CLOUDFLARE

白皮書

# 制定網路現代化策略

# 目錄

# 傳統網路：實現數位現代化的障礙

若要在瞬息萬變的商業環境中脫穎而出，敏捷性至關重要。但敏捷性不僅僅是領導力和決策的問題。敏捷性還取決於組織執行變更的能力。必須以一種靈活適應而不崩潰的方式建立系統。業務必須能夠重新調整，以適應新的營收模式、支援新的應用程式和連接世界各地的人們。

隨著組織重新裝備以獲取競爭優勢，敏捷性成為數位現代化專案的主要期望成果之一。當考慮到傳統企業網路的現狀時尤其如此，該網路在提供通訊和實現協作方面發揮著至關重要的作用。企業網路一直頑固地抵制變革，這是有充分理由的。其設計原本是為了承受對系統的衝擊，而變革需要付出巨大的代價和努力。

有時變革是可以預料的，因為它們隨著時間的推移而發生，例如，雲端對資料中心的影響。隨著網路的發展，外部市場力量正在推動迅速的變革，有時甚至是在一夜之間發生。例如，這場疫情給我們帶來了慘痛的教訓，對於一些公司而言，無論是迅速增加遠距工作能力、保持員工生產力，還是根據空蕩蕩的辦公室中閒置網路耗費了多少預算來管理成本，都是相當困難的。

總觀上述諸多困難，很明顯，一些公司不僅能夠適應變化，還能蓬勃發展。這不僅僅是管理層能否提供正確商業決策的問題，也是企業轉型和執行能力的問題。對於 CIO 而言，必須制定策略來應對變革，更換工具來支援未來需求，並讓 IT 成為變革的加速劑而不是阻滯劑。

由於對內部部署網路進行了大規模的投資，實施現代化並不是一個簡單的決策。為了充分實現網路現代化的優勢，有必要審視一下必須實現的目標，以確定必須進行哪些變革。

# 瞭解旅程

當您考慮多年來網路設計的最佳做法時，有充分的理由說明為什麼存在如此多的複雜性。幾十年來，組織利用一層又一層的新技術擴建並加強網路。隨著每一代網路設計以及每一次創新的推出，網路變得越來越複雜。組織沒有追求簡單的機會，而增加新技術往往會讓速度、韌性和安全性變得更加複雜。

利用雲端交付的網路和安全服務，我們現在正處於企業網路設計新一代變革的最前沿。透過使用雲端交付的服務來延伸網路，組織可以處理新的使用案例、延伸涵蓋範圍，以及保護遠遠超出資料中心的應用程式。這是一個大大簡化網路的機會，因為服務交付基於與雲端提供者 PoP 的現有網路連線構建，而無需中斷連線來插入另一個設備。內部部署網路和雲端服務之間的網路保持不變，同時向雲端服務中插入新服務並利用這些服務。

問題在於，並不是每個雲端交付的網路和安全平台都是相同的，而且也不總是很容易就能看出它們之間的差異。許多平台在現代化旅程中都沒有太大的優勢。為了瞭解這些差異，有必要制定網路現代化的目標，以避免用一個帶來複雜性的產品來取代另一個帶來複雜性的產品。

# 四條主要網路流量路徑

在評估網路現代化專案的範圍時，請考慮您的網路覆蓋了大量的接觸點，其中一些接觸點與相同的基礎架構相交（例如，流量輸入、輸出以及由東向西通過您的核心網路），還有一些接觸點在基礎架構外部運作（例如，公有雲端網路）。

**輸入流量：** 鑒於部分網路暴露於網際網路，有必要維護輸入防禦來提供保護，以防使企業癱瘓或入侵企業的企圖得逞，同時仍然允許合法使用者的流量通過。傳統的周邊防禦可能會不堪重負，需要一些功能來應對分散式阻斷服務。

**輸出流量：** 與網際網路以及基於雲端的應用程式的連線需要原則，來為安全的商業使用提供防護機制，例如，防禦威脅和資料外流。鑒於使用者位置的多變性，組織實作了混合的輸出保護技術，包括防火牆等內部部署設備（用於使用者在網路上時）、DNS 解析程式以及 SWG 和 CASB 等基於雲端的代理（用於使用者在遠端時）。

**WAN 網路：** 為了支援雲端優先計畫和啟用 IoT 的裝置，正在重新設計 WAN 及其覆蓋的邊界（包括園區和分支機構）。因此，傳統網路拓撲正在撤銷回傳至資料中心，轉而採用直接存取網際網路的架構。隨著這些領域網路的快速發展，插入安全性反而變得更複雜了。在很多情況下，內部流量路徑仍然依賴於邊緣部署的安全設備，從而阻礙了組織的轉型進展。

