產品說明
GigaSMART

產品描述

GigaSMART® 技術將 Gigamon 安全訊息派送平台的智慧化和性價比擴展至強化監測架構和提升工具設備的性能。客戶可使用一系列應用服務，優化從網路發送至用作監測、管理和保護該網路的工具設備的流量。Visibility Fabric™（流量視覺化矩陣）內部所有節點設備均可調用 GigaSMART 先進的處理引擎，不受連接埠或卡槽的限制。多個 GigaSMART 引擎可以合併以處理更大流量負載，也可以指定為某特定應用所專用。透過合併多個操作或串接多項服務，可以一次性對流量實施多個處理功能，例如在去除重複封包後輸出 NetFlow 及其它網路 metadata 或解密 SSL，或者在實施負載平衡並發送至工具設備前先移除流量的 VLAN 表頭。

透過去除重複封包和封包裁切功能，消除無關內容，使得網路監測工具設備的效率得到提升。 借助 SSL 解密功能，經過解密的明碼封包可發送至 out-of-band 的監測工具設備，從而實現對加密 session 的檢視。敏感資訊遮罩功能允許網路安全團隊隱藏密碼、金融帳號或醫療資料等保密資訊，從而保證企業能夠符合 SOX 法案、HIPAA 法案和 PCI 標準的規定。透過源埠標籤和時間戳記功能，組織機構可以在收集流量時添加來源或時間等資訊，提高精準度。調式性封包過濾技術或負載平衡技術支援更強化的數據封包分配功能，提供更強大的數據封包內容檢視，若同時結合表頭移除功能，去除無關的協議表頭，將可讓工具設備更高效率地運作。應用 session 過濾功能能夠辨識和發送與應用 session 相關的流量至資安設備，從而提高它們的效率和性能。

GigaSMART 引擎先進的處理能力，也能利用到對流入的流量進行匯總和輸出 NetFlow 及其它 metadata 統計資料。將 NetFlow 統計資料生成任務轉移至 out-of-band 的 Gigamon 視覺化矩陣，便可以減少消耗昂貴的生產網路資源來進行統計的風險。跨遠端網站和巨量資料環境下的增強型 flow 資訊可用來推導使用模量排名、應用排名等眾多統計資料，以更有效地規劃網路容量和實施安全性原則。

透過 GTP 關聯功能，服務供應商將能更可靠地過濾和發送指定用戶的session (包括 GTP-c 和 GTP-u) 至監測和分析工具設備。針對活躍使用者設備的 IP (UE IPs)，Gigamon 的 FlowVUE™ 應用提供了一個跨 GTP-u 隧道的採樣範例。所有使用者終端相關的數據封包都會被發送到與使用者相對應的監測工具設備，從而保持使用者流量樣本的完整性。透過對使用者設備上的流量進行過濾和抽樣，然後將所有需要檢視的相關 session分送至與使用者相對應的監測工具設備，既智慧化地減少資料處理量，同時又能夠在現有成本框架內實現巨量資料輸送量的處理。

