Brought to you by

NETSCOUT

Security Visibility at Scale

for dummies

A Wiley Brand

NETSCOUT Special Edition

Achieve proactive security operations

Drive increased business assurance

Simplify adds, tests, and changes

Chad Russell

About NETSCOUT

With more than 30 years of research into network operations, NETSCOUT has developed the unique ability to capture, order, and analyze all of the network traffic in real time. NETSCOUT nGenius Packet Flow Switches optimize the flow of traffic from the network to security systems and monitoring tools. These appliances collect and organize packet flows — creating a unified packet plane that logically separates the network from the tools.

Packet flow switches are used by enterprises and service providers alike to optimize and scale out both service assurance and cybersecurity deployments, so that IT managers can spend less time in adding, testing, and managing their tools. For more information, please visit **www.netscout.com/PFS**.

Security Visibility at Scale

NETSCOUT Special Edition

by Chad Russell

for dummies®
A Wiley Brand

Security Visibility at Scale For Dummies®, NETSCOUT Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-37962-1 (pbk); ISBN 978-1-119-37950-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher’s Acknowledgments

We’re proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Senior Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Susan Blessing

Production Editor: Magesh Elangovan

Table of Contents

Introduction

In the world of network security, change is the only constant. Threats such as ransomware, persistent threats, and nation-state actors have emerged and continue to evolve in complexity and volume. The scales are tipped against the defender.

Generally, threat actors are better organized and funded than ever before, while at the same time IT security teams are understaffed. The uneven playing field places a greater emphasis on security tools and architectures to ensure true business assurance.

About This Book

With the advent of the cloud and the Internet of Things (IoT), security threats are increasing in scope and volume. Network architects and business leaders are challenged with facilitating complete and timely network security visibility without affecting production environments.

This book shows you how architecting a modern security visibility network infrastructure can help your business adapt to new threats, lengthen the usefulness of your current security tool investments, and enhance uptime and availability to drive increased business assurance.

Foolish Assumptions

For this book, you should have a basic understanding of networking protocols and architectures. You should also understand the basics of network security.

Icons Used in This Book

REMEMBER

I use this icon when you need to stop for a second and make sure you recall a key concept before moving ahead.

TIP

You'll want to keep certain details in mind as you analyze your own security visibility environment. When you see the Tip icon, put that information in your back pocket to save for later.

TECHNICAL STUFF

There are a few small pockets of depth in this book. I use this icon to call out the technicalities.

WARNING

Throughout the book, I point out places where you might need to take some extra consideration.

Beyond This Book

There is only so much I can cover in this book. For more information, please visit `www.netscout.com`.

Where to Go from Here

After reading this book, you will have a better understanding of some of the key challenges that are specific to network security visibility. As either a technologist or a business leader, you will understand the direction that the security visibility industry is taking and how you can best suit these emerging trends to fit your current and evolving business requirements.

IN THIS CHAPTER

- » Understanding business assurance
- » Surveying the state of security threats
- » Recognizing obstacles to visibility

Chapter 1 Seeing the Entire Threat Landscape

The threat landscape is constantly expanding. The sheer number of threats and amount of overall network traffic processed by organizations is compounding exponentially year over year. The number of devices is increasing, as well as the number of attacks and attack sophistication.

From the perspective of the chief information officer, chief information security officer, and line-of-business executives, this means that in order to deliver business assurance, you need the right combination of staff, skills, expertise, and technology.

Understanding Business Assurance

Business assurance is a powerful combination of service assurance and cybersecurity. It's at the heart of what keeps business moving and progressing. Without business assurance, predictability is at risk.

Service assurance

Assuring uptime and performance of network services allows the business to execute the vision of the board and the chief executive officer. In this context, service assurance involves the establishment of predictable performance, which is achieved through agile service visibility. Service assurance is about making sure that applications are working the way they should for end-users, the network is functioning optimally, and unified communications do not exhibit glitches.

Cybersecurity

While service assurance focuses on performance and uptime, cybersecurity ensures the integrity of the network. It focuses on the protection of the sensitive data traversing your network. To gain this level of insight without affecting the network, you must have a service visibility architecture that allows you to deploy security tools inline or passively without compromising performance or availability.

REMEMBER

Business assurance solutions reduce risk and streamline operations.

