解決方案概述

強化混合雲與多雲的邊界防護，推動數位促進

執行摘要

數位促進（Digital Acceleration，DA）的目的就是要讓各種規模組織和各類不同部門，達到提高生產力、提升運作速度，及改善成本結構。藉由雲端及遠端作業是讓客戶、合作夥伴和員工能夠從任何位置存取應用程式和資料，是推動數位促進的關鍵能力，組織會利用公有雲、私人雲及虛擬分點等策略，來完成他們的 IT 推動計畫。

除此之外，大多數組織會在虛擬分點部署 SD-WAN（軟體定義廣域網路），而也有某些組織會使用虛擬平台來達成這個目的。

超過 76% 的組織機關部署了混合雲或多重雲方案[1]

由於雲端、遠端工作，及虛擬平台市場應用的成長快速，網路安全所面臨的挑戰也與日俱增，並且遍佈在不斷擴張的攻擊面上。組織必須跨雲端網路架構建立適當的安全狀態監控，才能降低資安風險、確保規範，並提升靈活性。

FortiGate-VM 能提供完整的雲端網路安全性

在雲端、虛擬資料中心和虛擬分部的「IT 架構」和「應用程式」部署經常會受到外部攻擊和內部威脅的影響。若缺乏有效的威脅防護，組織就必須面對財務衝擊和名譽損傷的風險。而不完整的解決方案和單一性產品也會成為組織的挑戰，並因此產生資安落差且提高風險。

無論是橫跨地端，還是在雲端，若要確保企業應用程式和資料的安全，網路防火牆始終是最有效的工具。防火牆可以降低部署複雜度以及成本，同時需要相關技能來有效率地提供有效的安全狀態。

Fortinet FortiGate-VM 虛擬次世代防火牆是架構在 FortiOS 資安網路作業系統上，這和硬體式的 ForitGate 防火牆使用相同作業系統，它能提供企業等級安全在可以擴充至整個攻擊面，包含有效保護公有雲與私人雲、虛擬資料中心，以及虛擬分點。

進階功能

整合式的安全性與網路功能

FortiGate-VM 透過高效能的次世代資安防火牆來保護網路和應用程式，並提供進階路由功能，藉以部署任意規模的安全網路，同時還支援 SD-WAN 以智慧方式控制應用程式流量，進而改善終端使用者的體驗。只需要單一FortiGate-VM，就能提供這些先進的功能。

進階防護

網路威脅型態不斷進化，攻擊方式也越來越複雜。為了對抗這些威脅，FortiGate-VM 會利用人工智慧（AI）和機器學習技術來阻止進一步的攻擊，其技術來自於 FortiGuard 全球威脅情資。

自動化

為了讓營運團隊更加靈活，FortiGate-VM 支援自動化功能。方法是透過雲端專屬範本工具，以及非雲端的第三方架構。IT 團隊可以快速部署網路安全設施，輕鬆調整營運規模，並整合至開發維運（DevOps）流程當中。

使用案例

虛擬資料中心與私人雲的安全性

大多數的組織正逐漸將傳統資料中心轉型為虛擬資料中心或私有雲，他們會使用軟體定義網路（Software-Defined Networking，SDN）、遠端員工以及虛擬桌面基礎架構（Virtual Desktop Infrastructure，VDI）。但使用這些技術會產生新的資安挑戰。

