白皮書

Zero Trust Network Access 藍圖

誰應該閱讀這份指南？

網路架構設計師、資安工程師、技術長、資安長及其他 IT 與資安決策者，皆可透過此份指南獲益。

對於負責針對 Zero Trust Network Access (ZTNA) 專案進行範圍界定、設定、部署、導入和管理的人員來說，本指南提供全方位的檢視，說明潛在效益以及用於不同系統時的差異。本指南包括：

- 傳統應用程式存取方法的限制和安全瑕疵，以及為什麼需要 ZTNA
- ZTNA 的元件及其運作方式
- Akamai Enterprise Application Access 和 Akamai MFA 如何快速又輕鬆地提供 ZTNA

隨著商業世界的不斷轉變，加上網路威脅日漸增加，許多公司都正在重新審視其網路防禦能力。傳統網路架構仰賴各方都能存取應用程式的集中式位置，這讓許多公司都已開始意識到這樣的方法會使其容易遭到攻擊。這種深溝堅壘之安全模式的概念是保護邊界，同時假設在邊界內的所有人都可以信任，這使得許多公司在現今行動連線與雲端環境中面臨到網路攻擊的風險。有遠見的公司都開始改採用 Zero Trust 架構概念，來保護重要的資產。Zero Trust 專案的核心原則就是保護網路。本白皮書詳細說明為何傳統軸輻式網路安全方法已不敷使用，以及為何改用 ZTNA 能更有效地保護重要資產，並成為全方位 Zero Trust 架構的重要關鍵。

企業的改變步調從未如此快速

企業營運與使用技術的方式不斷演進，其速度比以往更快。運算的演進促使企業快速地從將業務應用程式代管在內部部署資料中心，轉換為使用多個公有雲、私有雲或混合式方法 (同時採用內部部署及公有雲/私有雲)。

商業模式的演進也促使了實體間的協同合作增加，並催生為合作夥伴與供應商提供應用程式及資源存取權的需求。

最後，由於企業持續採用遠端或混合式工作，因此使用者現在可從任何位置使用受管理和未受管理裝置存取業務應用程式與資源。

由於有這些變化，因此管理應用程式存取的傳統方法已不敷使用，所有公司現在都必須採用新的方法，確保無論應用程式被代管於何處或使用者位於何處都能安全存取。

傳統應用程式存取

20 多年來，許多公司一直都仰賴防火牆來建構強大安全邊界，並且一直都信任邊界內的使用者。這就像是把網路當作有護城河的城堡：厚實的城牆和嚴密看管的大門形成保護城堡 (在此情況下就是網路) 的邊界，只有擁有正確憑證的使用者才能存取。進入之後，使用者就能存取透過 Microsoft Active Directory 等身分識別供應商 (IdP) 解決方案提供的特定應用程式，而能存取的應用程式則會因使用者身分而有不同。

然而，使用平整型網路時，使用者實際上可以透過 IP 存取整個網路，這表示他們可以探查其他伺服器和應用程式。例如，若 IdP 設定正確，使用者可能可以找到代管薪資應用程式的伺服器，但在他們嘗試登入應用程式時就會遭到拒絕存取。

為了修正這種不受限制的橫向移動問題，許多公司透過虛擬本機存取網路 (VLAN) 將應用程式分割在不同的防火牆區段內，並針對個別使用者或群組強制執行以 IP 範圍為基準的規則，但這種方法現在已經過時。這樣的程序十分脆弱，且易發生錯誤。試想正有人在執行維修，將機器移至新的機架，或需要重新設定 IP 至新範圍的情況。這時使用者就會突然遭封鎖，開始撥打技術支援電話。或是某項軟體升級可能需要變更應用程式的架構，並在工作流程中將使用者重新導向至另一部機器。但新機器尚未更新防火牆原則，導致特定使用者或群組無法存取。

這種架構極端複雜，需要應用程式擁有者、網路管理員和安全團隊之間的變更經過密切協調，才能確保零停機時間。

我們知道未妥善協調時，通常會發生什麼事。系統管理員希望遵守最佳實務，但是當時間急迫，他們就不得不使用惡名昭彰的 IP ANY/ANY ALLOW 規則暫時維持系統運作，讓受影響的使用者獲得存取權，直到能夠診斷並修正根本原因。然而，企業通常沒有時間回頭復原這些變更，而這些快速修正會隨著時間而減損公司的資安布局。

