NIAGARA NETWORKS

ENABLING VISIBILITY INTELLIGENCE FOR OPTIMIZED **SIEM OPERATIONS**

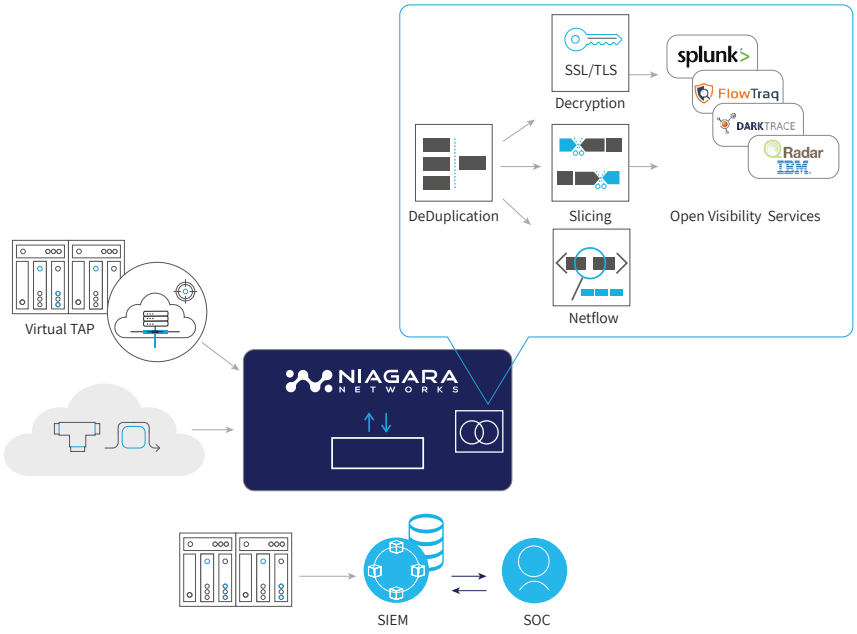
INTRODUCTION

Cybersecurity threats continue to be more sophisticated and advanced with each day, for many organizations fighting these threats is a daily battle. Security Information and Event Management, in short SIEM is a valuable toolset for a SOC to aggregate and correlate the information from the network and the IT environment to provide reports, dashboards, watchlist, alarms, etc. for the quick investigation of security threats. The amount of data collected by SIEM from multiple sources of digital infrastructure is enormous and the correlation of these vast amounts of data is not always trivial. Therefore, it is important that relevant, and preferably, optimized data is sent to the SIEM tool only to reflect the most accurate data to security analysts in SoC, including the efficiency of data lake processing by advanced SOAR (Security Orchestration, Automation and Response) solution stack.

Niagara Networks Packer Brokers combined with the Open Visibility Platform (intelligence- and virtualization) enables the collection, aggregation and filtering of data from many locations and different sources in the network, regardless of physical or virtual networks, and feed the SIEM tools with optimized data they really need by filtering specific traffic patterns, perform session-aware load balancing and reduce packet duplicates that can saturate and create false positives by SIEM tools. The deployment of Visibility Virtualization enables embedded centralized and decentralized inspection of network flows by agile and flexible NFV-based deployment hub for cutting edge virtual applications giving you the freedom to choose and spin-up the best solution for your SecOps and NetOps needs.

The Open Visibility Platform can host SIEM Collectors to form consolidated traffic flow to the SIEM. A collector collects information from the network and forwards it to the main SIEM platform for processing and correlation. Niagara Networks can enhance this capability by hosting collectors in the Open Visibility Platform at a single location for better performance, less bandwidth usage, and lower total cost.

- SIEM intelligent access to data flows – over 80% of data can be filtered to maximize tool efficiency and scale
- An accurate feed of data from on-prem or cloud via physical or virtual TAPs and intelligent filtering/aggregation
- Network architectural simplicity to enable deep visibility across all layers for SecOps
- Field-proven interoperability with industry leading SIEM platforms



NIAGARA NETWORKS

Full Network Visibility

The combination of physical TAPs, Bypass switches with TAP functionality, and Virtual TAPs can provide full visibility in the physical as well as in the virtual network environment but it will often introduce a certain number of duplicate packets which not only increases the amount of data captured from the network but can also disrupt the correct behavior of SIEM tools. Deduplication, part of the Open Visibility Intelligence functionality enables the removal of duplicate network traffic and optimizes the bandwidth to the connected SIEM tools.