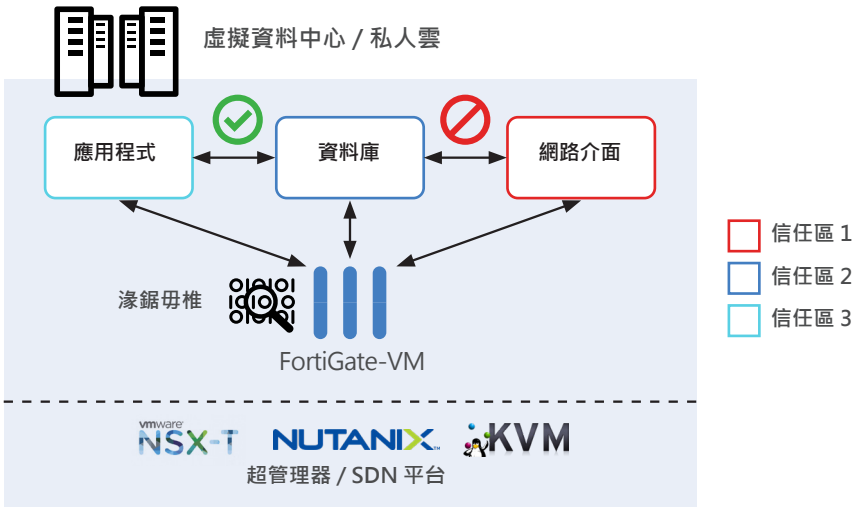


圖 1：東西向工作負載防護

VMware NSX 與 Nutanix Flow 之類的 SDN 環境不只會用在虛擬網路上，有時還會用來對虛擬工作負載進行微隔離。這種用途並不常見，而威脅可能會隱藏在信任區所允許的流量當中，且可能導致攻擊產生橫向傳播。FortiGate-VM 支援這些 SDN 平台的服務鏈整合，讓你能靈活加入各種進階資安服務，像是 IPS、AMP、沙盒、AV 或 DNS 防護，並在微隔離之間對通過的流量進行檢查和防護，保護東西向之間的邊界。

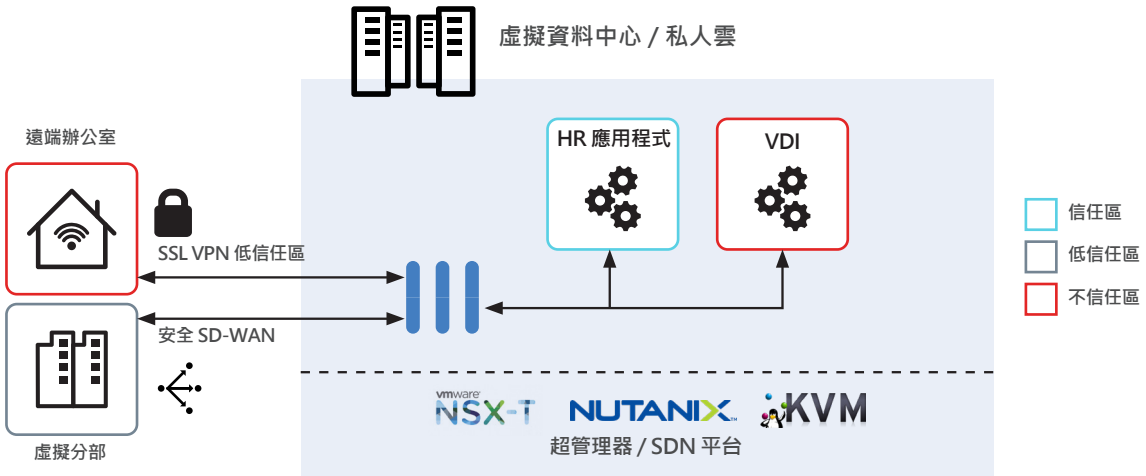
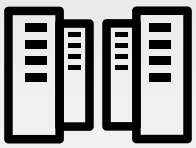


圖 2：安全存取與切分。

現今的組織尋求無論從何處來的使用者都能安全存取 IT 應用程式而採用了 VDI 遠端工作模式，這會讓網路流量很可能會來自未受控管或由使用者控制的裝置，並直達 IT 資料中心核心，為威脅發動者帶來暴露漏洞的機會，並攻擊其他敏感的工作負載。FortiGate-VM可以用來分隔進出這些位置的流量，並將其移入信任區，以避免威脅擴散。從這些位置來的網路流量或許已經經過了網際網路和其他不安全的網路。FortiGate-VM 支援 SSL-VPN，讓遠端員工可以安全連線，並同時支援安全 SD-WAN 連線，讓你可以安全地連線至虛擬分部位置，藉此提升安全性和應用程式效能。

部署多部 FortiGates 裝置時，可以透過 FortiManager 來整合虛擬和實體防火牆原則的架構，藉以簡化網路安全的部署和營運難度。



超超過 67% 的組織機關 持續將超過 50% 的工作負載於橫跨地端的資料中心運行。[2]

雲端連線防護

許多組織正在將需要全球存取或彈性調整規模的特定應用程式轉移至公有雲上。但他們也必須為存取這些雲端應用程式的工作負載提供安全的連線方式。雲端服務供應商會透過 VPN閘道，將使用者的流量導入其虛擬私人雲（VirtualPrivateClouds，VPC；或是 VNet）。但這個方式有許多限制。

一般來說，組織會使用不同的橫跨地端 VPN 設備，若再加上雲端服務供應商的閘道，就會大幅增加管理複雜度。此外，雲端服務商會針對 SSL VPN 給予完全不同的服務。雲端 IPSec VPN 閘道同時也有頻寬限制，這點對許多大型企業來說相當不切實際。