Surveying the State of Security Threats

With the advent of streaming video, mobile, and Internet of Things (IoT) devices, network traffic and potential embedded threats present themselves as a larger number of needles in an ever-growing haystack of network traffic.

This means that a security professional’s view of the threats must be real-time, contextual, historical, current, and complete.

The threat landscape

The threat stage includes an ever-increasing number of actors. Some of these actors include governments and organized crime networks.

These entities are leveraging tools in the form of ransomware, distributed denial-of-service (DDoS) attacks, polymorphic worms and viruses, and social engineering as part of a complex and well planned kill chain to disrupt businesses and *exfiltrate* sensitive information (transfer data from a computer without authorization).

Well-organized and well-funded attackers are striking businesses of all types and sizes through command and control networks that carefully orchestrate blended threats to exercise financial and political advantage. These attacks can degrade services and subsequently reduce an IT team's ability to provide business assurance.

REMEMBER

The attackers have time on their side. As often said, defense is much more difficult than offense. The attacker only needs to be right once.

The defender, on the other hand, needs to be right every single time. This is a difficult proposition considering that attackers know what they are going to do and when. Defenders must constantly be on the ready. Defense wins championships, right?

Knowing the key threat landscape developments is critical:

- **More threat types and categories:** New threat types such as ransomware, advanced persistent threats (APTs), and botnets
- **More complex actors:** Nation-state/cybercrime organizations
- **Blended threats:** Attacks incorporating multiple threats such as ransomware, worms, and DDoS attacks
- **Proliferation of botnets and dark net tools**

One emerging threat category is the advent of Internet of Things (IoT) botnets. Devices such as IP traffic cameras and home sensors can be compromised "en masse" to leverage as botnet zombies and further compound the headaches associated with DDoS attacks.

Many hackers use DDoS attacks as diversions while embedding surgical strikes in their midst. To defend against this technique, analysis of traffic must be at line rates, aggregated, correlated, contextual, and complete without affecting legitimate network traffic.

Collecting and correlating data at the perimeter is not enough; networks must monitor insider threats and all traffic within the core switching environment. The necessary monitoring adds exponential complexity and load to network environments that are already bursting at the seams.

REMEMBER

Five prominent types of data breaches include:

- Insider breaches
- Spearphishing/social engineering
- Exploits against unpatched systems
- Lost devices
- Compromised endpoints/botnets

Cost of cybercrime

When calculating the true impact of cybercrime, you must calculate a number of quantitative and qualitative factors. Let's face it — when you're putting together a business case, the first thing you're asked is for an itemized list of tangible costs, expenses, and benefits.

This is an interesting discussion. One reason is that some of the top companies in the world own an ever-decreasing number of assets. One of the largest transportation companies in the world (Uber) owns no cars. Companies such as Airbnb and Alibaba have more than 80 percent of their net worth tied up in intangible assets.

In the past, business leaders were quick to dismiss intangibles. Today, these "negligible intangibles" make up a majority of many modern businesses.

As part of a survey of more than 2,000 executives and employees worldwide, the Ponemon Institute states that hacking attacks cost the average American firm $15.4 million per year, double the global average of $7.7 million annually. Offsetting these costs is critical to the bottom line for organizations.

So what are the primary impacts and outcomes of security incidents? The primary outcomes of security incidents are:

- Loss of business through service downtime
- Brand reputation loss due to reporting of the incident
- Direct losses impacting customer accounts

WARNING

So what's driving these costs? Here are some of the causes:

- Remediation costs
- Loss of customers
- Business disruption
- Regulatory fines
- Legal costs
- Negative public relations
- Direct financial loss
- Notification costs
- Credit card reissues, identity theft repair, and identity monitoring services

Recognizing Obstacles to Visibility

So, am I telling you that you need to upgrade your 747 Rolls-Royce engines to rocket engines without landing the plane? In short, yes.

Change management

Network speeds are on the increase. First there was 1GB, then 10GB, and now 40GB speeds are the new core switching standard. Some enterprises have already migrated to 100GB in their cores. That's great, and we all appreciate speed, but what does that mean for security infrastructure? Well, in the traditional world of network visibility, we utilize Test Access Points (TAPs) or deploy devices inline. In those types of environments, we must match line rates with device processing speeds.

