NIST Special Publication 800-207

Zero Trust Architecture

Outline

1. Introduction
2. Zero Trust Basics
3. Logical Components of Zero Trust Architecture
4. Deployment Scenarios/Use Cases
5. Threats Associated with Zero Trust Architecture
6. Zero Trust Architecture and Possible Interactions with Existing Federal Guidance
7. Migrating to a Zero Trust Architecture

縮寫表格

英文縮寫	英文全名	中文
MAC	Media Access Control	媒體存取控制
SWAM	Software Asset Management	軟體資產管理
HVA	High Value Asset	高價值資產
IPv4	Internet Protocol version 4	網際網路協定第4版
IPv6	Internet Protocol version 6	網際網路協定第6版
NIC	Network Interface Card	網路介面卡
LAN	Local Area Network	區域網路
IT	Information Technology	資訊技術

Outline

1. Introduction
2. Zero Trust Basics
3. Logical Components of Zero Trust Architecture
4. Deployment Scenarios/Use Cases
5. Threats Associated with Zero Trust Architecture
6. Zero Trust Architecture and Possible Interactions with Existing Federal
7. **Migrating to a Zero Trust Architecture**

Migrating to a Zero Trust Architecture

7.1 純零信任架構

- 在全新建置（greenfield approach）的情境下，可以從零開始打造一個零信任架構。
  - 假設企業清楚知道營運所需的應用程式 / 服務與工作流程，就能依據零信任原則，針對流程設計架構。
  - 當流程被確認後，企業就能鎖定所需的元件，並透過工程設計與組織協作來建置基礎設施並完成元件設定。
- 在實務上，對於聯邦機關或任何已經擁有既有網路的組織來說，建置純零信任架構通常不可行。
  - 若組織被指派新任務，需自行建立一套基礎設施（應用程式、服務或資料庫），此時組織可以依照零信任原則，以及安全系統工程（secure system engineering）[SP800-160v1]$_{[1]}$的做法，設計所需的新基礎設施，
  - 例如：在授予存取權限之前，先評估使用者的可信度，並且在新資源周邊建立微型邊界（micro-perimeters）。
  - 能否成功取決於這套新基礎設施對既有資源（例如：身份管理系統）的依賴程度$_{[2-1]}$。

Migrating to a Zero Trust Architecture

7.2 混合零信任與邊界防禦架構

- 對任何大型企業來說，要在一次技術更新週期內就完全轉換到零信任架構，幾乎不可能。
    - 在企業內部，導入零信任的方法，通常是一次只轉換一個業務流程。
- 企業需要確保共同的基礎元素（例如：身份管理、裝置管理和事件日誌紀錄）有足夠的彈性，能夠在零信任與邊界防禦並存的混合式安全架構下正常運作。
- 將一個現有的工作流程遷移到零信任架構時，通常需要部分重新設計。
    - 若企業尚未在流程中採用安全系統工程[SP800-160v1]，可藉此機會一併導入。

Migrating to a Zero Trust Architecture

7.3 將零信任導入邊界防禦架構網路的步驟

- 導入ZTA，組織必須完整且詳盡的掌握自身的資產（實體與虛擬）、主體（包含使用者權限）、以及業務流程。
  - 這些資訊會在PE評估資源存取請求時被使用；若資訊不完整，PE可能因缺乏足夠資訊而拒絕存取請求，這種情況在組織內部存在不明的「影子IT[2-2]」時特別嚴重。
- 在導入ZTA之前，應先進行資產、主體、資料流與工作流程的盤點，並將盤點內容對照業務流程檢視。
  - 如果對現行作業狀態沒有掌握，企業就無法判斷需要建立哪些新的流程或系統。
- 在完成初始盤點後，將進入定期維護與更新的循環，更新可能會改變業務流程，並必須對業務流程進行評估。
  - 例如：更換數位憑證的供應商，表面上看似影響不大，但可能涉及憑證根儲存管理[3]、憑證透明度日誌監控以及其他不易發現的因素。

Migrating to a Zero Trust Architecture

7.3 將零信任導入邊界防禦架構網路的步驟

- 導入ZTA的每個步驟可以對應到RMF[SP800-37]中的流程，因為導入ZTA本質上就是一個降低機關業務功能風險的過程。
- 如圖 12 所示，可視化導入ZTA的過程。

