Increasing Visibility with Ixia's Vision ONE

Serge Borso

A SANS Product Review

Increasing Visibility with Ixia's Vision ONE™

Written by **Serge Borso**

April 2019

Sponsored by:

Ixia,
a Keysight Company

Introduction

Large enterprises have many security and network related needs, from traffic monitoring and inspecting decrypted traffic, to regulatory requirements and understanding bandwidth utilization. Network packet brokers (NPBs) tackle this challenge by providing a way to increase visibility across the network so networking tools can perform at peak efficiency. Ixia's Vision ONE helps solve the issue of brokering traffic at impressive line rates. Moreover, it enables organizations to understand traffic better and, ultimately, protect their environment by getting the most out of their networking and security appliances.

SANS reviewed Vision ONE to understand how it performs from a basic packet broker perspective, on an inline deployment and how it handles application development. To do so, we considered typical enterprise deployment scenarios where an NPB would be implemented in various capacities. Specifically, we wanted to explore the most relevant circumstances for such a tool and the features that would aid our efforts in monitoring inline and out-of-band packets. Our other goals were to learn more about how this product dealt with encrypted payloads and high throughput, how it could be tuned to increase efficiency and whom would benefit the most from implementing Vision ONE.

Packet Broker Essentials

While NPBs have a wide variance in how they work and what they offer, they generally provide specific essential capabilities. These include capturing all traffic sent to the NPB device from a SPAN or tap port, deduplication of traffic and providing a means to make the data available to a multitude of tools. Packet brokers are neither the endpoint nor the primary consumer of packets; rather they act as intermediary devices to ensure network monitoring and security tools get the data they need to do their jobs. Because of this, NPBs are logically positioned on the network, as seen in in Figure 1, to ensure they capture all traffic possible and have the capacity to deal with this traffic to downstream devices.

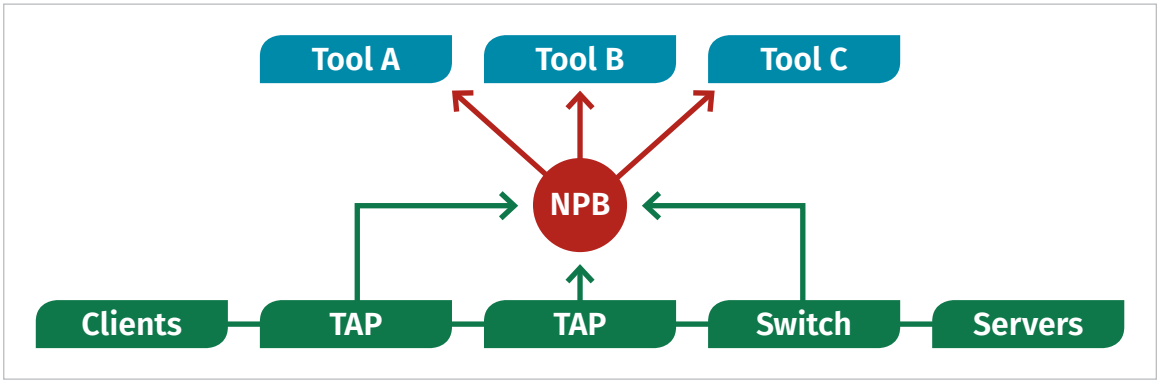

Figure 1. How NPBs Are Positioned on the Network

Flexible Filtering

Vision ONE is Ixia's latest packet broker technology and comes in the form of a 1RU hardware appliance, accessible via a modern web-based GUI controlling all the essential components of the device. To review Vision ONE, we used a demo virtual appliance as our test environment. As with other network devices designed to broker traffic, Ixia's Vision ONE is well-suited to sit wherever it has the most significant effect on traffic visibility for the network.

Visibility is an essential concept in network traffic monitoring. Security personnel need the ability to ensure security devices (for example an IPS or IDS, where Vision ONE sends its traffic) and other such tools see the most relevant traffic for them to perform adequately. Visibility doesn't, however, always mean seeing 100 percent of *all* traffic; there are times when it means seeing 100 percent of *actionable* traffic. For instance, if an organization allows streaming entertainment services, it doesn't necessarily need or want to send that traffic down the path of deep packet inspection. However, if the traffic is aimed at financial production systems, then it merits closer examination.