So what about those 1GB intrusion prevention system (IPS) devices? Am I telling you that you need to upgrade those every time you upgrade your switching infrastructure? Suppose you upgrade them to 10GB. What happens when you move to 40GB?

REMEMBER

Change is the new normal. Network architects must design solutions that accommodate change. Just as the development world has adopted agile development and micro-services architectures, architects must consider a similar approach with infrastructure and networking services.

Security solution churn

Well, back to our change management discussion. To match your new switching line rates, you can bite the bullet and upgrade the inline devices (such as firewalls and IPS devices), but that seems to be a fairly rigid and costly approach.

As far as the out-of-band devices such as intrusion detection systems (IDS) are concerned, what are the ramifications of simply sticking with the 1GB devices? Well, if the new switching infrastructure is pumping out 10GB per port and your IDS has only three 1GB ports, you obviously need to drop some traffic.

These are the key security visibility considerations:

- Addition of security solutions to address new threats.
- An increasing number of threat categories, including advanced threat management, network forensics, IDS, IPS, cloud provider security, data loss protection (DLP), email security, and proxy security.
- More visibility is required into core networks because of insider data breaches potentially causing network disruption.

TECHNICAL STUFF

So what about new classes of threats? Your security people are now saying that DLP was brought up as a key concern in the last external pen test. They are recommending a DLP appliance that is inline.

Some additional questions that come up operationally include:

- Where do I place these new devices in the inline chain?
- What happens when the line rate of these devices outdates my new switching and routing infrastructure?

- What about all the non-relevant traffic that my inline security devices are processing, such as streaming content and headers?

WARNING

The considerations are several-fold. Make sure you are thinking several steps ahead. New devices, capabilities, speeds, and feeds will be the norm.

Complex inline deployments

Because of many of the challenges that have been brought up to this point, some organizations have not maximized their use of inline blocking technologies.

These are the barriers to turning on inline blocking:

- Data throughput and parsing concerns
- Concerns with interoperability with monitoring support infrastructure
- Existing bandwidth limitations
- Network rigidity
- Multiple points of failure

Implications to your network

Ultimately, if your security controls are affecting your ability to deliver services to your customers and end-users, you have an issue. It's almost a denial-of-service issue if you think about it. Except that the culprit isn't an attacker; it's your network architecture.

TECHNICAL STUFF

Network implications of the aforementioned challenges include:

- Disparate security control points without aggregated visibility
- Disruptive and expensive security upgrades
- Service and operational risk
- Under- and over-utilization of security tools
- Negative impacts to speed, performance, and availability

REMEMBER

Business assurance is a powerful combination of service assurance and cybersecurity. It's at the heart of what keeps business moving and progressing. Without business assurance, predictability is at risk. To deliver business assurance, you need the right combination of staff, skills, expertise, and technology.

IN THIS CHAPTER

- » **Looking at standard network visibility**
- » **Capturing network traffic using TAPs**
- » **Designing a purpose-built visibility infrastructure**

Chapter 2 Understanding Security Visibility Basics

Security visibility serves as a foundational element for business assurance. As a chief information officer or chief information security officer, you need an infrastructure that collects all the right data all the time. There are more haystacks and more needles, and you have a limited amount of human resources and technology.

You need an approach that is efficient, agile, and scalable.

Looking at Standard Network Visibility

Although I've titled this section "Standard Network Visibility," you could just as easily call it "Legacy Network Visibility." To be clear, the use of Switched Port Analyzer (SPAN) ports, and to some extent Test Access Points (TAPs), represents an outdated and largely ineffective approach. This section helps you understand why.

SPAN ports

You can configure SPAN ports to mirror traffic from all the switches' networking interfaces for the purpose of monitoring and analysis. SPAN ports are used to analyze traffic for performance and security deviations. When under significant load, switches are designed to start dropping packets sent out to SPAN ports to ensure that production traffic going through the switch is not affected. This means you are no longer able to perform the necessary monitoring.

Network interfaces

Network interfaces typically are either copper based or fiber based. Common speeds are 100MB and 1G. Newer interfaces and transceivers support 40G and 100G line rates.

