VMware 服務定義的防火牆

使用專門建置的內部防火牆，保護您的分散式資料中心

概觀

VMware 服務定義的防火牆是一種分散式的水平擴充*內部防火牆*，其使用基礎架構的原生安全性來保護所有東西向流量，進而大幅簡化安全部署模型。

主要優勢

- 降低風險 – 運用基礎架構內建的唯一防火牆，避免攻擊者在多雲環境中橫向移動。
- 確實達到合規 – 透過輕鬆建立虛擬安全性區域，以及針對敏感應用程式和資料的完整第 7 層安全性涵蓋範圍，即可證明其合規性。
- 加速安全性作業– 安全性跟上開發的速度，在內部部署實現擺脫實體基礎架構限制的真正公有雲體驗。
- 簡化安全性架構 – 不需要重新設計網路、流量回流或管理代理程式，大幅簡化網路部署與運作。

現代化分散式應用程式需要全新防禦功能

在瞬息萬變的世界中，企業需要以更好的方式防禦不斷增加的動態工作負載，以及相對應的大量東西向 (內部) 網路流量，進而抵禦網路攻擊。傳統的應用裝置型安全性解決方案不再足以保護當今的應用程式，而專為南北向流量設計的週邊防火牆也未能有效達到動態工作負載所要求的控制能力與效能。現在改用*內部防火牆*，用分散、精密的強制執行方式保護東西向流量，同時降低營運成本與複雜度。

內部防火牆內建於基礎架構而非外加

*VMware 服務定義的防火牆*是一種分散式的水平擴充內部防火牆，其使用基礎架構的原生安全性來保護所有東西向流量，進而大幅簡化安全部署模型。內含一個分散式防火牆、一個*入侵偵測系統與入侵防禦系統* (IDS/IPS)，以及透過 *VMware NSX® Intelligence™* 執行的深入分析工具 (參見圖 1)。透過服務定義的防火牆，安全性團隊可保護品牌避免遭受內部威脅，並且將網路攻擊突破傳統網路週邊所造成的損害降至最低。

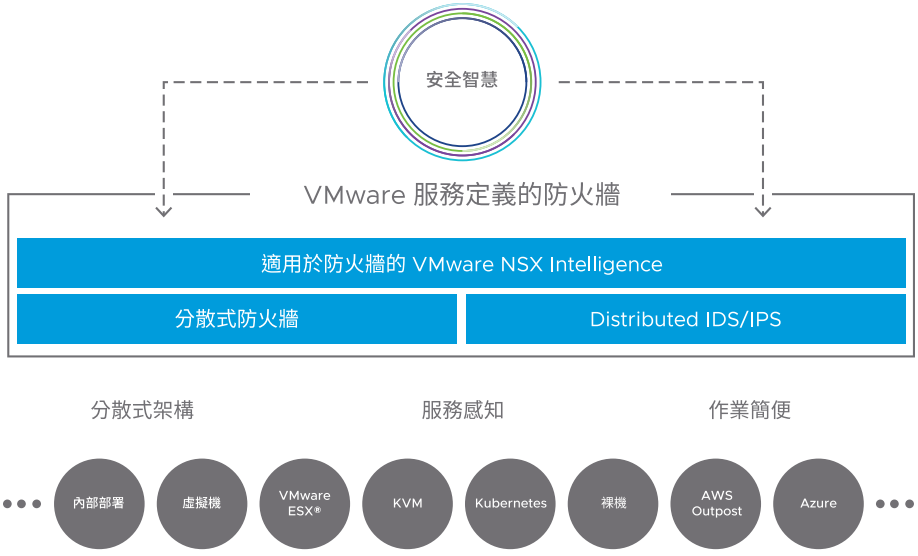

圖 1：VMWARE 服務定義的防火牆架構。

使用情境

- 快速部署網路區段 – 完全在軟體內定義，可用有彈性的方式快速建立及重新設定網路區段、虛擬安全性區域或合作夥伴網域。
- 避免攻擊進行橫向移動 – 涵蓋至第 7 層的具連線狀態防火牆層，包括應用程式識別和使用者識別原則，加上進階威脅防護功能，大大保障東西向流量的安全性。
- 滿足合規需求 – 透過檢查所有流量，符合法規需求。透過軟體內的分散式入侵偵測系統/入侵防禦系統消除盲點，整個涵蓋範圍一覽無遺。
- *微分段*實現零信任 – 在多雲環境的應用程式、服務與工作負載之間，輕鬆建立、強制執行及自動管理精密的微分段原則。

深入瞭解

查看以下資源，深入瞭解內部防火牆如何保護現代化分散式應用程式：

- 閱讀 *VMware 服務定義的防火牆*。
- 造訪 *VMware NSX Data Center 產品頁面*。

如需瞭解詳細資訊，請洽詢您的 VMware 業務代表。

主要功能

分散且精密的強制執行

服務定義的防火牆以分散、精密的方式強制執行安全性原則，將保護力與控制力往下延伸至工作負載層級。

延展性與總流量

服務定義的防火牆具有分散的特性，因此擁有彈性，可隨著工作負載加速或減速進行自動調整。

應用程式內能見度

服務定義的防火牆自動判定工作負載與微服務之間的通訊模式，根據該等模式提出安全性原則建議，以及檢查該流量是否遵守已部署的原則。

宣告式 API

透過服務定義的防火牆，安全性團隊可跟上開發速度，在內部部署實現真正的公有雲體驗。API 導向的物件型原則模型確保新的工作負載自動繼承相關安全性原則。

集中化管理

集中定義安全性原則後散佈至整個網路，無論工作負載何時建立或除役，都可由服務定義的防火牆自動調整原則，無需人工介入。

基礎架構的原生安全性

外加式的安全性解決方案無法提供當今安全性團隊所需要的延展性、靈活性和成本效益。VMware 服務定義的防火牆是唯一安全性原生於基礎架構的解決方案，具有分散、服務感知和作業簡便的特性。有了 VMware 的內部防火牆，資訊安全長及其團隊便能降低風險、確認合規性，並且跟上開發速度。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com
11073 台北市信義區松仁路 100 號 38 樓之一台北南山廣場辦公大樓 電話 +886-2-3725-7000 傳真 +886-2-3725-7010 www.vmware.com/tw

文件編號：516912aq-so-svc-dfnd-fw-uslet-Final_ZHTW 4/20