企業資安長的零信任存取有效指南

提供對所有設備和用戶的持續可見性和控制管理

目錄

內容提要

網路存取的最佳實踐規範了零信任存取 (Zero-Trust Access, ZTA) 方法。希望實施 ZTA 的企業資安長們會發現許多目的在滿足美國國家標準與技術研究院 (NIST) 零信任架構要求的技術[1]。然而，讓所有相關技術協同工作來防止安全漏洞可能是一項挑戰。

Fortinet 擁有數十年網路安全經驗並密切遵循最新標準，我們發現最有效的 ZTA 策略，即在三個關鍵領域為管理者提供可見性和控制管理，這三個關鍵領域為：誰在網路上，網路上有什麼，以及正受管設備離開網路時，會發生什麼。

簡介

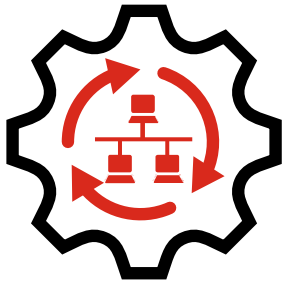
隨著數位創新 (DI) 的應用越來越廣，企業資安長看著他們的網路受安全威脅越來越大。由於網路現在有許多“端點設備”，因此很難建立單一的防禦，導致許多根據傳統的防護策略變的無效，並且，用來區分內部信任用戶與外部未知或不可信用任用戶變得越來越困難；員工和承包商經常是重大網路漏洞的來源，即使是合規用戶也可能成為攻擊的載體，因為他們經常帶著他們的個人設備在網路內外漫遊，不斷威脅著企業網路安全。

因此，資安長不得不重新考慮請求存取網路資源的用戶與設備的信任基礎。最佳存取網路的作法已經從信任網路中的一切，到一次驗證後再信任，再到不信任任何設備或用戶，只提供最低授權的存取。這種最新存取模型的常用縮寫即是零信任存取 (Zero-Trust Access)，或簡稱“ZTA”。

對 ZTA 的要求在最初創造該術語之後的十多年裏一直在不斷完善。NIST 最新的零信任體系架構承認 ZTA 是一項正在進行的工作。因此，它沒有定義架構的細節，而是提供了一套原則，並建議資安專業人員向 ZTA 的過渡視為一段旅程。

作為企業資安長，在這一旅程中，Fortinet 開發了一種有效的 ZTA 解決方案。這種方法有三個支柱：

- ZTA 解決方案必須提供對連接到網路設備和用戶們以及他們試圖存取的網路資源擁有持續的可見性。
- 無論設備類型、位置或存取方法為何，解決方案都必須能夠強制執行安全原則。
- 當設備離線時，仍然能夠保持持續執法與可見性。



網路有越來越多的“端點設備”，這導致了傳統的存取策略變的無效。“零信任存取”是已逐漸成為普遍的網路存取模式，一個完成的解決方案是成功的關鍵。

查看和控制誰在網路上

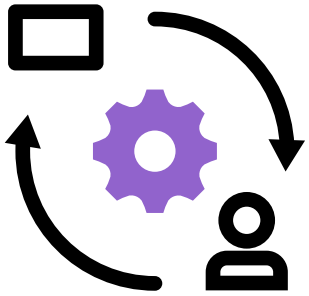
無國界的數位企業需支援的用戶越來越多，除了傳統的員工之外，還有存取需求的承包商、供應鏈、合作夥伴和客戶等等用戶，這些資料和應用程式可能常駐在本地資料庫或雲端。規範網路資源時就包括能夠識別請求存取的用戶與驗證用戶是否有權存取。

防洩密的識別和身份驗證

用戶的身份很容易被洩露。駭客可以透過暴力手段獲得用戶的帳號和密碼，許多用戶的密碼通常很弱，這對有經驗的駭客來說通常很容易破解，或者透過電子郵件網路釣魚方式取得用戶名和密碼。出於這個原因，許多企業增加多因素身份驗證 (MFA) 防範。MFA 包括用戶知道的東西，例如：用戶名稱和密碼，以及用戶所擁有的東西，例如：產生一次性授權碼或根據軟體的授權碼產生器。到 2024 年，預計有 70% 的應用程式將使用 MFA。[2] 而新興的生物識別解決方案——指紋、面部掃描和虹膜掃描——也有望最大限度降低個人資料被盜的風險。

最低權限授權

第二個挑戰是防止經過身份驗證的用戶濫用存取權限。為此，企業的資安長們應只提供授權最低權限存取策略，根據他們在企業中的角色或與企業的關係，將存取權限限制在用戶需要的最低程度。身份驗證和授權應與企業的網路安全基礎架構 (以及根據政策的活動資料庫) 整合，以實現最低權限存取策略的自動化與輕鬆管理。確保這些安全政策不會妨礙生產力或用戶體驗。資安長應考量支援單點登錄 (SSO) 功能並以最小延遲的 ZTA 解決方案進行相關的佈署。這兩個功能都有助於促進合規性並增加用戶的便利性體驗。