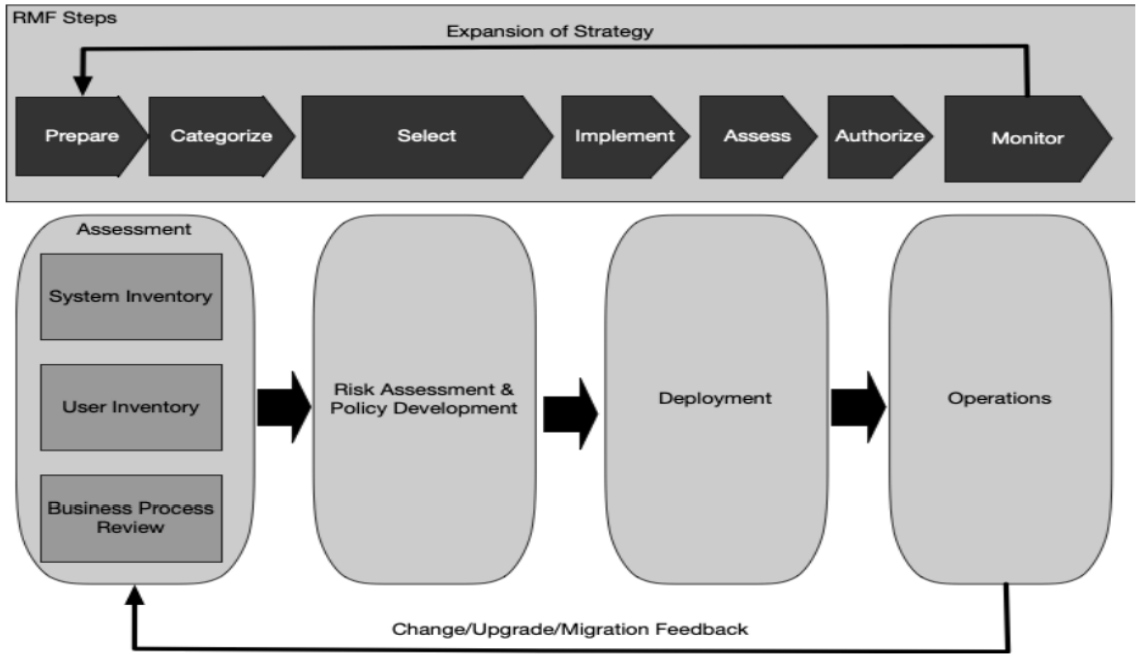

Figure 12: ZTA Deployment Cycle

Migrating to a Zero Trust Architecture

7.3.1 辨識企業中的行為主體（actor）

- 零信任企業能夠運作，PE必須掌握企業主體資訊。
    - 主體可以包含人類使用者，也可能包含非人實體（NPEs），例如與資源互動的服務帳號。
- 擁有特殊權限的使用者（例如開發人員或系統管理員），在被指派屬性或角色時，需要額外的審查。
    - 在許多傳統安全架構中，這些帳號往往擁有全面性的權限，可以存取所有企業資源。
- ZTA應該允許開發人員與管理員保有足夠的彈性，以滿足他們的業務需求，同時透過日誌與審查行為來識別存取的行為模式。
- ZTA部署中，管理員可能被要求符合更嚴格的信任等級或標準，這些標準可參考[NIST SP 800-63A, Section 5][4]。

Migrating to a Zero Trust Architecture

7.3.2 識別企業擁有的資產

- ZTA的一項核心要求是能夠識別並管理各種裝置。
  - ZTA也要求能夠識別並監控那些雖然不屬於企業所有，但可能連接到企業網路基礎設施或存取企業資源的裝置。
  - 資產包含硬體元件（例如：筆電、手機與IoT裝置）和數位資產（例如：使用者帳號、應用程式與數位憑證）。
- 企業難以完整盤點所有資產，因此企業應具備能力，能夠快速識別、分類和評估新發現並存在於企業基礎設施上的資產。
- 企業需建立資產清單與資料庫，並能設定、監控、檢視與更新各種資產（含虛擬資產與容器[2-3]），同時掌握其實體與網路位置，以支援存取評估。

Migrating to a Zero Trust Architecture

7.3.2 識別企業擁有的資產

- 非企業所有的資產，以及企業擁有但未正式管理的「影子IT」，也應該盡可能被盤點。
    - 盤點內容可能包含企業可見的資訊（例如：MAC位址[2-4]、網路位置），並可由管理員補充資料，而這些資訊不僅用於存取決策，還能提供企業做監控與鑑識紀錄。
- 某些ZTA的作法（特別是以網路為基礎的方式），可能讓影子IT元件無法使用，因為它們未被納入網路存取政策。
- 已建立CDM計畫功能的機關，例如硬體資產管理（HWAM）和軟體資產管理（SWAM）[5]，實施ZTA時能運用豐富的資料。
- 機關也可能擁有一份零信任候選流程清單，清單包含高價值資產（HVA），這些資產被認定為機關任務的關鍵。
- 這些計畫必須具備擴展性與適應性，能因應企業變化而調整，並在導入ZTA時，能納入新增的資產、服務與業務流程。