**公有雲端網路：** 隨著組織在多個雲端擴建應用程式，建立並維護點對點的網路和安全設定變得越來越難。設定和管理網路會耗用時間和資源，而把這些時間花在專案開發上將是更好的選項。

這些流量路徑中的每一條都有很多技術，組織會在其網路內實作或從雲端使用這些技術。鑒於現代化專案涉及多個方向的流量路徑，有必要規劃四個方向的完整網路現代化旅程，以避免因為發生架構錯誤而限制可獲得的轉型優勢或需要多種不同的技術來處理未解決的使用案例。

# Cloudflare 的全球連通雲

您可以考慮使用 Cloudflare 的全球連通雲來實現網路現代化。其構建理念為：使用可組合且可程式設計的架構，為您的使用者以及支援雲端的業務基礎架構和應用程式提供網路和安全服務。因此，它可以在您的現代化之旅中同時滿足目前和未來的需求。

使用 Cloudflare，您不必插入設備，只需啟用服務，即可新增功能和支援新的使用案例。與 Cloudflare Anycast 資料中心的連線保持不變，但您可以透過統一的管理介面設定和部署服務來處理流量。您可以在解決目前需求的同時，部署平台來支援未來的使用案例，進而支援整個網路現代化之旅。

與其擴建全球基礎架構，不如使用我們的基礎架構。Cloudflare 全球網路將為您的組織帶來快如閃電的速度。Cloudflare 網路與幾乎所有服務提供者和雲端提供者直接連線，在大約 50 毫秒內即可連線到全球 95% 的網際網路人口。

# 實現網路現代化的關鍵使用案例

首先，從那些為組織帶來業務影響和最有用好處的使用案例開始。這些使用案例並未指定特定的順序，因為每家企業都有自己的優先順序。最重要的是要解決近期需求，同時還要確立一個架構，無論您採用哪條路徑，都可支援網路現代化旅程。

| | 現代化專案 |
|---|---|
| **分支機構連線**<br>降低成本、提升使用者體驗 | • 從 MPLS 轉換至全球連通雲<br>• 從 SD-WAN 轉換至全球連通雲 |
| **保護面向公眾的基礎架構**<br>延長 FW、DMZ 投資的生命週期 | • 減少網路防火牆的負載<br>• 將 DMZ 安全性轉移至全球連通雲 |
| **簡化企業網路**<br>實作 Zero Trust 以提高安全性並減少資本支出 | • 減少/消除 DMZ<br>• 使用 ZTNA 取代 VPN<br>• 消除對 LAN 的信任升級<br>• 加速併購的連線 |
| **連線並保護您的雲端**<br>在應用程式中充分利用每一個雲端 | • 構建與保護應用程式<br>• 利用開發人員服務集中核心功能 |

## 分支機構連線

WAN 網路的一個重要部分是連結較小的網站（例如，分支辦公室或商店），這依賴於將使用者和裝置連線至應用程式。傳統的中心輻射架構使用昂貴的 MPLS 電路將網站連結至資料中心，但隨著支援雲端應用程式的需求不斷增加，越來越多的組織使用透過寬頻直接存取網際網路的架構。

SD-WAN 尋求讓網路連線更加可靠，但與安全性插入的關係並不完美。大多數 SD-WAN 架構依賴於大量的邊緣設備和本機防火牆對 SD-WAN 結構強制執行安全性原則，並且僅針對輸出流量使用 SSE/SASE 整合。

使用 Cloudflare 的全球連通雲進行分支機構連線並支援您的完整遷移路徑，無論是擴充還是取代傳統服務。Cloudflare 使用基於「輕邊緣/重雲端」理念的架構來提供網路和安全服務。使用 Cloudflare Magic WAN，促進分支辦公室、零售地點或工廠車間等網路位置之間的網站到網站連線。它可為您的整個企業網路提供安全、高效能的連線和路由，從而降低成本和營運複雜性。為了安全起見，Cloudflare Magic Firewall 與 Magic WAN 無縫部署在一起，讓您能夠在流量通過 Cloudflare 的網路傳輸時強制執行網路控制原則，無論是南北向還是東西向。

## 保護面向公眾的基礎架構

企業網路和 DMZ 可定址並暴露於網際網路，因此，需要採取措施來阻止攻擊者造成傷害。在一個理想的世界中，傳統網路防火牆可以檢查並丟棄所有不需要的流量，但每個防火牆的處理能力都是有限的（可用的頻寬、使用率/運算、工作階段計數等）。攻擊者能否得逞只是規模的問題，即攻擊者能否產生足夠的雜訊來壓垮公司在不同的網路通訊協定層中運作的能力。