VPN 帶來複雜性、效能和安全性的額外挑戰

對於遠端使用者而言，虛擬私人網路 (VPN) 通常可為代管於邊界內的內部應用程式提供存取權，然後提供公司網路的直接通道式存取權。

為了管理使用者對應用程式的存取權，公司經常會新增專用的應用程式傳遞控制器，或使用 VPN 解決方案內建的存取控制功能。目標是無論使用者位於何處，都要符合應用程式的存取權。若使用者在邊界內時無法存取 CRM 應用程式，則在透過 VPN 連線時應同樣拒絕其存取。儘管目標如此，但由於在兩種使用案例之間同步處理應用程式權限和快速修正相當複雜，可能導致使用者獲得非預期的應用程式存取權。

約聘人員、合作夥伴和供應商的應用程式存取權

企業也經常使用 VPN 來允許約聘人員、合作夥伴公司或供應商從遠端存取應用程式。例如，公司可能會允許其財務系統的外部存取權，以允許供應商提交發票。透過 VPN 允許第三方應用程式存取會帶來額外的安全風險，因為公司不再保有端對端的安全性。如果具備 VPN 存取權的第三方裝置出現破口，攻擊者就能存取公司的網路。

VPN 與效能

在效能方面也存在相同的取捨。VPN 最單純的形式就是將所有流量傳回資料中心基礎架構。這可能造成有效使流量加倍的髮夾彎效益，導致網際網路內容與軟體即服務 (SaaS) 存取極慢。

為克服此效能負擔，系統管理員常會部署分割通道，並再度標記哪些 IP 範圍應送入 VPN、哪些應直接送出網際網路。在僅有單一內部邊界時，此方法可能十分簡單有效。然而當企業開始增設多個資料中心和虛擬私有雲端供應商時，就會開始變得更複雜。系統管理員必須判斷應否於每一個資料中心安裝 VPN 彙總工具，並研判如何有效地管理多點分割通道。

這並不是說 VPN 沒有價值。事實上正好相反。多資料中心基礎架構中的站對站存取就是 VPN 架構能夠大放異彩的一個情況。然而，對於存取應用程式的使用者而言，網路層級存取並非正確的典範，因為網路層級存取會使簡易性與安全效能難以兩全。

對攻擊者來說，網路型應用程式存取權是個好消息

目前為止，我們著重於為所有員工提供網路層級存取權的相關風險與挑戰。然而，這種方法也會使企業暴露於另一種風險中：網路犯罪者若利用竊取的使用者憑證或安全弱點，也有可能獲得不受限制的全網路存取權。舉例來說，如果攻擊者使用遭入侵的員工憑證取得 VPN 存取權，就能在網路中橫向移動，以尋找、存取和攻擊高價值目標。

這些方法可能會導致發生嚴重外洩

理論上來說，使用這些方法可以安全且最順暢地管理應用程式存取權。貴公司甚至可能已經採用其中某種組合。問題在於維持這在作業生命週期內永不出錯實在太難；從部署、維護到提供適當的安全與效能，這些作業太過複雜。許多案例中，企業說服自己因為員工能夠存取應用程式，所以一切必然已屬最佳狀態。等到當上述的一項臨時修正導致重大資料外洩或嚴重的效能衰退，使服務中斷或員工生產力受限時，企業才發現原來自己毫無防備。

Zero Trust 應用程式存取方法

考量到邊界安全防護方法固有的缺陷，以及在管理應用程式存取時所面臨的特定挑戰，新興的 Zero Trust 網路安全模式提供了更好的替代方案。此模型首先由 Forrester Research 在 2010 年推出，是一種企業用來改造 IT 基礎架構、安全性原則和業務程序的架構。

其背後原則相當簡單，但效用非常強大：信任與位置無關。不能因為對象位於防火牆內側就信任它。而是該改成無論是在何處發生的任何動作，都只有在明確允許的情況下才應被信任。到最後，只有*應該*發生的*可以*發生。移除對所有不必要動作的絕對信任，因為此舉只會產生風險，不會創造價值。

這需要強式驗證與授權，且系統在建立信任之前不應傳輸資料。同時，系統亦應運用分析、篩選和記錄機制，確認對象行為並持續監控可疑徵兆。

若能如此從本質上改變，就能夠讓過去這十年當中的許多安全破口事件免於發生。攻擊者無法再針對邊界進行弱點攻擊，然後入內奪取您的機密資料與應用程式。現在沒有需要跨越才能存取的護城河。有的僅是應用程式和使用者，且兩者均需相互驗證並確認授權之後才能夠存取。

Zero Trust Network Access

ZTNA 是以這些原則為基礎的架構，能以嚴密的驗證、授權和背景資訊為基礎，為應用程式與資源提供安全的存取。ZTNA 架構僅會為使用者提供工作所需的應用程式存取權，而不是整個網路的存取權。運用 ZTNA 方法，使用者的所在位置將不再造成影響，也不再有邊界內外的概念。無論是內部部署、公有雲或私有雲，應用程式的代管位置不再造成影響，因為經過驗證的使用者只能存取其獲授權使用的應用程式。

例如，銷售部門的員工只能存取與其銷售職務相關的應用程式，無法存取人力資源或財務應用程式。

Akamai ZTNA 的運作方式

Akamai Enterprise Application Access 和 Akamai MFA 可讓您移轉到 ZTNA 架構，這對實現 Zero Trust 來說，可說是極為重要的一個步驟。

Enterprise Application Access 是位於雲端且具備身分識別能力的代理伺服器 (IAP)。其提供彈性化且可調整的服務，並具備基於威脅情報、裝置狀態和使用者身份識別資訊等即時訊號的精密決策功能。Akamai MFA 是一種多重因素驗證服務，可提供強度最高的驗證，確保要求存取的使用者是其本人。

首先，您需要在防火牆後方執行一個稱為 Enterprise Application Access 連接器的小型虛擬機器，但仍可連線至您的應用程式。此系統無需 (亦*不應*) 存在於 DMZ 內。其位址應落於私有 IP 空間，不可直接從網際網路連線。事實上，它看起應與防火牆內其他任何應用程式都一樣。

若要支援多雲端環境，可將連接器部署於您的內部部署資料中心內，或部署於私有或公有雲端。

Enterprise Application Access 連接器會立即建立與 Akamai Connected Cloud 之 IAP 的輸出加密連線。連線至 IAP 後，連接器會下載其組態，並準備好進行服務連線。連接器與 IAP 之間為輸出連線，可讓您關閉所有連入的防火牆連線，在公開網際網路上幾乎看不見應用程式。

IAP 會執行使用者連線至應用程式前的所有預先處理，包括驗證、授權，以及裝置安全性與狀態檢查。當使用者試圖存取應用程式時，會藉由 DNS CNAME 導向至 Akamai，進而連線至 IAP。假設終端使用者及其裝置皆通過所有檢查，接著即轉往驗證、多重因素驗證和單一登入功能，然後執行裝置身分識別功能。

待使用者與機器均通過授權，即會將終端使用者的連線縫接於 Enterprise Application Access 連接器的輸出連線。使用者工作階段的流量會經由這段縫接的 IAP 送達 Akamai Connector，然後連線至要求的應用程式或服務。至此階段，即建立了完整的資料路徑，且持續並動態地根據身分識別、裝置和使用者環境，強制執行所有存取決策。

這種存取方式帶來明確且顯著的優勢。最需要效能和安全的活動均於網路邊界接近終端使用者之處進行，而 Akamai 在全球 134 個國家或地區擁有逾 4,200 個位置。

不僅如此，連入應用程式的機密路徑也經由反向應用程式通道，有效地移除邊界的 IP 可見度，降低流量攻擊的可能性。

由於 Enterprise Application Access 能直接整合公司的身分識別基礎架構，即便使用多個目錄和身分識別服務供應商，也能快速部署 ZTNA 服務，無需變更現有的身分識別基礎結構或架構。

針對不支援現代驗證通訊協定的舊版應用程式，Enterprise Application Access 的 IdP 橋接功能可為 SAML 式 IdP 提供驗證，並將驗證權杖轉譯為舊版應用程式所支援的驗證通訊協定。

Enterprise Application Access 這種 IAP 型的做法之所以誘人，正是因為採用應用程式層級存取。應用程式層級存取的效能與安全和複雜度*脫勾*。

只要將位置相近的應用程式 (例如架設於同一個資料中心或相同虛擬私有雲端內) 置於私有網路 IP 空間或管制下的 VLAN，再於其微邊界中架設存取代理伺服器，即大功告成。就是這樣，您已經完成了。

應用程式擁有者能夠自行於存取代理伺服器設定安全原則，例如規定誰能夠存取、為何能夠存取等原則，而且使用者的所在位置甚至毫無限制。由於沒有任何網路邊界包覆終端使用者，因此內部與外部部署毫無分別。在咖啡廳工作的員工與辦公室座位上的員工完全相同。重要的只是該使用者是否經過授權，以及電腦本身是否安全。

應用程式層級存取的部署與使用雖然非常簡單，卻能擁有同級最佳的效能。無論使用者和應用程式所在位置，均可如常連線網際網路直接存取應用程式，讓網際網路封包路由不必經由非處於路徑上的彙總工具或中繼點，即可到達目的地。

事實上，應用程式層級存取能讓公司內部網路簡化為單純的訪客 Wi-Fi。別忘了，Zero Trust 真正要生效，就不能給予內外使用者差別待遇。預設不會信任任何人。