Application Awareness

Application layer filtering, also known as layer 7 filtering, is another method to optimize the data sent to the SIEM tools, either by removing applications that do not require an inspection (Video, IPTV, etc.) or precise selection of targeted applications for which the traffic is to be inspected by a specific SIEM tool.

Tool Optimization

Many SIEM tools are based around inspection of a packet's meta data, the source and destination IP address, and TCP/UDP ports. The actual payload is not used in the inspection and reporting process. This payload however can take up to 95% of the packet. By removing the payload from the packet, also known as packet slicing, the packet size and consequently the amount of bandwidth to the tool can be significantly reduced.

Optimized Flow Information

NetFlow or its newer counterpart IPfix is often a welcome source of flow information as it provides vital information about the applications and traffic in the network. Unfortunately, the commonly used NetFlow/IPfix sources, routers and switches, generate NetFlow on a sampling basis which only provides limited flow information. Using the filtering capabilities of the packet broker, the Open Visibility Platform can generate NetFlow/IPfix information for all selected flows.

SSL/TLS decryption

With the vast majority of internet traffic now encrypted and increasing portions of network traffic encrypted as well, security operations teams gained another challenge combatting malicious traffic and securing the network. Niagara Networks' Open Visibility Platform enables SSL/TLS decryption to enable payload inspection but can also be combined with any of the other Open Visibility functions like NetFlow generation for full encrypted DNS reporting, or even more sophisticated policy-based privacy compliance, by masking the required field before delivery to SIEM collection and inspection tools.

Niagara Networks' decryption solution improves the security and deployment of MITRE Att&ck framework by providing decrypted network traffic for detailed log analysis.

Open Visibility Virtualization

On top of the Open Visibility Intelligence functionality, OVP provides Open Visibility Virtualization. With the virtualization functionality, Niagara Networks enables customers to run applications, third party as well as homegrown, as a seamless part of the packet broker. Open Visibility Virtualization enables rapid deployment of security tools but also provides the ability for decentralized traffic inspection and reporting. It also provides the ability to run third-party network sensors receiving their data from many network locations thereby removing the need to deploy separate physical sensors across the network.

SUMMARY

For Security Operation Centers, SIEM solutions are an important means to manage the digital infrastructure and to analyze incidents. The amount of data to be analyzed however is huge. Removing irrelevant data and providing optimized data to the SIEM tools is a necessity for successful cybersecurity threat detection, prevention, and remediation, including the baseline process of organizational digital assets sustainability. Niagara Networks' Open Visibility Platform– a unified platform with embedded functions of packet broker, bypass, active TAP, and flexible NFV-based deployment hub for cutting edge virtual applications giving you the freedom to choose and spin-up the best solution for your SecOps and NetOps needs and empower any SIEM tools to operate efficiently and avoid any blind spots in a big cybersecurity complex architectures.

Feature	Benefit for SIEM Operations
Packet Slicing	Remove packet's payload preserving meta data for flow analysis
DeDuplication	Remove duplicate packets from the traffic flow and only forward the first packet to the inspection or reporting tool(s)
NetFlow Generation	Generate NetFlow or IPFix information from a sampled or unsampled traffic flow and offload this functionality from switches and routers
Application Layer Filtering	Application recognition for filtering purposes
Data Masking	Mask specific payload like cerdit card numbers, bank accounts and other personal identifiable information, based on offset masking or combined with regular expression search and meeting data compliance for privacy regulations: GDPR, CCPA, HIPAA, PCI-DSS, and More
ERSPAN Tunnel Termination	Terminate ERSPAN tunnels. For transport for tapped traffic over ERSPAN tunnels
Regular Expression Search	Filter packet payload using PERL regular expressions
SSL/TLS Decryption	Decrypt SSL/TLS encrypted traffic for inspection and reporting purposes. Supports SSL 3.0 and TLS1.0, TLS1.1, TLS1.2 and TLS1.3
GTP Correlation	Correlate GTP-C and GTP-U for load balancing GTP traffic across multiple tools - Mobile SIEM use case
GTP Load Balancing	Load balance correlated or uncorrelated GTP traffic across multiple tools-Mobile SIEM use case
GTP Filtering	Filter GTP traffic on multiple GTP protocol and subscriber fields - Mobile SIEM use case

NIAGARA NETWORKS

Packet Slicing

Packet Slicing truncates packets thereby preserving the the information in the packet (header) that is required for network or traffic flow analysis.Packet slicing analizes the header and slicing can slice after a named header (IP, UDP, TCP, VLAN etc.). Packet Slicing removes payload that may be irrelevant to network monitoring and security analysis and improves the performance of analysis tools. By removing the payload, Packet Slicing also removes sensitive data which makes compliancy to security and confidentiality regulations easier.

