NSX DISTRIBUTED IDS/IPS 常見問題

問： 什麼是 NSX Distributed IDS/IPS？

答： Distributed IDS/IPS 是一款專門打造的先進威脅偵測引擎，可用來偵測多雲環境中東西向網路流量上的橫向威脅移動。獨特的分散式架構結合精確的應用程式情境，讓安全性團隊在更換離散應用裝置的同時，還能輕鬆符合法規，並建立虛擬 DMZ，而無需實際區隔基礎架構。

如需定位、使用情境、競爭優勢及優點的詳細資訊，請參閱 Vault 頁面的下列資源：

- 解決方案簡報
- 技術白皮書

問： 何時開始提供？

答： 將在 NSX-T Data Center 3.0 版本先行引入 IDS 功能，其他眾多功能則會隨著其他版本陸續推出。後續發行版本亦將包含 IPS 功能。

問： 這些功能將納入其中一個現有的授權版本，或當成 NSX-T 的部分產品單獨銷售？

答： 尚待確認。我們將在 NSX-T Data Center 3.0 正式版發佈的前幾週取得更多資訊。

問： 誰是 NSX Distributed IDS/IPS 的目標客戶 (使用者)？

答： 負責部署和管理服務定義 IDPS 的網路安全性架構設計師/工程師是本產品的主要對象/角色。

問： 相較於其他 IDS/IPS 解決方案，我們的解決方案有哪些技術競爭優勢？

答： 以下是值得注意的關鍵競爭優勢：

1. **分散式分析**：流量分析將分散至每一個工作負載，進而消除應用裝置只檢查區域邊界流入/流出流量時的盲點，同時還能維持簡單的操作模型。這個檢查功能會按工作負載數量以線性比例調整，幾乎可以完全消除離散應用裝置的總流量限制。多重分析功能的單程處理方法使延遲和運算額外負荷降至最低。
2. **依據情境精選簽名分送**：依據對執行中應用程式的認知，僅分送給每個工作負載相關的威脅簽名並進行評估。這可大幅降低主機上的運算額外負荷，提高逼真度相符並大幅降低誤判率
3. **應用程式情境導向威脅偵測**：此引擎部署在每台主機上，依據其在虛擬化管理程序中的權限定位，充分瞭解執行中的應用程式和軟體，而無需猜測來源或目標應用程式。這樣一來，可以更清楚分類警示，使用者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。
4. **原則與狀態行動化**：透過 IDS/IPS 引擎和分送至每個工作負載的相關原則，這些原則及完整狀態會隨著工作負載移動而不會丟失任何流量，也就沒有防火牆原則過時或編寫網路備援原則的程式問題

問： 我們的解決方案有哪些策略優勢？

答： 以下是值得注意的主要優勢：

1. **靈活彈性的總流量**：在每個工作負載中嵌入 IDS/IPS 功能後，容量即會隨著應用程式按線性比例自動調整，檢查所有流量而不會造成硬體瓶頸，也無需使用總流量更高的昂貴應用裝置。
2. **簡化網路架構與作業**：分散式架構不需要透過回流傳輸將流量傳送至集中式應用裝置，得以簡化網路設計並降低網路壅塞現象。使用單一的防火牆管理功能和功能強大的屬性型原則建構，操作人員就可以進行精密操控，在每個工作負載或跨區域啟用和設定 IDS 功能，而不受基礎網路建構的限制。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
11073 台北市信義區松仁路 100 號 台北南山廣場辦公大樓 38 樓之一 電話 +886-2-3725-7001 傳真 +886-2-3725-7010 www.vmware.com/tw

NSX DISTRIBUTED IDS/IPS 常見問題

3. **提高工作負載的零誤判率**：準確且詳細的應用程式情境可讓 IDS/IPS 引擎精選出各工作負載的規則集，進而提高簽名的逼真度相符、使安全性團隊能夠大幅降低誤判率，以及更有信心將更多工作負載移至 IPS (區塊) 模式
4. **提高現有運算容量的使用率**：重複使用每台主機上現有的閒置運算容量，並縮減使用專用應用裝置的需求，即可降低成本

問： NSX IDS/IPS 解決方案與此領域的其他解決方案相較之下，競爭規模為何？

答： 請參閱 Vault 頁面的 IDS/IPS 市場規模。

問： 如何選擇部署類型 – 1) 原生 IPS/IDS 解決方案 2) 使用協力廠商 IDS/IPS 合作夥伴解決方案的服務增強

答： NSX 是支援多種選擇及彈性的平台。客戶可以視需求選擇原生或協力廠商 IDS/IPS 解決方案。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
11073 台北市信義區松仁路 100 號 台北南山廣場辦公大樓 38 樓之一 電話 +886-2-3725-7001 傳真 +886-2-3725-7010 www.vmware.com/tw