Capturing Network Traffic Using TAPs

Network TAPs are hardware devices that provide a means of accessing data flowing across a physical network connection. In its simplest form, a TAP is a device with an input and two outputs. The extra output typically is used by passive monitoring devices. Because networks are normally bi-directional, TAPs usually have two network inputs (one for each direction), two network outputs, and two monitoring outputs.

Types of TAPs

TECHNICAL STUFF

Although the technology behind TAPs is fairly basic in nature, you can deploy TAPs in several ways. These include:

- **Network: 1:1 relationship:** For a given input, all network traffic is sent to a monitoring network.
- **Aggregation: M:1 relationship:** A given number of inputs from the production network are aggregated to a single output, which connects to a monitoring network.
- **Regeneration: 1:M relationship:** In this scenario, a single copy of production traffic is duplicated "X" amount of times for different monitoring devices.

FAILING OPEN VERSUS FAILING CLOSED

TAPs support only fail-open configurations. If a TAP loses power, all traffic is allowed through the device functioning similarly to a network hub. TAPs do not support fail-closed configurations.

TAP deployment — inline versus passive

Network security systems fall into two categories: active and passive. Active systems are referred to as *inline* systems.

TAPs with passive systems

Passive systems typically operate *out of band*, meaning that they are in a listen-only mode and simply collect copies of traffic going through certain switching infrastructure on your network. Over time, technologies such as SPAN ports and TAPs have been a common means of replicating production traffic.

Common passive network security systems include:

- **IDS:** Intrusion detection systems
- **Network forensics:** Tools that historically catalog network data for forensics analysis and correlation

Security operations centers use passive security systems to report on network-based threads and serve as a basis for capacity planning.

REMEMBER

Network TAPs are hardware devices that provide a means of accessing data flowing across a physical network connection. In its simplest form, a TAP is a device with an input and two outputs. Because networks are normally bi-directional, TAPs usually have two network inputs (one for each direction), two network outputs, and two monitoring outputs.

Examples of passive network performance tools include:

- **Application performance monitoring:** Allows application owners to see applications, trends, and performance at a glance

- **Network performance monitoring:** Allows network operations teams to address performance issues and conduct capacity planning exercises
- **Unified communications monitoring:** Monitors unified messaging protocols, such as Voice over IP (VOIP) and SIP connections
- **Network behavior analytics:** A way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal baselines

TAPs and inline tools

Active or "inline" network tools are literally in the path of production traffic. The most common example of an inline security tool is a firewall; traffic has to go *through* the firewall, not routed around it. Over time, the traditional approach to incorporating inline security systems has been to physically cable them directly to the production switching and routing infrastructure.

Types of inline security systems include:

- **IPS:** An intrusion prevention system (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- **Application layer/next-generation firewalls:** A next-generation firewall (NGFW) is an integrated network platform that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using inline deep packet inspection (DPI).
- **Secure email gateways:** These solutions protect email clients and can enforce company policies on email use and information leakage. A secure email gateway filters unwanted email suspected of containing malware or phishing, and enforces corporate and regulatory policy compliance.
- **Web security gateways:** Secure web gateway solutions protect web-surfing PCs from infection and enforce company policies. A secure web gateway is a solution that filters unwanted software and malware from user-initiated web/Internet traffic and enforces corporate and regulatory policy compliance.

- **DLP devices:** Data loss protection (DLP) is a set of technologies and inspection techniques used to classify information content contained within an object — such as a file, email, packet, application, or data store — while at rest (in storage), in use (during an operation), or in transit (across a network).
- **DDoS prevention systems:** Distributed denial-of-service (DDoS) systems are generally comprised of content distribution networks that can absorb the load of traffic at the Internet's edge.

Examples of inline network performance optimization tools include:

- **WAN optimization:** Wide area network (WAN) optimization and acceleration technologies are strategic tools that are focused on accelerating a broad range of protocols and applications across the WAN/Internet.
- **Web caching:** This provides temporary storage (caching) of web documents, such as HTML pages and images, to reduce bandwidth usage, server load, and perceived lag, such as forward and reverse proxy servers with caching enabled.
- **Application acceleration:** Application acceleration uses a number of technologies to improve application performance and response time over network connections.
- **Traffic shaping (QoS):** This is a network traffic management technique that delays some or all datagrams to bring them into compliance with a desired traffic profile.