不只是流量。接受輸入流量會向未經驗證/預先驗證的流量打開攻擊面。甚至在系統上沒有帳戶的攻擊者也可以利用應用程式和作業系統中的缺陷。憑證填充（即使用從其他洩漏事件中獲得的已知使用者名稱/密碼登入）也是一個重大的風險來源。透過將 Zero Trust 原則套用至 DMZ 中的應用程式，組織可以減少網際網路暴露，並在可能的情況下消除這種暴露。

組織可以透過套用縱深防禦來吸收組織面向公眾的基礎架構上游的惡意流量，從而改進網路保護。透過 Cloudflare Anycast 網路部署且內建了 Magic Firewall 的 Cloudflare Magic Transit 充當組織的前門，可篩選掉不必要的惡意流量，僅提供乾淨的輸入流量。

當網路防火牆在設備上執行 DDoS 緩解時，它仍然必須先處理連線，然後才能斷開連線。使用 Cloudflare，我們的網路會廣播客戶的首碼，從而吸引原本會流向周邊防火牆的流量。憑藉 Anycast，我們透過在所有資料中心之間分配負載，有效緩解了 DDoS 攻擊。殭屍網路的成員可看到最近的 Anycast PoP，它根據 Magic Transit 和 Magic Firewall 原則處理流量。

## 簡化企業網路

簡化帶來了很多現代化優勢。如果 IT 團隊在設計時減少要分解的組成部分，則可以提升網路可靠性，而對存取權限採用 Zero Trust 拒絕全部的方法，則可以提高網路安全性。

若要簡化網路，請考慮：

### 從 DMZ 遷移

網路 DMZ 是一個令人頭疼的運作難題，因為它們對 zero-day 漏洞利用特別敏感。攻擊者無需存取內部網路即可與 DMZ 中的伺服器通訊，因此，組織必須保持警惕以防止利用和濫用。

然而，儘管 DMZ 在過去發揮了重要作用，今天還需要它們嗎？DMZ 作為一種網路建構的重要性不斷下降，因為可以採取替代方式來構建和託管應用程式。

- 對於面向公眾的應用程式，將工作負載遷移至公有雲端在經濟和技術方面均有優勢。
- 使用 SaaS，很多類型的面向公眾和私人應用程式根本不需要在客戶管理的基礎架構上執行。

因此，從安全和網路設計角度來看，開始思考如何減少或消除對 DMZ 的需求是很實際的。不僅從運作的角度來看是有意義的，消除網路基礎架構（例如，防火牆、WAF 和提供支援的負載平衡器）還能大大簡化架構。

為了將存取權延伸至員工、合作夥伴和承包商而部署在 DMZ 中的私人應用程式呢？將其隔離在私人網路中，並使用 Zero Trust 網路存取將存取權延伸至員工及合作夥伴，這會更加安全。

使用ZTNA，您可以透過消除應用程式的輸入網路流量，來有效地減少攻擊面。ZTNA 透過 Cloudflare 的全球連通雲，對資源進行基於上下文的代理存取，不僅消除了在網路防火牆中開啟連接埠的需要，同時還可讓安全團隊完全瞭解哪些人員可以存取哪些資源。

### 使用 ZTNA 取代 VPN

使用 VPN 存取應用程式的日子越來越少。從網路設計的角度來看，讓使用者透過一條非常長的通道來存取網際網路和雲端是不切實際的。而透過 VPN 將使用者（以及有可能遭入侵的端點）置於網路上也是一種重大的安全風險。

應用程式存取並不是 VPN 的唯一功能。在某些情況下（例如，端點管理和伺服器發起的通訊），組織需要與端點進行更廣泛的網路連線。以往，這些使用案例利用 VPN 在兩個方向上的網路連線，難倒了市場上的早期 ZTNA 產品。由於沒有替代方案，組織同時執行 ZTNA 和 VPN。

若要實現網路基礎架構現代化，組織可以使用 Cloudflare 的 ZTNA 來整合功能。這是因為使用 Cloudflare，組織可以同時支援經典 ZTNA 使用案例以及伺服器發起的雙向流量。這些功能可幫助組織透過消除 VPN 來使應用程式安全有效地存取所需資源，並進一步提升安全性和簡便性。

### 消除對 LAN 的信任升級

由於混合式工作，人們不管是在辦公室還是在任何其他地點，其工作方式都相差不大。實際上，當使用者經常在咖啡店和共用工作區中不受信任的公用網路上工作時，尤其如此。

在某種程度上，開放的公用網路就是 Zero Trust 的體現——既沒有人有特殊權限存取，也沒有人或事物是值得信賴的。如果原則上可以在共用工作區、家庭辦公室和咖啡店中工作，為什麼不能也消除企業網路中的信任呢？