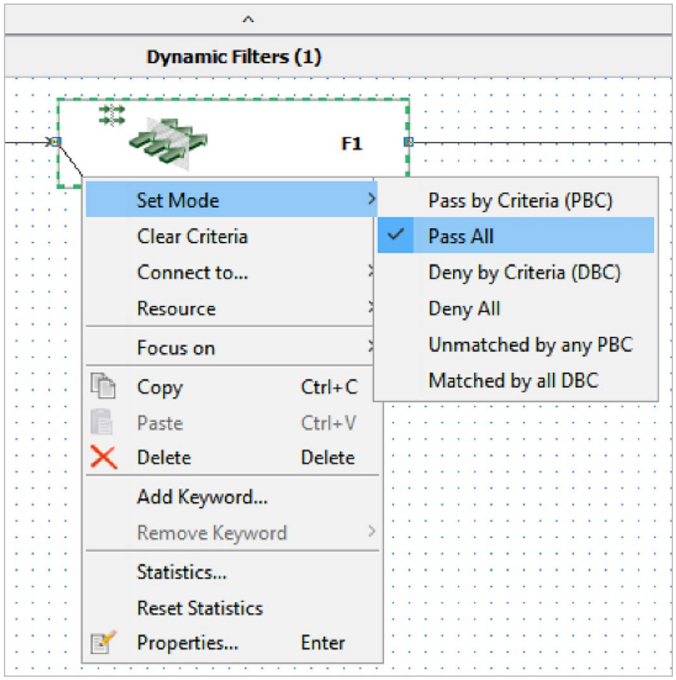

Figure 2. Configuring a Dynamic Filter

The drag-and-drop web-based interface of the Vision ONE control panel enables the network engineer to filter traffic to meet specific needs. The engineer could easily create a new filter and configure how it should work based on the receiving ports, filter criteria and the various modes of operation illustrated in Figure 2. With this setup, the engineer could pick whether to pass all traffic unfettered to another device or granularly filter which traffic to send to which device(s).

Line Rate Deduplication and Header Stripping

One of the primary functions of a packet broker is to ensure security and monitoring tools get the information they require to perform at peak efficiency. Two ways the Vision ONE system helps achieve this is by line rate deduplication, which ensures duplicate packets don't get passed along, and header stripping, which provides packet grooming to save on subsequent processing. This is especially important in both traditional networks and software-defined networks (SDN), where there can be substantial amounts of duplicate traffic from the BiDi taps.

Deduplication of packets is an essential task that Vision ONE automates in its PacketStack feature, thus supporting packet grooming techniques such as packet trimming and protocol stripping (see Figure 3).

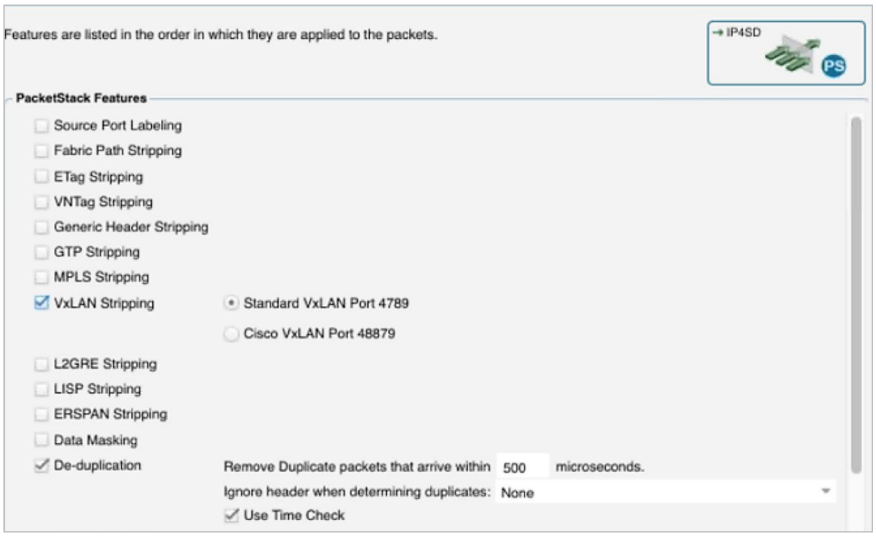

Figure 3. Packet Processing Options

By providing the ability to remove protocol information from packets, Vision ONE can reduce overhead to make security and monitoring tools more efficient. Specifically, by reducing the actual size, in bytes, of a given packet via this method, downstream devices receiving the groomed packet inherently expend less effort as there is less packet information to ingest, parse and process. Also, by identifying and stripping the protocol, analysts can selectively dictate which types of traffic should be routed to a specific device for further analysis.

Aggregation and Replication

Within Vision ONE we were able to use the web-based graphical interface to combine data from multiple sources and forward this traffic to a single tool or multiple tools. One of the benefits of aggregating traffic in this way is the security and monitoring tool's ability to handle higher throughput than it could previously. By using Vision ONE, we aggregated the input from multiple sources to feed a single output device. We could make this a one-to-one correlation (1:1), a one-to-many (1:N), many-to-one (N:1) and many-to-many (N:N) setup as shown in Figure 4.

