為現今企業建構安全的遠端連接解決方案

目錄

概述

許多組織使用虛擬專用網路（VPN），其功能類似於返回公司網路的通道，但完全依賴 VPN 存在資安風險。即使在疫情大流行結束後，企業的首席資安長也需要更好的策略來支援遠端辦公，因為許多員工很可能，至少部分時間都將繼續以遠端的方式工作。鑒於 VPN 的局限性以及現今網路的動態和分散式的特性，很明顯，需要一個更好的解決方案。零信任網路存取（ZTNA）是 VPN 遠端存取的進化。它簡化了安全連接，無論使用者或應用服務位於何處，都可以提供對應用服務的無縫存取。

54% 的就業成年人表示，當新冠病毒爆發結束時，他們仍希望全部或大部分時間居家工作。[1]

介紹

最近遠端辦公的興起使人們關注到虛擬專用網路（VPN）的局限性。多年來，VPN 一直是存取企業網路的方法，但 VPN 有一些嚴重的缺點，特別是在資安領域。

最大的問題是 VPN 採用基於邊界防護安全的做法。使用者透過 VPN 用戶端軟體進行連接，一旦他們從邊界進入，他們通常可以廣泛存取網路，每次以這種方式自動信任設備或使用者時，都會使組織的資料、應用服務和智慧財產權面臨風險。

除了使用 VPN 進行遠端存取的問題外，網路營運商也在尋找更好的方法來保護其應用服務。如果某些應用服務位於雲端，而某些位於本地，將很難有一致通用的管理和控制方法，尤其是當某些使用者位於工作場所內而其他使用者位於遠端工作時。將應用服務部署到雲端中可能會使它們暴露給不受歡迎的攻擊者，增加資安風險。

超越VPN

零信任網路存取（ZTNA）提供了更好的遠端存取解決方案，還解決了與應用服務存取的相關問題。「零信任」的含義聽起來正如它的樣子。使用此安全模型時，即假定沒有使用者或設備是可信的，並且在未驗證使用者和設備是否有權存取的情況下，不會對任何資源的存取授予信任。

由於 ZTNA 的出發點是不會因所在位置而給予一定程度的信任，因此使用者在何處工作變得無關緊要。無論使用者或設備位於哪個實體位置，都適用相同的零信任方法。由於任何設備都被視為可能被感染，並且任何使用者都可能進行惡意行為，ZTNA 的存取策略反映了此一現實面。

與具有不受限制存取的傳統 VPN 不同，ZTNA 僅在使用者和 / 或設備透過身份驗證後，才將每個會談的存取授權授予各個應用服務和工作流程。對使用者進行驗證和身份認證，以確保他們存取應用服務之前被授予存取授權。每次存取應用服務時，還會檢查每個設備的授權，以確保設備滿足應用服務的存取策略。

認證授權會考慮各種情境資訊，包括使用者角色、設備類型、設備合規性、位置、時間以及設備或使用者連接到網路或資源的方式。

使用 ZTNA 後，一旦使用者提供了適當的存取憑證（如多因子認證與端點驗證）進行連接，就可以授予他們所謂的最低權限存取授權。使用者只能存取執行其作業所需的那些應用服務，而其他的則一概不能存取。

存取控制不會在接入點結束。ZTNA 依認證身份為基礎而不是保護網路中的位置來運作，這允許策略能端到端地跟隨應用服務和其他交易會談。透過建立更層級的存取控制，ZTNA 提供終端使用者更有效的解決方案，並在需要時提供存取控制的策略執行。

儘管 ZTNA 身份驗證過程提供了身份驗證點，但與傳統 VPN 不同，它沒有指定身份驗證的方式。隨著新的或不同的身份驗證方法的實施，它們可以無縫地新增到 ZTNA 策略中。新的身份驗證方法可以幫助消除密碼和憑證薄弱或被盜相關的問題，解決某些物聯網（IoT）設備安全性不足所帶來的挑戰，或者新增額外層級的驗證以存取機敏性資訊或關鍵資源。

ZTNA vs. VPN

對於使用者來說，ZTNA 比 VPN 更容易管理。使用者不再需要記住何時使用 VPN 或完成連接過程。也不會因為有人忘記斷開連接，通道被意外打開的風險。使用 ZTNA，使用者只需點擊應用服務即可立即獲得安全連接，無論應用服務是在本地、公共雲中還是在私有雲上。此通道是隨需建立，對使用者通透無感。由於網路不再是信任區域，因此無論使用者在內網或外網，都會建立相同的通道。加密通道以透明的方式進行，在後台提供安全性。

在應用服務端，由於使用者要連接回控管實施點，然後將該連接代理轉發到應用服務，因此應用服務可以存在於本地、私有雲或公有雲中，而所有這些都隱藏在網際網路之外。該應用服務只需與控管實施點建立連接，以確保它們免受駭客或網路機器人的窺探。