表1: 軟體功能及其好處

GigaSMART 功能/應用程式	好處	GigaVUE H 系列[1]	GigaVUE-2404
SSL 解密	• 提供對加密 session 的可視性 • 發送加密數據封包至多種頻外工具設備：IDS (入侵偵測系統)、DLP (資料防丟失系統)、APM (應用性能管理)、CEM (客戶體驗管理) 等 • 透過加密和基於角色的存取控制來保護 private keys	✓	✗
去除重複封包	• 當數據封包被多個收集點收集時，每個被重複收集的數據封包都只被發送一次，從而減少工具設備的處理資源 • 消除因 VLAN 間通訊或錯誤的交換器配置而導致的數據封包重複	✓	✓
調適性數據封包過濾	• 過濾包括 VXLAN、VN-Tag、GTP、MPLS 在內多種高級封裝表頭，以及封裝在第 3層 / 第 4層數據封包中的內容 • 使用基於 Regular Expression 匹配模式的篩檢程式，實現應用層高度視覺化 • 在儲存數據封包之前遮蔽其中包含的隱私和敏感性資料，確保符合 SOX 法案、PCI 標準和 HIPAA 法案的規定。 • 包含 GTP 關聯	✓	✗
應用 session 過濾	• 發送與應用 session 相關的流量至安全應用設備，提高安全應用設備的效率和性能 • 對相關流量按特徵進行分類，以過濾視頻流、電子郵件、web 2.0 和其它商業應用的流量 • 發送從 session 開始到 session 結束的所有數據封包至安全和檢視工具設備，使流量完全可視	✓	✗
NetFlow 與 Metadata 生成	• 替代網路裝置承擔了 NetFlow 與 metadata 統計資料的生成任務，並且能夠從任意流量中生成 URL 和 HTTP 響應代碼等專用於網路安全的關鍵中繼資料 • 實現高保真、非抽樣、 1:1 流量統計 • 輸出記錄至高達六(6) 個支援 NetFlow v5/v9 和 IPFIX 的收集器	✓	✗
GTP 關聯	• 精準過濾、複製和發送需要監測的使用者 session，優化工具設備性能 • 將關聯使用 者session (control和data) 的工作，從工具設備卸載，提高輸送量 • 便於深入檢視對等網路中的漫遊使用者 • 包含調適性數據封包過濾技術的使用許可證；GTP 白名單功能需要 FlowVUE 的使用許可證	✓	✗
FlowVUE	• 對活躍行動使用者設備進行流量辨識採樣，選擇性地減少發往監測工具設備和分析工具設備的流量 • 即時減少資料分析輸送量，維持或提高 CEM (客戶體驗管理)水準 • 將巨量資料轉化為可管理的資料，瞬間可以獲取重要結果	✓	✗

表1: 軟體功能及其好處

GigaSMART 功能/應用程式	好處	GigaVUE H 系列[1]	GigaVUE-2404
負載平衡	• 依據多種選項，在多個連接埠間分發流量：散列法 (hashing)、頻寬、累計流量、數據封包速率、連接和輪詢 • 依照權重分發流量, 支援不同工具設備容量 • 使用 IP、IP-and-Port、five-tuple 和 GTP-u tunnel ID 等散列法選項 • 負載平衡功能內建在所有 GigaVUE H Series GigaSMART 使用許可證中，NetFlow (包括 Metadata engine) 除外	✓	✗
表頭移除	• 無需由監測工具設備來譯解協議 • 透過移除表頭，更便於數據封包過濾、彙聚和負載平衡 • 支援隔離的表頭和協議: ISL, Cisco FabricPath, VXLAN, VN-Tag, VLAN, MPLS, GRE 和 GTP-U	✓	✓
隧道技術	• 採用 IP/UDP 或 L2GRE 封裝，把遠端網站的數據封包發送至中心的監測工具設備 • 透過 L2GRE 隧道，將虛擬化工具設備整合到視覺化矩陣中	✓	✓
ERSPAN 端接	• 端接 ERSPAN 隧道，整合、過濾和轉發相關 ERSPAN 通訊 • 將 ERSPAN III 時間戳記轉換成一種監測工具設備可識別的格式 (僅適用於 GigaVUE H 系列設備)	✓	✓
數據封包裁切	• 減小數據封包體積，以提高處理和監測的輸送量 • 保留數據封包關鍵相關內容，減少處理量 • 顯著提升取證記錄工具設備的性能	✓	✓
敏感資訊遮罩	• 從 64 到 9000 位元組的偏移量覆蓋數據封包資訊 • 隱藏包括金融和醫療資訊在內的隱私資訊	✓	✓
源埠標記	• 向數據封包添加用於指出進入連接埠的標籤 • 易於識別數據封包的來源	✓	✓
時間戳記	• 為數據封包附加時間戳記，方便故障排除和衡量應用回應時間、抖動和延遲 • 網路分析得以在一個集中地點進行，而不是在多個網路終端上	✗[2]	✓