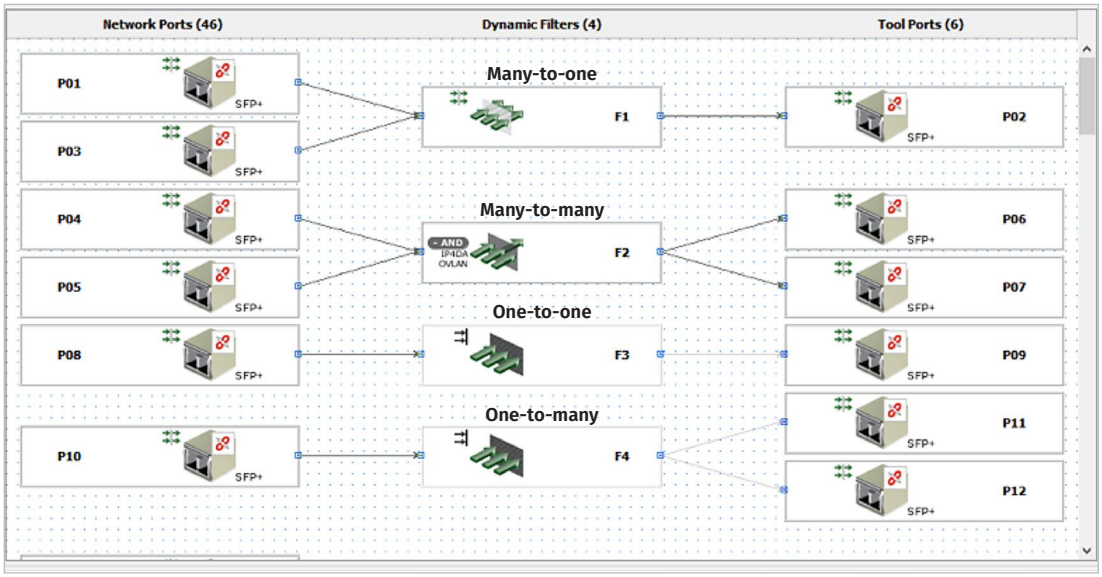

Figure 4. Many-to-one, Many-to-many, One-to-one and One-to-many Setup Options

The Vision ONE system makes replicating traffic easily achievable. This type of use case ensures the system passes production traffic for a new application to the firewall and routes it to the web farm. At the same time, the system sends traffic to a web application firewall (WAF) to support its learning mode. This way normal operations can continue while the system vets the WAF prior to putting it in blocking mode.

Overlap Rule Handling

It's relatively simple to use an NPB in a single network to process security device traffic. What becomes a bit more complicated is setting up multiple networks to talk to multiple security and monitoring tools—each with variations and subsets of ingress traffic. The complexity derives from multiple and overlapping rules aimed at handling traffic flow. It can manifest itself when security personnel need to provide multiple tools with the same traffic or overlapping traffic, as would happen when they want to ensure a security device and a monitoring tool receives traffic tagged for specific VLANs.

Vision ONE accounts for these complexities by providing a means to prioritize the traffic and make sense of the overlapping rules without dropping packets or establishing too high of a priority to rules. This results in an engineer having the ability to choose which tools and devices should receive traffic, even if it's redundant traffic, and ensures each device will receive 100 percent of the packets defined by each ruleset.

Agile Deployment of Inline Security Tools

Some security tools, such as IDS, are passive in that they simply listen to the traffic directed towards their interface(s). Others, like IPS, are considered active inline tools, meaning these types of devices need to actively alter the traffic flow by dropping or otherwise blocking packets to help protect the environment. Using an NPB like Vision ONE can help with the deployment of such inline security tools in a variety of ways, as seen in Figure 5, which we will explore next.