零信任存取解決方案應嚴格進行存取控制策略，同時提高授權用戶的生產力和體驗。

查看和控制網路上的內容

雖然資安長非常關注用戶的不合規和不可預測的行為，但他們應該同樣關注存取的網路設備。其中包括用戶終端設備 (桌上型和行動設備)、有聯網的辦公設備、前端零售系統 (例如：POS)、相關營運設備或眾多的 IoT 物聯網設備。目前對 IoT 設備的成長預測各不相同，但大多數人預計在未來幾年全球將達到數十億。管理這些設備的挑戰在於它們的廣泛分佈、層級不同以及傳統設備缺乏對標準通信協議的支援。資安長們可以為公司的資安管理員解決這些端點管理所帶來的挑戰，為他們提供有效發現、分類和控制網路上的所有東西的所需工具。

網路存取控制 (NAC) 應在數秒內提供設備的可見性

為了及時掌握網路上的任何狀況，資安長們需要網路存取控制 (NAC) 工具，NAC 存取工具可以在用戶請求存取網路時快速自動識別和設置每台設備，並掃描是否有漏洞。在偵測的過程中，NAC 解決方案應需檢測 MAC 身份驗證繞過 (MAB) 攻擊企圖並記錄這些事件。它還應該與其他網路設備和安全基礎架構裏的各元件即時共享所收集的資訊。

NAC 的識別過程應在幾秒鐘內就需完成，以盡量減少設備被破壞的風險。出於這個原因，資安長們應該對依賴流量掃描的解決方案保持警惕，相關解決方案允許設備在識別過程中連接網路。然而，掃描過程需要長達半小時，在等待期間，網路極可能會受到破壞。

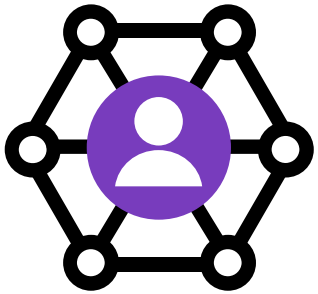
另一個需注意的地方跟 802.1X Wi-Fi 無線網路協定有關。在無線網路中，每個用戶端都有一個請求者作為通信控制的一部分，好讓 802.1X 方便執行。然而，根據 802.1X 的解決方案在交換網路上的部署非常繁瑣。在理想情況下，NAC 解決方案應該從中心位置來部署，並跨有線和無線網路中提供一致的操作，有了中心位置，NAC 解決方案不需要在每個設備位置都要安裝傳感器，增加部署與管理的成本。

在微分段實現零信任存取控制

存取控制對所有設備都非常重要，但對 IoT 設備來說非常具有挑戰性。這些設備通常是低功耗、小型設備，沒有額外的 CPU 或記憶體來支援安全掃瞄。且這些設備還常採用非標準的作業系統，這些作業系統不一定用於防護端點設備的安全，因此，設備常常是不可靠的，所以網路本身提供的安全就顯的非常重要。

由於 IoT 的大規模部署，資安長們在考慮 ZTA 解決方案時必須優先考慮對 IoT 的控制。存取控制不能在設備本身中實現，因此必須來自網路。實現這一點的方法是使用新世代防火牆 (NGFW) 對網路進行微分段，將類似的 IoT 設備分組在一起。這從兩個方面强化了網路。首先，它打破了網路的橫向 (東西) 路徑，使得駭客和蠕蟲更難訪問這些設備。其次，它降低了被感染設備成為駭客攻擊網路其餘部分的媒介風險。

與其他 ZTA 解決方案一樣，NGFW 的架構應能夠以最小的延遲處理所有分段間的流量。這將確保 ZTA 設備控制機制不會阻礙企業的生產力。



資安長應確保資安管理員擁有所需的工具，以便從一個中心位置有效地發現、分類和控制網路上的一切。

控制網路外的受管設備

數位企業一個特徵是網路連接和使用的短暫性。雲端服務實現了無處不在的存取，這意味著用戶可以進行漫遊，在一個位置斷開設備的網路連接後，在另一個位置重新連接。他們也可能在一台設備開始工作，並繼續在另一台設備上工作。當設備離開網路時，控制受管理的設備是一個挑戰，因為即使設備在第一次連接到網路時是安全的，它們也可能在離線時被破壞，並在返回時感染網路。

為了克服這一項挑戰，資安長應將端點設備安全視為 ZTA 解決方案的一部分。端點安全解決方案應提供離網控制，包括漏洞掃描、Web 過濾和修補策略。它還應該為虛擬專用網路 (VPN) 連接提供安全和彈性的選項。與身份管理工具一樣，端點安全解決方案應支援 SSO 功能以便於使用。一旦端點設備連接到網路，端點安全解決方案應將設備狀態資訊中繼到其他網路和安全元件，以進行風險評估並確定適當的存取層級。

總結

零信任存取控制並不是一個新概念。因此，資安長可能會被有關 ZTA 技術和解決方案的建議所淹沒。比如：美國國家標準暨技術研究院 NIST 公布了 SP 800-207 標準文件[3]，成為美國政府採用 ZTA 指南，在 2021 年 5 月的行政命令中，更是規定在地政府機構要在 60 天內，制定實施 ZTA 計畫。與領先的網路安全供應商合作，選擇整合與自動化的工具，可以幫助克服 ZTA 網路存取的關鍵挑戰。

[1] Scott Rose, et al., "Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture," NIST, February, 2020.

[2] Michael Kelley, et al., "Gartner Magic Quadrant for Access Management," Gartner, August 12, 2019.

[3] Scott Rose, et al., "Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture," NIST, February, 2020.

www.fortinet.com/tw

August 18, 2021 3:23 PM

ebook-effective-zero-trust-access

693421-B-0-EN