消除信任並不需要推進網路設計，而是簡化它。與其為經過驗證的使用者建立升級的存取權並使用網路原則開啟與資源的連線，假定整個網路都不可信反而安全得多。採用透過 SASE 表示的安全性，組織可以存取所需的應用程式，並具有適當的安全性來確保安全，且無需對網路本身進行任何信任假定。Zero Trust 並不是向網路增添信任，而是除去信任，我們移除過去的明確權限和過度權限，達到一個更好更安全的狀態。

### 加速併購活動的連線

組織使用併購作為工具來獲取原本無法立即使用的業務資源和功能。為了利用機會，組織必須快速執行，讓合併後的公司優於其各部分的總和。然而，IT 往往無法快速移動，因為兩個組織的應用程式和基礎網路基礎架構很少能夠輕鬆地結合在一起。

為了加速併購的連線，組織可以將應用程式存取作為一項獨立於網路整合的任務來處理。設計一個融合網路架構的時間表可能長達數年，但應用程式存取不必依賴於如此遙遠的里程碑。

這是因為第一天的情況實際上就是一個 Zero Trust 使用案例，即不受信任的網路上的受信任使用者仍然需要存取應用程式。使用 Cloudflare One 擴展存取，它可提供實現併購連線的方法，而無需以融合網路存取為條件。

## 連線並保護您的雲端

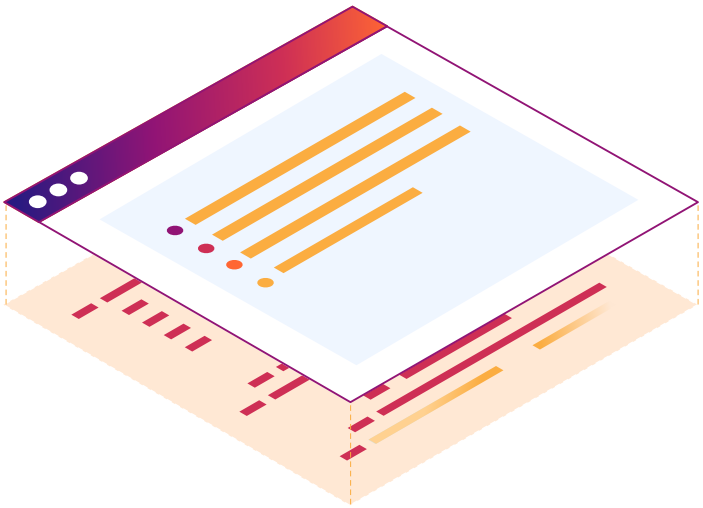
隨著雲端開發的發展，在一個雲端中重新利用另一個雲端中的元件將大有助益。正如每個組織都會隨著時間的推移變成多雲端一樣，每個組織也都會隨著時間的推移而變得需要管理公有雲端網路。應用程式開發往往是部落性的，在組織的不同部門中，DevOps 更偏好他們最熟悉的工具。然而，開發組織功能來管理不同雲端間的連線是非常複雜的，因為工作所涵蓋的工具集基於完全不同的架構而構建。

多雲端複雜性的另一個方面是混合雲端領域。混合雲端混合了內部部署私人雲端和虛擬私人雲端。這些網路有時使用專用網路（如，AWS Direct Connect）構建，不僅成本很高，而且僅限於一個雲端。在組織構建多雲端應用程式時，他們未必想要為每個雲端承擔專用網路的費用。

請使用 Cloudflare 來協調並連接公有雲端網路服務，而不是直接為一個又一個應用程式構建網路和安全性。我們認為，Cloudflare 的全球連通雲在這樣一種架構中發揮著完美的作用，它是透過廣泛的 Cloudflare 網路在雲端之間傳輸流量的理想場所。隨著公有雲端網路管理功能的增加，現在，客戶還可以透過 Cloudflare 協調工作負載連線的設定。

我們的公有雲端網路不僅僅協調基礎管道。我們的架構還提供開發人員服務，用於構建及整合多雲端應用程式。這款開發人員平台提供一個豐富的基礎技術生態系統，它基於開放原始碼和開放標準而構建。您可以選擇使用這款開發人員平台的所有元素，也可以僅使用您選擇的部分，而不必受限於指定雲端中的特定服務。

# 後續步驟



若要採取網路現代化旅程的後續步驟，請聯絡 Cloudflare，讓我們來幫您制定策略。我們與成千上萬名客戶密切合作，幫助他們將架構轉換到了 Cloudflare 的全球連通雲。

**如需詳細資訊，**
**請造訪 http://www.cloudflare.com/zh-tw/**

CLOUDFLARE



**+ 886 8 0185 7030 | enterprise@cloudflare.com | cloudflare.com/zh-tw**

REV:BDES-5483.2024JAN30