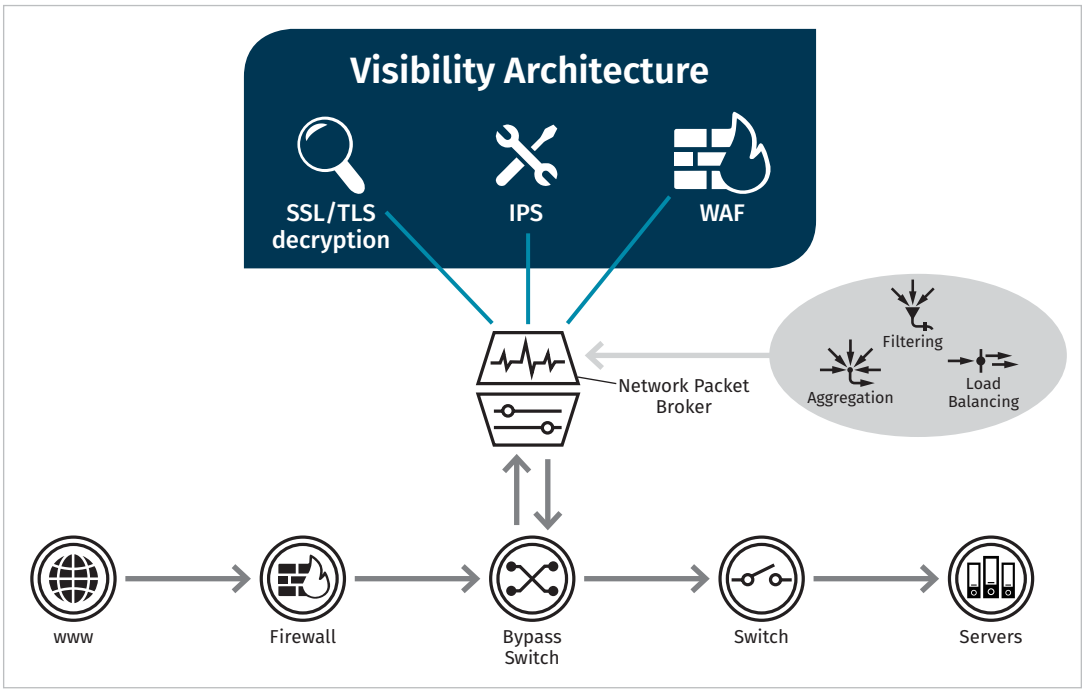

Figure 5. An NPB and Deployment of Inline Tools

Heartbeat Variants

A heartbeat acts as an indicator a system is alive. With each heartbeat users gain a level of confidence the system is online and doing its job. Because inline systems will impact the flow of traffic, it is vital to ensure these systems are online and more importantly, taking action when they are not available. Vision ONE's interface lets us specify the frequency of the heartbeat to control how fast or slow a system will failover, as shown in Figure 6. Vision ONE's granular control of heartbeat vitality helps to ensure a healthy network.

By default, Vision ONE comes preconfigured with several immutable heartbeat templates for common vendor devices (see Figure 7). These are already tuned to the respective manufacturer's desired interval, retry and timeout, making for easy implementation and integration with the Vision ONE appliance.

Regardless of whether we use a template or configure our own custom heartbeat based on what we think is appropriate for the tool, the takeaway is the same: Vision ONE provides fine control over when a device or High Availability pair should failover.

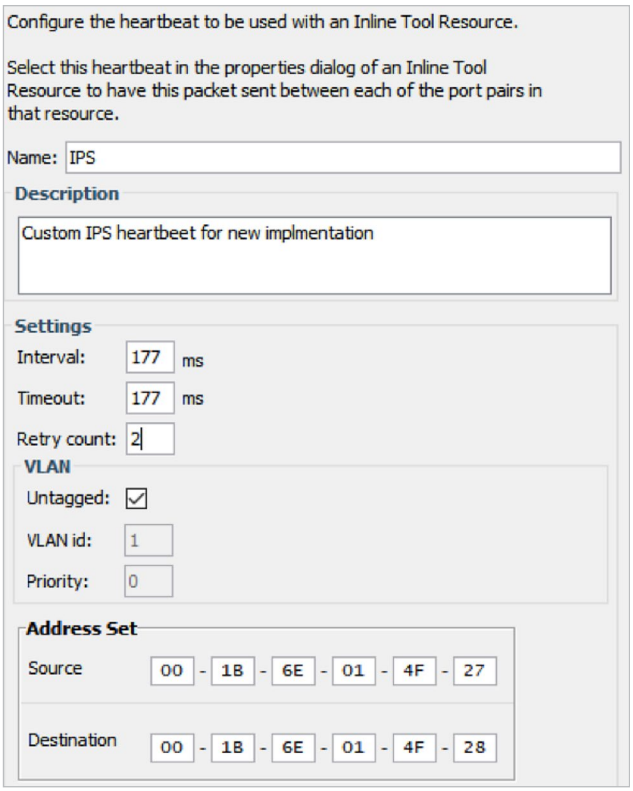

Figure 6. Configuring a Custom Heartbeat

Fail Open and Fail Close Operation

The concept of *failing open* refers to an outage or an issue with an inline device that either no longer performs its role or is otherwise offline or unresponsive but still needs traffic to flow. In this situation, the device is said to be configured to fail open since the flow of traffic is unimpeded despite the device not being online. In some situations, this is preferable to *failing closed*, which means the flow of traffic is halted in the event a device is not responsive. These distinctions are relevant because an organization must determine which state it prefers: inspecting all traffic entering the network to ensure it's not malicious even if it means experiencing downtime (a failing closed situation), or favoring connectivity so the end user experiences no downtime even at the expense of allowing potentially malicious traffic to enter the network (failing open). Regardless of the choice, Vision ONE provides for both operations (see Figure 8).