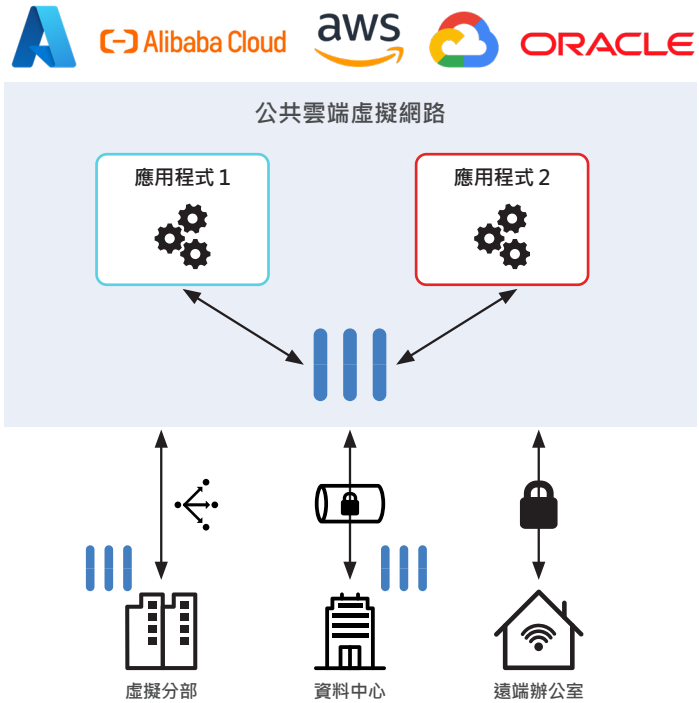


圖 3：公共雲連線防護。

FortiGate-VM 可以用來降低連接至公共雲的複雜度，只要同時在虛擬分部和 VPC 或 VNet 當中使用 FortiGate-VM 就能達成。此外，FortiGate-VM 還能為遠端使用者提供 SSL VPN 連線、從資料中心透過 IPSec VPN 連線，以及為各地分部提供 SD-WAN 連線。FortiGate-VM 有不同規格，可以擴充 IPsec 頻寬，也能使用雲端服務供應商的負載平衡器來擴充 SSL VPN 的存取能力。提供高效能連線重要關鍵，FortiGate-VM 能確保公有雲連線的安全與穩定。

公有雲的安全性

組織在雲端轉型的擴張階段時，會啟用許多虛擬網路（VPC），某些組織甚至達到數百個 VPC 的程度。他們同時會面對網路路由以及安全性的問題。VPC 數量和雲端工作負載越高，就代表更多風險和漏洞。只要在工作負載和 VPC 之間缺乏存取控制權，就有可能會導致橫向攻擊和資料外洩。

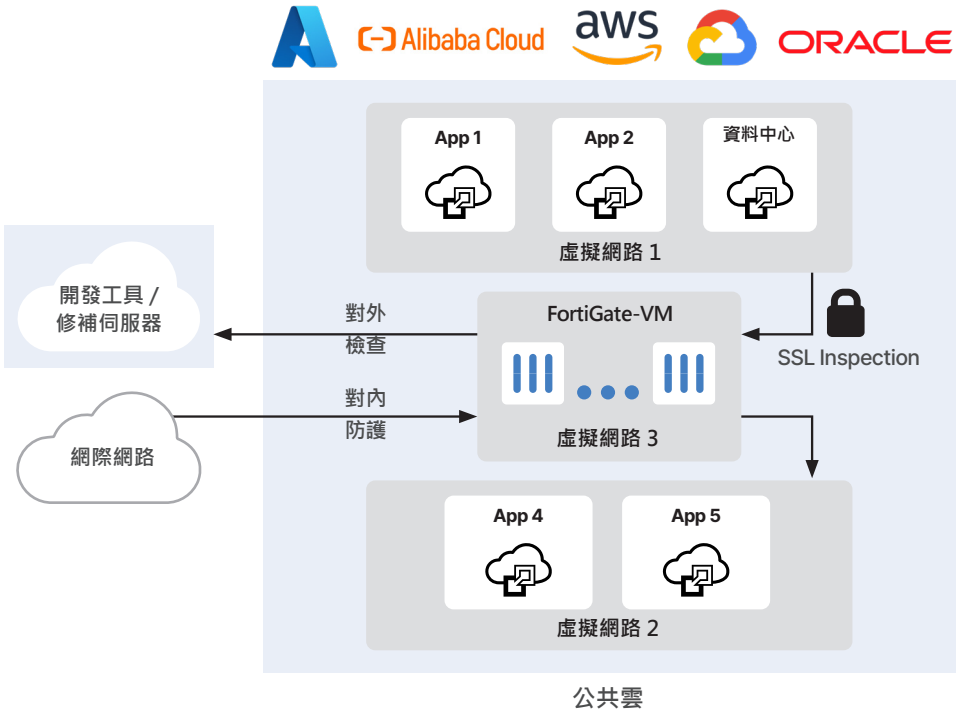


圖 4：確保公共雲邊界安全

FortiGate-VM 可以在應用程式工作負載流量當中具有深層的可視性，藉以確保合乎 IT 與法規的規範。在許多狀況中，應用程式工作負載會存取開發工具，像是 GitHub 與修補伺服器，以取得作業系統和應用程式更新。FortiGate-VM 可以使用 URL 過濾來檢查並控制向外的流量。這些雲端應用程式會由不同類型的使用者從許多地方存取，而 FortiGate-VM 支援進階安全功能，像是 IPS、沙盒、惡意軟體防護（Anti-Malware Protection，AMP），以及病毒防護（Anti-Virus，AV），以防護來自網際網路各處發動的外部惡意攻擊。

那些部署大規模雲端的組織，或許會想要集中管理安全性檢查和 VPC 之間的路由方式，來簡化資安營運，並更有效率地套用《Gartner® Critical Capabilities》中的規範與政策。透過支援 BGP 路由和進階威脅防護，FortiGate-VM 可以部署為高可用性模式，而且只需要一台稱為資安服務中心（Security Services Hub）的中心化 VPC，藉此簡化網路架構，並提供公共雲企業級的安全性。

Fortinet 在 2022 年公共雲端使用案例獲得網路防火牆項目第 2 名[3]

多雲安全性

轉移至多雲時，也要面對技術上的挑戰，尤其是路由和應用程式流量的安全性。而且必須考量每個雲、雲端內部，以及跨雲端之間這幾個層面。組織也會需要為橫跨地端位置，像是分點、資料中心，以及遠端員工提供高速連線，以便供應最佳的應用程式體驗。但在此同時，組織也需要降低營運成本和管理複雜度，方法是運用本方案，來排除多且雜亂的雲端服務商控制台的需求與多雲部署衍生出的重要挑戰，避免在雲端部署和橫跨地端位置時，分散的網路架構和資安政策。

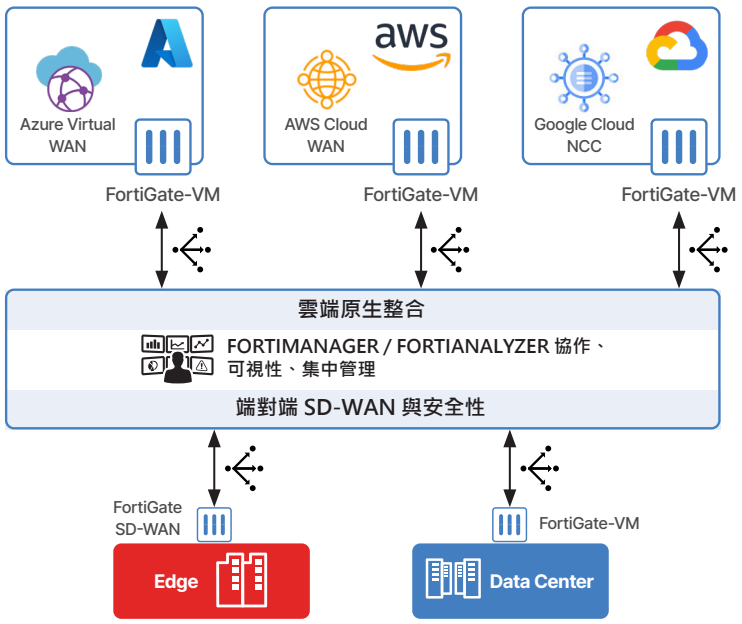


圖 5：安全多重雲端 SD-WAN。

FortiGate-VM 提供 SD-WAN 連線能力，以及持續為橫跨多雲和虛擬資料中心的威脅提供可視性。FortiGate-VM 支援的安全多雲 SD-WAN 功能，緊密整合了雲端的原生網路管理服務，像是 Azure Virtual WAN、AWS Cloud WAN，以及 Google Network Connectivity Center，讓 IT 團隊可以對流量路由橫跨地端位置，以及至各個雲端 VPC 和 VNet 的設定進行簡化。SD-WAN 覆蓋網路可以用來連接雲端之間的應用程式工作負載，並讓它們的網路政策更加一致，提供更好的應用程式體驗。FortiGate-VM 也可以在多雲上部署為防火牆織網的一部份，藉以執行一致的資安政策，並建立有效的安全狀態。