DeDuplication

Packet deduplication refers to the capability for removing packet duplicates prior to network data being forwarded or transmitted to network analysis tools for the purpose of monitoring, analyzing, and recording. This typically causes a substantial reduction in the volume of traffic handled by such tools enabling an increase in their operational efficiency, a reduction in false positive errors generated.

Netflow/IPfix generation

Netflow, developed by Cisco, is a network protocol system that collects and analyzes the network traffic as it flows in or out of an interface. This data is then analyzed to create a picture (NetFlow) of network traffic flow and volume which can be used by network analysis and reporting tools. Netflow is now is now part of the Internet Engineering Task Force (IETF) standard as Internet Protocol Flow Information eXport (IPfix).

Application Layer Filtering

Application layer filtering goes beyond packet filtering and allows to be much more granular your control of what data is sent to (inline) security, analysis and reporting tools . While packet filtering can be used to completely (dis)allow traffic send to, or received from a specific TCP or UDP port, application layer filtering allows for filtering of specific applications (Office 365, Netflix, Youtube, and many others).

Data Masking

Data masking, sometimes called data obfuscation is the process of hiding original data using modified content. The main reason why data masking is used is to hide sensitive data in in a data flow. Data masking can be useful for organizations dealing with

- Personally identifiable information (PII)
- Protected health information (PHI)
- Payment card information (PCI-DSS)
- Intellectual property (ITAR)

ERSPAN tunnel Termination

ERSPAN, a Cisco proprietary protocol, allows for remote SPAN (Switched Port Analyzer) ports over routed networks. SPAN ports carry traffic copied from another physical port on a switch or router for traffic analysis. The ERSPAN protocol enables this copied traffic to be sent across a routed network to a central location for analysis of multiple SPAN feeds.

GTP Load Balancing

To distribute GTP traffic across multiple monitoring tools two options are available:

Uncorrelated load balancing: each tool receives a stateful subset of the GTP-U traffic and a full copy of the GTP-C traffic belonging to all GTP-U.

Correlated load balancing: each tool receives a stateful subset of the GTP-U traffic and the GTP-C information belonging to the received GTP-U sessions.

GTP Correlation

GTP correlation performs stateful correlation of the GTP- U (user plane) and GTP-C (control plane) traffic, GTP correlation can be used for load balancing the output traffic belonging to the same subscriber to a unique output port. Together with GTP filtering the amount of data send to the monitoring tool(s) can be reduced even more.

GTP Filtering

To reduce the number of GTP sessions to the monitoring tool(s) or to create a specific subset of the GTP sessions in the network, GTP filtering can be used.
GTP filtering allows the sessions to be filtered using several filtering criteria like IMSI, APN, Inner IP etc.

Regular Expression Search

In contrast to regular IP header filtering the regular expression filtering supports a much more flexible filtering method based on PERL regular expression patterns.
The regular expression can be applied to the header part of the packet or on the complete packet including the payload. The latter can be combined with data masking. Two outputs are available to enable forwarding of matched and masked traffic to different outputs.

SSL decryption

Encrypted network traffic can be decrypted for out-of-band inspection and/or reporting as well as inline traffic inspection. SSL decryption enables.

- Deep visibility into encrypted data traffic
- Powerful combination of decryption platform and the on-board resident 3rd party security & network applications, delivering a cyber threat detection multiplier
- Seamless support for network tap, or inline bypass deployments on the same platform
- Encrypted traffic can be collected from multiple interfaces - from 1GbE up to 100GbE
- Decrypted traffic packet brokering to multiple tools based on policy rules – decrypt once, use many and various intelligent packet manipulations (masking, filtering, steering and more)
- Off load / minimize performance hit for individual tools

ABOUT NIAGARA NETWORKS

Niagara Networks™ is a Silicon Valley based company that pioneered the Open Visibility Platform™ to bring desperately needed agility to network security.

Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

We Design, Develop and Manufacture our Products in Silicon Valley, USA.

NIAGARA NETWORKS

150 E Brokaw Road
San Jose, CA 95112, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529