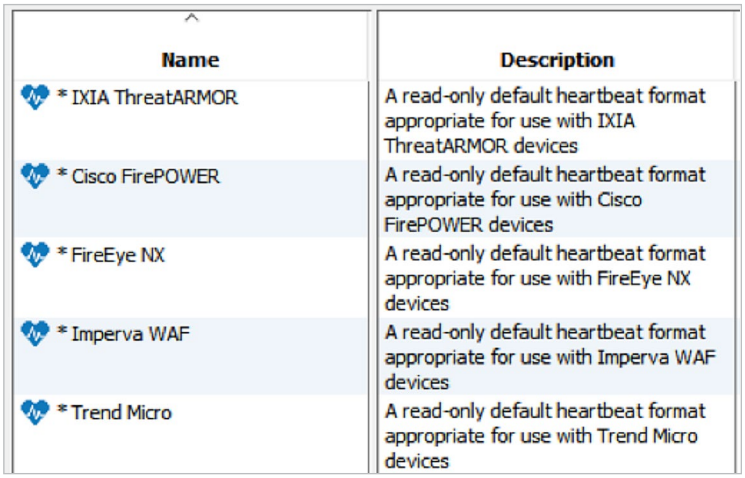

Figure 7. Default Heartbeat Options for Some Popular Technologies

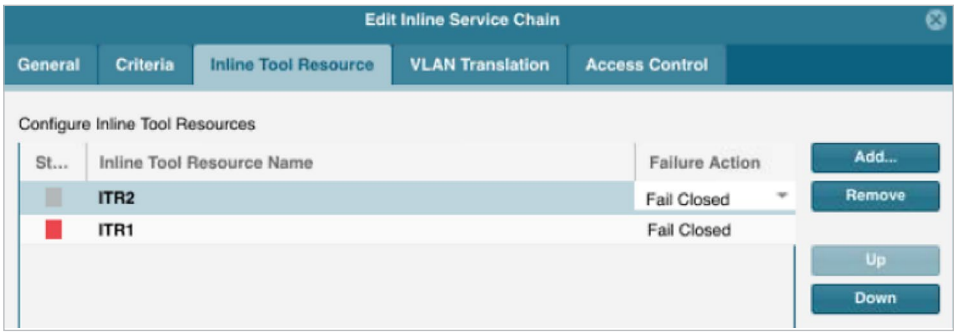

Figure 8. Choosing to "Fail Closed"

Load Balancing to Provide N+1 Survivability

Load balancing is a means to ensure the most important devices can survive a failover event when one device is no longer operational. In most network architectures, inline devices are paired with two or more of the same devices performing the exact same role with nearly identical configuration. This way, when one device loses power, has a faulty configuration pushed to it or for any other reason ceases to operate normally, the secondary device handles traffic as if there were no issues. See Figure 9.

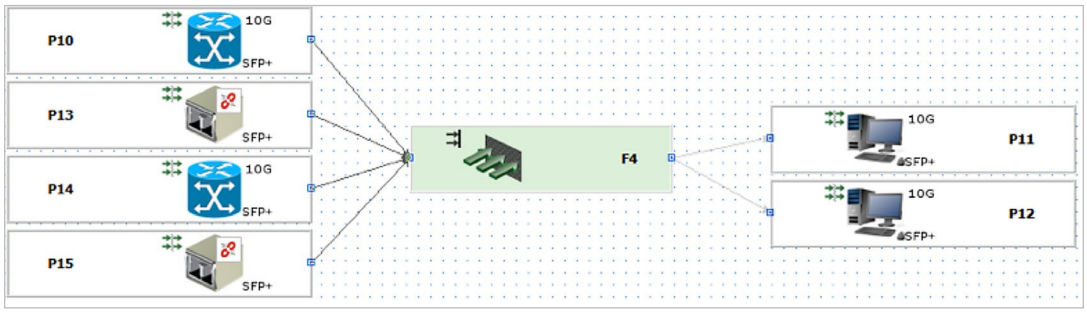

Figure 9. Beginning Concepts for Load Balanced Traffic

Enterprise networks are architected to handle devastating situations gracefully and without interruptions to services. Meeting this expectation of no downtime is the challenge for Vision ONE, and it meets that challenge thanks to the appliance's integrated options.

With Vision ONE, we can handle the task of load balancing with relative ease. Imagine a scenario where an organization's load is 40Gbps and it leverages Vision ONE to broker this traffic by splitting the load to two devices capable of handling 20Gbps each. The organization could conceivably continue to share the load across multiple devices based on how much capacity each device has. To do so, the security team would create a dynamic filter using the graphical drag-and-drop interface. The incoming traffic is on the left, dynamic filter in the middle and security devices ready to take the incoming 40 Gbps of traffic on the right. By configuring specific ports as ingress/egress and dragging the connection lines to each, it is possible to effectively configure a load balanced solution. It is important to remember, though, to add a duplicate Vision ONE appliance to remove the single point of failure.

Ideally, no organization wants to suffer an outage, but there are limits to redundant systems and differing architectures can impact network availability.

Flexible Service Chaining

Service chaining is the idea of utilizing multiple tools to perform various tasks as they relate to packet inspection, routing and decision making for a particular set of services (see Figure 10). This would be akin to the common tasks of sending packets through a firewall, an IDS or an IPS through a WAF to a SIEM and ultimately to application services to process the actual requests. This chaining process may be required to support the business and could be thought of as normal operations in many environments.

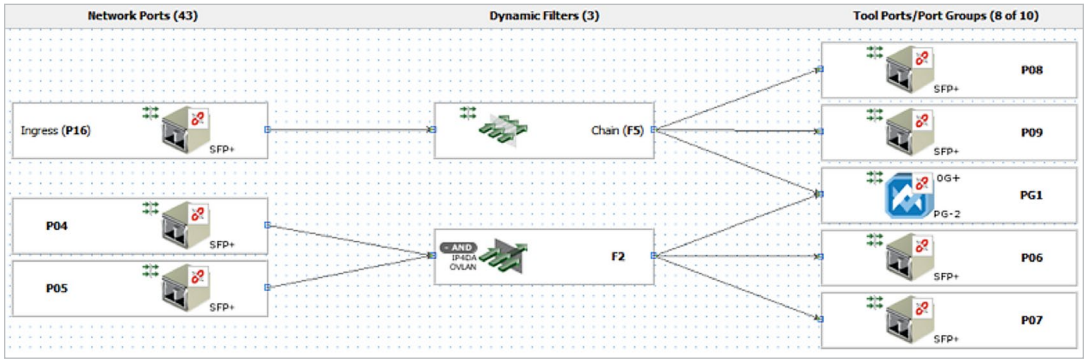

Figure 10. Service Chaining

Vision ONE can play a crucial role as the central manager of operations in terms of brokering the packets feeding each one of the devices. A potentially interesting use case would be in decrypting traffic: As the encrypted payload enters the network, Vision ONE oversees the decryption of the packet. Farther down the chain, it inspects and replicates the decrypted plain text contents to the IDS. This means devices needing to see the unencrypted contents don't have to duplicate the effort of performing the decryption.