Migrating to a Zero Trust Architecture

7.3.3 識別關鍵流程並評估執行流程所帶來的風險

- 機關應該進行的第三項盤點，是識別並排序業務流程、資料流，以及它們與機關任務之間的關聯
- 企業可先從低風險的業務流程進行首次的ZTA轉換，以避免中斷對組織造成重大影響。
- 使用雲端資源或遠端工作的業務流程適合導入ZTA，可提升可用性與安全性。
    - 與其將企業邊界延伸到雲端，或透過VPN讓用戶連回企業網路，不如讓用戶直接請求雲端服務。
- 規劃人員應考量導入ZTA的取捨，如效能下降、使用者體驗受影響，甚至流程更脆弱。

Migrating to a Zero Trust Architecture

7.3.4 為零信任候選流程制定政策

- 識別候選服務或業務流程，取決於：該流程對組織的重要性、受到影響的主體群，以及該流程目前使用資源的狀態。
  - 資產或流程的價值可依其風險評估，並透過NIST風險管理框架[SP800-37]來判定。
  - 資產或流程被確認後，還需要識別所有的上游資源（例如：身份管理系統、資料庫和微服務）、下游資源（例如：日誌紀錄和安全監控），以及與該流程相關或受影響的實體（例如：主體和服務帳號）。
  - 例如：一個僅供特定企業主體使用的應用或服務（例如採購系統），可能比一個全企業主體都依賴的應用或服務（例如電子郵件系統）更適合作為優先導入的候選。
- 企業管理員需針對候選業務流程所使用的資源，決定一組評估準則（採用基於標準的信任演算法），或決定信任等級的權重（採用基於分數的信任演算法）。
  - 在調整階段，管理員需修正標準或數值，以確保政策有效且不妨礙資源存取。

Migrating to a Zero Trust Architecture

7.3.5 識別候選解決方案

- 在制定好候選業務流程清單後，企業架構師可以整理出候選解決方案清單，以下是需要考慮的因素：

1. 該解決方案是否需要在用戶端資產上安裝元件？
2. 這個解決方案是否能在業務流程資源完全存在於企業內部時運作？
    - 有些解決方案假設請求的資源會位於雲端（南北向流量），而不是在企業邊界內部（東西向流量），且候選流程資源的位置會影響解決方案選擇與ZTA設計。
3. 該解決方案是否提供記錄互動以供分析的方式？
    - 蒐集並利用與流程相關的資料，並在PE進行存取決策時使用

Migrating to a Zero Trust Architecture

7.3.5 識別候選解決方案

4. 該解決方案是否對不同的應用程式、服務與協定提供廣泛支援？
    - 有些解決方案可能支援廣泛的通訊協定（例如：Web和Secure Shell等）和傳輸協定（例如IPv4和IPv6），而另一些可能僅專注於少數情境（例如：僅支援Web或電子郵件）。
5. 該解決方案是否需要改變主體行為？
    - 有些解決方案可能會要求額外的步驟來執行特定的工作流程，這可能會改變企業主體執行流程的方式。

- 其中一種做法，將現有業務流程建模作為試點計畫（pilot program），可設計成用於多個流程或單一案例，作為ZTA的驗證場，在主體正式轉移前先行測試。

Migrating to a Zero Trust Architecture

7.3.6 初始部署與監控

- 一旦選定候選的工作流程與零信任架構元件，就可以開始進行初始部署。
- 新的零信任業務流程可以先以「僅回報模式」運行一段時間，以確保政策有效且可行。
  - 僅回報模式：大部分的存取請求仍應被允許，但要記錄日誌與連線追蹤，並與初步制定的政策進行比對。
  - 一些基本政策（例如：拒絕未通過MFA的請求，或來自已知攻擊者控制或遭竄改的IP位址）應被強制執行、記錄。
- 在初始部署之後，存取政策應該放寬一些，以便從零信任流程的實際互動中收集資料。
  - 建立該流程的基準活動模式後，就能更容易辨識出異常行為。
- 如果無法以較寬鬆的方式運行，企業網路管理員就應該密切監控日誌，並依照實際操作經驗來調整存取政策。