Inline or "active" network performance tools have traditionally been hard wired to the production switching infrastructure. Network engineers deploy network performance tools in order to modify production traffic in a way that optimizes performance.

Passive TAPs versus bypass TAPs

Bypass TAPs (or bypass switches) are typically used for inline deployments such as those described in the preceding section. The purpose of a bypass TAP is to ensure that traffic continues flowing in the event that an inline system such as a firewall or IPS fails.

Managing Packet Flows with a Visibility Infrastructure

Packet flow switches (also known as *network monitoring switches* or *network packet brokers*) are appliances that are specifically designed to switch and optimize packet flows from the network to cybersecurity and service assurance platforms.

Defining packet flow switching

Packet flow switches optimize traffic for consumption by performance tools and security systems, either inline or passive, or both.

Packet flow switches provide key functionality that allows more efficient system performance. Some of these features are:

- **Aggregation:** Combining multiple source streams into a common stream for tool consumption.
- **Replication:** Involves making additional copies of a given traffic stream needed by multiple devices.
- **Addressing line rate discrepancies:** Packet flow switches decouple physical device connections with differing line rates and manage the disparate speeds (referred to as *rate* or *speed conversion*).
- **Microburst handling:** Measuring and mitigating the effects of microbursts, which manifest themselves during aggregation or speed conversion.
- **Load balancing:** Balancing sessions across devices based on capacity and availability.
- **Filtering:** Filtering out unnecessary traffic and forwarding only relevant traffic based on tool requirements and capability.

Packet flow switching versus TAPs and SPAN ports

SPAN ports and TAPs make simple bulk copies of traffic. SPAN ports tend to drop traffic when the switch becomes overwhelmed with traffic. How does it decide which traffic to drop? Were those packets important?

Here's a real-world example of why this can be important. You are the CIO of a large online retailer. It's a Tuesday afternoon much like any other. You receive a phone call saying that your e-commerce site is under a DDoS attack. The security operations team is focused on minimizing the impact of the DDoS attack and making sure that all critical services stay online. Six hours later, the attack subsides, and the staff that was on call can go home and get some rest.

Three months later, the Secret Service contacts your compliance department to notify you that you've been breached. Customer account information for more than 30,000 accounts has been exfiltrated and is for sale on the dark web. You ask your compliance officer when the breach happened, and the response is that it happened about three months ago, on a Tuesday afternoon.

But wait — it was only a DDoS attack, right? Well, embedded within that DDoS attack was a surgical breach. The DDoS attack was a diversion and was not detected because the SPAN ports on your switches were overwhelmed and were dropping traffic. As a result, your IDS tools weren't seeing everything that was happening. You didn't have full security visibility.

A packet flow switch could have been used to filter out irrelevant traffic from the DDoS attack so that your IDS appliances could see the surgical strike. Additionally, your IDS systems would not have been overwhelmed because your packet flow switching infrastructure was filtering out the noise.

TIP

This story isn't fictitious. I've seen similar situations play out much as I describe in this scenario. Make sure you have a well thought-out security visibility design that utilizes packet flow switching to ensure business assurance.

Why performance matters

So the impact of DDoS attacks brings up the issue of performance. Why does performance matter? In the preceding example, the IDS appliances operate at a 1GB line rate but the network switching infrastructure is running at 10GB line rates and was at full capacity.

If you were using TAPs, the IDS systems wouldn't have been able to handle the load. If you had a purpose-built packet visibility infrastructure utilizing packet flow switching for your IDS infrastructure, you could have made sure only the relevant traffic was being filtered down to your IDS systems so they could operate at capacity and not miss a surgical strike that was embedded in a DDoS attack.

But the answer isn't even as simple as that. When you're filtering traffic, performance matters. You need to keep up with the traffic that is filtered at line rates. Some solutions do this in software with generic server appliances, while others use ASIC chipsets and operate at the hardware level. This capability becomes especially important when you have inline security and performance appliances.