Tight Integration of Active SSL Encryption/Decryption

It is useful for a packet broker to perform active SSL/TLS decryption, because a multitude of other tools will need access to the decrypted data for inspection.

Over the better part of the past decade, there has been a significant push by the security community to encrypt all traffic, not just web-based and application traffic. With the advent of encrypting everything came the reality security professionals can't inspect what they can't see, and the business of SSL decryption tools came into focus. The Vision ONE platform supports inline and out-of-band decryption of traffic. See Figure 11.

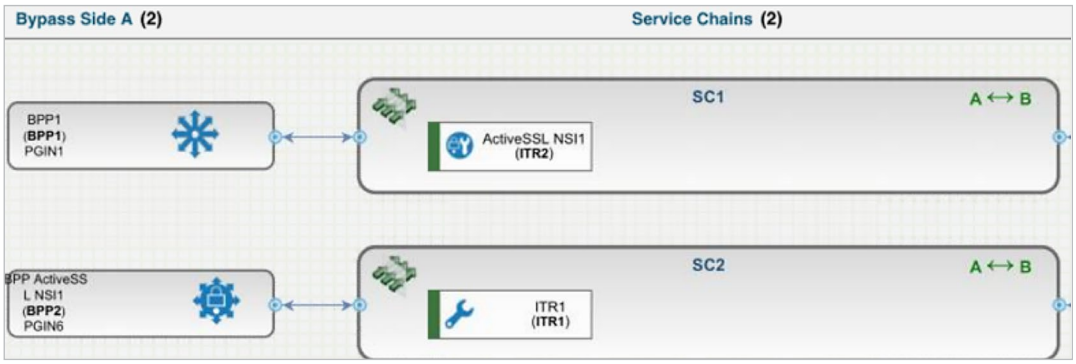

Figure 11. SSL/TLS Decryption Configuration Using Service Chains

Without a packet broker performing this decryption process, it would become much more cumbersome to configure each device independently to achieve the same result. Specifically, if each device required decrypted payloads for inspection, security personnel would have to configure each device to perform its own decryption, which results in significant overhead, processing, management and maintenance.

Encrypted sessions are designed for end-to-end encryption and every step where there is a need to break that encrypted connection introduces not only more complexity and work, but also a security shortcoming requiring security personnel to pay extra attention to that device. The reason for this is the sensitive nature of encrypted traffic—once it's decrypted, there is risk associated with who has visibility into the payload. Centrally managing this decryption process via Vision ONE can both decrease complexity and the burden of dealing with sensitive information crossing multiple devices. We'll cover this topic in greater detail in the "Data Masking" section later in this paper.

Application Detection and Metadata Delivery

A packet broker can inspect traffic and detect the application signature in use so it can intelligently determine where to send the traffic based on the signature. This is helpful for selectively sending traffic to specific devices and avoiding the need to send all traffic through every toolset.

Vision ONE's AppStack feature set can identify applications, filter data based on geolocation and application type and provide capabilities for packet capture. It also offers a custom regex filtering option for customized tuning.

Signature-based Application Detection

The platform has signatures for hundreds of applications and can detect and identify custom applications as well. These capabilities could become valuable to explore as part of an implementation to reduce the overhead on security tools. There may not be a need to provide deep packet inspection or data loss prevention for specific flows. By leveraging a signature-based solution, the security team can avoid overwhelming or even spiking other devices when the broker sends traffic to them.

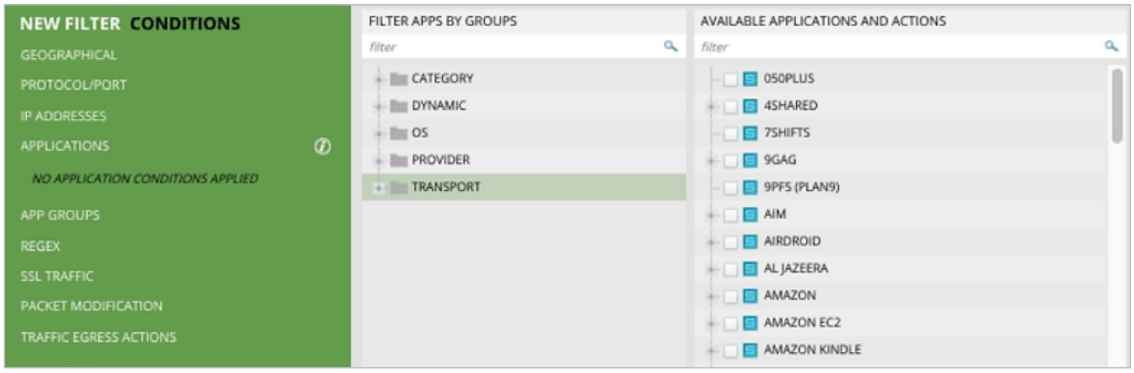

Figure 12. Signature-based Detection in Action

Administrators can further discern potentially malicious traffic and make decisions on how to handle traffic based on the application and its subcategories such as genres of movies provided by streaming media services. Then, by looking at the filtered output from this process, security teams can use this information to determine which device to send the data to for further processing or delivery. Figure 12 illustrates the process.