Migrating to a Zero Trust Architecture

7.3.7 擴展零信任架構

- 當企業累積足夠的信心，並且將工作流程的政策加以調整改善後，就會進入穩定的營運階段。
  - 網路與資產仍需被監控，流量也必須記錄，但因為不再出現重大問題，所以回應和政策修改的頻率會降低。
  - 相關資源與流程的主體與利害關係人，也應該提供回饋來幫助改善運作。
- 此階段，企業管理員可規劃下一階段ZTA部署，並和先前的推行方式相同，先識別候選流程與解決方案並制定初步政策。
- 如果工作流程發生變化，現行的零信任架構就需要重新評估。
  - 系統若有重大變動，例如：新增裝置、軟體重大更新（特別是零信任的邏輯元件），或組織架構的改變，可能會導致工作流程或政策需要調整。
  - 實際上，整個流程都應該被重新檢視，但可以假設先前已有部分工作完成，例如：如果購買新裝置，但沒有新增使用者帳號，則只需要更新裝置清單即可。

Appendix

1. 安全系統工程（Secure System Engineering）[SP800-160v1]
2. 名詞、語句解釋
3. 憑證根儲存管理
4. [NIST SP 800-63A, Section 5]
5. 軟體資產管理（SWAM）

Appendix

1.安全系統工程（Secure System Engineering）[SP800-160v1]

- 傳統資訊安全通常在系統完成後才加上防護，但這容易留下漏洞，而[SP800-160v1]提出一種工程方法，讓安全性從一開始就融入系統設計與建置。
- 核心內容：

1. 原則：安全不是附加功能，而是系統本身的基礎屬性，並與任務需求緊密連結。
2. 系統思維：不只看單一元件，而是把整個系統（技術、人員、流程）當作一體。
3. 架構設計：把安全性設計進元件與流程。
4. 持續改善：安全不是一次性任務，而是持續的工程過程，需透過回饋與監控不斷改善。

Appendix

名詞、語句解釋

2-1.能否成功取決於這套新基礎設施對既有資源（例如：身份管理系統）的依賴程度。

- 依賴高：新ZTA依賴舊系統，若舊系統有漏洞或限制，就會拖累新環境； 依賴低：新ZTA更能獨立運作，不容易被舊系統影響。

2-2.影子IT

- 雖然是企業擁有，但並未像其他正式資源一樣被管理的資源，可能來自員工或部門私下安裝或使用的系統、服務或伺服器。

2-3.容器

- 標準軟體套件，應用程式和其相關設定檔組合在一起，並一致運行。

Appendix

名詞、語句解釋

2-4.MAC位址

- 在網路介面卡 (Network Interface Card, NIC) 的硬體位址，用來在區域網路（LAN）中唯一識別一個設備。

Appendix

3.憑證根儲存管理（Certificate Root Store Management）

- 管理「可信任的憑證授權中心（CA）清單」，確保電腦或瀏覽器只信任安全、合法的憑證。
- 核心內容：

1. 維護清單：決定哪些CA的「憑證根」能進入清單，哪些要移除。
2. 審查與監控：檢查CA是否遵守安全規範（例如憑證發放流程是否正確）。
3. 更新與修補：定期發佈更新，確保用戶端裝置上的「信任清單」為最新。
4. 應對事件：如果某個CA被駭客入侵或誤發憑證，就會將其踢出清單，避免使用者受害。

Appendix

4. [NIST SP 800-63A, Section 5]

- 文件名稱：《數位身份指引，第五章節：身份解析、驗證與確認》。
- 如何實際進行身份證明的三個步驟。
- 核心內容：

1. 身份解析：確保使用者提供的資料能夠唯一識別一個人。
2. 身份驗證：驗證這些身份資料是否真實、有效。
3. 身份確認：確認申請人本人就是該身分資料的合法持有人。

Appendix

5.軟體資產管理（SWAM）

- 一種系統化的流程、政策與工具集合，目標是對組織內所有軟體進行盤點、管理與控制。
- 核心流程：

1. 發現與盤點：自動或人工掃描，列出所有軟體清單。
2. 分類：按照用途（業務應用、開發工具或系統服務）與重要性分級。
3. 驗證與比對：與「標準軟體清單和白名單」比對，確認是否授權、是否合規。
    - 標準軟體清單：企業允許安裝與使用的軟體清單；白名單：一種存取控制機制，只有清單上的項目才被允許存取。
4. 持續監控：偵測新增、移除或版本改變的軟體。
5. 風險管理：標記高風險軟體（過期、不再支援、存在漏洞）。