白皮書–2019 年 12 月

VMware NSX Distributed IDS/IPS

新的東西向安全性典範

vmware®

目錄

入侵偵測系統 (IDS) 誕生於 1990 年代後期，可用來偵測代表攻擊傳入的流量模式。在 2000 年初期，隨著 IDS 開始加入其他安全功能，入侵防禦系統 (IPS) 也焉然成形。多年來，IDS/IPS 已成為網路安全性堆疊中的標準功能。但即便在上述歷史沿革下，特定網路分段 (例如使用公有網路且位於企業周邊的網路分段) 卻因成本與作業複雜性的限制，而無緣使用 IDS/IPS。

隨著分散式應用程式與微服務崛起，資料中心內的網路流量正大幅倍增。在此同時，資料中心邊界也充斥著連往公有雲與終端使用者裝置的大量應用程式連線。正因如此，IDS/IPS 也越來越適合做為資料中心的安全層。過去，IT 經常需要在成本、作業複雜性與安全性涵蓋範圍之間做出取捨，而本白皮書所探討的新 IDS/IPS 架構方法，將可改變此一情況。

透過 VMware NSX 享有固有安全性

固有安全性架構為 VMware 安全性策略的一大基礎。所謂的固有安全性，是指內建於基礎架構中、散發至 IT 環境內，且具備應用程式感知能力的安全性。VMware 服務定義的防火牆建置於 VMware NSX® 的第 2–7 層平台上，可做為資料中心內的固有安全性策略，協助作業人員同時保護跨不同多雲環境的東西向流量。

NSX[1] 可因應兩大基本資料中心使用情境，也就是網路虛擬化與東西向安全性。網路虛擬化會將流量管理與基礎實體網路管理加以區隔。東西向安全性則能使用虛擬化管理程序所具備的安全功能，透過以每一流量為基礎的精細度，為資料中心指定與施行安全性原則。只要將兩者結合運用，即可透過網路與安全性虛擬化實現彈性十足的資料中心網路設計，並同時兼顧固有安全性。

NSX 已將安全性內建於網路虛擬化基礎架構中。這表示，安全功能會與基礎架構如影隨形，無需個別部署。此外，由於安全性控制能力位於虛擬化管理程序內，無法進行竄改，如此一來，控制能力就能與攻擊目標 (例如工作負載) 加以分離。

NSX 採用分散式架構。負責施行安全性的控制能力會配置於每個工作負載的虛擬網路介面中，並提供精密的機制來控管流量。NSX 不會像集中式應用裝置一樣，只具備有限的安全性能力，而且，網路流量也不需要以人為的回流傳輸方式導向網路安全性堆疊。

另外，由於 NSX 已整合至虛擬化基礎架構中，因此能見度可涵蓋所有應用程式與工作負載。NSX 能運用此一能見度汲取豐富的應用程式情境、密切追蹤工作負載生命週期，並將安全性原則管理作業自動化。

Distributed IDS/IPS

VMware NSX Distributed IDS/IPS™ 功能可為服務定義的防火牆提供額外的流量檢查功能[2]。而 IDS/IPS 實作所依循的固有安全性原則，則與服務定義的防火牆毫無差異。正因如此，NSX Distributed IDS/IPS 也可發揮服務定義的防火牆所具備的多項優勢。

1. 為了方便說明，本白皮書假設將 VMware NSX-T™ 部署於 VMware ESXi™ 環境中。
2. VMware，《VMware 服務定義的防火牆解決方案概觀》。

IDS/IPS 基礎概念

IDS/IPS 功能的主力基礎，是負責偵測流量模式的規則運算式引擎。這些引擎歷經精心設計，能使用設定語言來尋找已知的惡意流量模式。網路與安全性操作人員可使用 IDS/IPS 設定語言做為簽名，以參照所顯示的模式。現行的多數 IDS/IPS，也會在以簽名為基礎的偵測機制之外實作多項安全性技術，例如通訊協定與連接埠符合性檢查，以及異常流量偵測。

IDS/IPS 會定期連接私有雲，以更新包含簽名在內的偵測資訊。威脅研究組織會追蹤最新的攻擊與弱點，以建立、測試與發佈這項即時串流資訊。

IDS/IPS 通常會透過專屬的獨立應用裝置實作，或做為防火牆的一部分。若為專屬的獨立應用裝置，IDS/IPS 將採網路嵌入形式，並於通訊協定堆疊的第 2 層運作。若做為防火牆的一部分，IDS/IPS 將檢查防火牆先前所允許的流量，並於通訊協定堆疊的第 3 層運作。

無論採獨立形式或整合於防火牆中，市面上的傳統 IDS/IPS 多為各自為政的集中式應用裝置。針對需要進行 IDS/IPS 檢查的網路，操作人員會將這些應用裝置放置在預先定義的少數位置上，並於這些位置之間進行回流傳輸。

NSX 中的 IDS/IPS：運作方式

NSX Distributed IDS/IPS 採用的引擎，源自於知名且廣受推崇的開放式原始碼專案，Suricata。NSX 會為 IDS/IPS 引擎提供一個包括網路 I/O 與管理功能的執行階段環境，以呼應 Suricata 的理念。

NSX 使用防火牆來進行 IDS/IPS 功能的主機代管，以構建用以檢查流量的單程設計。根據設定而定，所有流量都會先通過防火牆，再進行 IDS/IPS 檢查。上述搭配防火牆進行的 IDS/IPS 功能主機代管機制，也可簡化網路安全性原則的呈現與執行。

如同圖 1 所示，NSX Distributed IDS/IPS 引擎會配置於使用者空間內，並連接至虛擬化管理程序核心中的防火牆模組。應用程式會傳送流量至虛擬化管理程序，以便與其他應用程式通訊，此時，防火牆將會檢查流量。隨後，防火牆會將流量轉給位於使用者空間內的 IDS/IPS 模組。

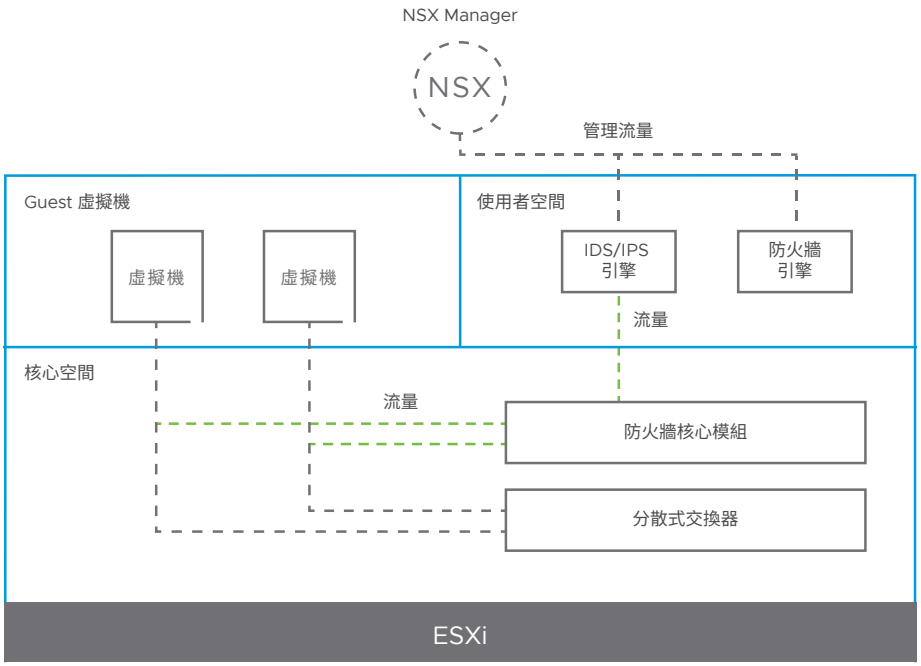

圖 1：NSX 中的防火牆與 IDS/IPS。

IDS/IPS 模組會使用簽名、通訊協定解碼器與異常偵測等機制，找出流量中的攻擊。如果未偵測到攻擊，就會傳回防火牆，以完成傳往目的地的後續傳輸作業。如果偵測到攻擊，則會產生警示並加以記錄。

位於流量接收端的目的地節點，也會執行類似的 IDS/IPS 檢查程序。不過，如果操作人員認為在目的地或來源之間擇一進行 IDS/IPS 檢查便已足夠，也可選擇略過目的地 (或來源) 的 IDS/IPS 檢查。

NSX Distributed IDS/IPS 的優勢

NSX Distributed IDS/IPS 採用的架構與傳統 IDS/IPS 大不相同。造成此一差異的最大來源，在於傳統 IDS/IPS 會使用各自為政的虛擬或實體應用裝置來集中執行檢查。相較之下，NSX 實作則採分散式做法，並完整整合至虛擬化基礎架構中：

- 實現流量最佳化 – 操作人員可搭配資料中心流入/流出點的防火牆部署 IDS/IPS，或將其部署在防火牆後方。需要進行 IDS/IPS 檢查的資料中心流量將被迫往返於集中式應用裝置之間，過程中將衍生回流傳輸模式，並耗用網路資源。NSX 可進行流量來源/目的地的 IDS/IPS 檢查主機代管 (如圖 2 所示)，不僅無需進行回流傳輸，還可簡化網路設計。
- 不會造成任何單一檢查瓶頸 – 在傳統 IDS/IPS 機制中，IDS/IPS 或防火牆應用裝置的檢查能力有限。操作人員需要不斷升級至最新一代的硬體應用裝置，才能提高檢查能力，此一過程不僅昂貴，也容易產生問題。NSX Distributed IDS/IPS 實作會使用伺服器的閒置容量來執行受保護的應用程式，並隨著新的工作負載加入進行線性擴充。因此，不僅不會發生單一檢查能力瓶頸，還可提供充分的檢查能力來因應資料中心流量。
- 完整涵蓋所有流量 – 迫於先前所提到的各項限制，網路與安全性操作人員經常必須選擇要進行 IDS/IPS 檢查的流量。許多時候，完成 IDS/IPS 檢查的流量僅佔防火牆整體流量的一小部分。或者，操作人員會將獨立式 IDS/IPS 配置於網路深處，以保護一小部分的伺服器，但此舉卻提高了網路設計的複雜性。在 NSX Distributed IDS/IPS 分散式實作中，您可將 IDS/IPS 檢查插入至每個工作負載的每個流量路徑中，繼而消除盲點。操作人員可精密控制每個工作負載的 IDS/IPS 功能設定，無需受限於底層網路架構。
- 提供依據情境精選與調整的簽名 – 傳統 IDS/IPS 會採集中模式，並配置於許多流量路徑中，往往需要啟用上千個簽章，才能一舉涵蓋所有流量。而所啟用的簽名數量與類型，則會大幅影響 IDS/IPS 的延遲情況與總流量效能。正因如此，操作人員需要花費大量的時間調整 IDS/IPS 簽名。相較之下，NSX Distributed IDS/IPS 實作則具備應用程式感知能力，可由 NSX 鑑藏每個工作負載的簽名。這樣一來，工作負載只需啟用一小部分的簽名，進而減少誤報情況。此外，IDS/IPS 引擎可修改核發給對應簽名的警示嚴重性，以因應應用程式情境與受保護工作負載的敏感性。舉例來說，信用卡資料庫的警示的矚目程度會比其他工作負載來得高。
- 工作負載行動化支援 – 在虛擬化資料中心內，工作負載可移至其他主機或資料庫 (透過 vMotion®)。傳統 IDS/IPS 無法直接且快速針對新的工作負載位置，重新設定安全性原則。而在 NSX 中，安全性原則可隨著工作負載的虛擬機 (VM) 一同移動。因此，無論將虛擬機移往何處，往返該虛擬機的流量都會受到保護。此外，由於 NSX 可將流量順暢傳送至新的位置，因此，移動期間既不會遺失流量，也不會中斷連線。

- 自動化原則生命週期管理 – 傳統 IDS/IPS 無法感知所保護應用程式的生命週期。因此，只要一建立新的工作負載，網路與安全性操作人員就需手動建立新的安全性原則，並於工作負載除役時修改這些原則。許多時候，操作人員必須小心翼翼，以防在頻繁建立新原則或清除過時原則期間出錯，因而耗費大量心力來確保安全性處於最新狀態。只要使用 NSX 的動態群組，操作人員就不必在可能出錯與保留現有原則之間陷入兩難。NSX 會在工作負載建立或除役時自動調整安全性原則，完全無需人為干預，因此，可避免發生工作負載未受保護，或累積大量過時安全性原則等情況。

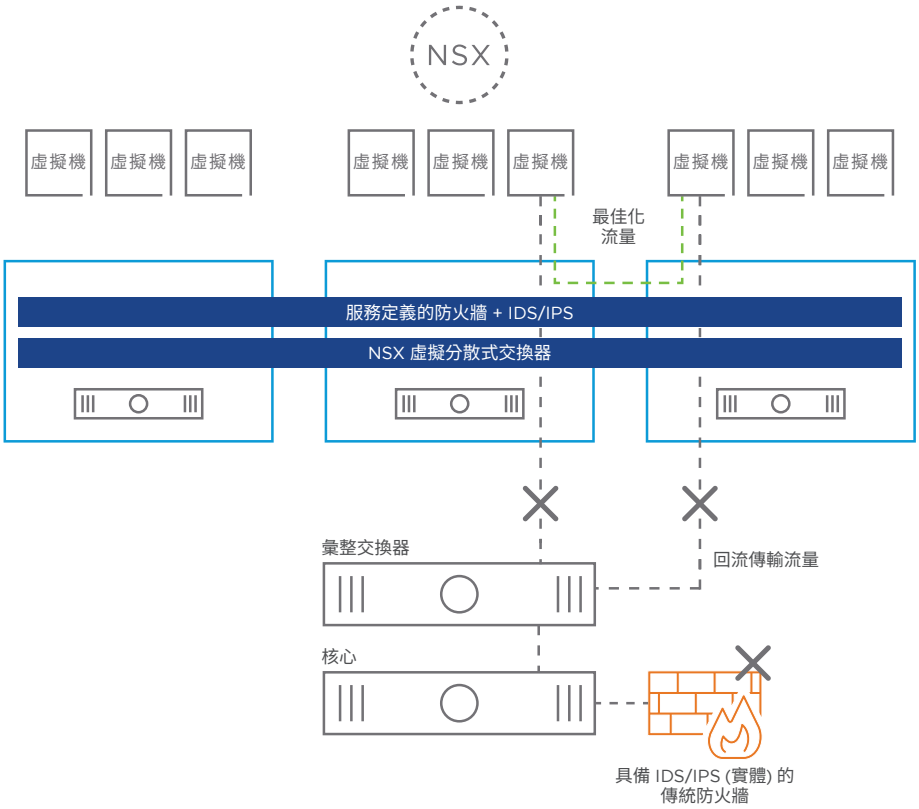

圖 2：NSX DISTRIBUTED IDS/IPS 可避免流量發生回流傳輸。

NSX Distributed IDS/IPS 使用情境

在服務定義的防火牆納入 IDS/IPS 功能，可協助操作人員使用自身的 NSX 部署來因應額外的安全性挑戰。以下提供了幾個常見的使用模式：

輕鬆符合法規要求

許多資料中心會負責代管敏感應用程式，例如包含醫療保健與財務資料的應用程式。通常，這些應用程式必須符合醫療保健領域的「健康保險可攜性和責任法案」(Health Insurance Portability and Accountability Act，HIPAA)，以及財務領域的「支付卡產業資料安全性標準」(PCI DSS) 或「薩班斯-奧克斯利法案」(Sarbanes-Oxley，SOX) 等合規需求。這些合規需求會指定使用 IDS/IPS，以防止資料外洩或遭竊。

只要使用 NSX Distributed IDS/IPS 功能，網路與安全性操作人員就能選擇僅在敏感應用程式的工作負載上使用 IDS/IPS，以滿足合規要求。NSX 採用軟體驅動方式，可透過將安全性原則傳播至所有相關工作負載來承擔此一重任，藉此免除購買與部署各自為政的應用裝置或防火牆的必要性。操作人員如需進行更深入的鑑識，或監控合規性，還可使用 VMware NSX Intelligence™ 等工具，追蹤往返於敏感應用程式的流量。

相關產品解決方案

- NSX Data Center：vmware.com/tw/products/nsx
- VMware 服務定義的防火牆：vmware.com/tw/security/internal-firewall
- 使用 NSX 進行微分段：vmware.com/tw/solutions/micro-segmentation

實作虛擬區域

有些組織需要建立直接連往與合作夥伴組織的網路連線。有些組織想要將業務單位與子公司視為中央 IT 部門的租戶。網路與安全性操作人員只要透過 NSX，就能使用防火牆與 IDS/IPS 來實作虛擬區域，以此因應上述需求。操作人員不必訂購、組裝或設定新的硬體式防火牆或 IDS/IPS，即可讓新的合作夥伴與租戶順利上線。同樣地，操作人員可將合作夥伴與租戶設為離線，而不必受制於先前所購買的硬體。

取代各自為政的 IDS/IPS 應用裝置

網路與安全性操作人員可定期重新架構一部分的資料中心，以整合安全功能。如果操作人員已決定將自身的資料中心網路虛擬化，就可立即使用 NSX Distributed IDS/IPS 分散式實作取代各自為政的集中式 IDS/IPS 應用裝置。在上述作業期間，網路與安全性操作人員可使用單一管理主控台 (VMware NSX Manager™) 同時管理旗下的防火牆與 IDS/IPS 功能。

偵測橫向威脅移動

有意侵入資料中心的入侵者，經常會從做為跳板的虛擬機橫向移動至代管敏感資料的虛擬機。為了採取上述橫向移動，入侵者往往會使用 Netcat 等工具來進行偵察。採用適當簽名機制的 IDS/IPS 可偵測嘗試偵察的行為，並通知網路與安全性操作人員。之後，操作人員可封鎖入侵者的行動 (包括透過 IDS/IPS)，或使用 NSX Intelligence 與其他工具來追蹤入侵者。

NSX Intelligence 與 NSX Distributed IDS/IPS

NSX Intelligence 為分散式資料收集與安全性分析引擎，可透過 NSX Manager (NSX 管理主控台) 加以存取。NSX Intelligence 可透過效率十足的方式，向 NSX 環境中的虛擬化管理程序收集中繼資料，並儲存資訊，以供後續使用。

NSX Intelligence 可提供詳盡且深入的應用程式相依性對應，將網路中的所有工作負載與流量視覺化，以協助操作人員全方位掌握自身環境。此外，NSX Intelligence 也會依據應用程式之間的流量模式，自動推薦防火牆安全性原則，進而大幅簡化微分段與內部防火牆的操作流程。最後，NSX Intelligence 還會持續監控每個流量，並讓操作人員將原則層疊至流量，以輕鬆證明與維護安全性原則合規。

NSX Intelligence 能做為視覺化與原則管理層使用，與服務定義的防火牆及 IDS/IPS 相輔相成。只要結合運用 NSX Intelligence、服務定義的防火牆與 IDS/IPS，即可打造完善且易於部署的內部防火牆堆疊，於資料中心內部提供固有安全性。

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