High-performing NetFlow Generation

Initially created by Cisco, the concept of *NetFlow* is typically used to collect and parse network metadata. This metadata is useful for troubleshooting network issues as well as getting aggregated information about what is happening on the network. With the ability to sort based on a variety of elements such as throughput, volume, geolocation and application data, the Vision ONE system can deliver the crucial information network administrators need to do their jobs.

As with other NPB interrelated components, NetFlow data can be sent to a capturing device to make sense of what is happening on the network (see Figure 13). This differs from full packet capture technology or even packet data because NetFlow is merely metadata describing the traffic itself.

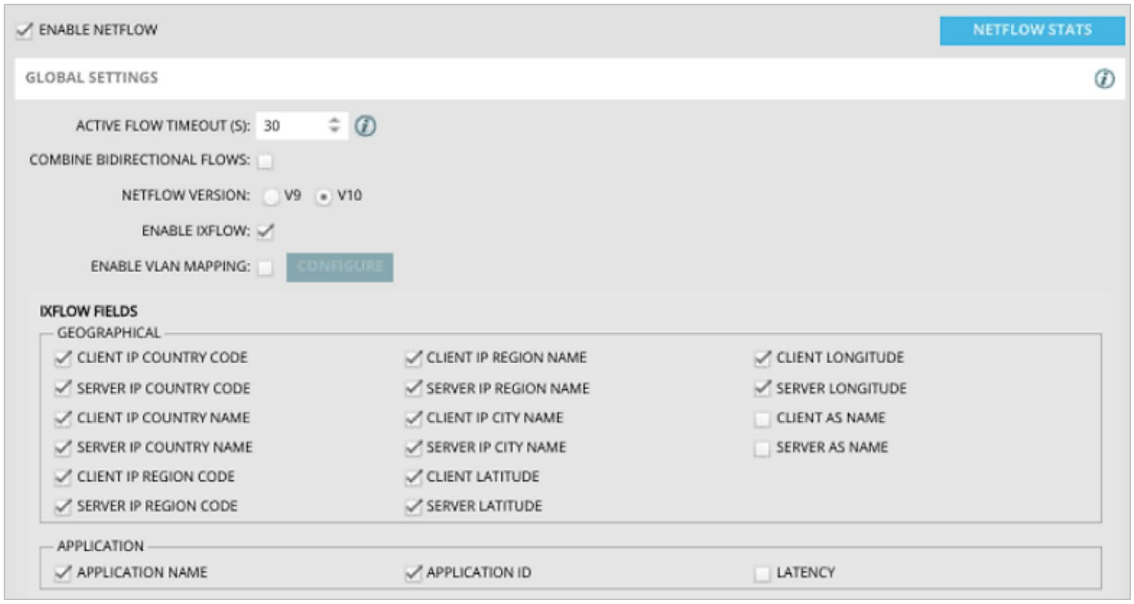

Figure 13. Configuring NetFlow

Threat Data Masking Insight

Many organizations strive to have the visibility full packet capture offers along with SIEM, IPS, IDS, WAF and a fully trained security or network engineer staff. One of the downsides, other than dealing with massive quantities of data and potentially needing to retain that data for long periods of time, is dealing with sensitive data. NPBs can extend network visibility to gather all packets, sending these packets to their intended destinations after being filtered, scanned and parsed by various security tools and network monitoring devices. With this goal, however, comes the reality security personnel don't always want responsibility for dealing with sensitive information if they don't need to. To help address this, Vision ONE provides a data-masking component enabling us to ensure sensitive information stays private.

Data Masking

The general idea behind data masking is to obscure sensitive information so it is no longer sensitive. This is akin to tokenization. A security device has a legitimate reason to inspect traffic; this is how it detects and prevents attacks against the organization. However, this same tool does not need to receive personally identifiable information such as credit card numbers or HIPAA data to do its job. The issue with some NPBs is while they can help in the decryption process, security teams don't necessarily want to hand that sensitive information to other devices. Vision ONE can mask the data to hide the sensitive portions and still support the inspection tools scanning for maliciousness.

In addition to health and financial data, another use case we wanted to explore was the organization using production data in the test environment. Even in most mature organizations, security teams sometimes see real user information populating test databases, a practice security teams recognize as a corporate security risk. This problem can be resolved by using Vision ONE as the data masking agent to provide realistic, near-production level data in the test environment but mask the sensitive bits to ensure no leakage (see Figure 14). This can be accomplished by either masking out (replacing specific matching strings) or by substitution, encryption or even shuffling. Depending on the criticality of the data, simply encrypting or hashing it would render it unreadable and thus conform to best practices.