單一平台管理與分析

不同的單一性產品會導致管理控制台大量增加，並對管理和營運造成嚴重負擔。組織不斷在尋求整合式管理方案，讓他們有辦法建立一體適用的資安政策、於橫跨地端和雲端部署的安全性上取得一致，並在雲端系統之間能持續保有可視性。

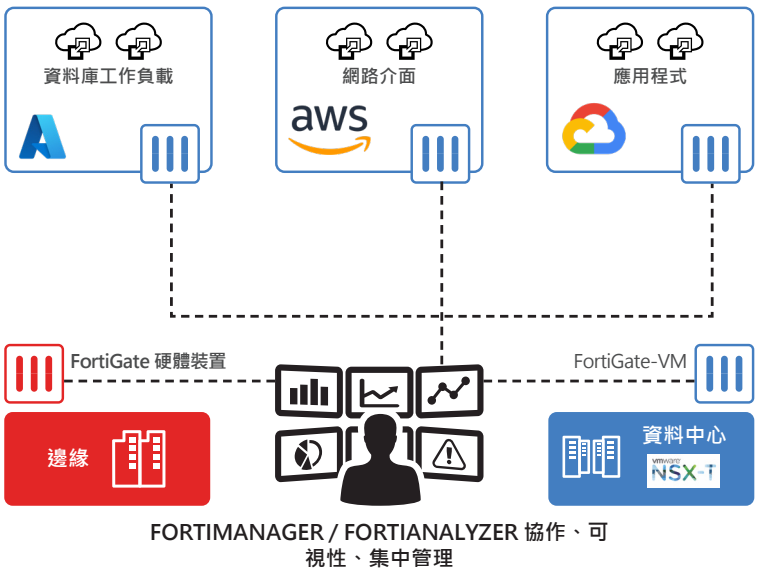


圖 6：單一平台管理

FortiManager 提供單一平台管理方式，可以在 FortiGate-VM 和實體 FortiGate 上定義資安政策，簡化雲端、虛擬 / 實體資料中心，以及分部位置的資安管理。FortiManager 也支援織網連接器透過 API 來整合雲端服務供應商與 SDN 平台管理工具。透過這些整合方式，FortiManager 便可以用來在多雲部署中協作資安政策。FortiAnalyzer 可為網路營運中心團隊提供重要的網路分析和監控。其可以從 FortiGate-VM 與實體 FortiGate 多重部署當中持續取得可視性，包括雲端和橫跨地端位置。組織即可藉此簡化雲端網路的管理與營運。

總結

透過 FortiGate-VM 解決方案，組織可以應用混合雲與多雲系統，同時避免提高複雜度。組織可透過公有雲和虛擬資料中心環境快速進行創新，且不須承擔風險或影響規範等問題，IT 團隊也可以為遠端員工、合作夥伴和客戶提供更好的應用程式體驗。

FortiGate-VM 的關鍵優勢

- 減少部署與營運複雜度，可透過持續為各種不同環境提供防護以及中心化管理來達成。
- 完整發揮雲端與 SDN 的投資效果，FortiGate-VM 整合了雲端供應商服務與 SDN 平台。
- 透過基礎架構的水平和垂直擴充，提供更高的頻寬，藉以改善終端使用者的應用程式體驗。
- 使用雲端式隨選消費服務，並為虛擬資料中心與虛擬分部部署提供動態調整平衡。

[1] "State of the Cloud Survey," HashiCorp, August 21, 2020.

[2] "2021 Cloud Security Report," Cybersecurity Insiders.

[3] Adam Hils, Rajpreet Kaur, "Critical Capabilities for Network Firewalls," Gartner, January 17, 2022. Gartner 並不替其研究出版品中提及的任何廠商、產品和服務 背書，也不建議技術使用者只選擇分數最高的廠商或其他指定項目。Gartner 研究出版品中包括了 Gartner 研究和諮詢組織的意見，其不應被解釋為事實的陳述。Gartner 不對此研究做出任何明示或暗示的擔保，包括任何對商品適售性或特定用途的適用性擔保。GARTNER 是 Gartner, Inc. 與相關組織在美國與國際的註冊商標和服務商標，且經允許用於此處。版權所有，侵權必究。

FORTINET

www.fortinet.com/tw

April 19, 2022 10:21 AM

1525370-0-0-EN