REMEMBER

Other reasons that packet flow switches and intelligence at the packet visibility layer are important include:

- **Sophisticated protocols:** Voice over IP (VOIP) and multicasting
- **Tunneled environments:** Generic Routing Encapsulation (GRE), Multiprotocol Label Switching (MPLS), and Internet Protocol Security (IPSec)
- **Traffic aggregation to centralized monitoring systems:** Requires specialized handling and tagging

Achieving operational simplicity

Every network designer knows that change is the only constant. Designers always strive to build environments that are agile and flexible, yet high performance.

You want to be able to introduce new security systems and upgrade capacity in a way that minimizes impact to your production network environments.

REMEMBER

Packet flow switches offer operational simplicity by:

- Increasing the reach of existing monitoring or security systems
- Avoiding costly and disruptive upgrades
- Simplifying change management

IN THIS CHAPTER

- **Building a unified packet plane architecture**
- **Optimizing the design**
- **Optimizing the use of network tools**

Chapter 3 Creating Packet Flow Visibility

To make the right decisions and enforce security, you must be able to see the entire network traffic landscape and parse it accordingly. To enable business assurance from a cybersecurity perspective, you must have a security visibility framework in place that accounts for inline and passive security systems.

Building a Unified Packet Plane Architecture

The right packet flow switch architecture allows you to logically separate your network from your network monitoring and security infrastructure. It simplifies tests, adds, and changes — without creating potential network disruptions or security holes.

Achieving service assurance and cybersecurity objectives

Networks are continually changing and expanding. Networking is undergoing a virtualization revolution much as servers have in the past decade. Software defined networking (SDN) is a driving architectural principle for modern networking deployments.

You need to have a packet visibility architecture that is logically decoupled from the underlying physical network in order to accommodate growth and change, and to extend the reach of existing performance and security tool sets.

Leveraging resources and skills

Cybersecurity skills are in high demand. Consequently, hiring experienced cybersecurity professionals is becoming more of a challenge than ever before.

Forbes magazine reported the global figure at 1 million cybersecurity job openings. Demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million.

The bottom line is that the haystacks of network data are multiplying exponentially, and the number of skilled security professionals available to manage this information is not keeping up with demand.

REMEMBER

More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.

Optimizing the Design

An architect can use any of several packet flow switch architectures to deploy a security visibility solution. These include daisy-chaining, hub-and-spoke, and mesh architectures. Mesh architectures are optimal because they offer the greatest fault tolerance and flexibility. Therefore, this section focuses on the mesh architecture.

Self-organizing mesh architecture

A mesh architecture for packet flow switching is only as capable as the packet flow switch technology that you choose to deploy. Because of the potential complexity of mesh configurations, the best practice is to leverage packet flow switches that can self-organize their topologies with minimal administrative intervention. If any of the links fail, traffic must be automatically redirected through available packet flow switching links in order to maintain traffic visibility and ensure security rule enforcement for both inline and passive security systems.

Characteristics of a self-organizing mesh architecture include:

- Self-healing
- Centralized administration
- Automated failover
- Dynamic load balancing

REMEMBER

When deploying inline packet flow switching, you have no room for error. Therefore, a self-organizing mesh architecture is necessary to achieve optimal network availability, integrity, and performance.

Scale and density

Security systems all have a limited amount of resources from a CPU, RAM, and interface perspective. Security architects often need to upgrade their security infrastructure in tandem with core network upgrades.

TIP

Packet flow switches can be less costly than security systems. By introducing this layer of abstraction between your security systems and the network, you drive down the cost and frequency of system upgrades. Additionally, by filtering out unnecessary traffic, you improve the operational efficiency these systems, reducing the need for frequent upgrades, which improves your bottom line.

Implementing a unified packet visibility architecture allows you to scale out and scale up. Packet flow switching landscapes should support traffic density of up to 40GB and 100GB. They also should support line rate buffering, utilizing hardware to minimize the latency that is specific to active security tool deployments such as intrusion prevention systems.

REMEMBER

These two factors affect packet flow switching density and scale:

- **Hardware versus software design:** Hardware is higher performance.
- **1GB/10GB/40GB/100GB line density:** Higher density is best for growth and performance.

Inline (active) versus out-of-band (passive) security deployments

Test Access Points (TAPs) only support passive deployments. You cannot use TAPs for inline systems such as firewalls or IPS installations. Traditionally, bypass switches have been used for inline devices to ensure that in the event of the failure of the inline device, the device can be bypassed altogether.

Bypass switching is a rudimentary approach because these switches do not apply any logic to incoming or outgoing traffic. Bypass switches are an on-and-off-only method. They essentially do nothing more than pull the security system out of the path if it is not responding.

In contrast to bypass switches, packet flow switches can provide the following capabilities for inline and passive security deployments:

- Packet slicing
- Stripping and de-encapsulation
- De-duplication
- Port and time stamping
- Line rate translation
- Microburst handling
- Advanced packet filtering

Logically linking to existing security systems

When using TAPs or bypass switch-based architectures, you are required to physically couple these devices inline with your production network architecture.

This requirement introduces rigidity into the architecture. What if you need to upgrade your switch architecture? How will that affect your inline and passive tools? Will you need to upgrade them simultaneously as a result? How much downtime will that introduce?

Also, what happens when you need to add a new security system into your architecture? More downtime, right?

And lastly, what if you need to change the order in which the data is processed by your inline security systems?

Obviously, lots of questions come up when you are dealing with the rigidity of TAPs and bypass switch-based network visibility deployments.

Now, what if you had a way to decouple your inline and passive security systems from the production network and logically chain them via software configuration? Well, the solution is at hand. Packet flow switching with NETSCOUT nGenius Packet Flow Switches (PFS) allows you to create logical chains for your devices without any modifications to physical connectivity. This solution virtually eliminates the downtime associated with security systems upgrades and environmental modifications.

Optimizing the Use of Network Security Systems

Extending the useful life of expensive network security systems drives down costs and minimizes changes to the production network. Techniques such as session flow-based load balancing and advanced packet filtering allow network engineers to fine-tune which traffic — and how much of that traffic — is sent to a particular device based upon that device's purpose and capacity.

Taking advantage of load balancing

Load balancing that can take sessions and packet flows into account enables administrative control of traffic distribution to security systems. This feature thus increases output capacity while maintaining session integrity and performance.

For example, you can capture a 40G network and automatically balance it across multiple 10G or 1G monitoring tool ports based on user-defined session criteria. The load balancing can operate in tandem with hardware-based filtering or independently.

Applying filtering

For packet filtering to be effective with inline security system deployments, it has to operate at line rates. It must be able to buffer, accounting for microbursts without dropping packets. You can achieve this result through hardware-accelerated packet flow switches.

Filtering out unnecessary traffic allows you to discard traffic that doesn't pertain to a particular security or monitoring system. For example, an inline IPS might not need to process every packet of a video stream but instead process some of the control protocol traffic instead. The result is a much smaller data footprint, which improves the effectiveness, efficiency, and performance of the IPS appliances deployed in your production environments.

IN THIS CHAPTER

- » Processing line rate traffic in hardware-accelerated packet flow switches
- » Advanced packet conditioning

Chapter 4 Conditioning and Manipulating Packets for Optimal Use

Optimizing packet flows for security and performance monitoring systems allows you to further the useful life of your existing tools from a capacity perspective. Packet flow optimization also ensures that you will not lose relevant traffic and maintain complete security visibility at all times.

Processing Line Rate Traffic in Hardware-Accelerated Packet Flow Switches

Certain applications and network protocols tend to be bursty and jittery in nature, such as voice and video. In some cases, switches and routers are designed to buffer data when forwarding to Switched Port Analyzer (SPAN) ports, which also increases the amount of traffic bursting out to your network security systems.

Because these bursts happen over very short periods, they are often referred to as *microbursts.*

Although network utilization may appear low over a span of hours, or even minutes, you will likely see spikes that exceed 100 percent at any given time. These spikes can occur at sub-second intervals and are a threat to network security visibility. If any of this microburst traffic is dropped or delayed, it can create holes in the overall security visibility of your network.

TIP

The NETSCOUT nGenius Packet Flow Switches (PFS) offer a microburst mitigation feature that provides the ability to measure at a sub-millisecond level and record the network utilization with a millisecond granularity. This capability provides evidence of the occurrence of microbursts, and you can use this data on a continuing basis to monitor the ongoing microburst activity within your network.

Handling microbursts

In order to prevent packet loss in microburst situations, you must have hardware with ample buffering capacity. Sufficient buffering allows the traffic to be normalized, relative to the speed of the receiving devices.