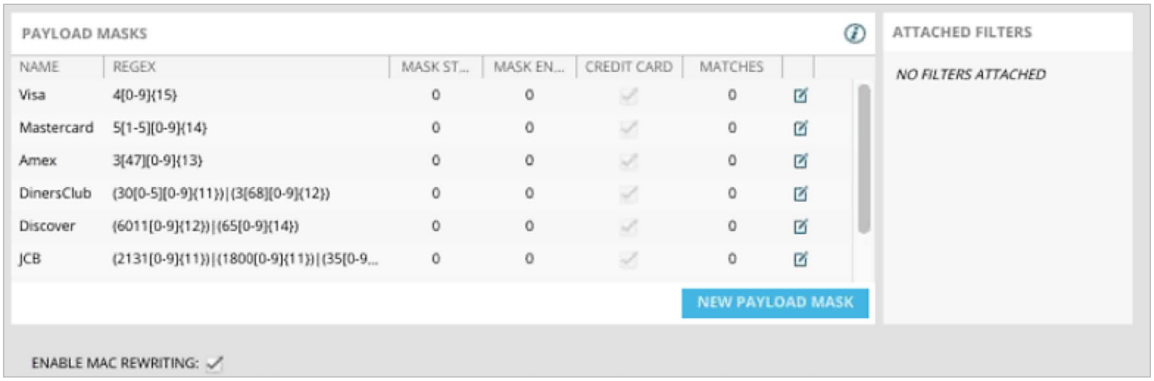

Figure 14. Implementing Data Masking

Conclusion

As a category, network packet brokers have seen many advancements, and appliances like Vision ONE now offer a suite of features that were formerly endpoint solutions. By leveraging even some of these features—including data masking, TLS decryption and signature-based application detection—organizations can experience a significant performance boost to their networking and security tools. Many larger organizations are planning to roll out 40Gbps or higher capacity networks in the short term, and with the increased throughput comes increased bandwidth utilization. This is likely to lead to significant purchases in the networking department and an increased focus on ensuring these purchases are capable of both handling increased traffic and supporting the organization. As an NPB, Vision ONE plays a critical role as the brokering technology overseeing proper packet delivery. To expand on this concept, consider the sheer volume of traffic our networking devices may be responsible for handling. Without the broker providing filtering, shaping and trimming, and without significantly reducing the encryption overhead, organizations face the potential of higher costs and increased latency.

Finally, delivery matters. Vision ONE seems to have delivered on the goal of reducing network complexity and future-proofing network architecture. As networking capabilities increase and the need for redundant solutions with line rate processing follows this trend, Ixia and Vision ONE are well-situated to help organizations achieve their goals with a full-featured network packet broker technology.

About the Author

Serge Borso, a SANS community instructor and analyst, teaches the Defending Web Applications Security Essentials and Web Application Penetration Testing and Ethical Hacking courses for SANS. As owner and principal consultant of SpyderSec, an information security organization, he leads penetration-testing engagements and has helped dozens of organizations improve their security posture. Serge's accomplishments include developing vulnerability management programs, creating security awareness training solutions and implementing a biometric security system for online banking. An active member in the InfoSec community, he serves on the board of directors of the large, active Denver chapter of Open Web Application Security Project (OWASP). Serge holds several security certifications, including CISSP, GPEN, GCFA, GWEB and GWAPT.

Sponsor

SANS would like to thank this paper's sponsor:

ixia
A Keysight Business

Last Updated: August 5th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Jose 2019	San Jose, CAUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Prague August 2019	Prague, CZ	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Minneapolis 2019	Minneapolis, MNUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS MGT516 Beta Three 2019	Arlington, VAUS	Aug 19, 2019 - Aug 23, 2019	Live Event
SANS Amsterdam August 2019	Amsterdam, NL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Chicago 2019	Chicago, ILUS	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Virginia Beach 2019	Virginia Beach, VAUS	Aug 19, 2019 - Aug 30, 2019	Live Event
SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS New York City 2019	New York, NYUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Hyderabad 2019	Hyderabad, IN	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, DK	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Philippines 2019	Manila, PH	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Munich September 2019	Munich, DE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Brussels September 2019	Brussels, BE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Canberra Spring 2019	Canberra, AU	Sep 02, 2019 - Sep 21, 2019	Live Event
SANS Network Security 2019	Las Vegas, NVUS	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, NO	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS Dubai September 2019	Dubai, AE	Sep 14, 2019 - Sep 19, 2019	Live Event
SANS Raleigh 2019	Raleigh, NCUS	Sep 16, 2019 - Sep 21, 2019	Live Event
Oil & Gas Cybersecurity Summit & Training 2019	Houston, TXUS	Sep 16, 2019 - Sep 22, 2019	Live Event
SANS Rome September 2019	Rome, IT	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Paris September 2019	Paris, FR	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Bahrain September 2019	Manama, BH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
Supply Chain Cybersecurity Summit & Training 2019	OnlineVAUS	Aug 12, 2019 - Aug 19, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced