舊系統、設備，持續監控和評估安全狀況。
如何分階段推動這些措施，是否有優先建議的順序或切入點?	• 實施基本網路區隔，建立基本的流量管理和監控系統。 • 盤點資產依據業務角色將主機、服務、裝置等分類，掌握分各系統間的實際流量與連線需求。 • 導入如軟體定義網路(SDN)或網路微分段等解決方案。 • 整合與SIEM或SOC串接，實現告警與事件處理的自動化機制。

Q & A

pwc.tw