Gigamon加密流量透視 SSL/TLS Decryption

Powered by the Gigamon Visibility and Analytics Fabric

如今，不良行為者正在利用加密技術來掩蓋50%的新惡意軟件活動，以隱藏傳送和正在進行的通信，包括數據洩露。 這個
因此，網絡和安全運營團隊不得隨意授予加密流量。
帶有許可的GigaSMART®解密功能的Gigamon可見性和分析結構使運營團隊能夠完全了解任何TCP端口或應用程序上的加密流量，包括TLS 1.3。

"默認情況下，超過94%的Google流量是經過加密的，而排名前100位的非Google網站中的96個（佔總吞吐量的25%）實現了加密。"

Source: https://transparencyreport.google.com/https/overview?hl=en

"多達40%的大型企業已經使用了TLS 1.3

Source: https://www.ssllabs.com/ssl-pulse/

"在2020年期間，超過50%的新惡意軟件活動將使用各種形式的加密和混淆來隱藏傳遞，並隱藏正在進行的通信，包括數據滲透。"

Source: Gartner Security and Risk Management Summit Presentation, The Role of Network Traffic Analysis in Today's Threat Environment, Jeremy D'Hoinne and Lawrence Orans, 17-20 June 2019

FIPS VALIDATED 140-2 LEVEL 2

KEY FEATURES

- 在任何TCP流量自動進行SSL和TLS檢測
- 一次解密，提供多種工具
- 基於策略的選擇性解密量
- 支持具有完善轉發保密性的所有高級密碼，包括TLS 1.3
- 支持SSL / TLS拆分代理

KEY BENEFITS

- 網絡上沒有盲點
- 傳統工具可以連接到結構
- 增強的工具性能
- 保留數據隱私和合規性
- 通過最新的加密標準實現最大的會話安全性
- 在客戶端和服務器端啟用獨立的安全算法

GigaVUE Cloud Suite for VMware

具有基於VMware網絡的全面虛擬化和自動化功能的智能流量可視性

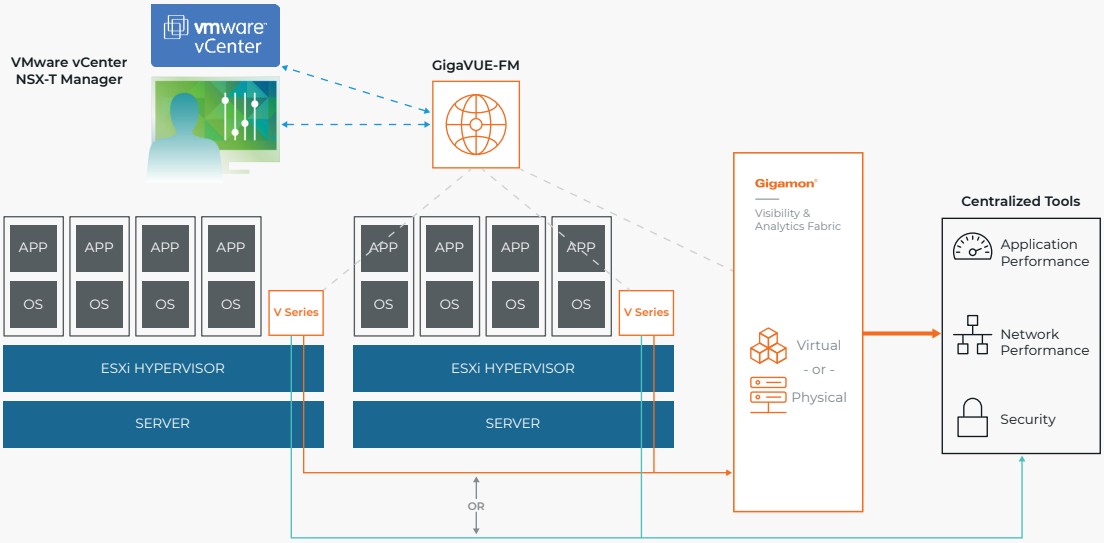

Figure 1. Certified integration of GigaVUE® Cloud Suite™ with VMware vCenter and NSX-T.

主要功能及效益

Traffic acquisition and local workload-based processing

- 輕巧的無代理vTAP降低了成本和復雜性
- 減少應用程序停機時間
- 自動擴展vTAP
- 按需上/下
- 獲取所有東西虛擬機工作負載流量
- 在每個虛擬機監控程序上提供完整處理
- DPDK對VM的影響最小，以實現高性能和大容量

Traffic aggregation, expanded processing and distribution to tools

- 靈活地將流量發送到聚合可見性節點或直接發送到工具
- 通過GigaSMART®CoreVUE™和應用程序智能選擇性處理流量
- 通過消除重複的數據包來提高整體效率
- 通過將流量鏈接到多個安全和監視工具的服務來簡化操作
- 監視會話支持靈活的流量過濾，數據包修改和轉發規則

Centralized multi-cloud management and orchestration

- 實現一個完全自動化的環境，包括對vMotion的支持
- 支持完全虛擬化的基礎架構
- 使用NSX-T動態服務插入自動實例化和配置V系列
- ATS自動選擇
- VM和接口可簡化水平擴展配置
- 跨多個雲的單一窗格管理，業務流程和可視化