VMware NSX Distributed IDS/IPS

使用進階威脅偵測強化 VMware 服務定義的防火牆

概觀

VMware NSX® Distributed IDS/IPS™ 提供一款軟體架構 IDS/IPS 解決方案，可協助安全性操作人員符合法規、建立虛擬區域，並偵測東西向流量的橫向移動威脅。

主要優點

- 彈性的總流量 – 檢查能力可隨同每個工作負載自動調整，繼而消除硬體瓶頸。
- 簡化網路架構 – 採用完整的分散式架構，不僅無需透過回流傳輸將流量傳送至集中式應用裝置，還可減少網路壅塞現象。
- 減少誤報 – 根據精準的應用程式情境來運用精選規則集，並提高簽名的逼真度相符，進而實現更多零誤報工作負載。
- 提高容量使用率 – 重複使用現有閒置運算容量，免除使用專屬應用裝置的必要性。

東西向流量偵測需求正不斷成長

隨著分散式應用程式與微服務崛起，內部網路流量正主導傳統的南北向流量。在此同時，資料中心邊界也充斥著邊緣與雲端應用程式，以及終端使用者裝置。今日的攻擊者不僅察覺到上述變化，更學習從原始攻擊點來積極橫向移動。正因如此，使用進階威脅偵測功能檢查東西向 (伺服器對伺服器) 流量，已成為保護工作負載與企業資料的重要關鍵。

分散式 IDS/IPS 可解決傳統安全性面臨的折衷取捨

VMware 服務定義的防火牆可提供市面上唯一一款專為保護東西向流量所建置的內部防火牆。其可將整個安全性堆疊虛擬化並散發至每個工作負載中，同時提供豐富的防火牆功能，包括第 4 層存取控制與具狀態的第 7 層網路控制能力。現行的服務定義的防火牆功能皆納入入侵偵測系統與入侵防禦系統 (IDS/IPS)。

IDS/IPS 早已成為網路安全性堆疊的標準功能。然而，從企業周邊連往公共網路，或位於符合法規區域邊界的特定網路分段，卻在成本與作業複雜性的限制下，無法充分運用 IDS/IPS。

VMware NSX Distributed IDS/IPS 可提供全新架構，一舉解決過去無法兼顧安全性涵蓋範圍與作業複雜性的兩難局面。VMware NSX Distributed IDS/IPS 採用全軟體方式，可將流量檢查功能移至每個工作負載中，並免除回流傳輸至離散應用裝置的必要性。在每個工作負載中部署與管理 IDS/ IPS 功能所帶來的作業簡便性，有助於實現不含盲點的全方位涵蓋範圍。

產品概觀

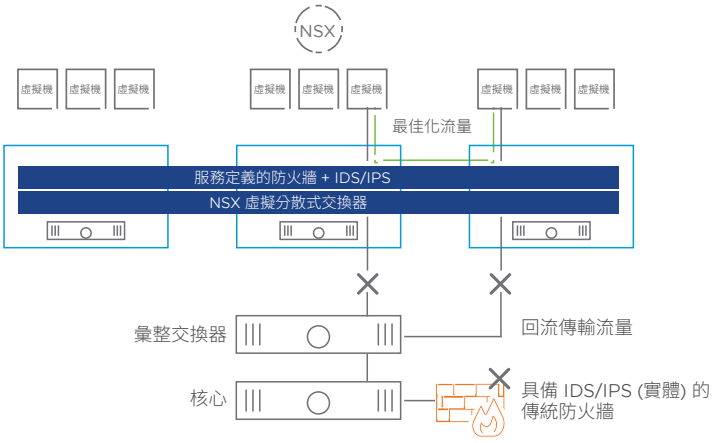

圖 1：NSX Distributed IDS/IPS 可避免流量發生回流傳輸。

使用情境

輕鬆符合法規要求 – 只要部署軟體，就能啟動敏感應用程式的流量檢查功能，無需購買昂貴的應用裝置。

虛擬化安全區域 – 為內部團隊與合作夥伴建立及自訂多個虛擬安全性區域，無需實際隔離網路。

取代各自為政的應用裝置 – 運用 NSX 的原生 IDS/IPS 功能來取代傳統的 IDS/IPS 應用裝置，以降低成本與複雜性。

偵測橫向移動威脅 – 使用以簽名為基礎的技術、異常偵測與通訊協定符合性檢查，檢查每個工作負載的東西向流量。

深入瞭解

如需 NSX Distributed IDS/IPS 的詳細資訊，請與您的 VMware 業務代表聯絡，或參閱以下資源：

- 深入探索 NSX Distributed IDS/IPS 的技術詳細資訊：vmware.com/tw/products/nsx-distributed-ids-ips
- 閱讀 VMware 服務定義的防火牆：vmware.com/tw/security/internal-firewall
- 造訪 NSX Data Center 網頁：vmware.com/tw/products/nsx
- 深入瞭解如何使用 NSX Intelligence™ 進行自動化原則探索：vmware.com/tw/products/nsx-intelligence-analytics-engine

NSX Distributed IDS/IPS 為應用程式感知流量檢查引擎，旨在分析內部的東西向流量，並偵測橫向威脅移動。這款引擎可在虛擬化管理程序中執行，以便將封包檢測最佳化。NSX Distributed IDS/IPS 結合領先業界的簽名集、通訊協定解碼器與異常偵測等機制，可找出流量中的已知與未知攻擊。此外，其也受惠於豐富的應用程式情境，能大幅降低誤判率，而且只會對主機帶來最低限度的運算額外負荷。

主要功能

分散式分析

IDS/IPS 引擎會分散至每個工作負載，以消除盲點，同時確保簡單的作業模式。這個檢查功能會按工作負載數量以線性比例調整，幾乎可以完全消除各自為政的應用裝置常見的總流量限制。

依據情境精選簽名分送

管理平台會依據對執行中應用程式的認知，僅啟用與每個工作負載相關的威脅簽名來進行評估。這可降低主機上的運算額外負荷，提高逼真度相符並降低誤判率。

應用程式情境導向威脅偵測

IDS/IPS 引擎可充分瞭解每台主機上的執行中應用程式，因此無需猜測來源或目標應用程式情境。這樣一來，就能更清楚分類警示，操作人員也可以排定這些警示的優先順序，以便進行更進一步的調查。

原則與狀態行動化

當工作負載移動時，原則與狀態也會隨之移動。工作負載可於新的位置自動受到保護，既不必手動設定，也不會遺失流量。

自動化原則生命週期管理

NSX 原則模式可自動為新的工作負載建立安全性原則，並於工作負載除役時淘汰舊的原則。已部署工作負載的安全性原則會保持一致，以避免發生累積大量過時安全性原則的情況，而這也是傳統網路安全性應用裝置面臨的常見挑戰之一。

延伸固有安全性

NSX Distributed IDS/IPS 可透過新增威脅偵測功能，延伸服務定義的防火牆的固有安全性方法。其運用服務定義的防火牆的基本原則，將安全性建置於基礎架構中，並將其散發至每個工作負載，藉此提供無所不在且垂手可得的安全性。NSX Distributed IDS/IPS 受惠於虛擬化管理程序與網路虛擬化層所提供的獨特應用程式情境，可讓提高偵測威脅的精準度、效率與更靈活性。

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