ZTNA 的理想最終狀態

無論在內部或外部，所有使用者均應強制透過具備身分識別功能的存取代理伺服器，以存取位於任何位置的所有應用程式。這些代理伺服器不僅應執行標準驗證，也應使用如 Akamai MFA 等防網路釣魚的多重因素驗證。此外，公司亦應具備可靠的裝置狀態功能，可取得裝置條件，以允許存取特定應用程式。

我們堅信 ZTNA 絕不止於驗證與授權。為了支援 Zero Trust 原則，在初始驗證和授權階段檢查的所有參數，應在啟動工作階段期間持續監控。偵測到任何變更都應觸發動作，例如重新驗證使用者、移除應用程式存取權，或限制對應用程式的存取等。

網路應用程式與 API 防護 (WAAP) 是一套關鍵安全系統，應放置於存取代理伺服器層之上，以確保終端使用者不會對內部應用程式發動 (無論是有意或無意) 應用程式層級攻擊。您可以在非 API 網站利用人機偵測等進階系統幫助確保惡意軟體不會隱藏於有效端點背後。Akamai 能夠透過 IAP 在 WAAP 內分層、偵測機器人程式、進行行為分析和快取。此設計旨在實現同級最佳的效能，並盡可能阻擋潛在的攻擊者，遠離您的實體機房、應用程式和資料。

當您將應用程式上線並透過存取代理伺服器提供服務後，分散式阻斷服務 (DDoS) 防禦就變得更為重要。您應該選用能夠為存取代理伺服器與微邊界吸收攻擊的服務供應商，讓系統在沉重負載下仍能繼續運作。

最後，為確保應用程式效能達到同級最佳狀態，並讓使用者接受並支持新的存取形態，您的存取代理伺服器均應設有能夠提供效能益處的前端網路。具體而言，您的系統應包含內容遞送網路和網際網路路由疊層，除了提供存取，更讓效能超越舊方法的極限。

威脅防護

Akamai Enterprise Application Access 這種解決方案能保護您的應用程式，防範惡意攻擊者。但是究竟該如何避免使用者因感染，例如裝置遭惡意軟體感染或憑證遭網路釣魚連結及登陸頁面竊取，而在無意之間成為攻擊者？這就是為何網路流量需要預防與偵測措施。

其中一種方法是部署雲端型 DNS 防火牆解決方案，例如 Akamai Secure Internet Access。本產品會檢查使用者發出的每個 DNS 要求，並套用即時威脅情報，如此便可將無害的要求解析為正常，但主動封鎖任何送往惡意網域的要求。如此可降低員工裝置遭惡意軟體或勒索軟體入侵，或遭受網路釣魚攻擊的風險。

摘要

在這個雲端與行動的時代，傳統的軸輻式網路架構及其採用的深溝堅壘安全邊界概念，已無法有效提供效能或安全保障。這是所有公司都必須開始處理的問題，否則會使他們處於弱勢狀態。未能轉型更安全的企業安全架構，已是當今企業資安侵害事件最大原因，而資料外洩的情況更是持續惡化中。簡言之，躲藏在網路邊界後方並不安全，因為邊界已不復存在。

後續步驟

該如何開始轉型為 Zero Trust Network Access 架構？

利用 Akamai 的雲端安全服務，您即可打造一套全方位的 ZTNA 架構，不僅在多雲端的環境中提供安全的應用程式存取功能，更能利用雲端幾乎完全排除企業內部網路的需求。

結合本公司先進的分散式 IAP 解決方案、防網路釣魚的多重因素驗證，再搭配功能強大的 Akamai Connected Cloud，您現在終於能夠輕鬆移轉無邊界環境，將應用程式逐一導入，不僅將轉型風險曲線幾乎降至於零，更能利用 Akamai 多年來經實證的效能與安全解決方案。

當您繼續落實 Zero Trust 架構，您可以信賴 Akamai 將伴隨貴公司每一步，協助將網路轉型為合適的架構，不僅以容易管理的方式提供應用程式與資料存取，更同時維持最高水準的安全和效能。

進一步瞭解利用 Akamai Zero Trust 產品組合滿足您的業務需求。

Akamai 驅動並保護線上生活。全球各地領先業界的企業都選用 Akamai 來建置、遞送及保護其數位體驗，協助數十億人每天的生活、工作和娛樂。Akamai Connected Cloud 是一個龐大分散式邊緣與雲端平台，能讓應用程式與體驗更貼近使用者，同時遠離威脅。若要深入瞭解 Akamai 的雲端運算、安全性與內容遞送解決方案，請造訪 akamai.com 以及 akamai.com/blog，或至 X (前身為 Twitter) 和 LinkedIn 追蹤 Akamai Technologies。2024 年 2 月發行。