ZTNA模型

供應商在其產品和服務中採用兩種主要方法來實施 ZTNA：用戶端發起或從服務端發起。

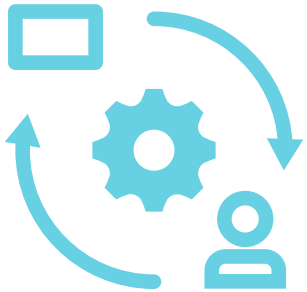
1. 由用戶端啟動的 ZTNA

由用戶端啟動的 ZTNA 模型有時稱為端點啟動的 ZTNA 模型，根據雲安全聯盟架構，最初被稱為軟體定義邊界（software-defined perimeter），此方法使用設備上的代理軟體來建立安全通道。

當使用者想要存取應用服務時，代理軟體會評估確定安全狀況。在收集使用者身份、設備位置、網路和正在使用的應用服務等資訊後，它會建構風險配置檔。然後，它透過代理連接回應用服務，如果資訊符合組織的規範，則授予對應用服務的存取授權。應用服務可以是本地應用，也可以是基於雲端的軟體即服務（SaaS）應用。使用用戶端啟動的模型具有一定的挑戰性，因為除非中央管理解決方案能夠協調部署和設定，否則在設備上管理代理軟體可能會成為 IT 的一個難題。 此外，非託管設備需要透過其他管道處理，例如網路存取控制器（NAC）。

2. 由服務端啟動的 ZTNA

由服務端啟動的 ZTNA 模型使用反向代理架構，有時也稱為應用服務啟動的 ZTNA。根據 BeyondCorp 模型，與用戶端啟動的 ZTNA 最大區別在於它不需要端點代理軟體。它使用瀏覽器插件程式建立安全通道並執行設備評估和狀態檢查。一個關鍵的缺點是它僅限於基於雲端的應用服務。由於應用服務的通訊協定必須是 HTTP/HTTPS，因此它將作法限制為網頁應用服務和通訊協定，例如透過 HTTP 的 SSH 或遠端桌面協定(RDP)。儘管一些較新的供應商正在提供額外的通訊協定支援，但該模型並不適合同時擁有混合雲和本地應用服務組合的公司。



"Gartner 預測，到 2023 年，60% 的企業將逐步淘汰傳統 VPN 並使用 ZTNA 模式。"[2]

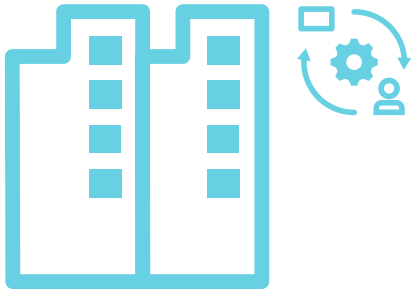
ZTNA的未來

採用零信任網路安全方法是一個涉及許多系統的過程，許多組織可能需要數年時間才能完全實施。但是，解決遠端存取問題是實現完整良好的零信任解決方案的第一步。

隨著企業遠端存取做法的轉變 ,通常是混合著使用 VPN 和 ZTNA。許多提供 ZTNA 服務的供應商正在與 SASE 服務結合使用。這種由服務端啟動的方法從雲端來提供安全控制，讓雲端應用服務的存取變得容易，但它可能會產生昂貴的 SASE 費用，並且可能在它可以支援的應用服務類型上受到限制。

建構完整的零信任網路存取解決方案需要多種元件，比如：用戶端、代理轉發、身份驗證和資安防護。通常，這些解決方案常常由不同的供應商提供，並且各個元件會在不同的作業系統上運作，並使用不同的控制台進行管理和設定，因此跨供應商建立零信任模式可能會遇到許多困難。

透過選擇整合和自動化工具，企業的首席資安長可以克服實施 ZTNA 的關鍵挑戰。使用基於防火牆整合和 SASE 的做法，無論使用者是在內網還是外網，他們都可以使用 ZTNA 功能，並透過相同的動態應用服務存取策略簡化管理。ZTNA 可以應用於遠端使用者、居家辦公室和其他位置（如零售商店），方法是提供對應用服務的遠端存取控管，讓這些存取更易於啟動，更快速，同時提供比傳統 VPN 更細緻的安全保護。



只有 15% 的組織已完成向零信任安全模型的轉變，該模型不會自動假定網路邊界內的任何人都受到信任。[3]

使用 ZTNA 進行安全的遠端存取

隨著越來越多遠端工作的增加，傳統 VPN 的局限性已經變得更加明確。從任何地方移動和工作的人越多，傳統的基於邊界管制的作法就變得越不安全。每次自動信任設備或使用者時，都會使組織的資料、應用服務和智慧財產權面臨風險。與傳統 VPN 相比，ZTNA 解決方案是保護遠端存取的更好方法，並且還改善了對應用服務存取的控制。

[1] Kim Parker, et al., "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020.

[2] Mike Wronski, "Since Remote Work Isn't Going Away, Security Should Be the Focus," Dark Reading, September 24, 2020.

[3] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

FORTINET

www.fortinet.com/tw

April 19, 2022 3:27 PM

911928-0-0-EN