To address the problem of microbursts, the NETSCOUT nGenius PFS high data-burst buffer (HDBB) provides a much larger than normal buffer behind network ports. This buffering allows you to aggregate traffic, load-balance, and convert line speeds without losing any traffic.

TIP

NETSCOUT provides 1,000 to 4,000 times more buffering behind each port than is available, in total, on a normal tap, and regulates microbursts with a minimum amount of latency. This capability ensures that you can address any and all threats as they occur.

Active inline aggregation translation

When you're aggregating active inline traffic, the importance of keeping every packet and ensuring that the respective inline security systems can handle the flows cannot be understated. Aggregation places stress on inline systems such as firewalls and IPS devices when used to combine traffic from multiple sources, speed-convert, or load-balance traffic. When multiple ports are aggregated, the potential for microbursts compounds itself, so expanding buffering becomes an increasingly critical requirement. In addition, nGenius PFS can track packets being aggregated by appending virtual local area network (VLAN) tags to the front of the packet, to the back, or none at all, instead keeping track of the packets via a virtual routing table of sorts. Many security systems are not able to process traffic with multiple VLAN tags, either skipping inspection altogether or incorrectly blocking legitimate traffic. Such *aggregation translation* alleviates any issues you may encounter when aggregating traffic from multiple network segments.

Advanced Packet Conditioning

Packet conditioning is at the heart of any capable packet flow switching solution. The point is to make sure that all traffic is captured with minimal latency. This data can subsequently be parsed at line speed ensuring that only relevant traffic is sent to a security monitoring device, and at a rate that it can actually handle.

Slicing

Different network security and performance monitoring systems are designed to act at different layers of the stack. For example, a next-gen application firewall may be focused on all seven layers of the stack, while an IDS device may only be designed to inspect layers 2, 3, and 4. When a device receives traffic that it can't process, it must strip away irrelevant data that consumes the device's network, memory, and CPU resources. This type of functionality is referred to as *packet slicing.*

Conditional protocol slicing supported by NETSCOUT nGenius PFS extends the capability of packet slicing by enabling users to perform packet slicing where the traffic is captured, anywhere in a network. Unlike competitive technologies, nGenius PFS performs conditional packet slicing, which enables users to set slice points at different offsets for each packet and specify the types of traffic to be sliced, such as HTTP and VoIP protocols.

The idea is to perform the protocol slicing at the point of capture, instead of at each analytical tool. Subsequently, you can use conditional slicing to deliver uniform and consistent packet slicing across network segments.

REMEMBER

Not all slicing is done to improve performance. For example, by acting at the point of capture, *conditional slicing* allows for the removal of end-user identifying information, thus reducing the risk of a privacy breach. This technique enables compliance with the Payment Card Industry Data Security Standard (PCI DSS) and other regulatory standards.

Stripping and de-encapsulation

In most cases, network monitoring and security systems are designed to deal with standard IP traffic. They are not designed to deal with various encapsulation and tunneling protocols that may be encountered on WAN and LAN links.

In some cases, the presence of such protocols can limit the network monitoring and security system's visibility into the traffic, thereby reducing overall security visibility.

Encapsulation protocols that can be challenging for monitoring tools to interrogate include Generic Routing Encapsulation (GRE), GPRS Tunneling Protocol (GTP), Multiprotocol Label Switching (MPLS), VLAN, Cisco Virtual Network (VN), and many more.

REMEMBER

The NETSCOUT family of packet flow switches has capabilities that permit de-encapsulating or stripping protocols from traffic, thus allowing your network monitoring tools and security systems to have complete visibility into traffic patterns on your various network segments.

De-duplication

In many cases, network traffic is *duplicitous* in nature, meaning that you may have the same copy of a particular packet introduced onto the network numerous times. Anyone who has analyzed a network capture on a tools network will tell you that quite a bit of additional overhead is introduced in the form of duplicate traffic. Sometimes the packet duplication is a function of a particular protocol, aggregation, load balancing, or even application behavior.

NETSCOUT nGenius packet de-duplication capability removes packet duplicates and provides a significant reduction in the amount of traffic sent to your tools network.

Reassembly

Packet flow switches with advanced hardware acceleration enable line-rate packet optimization for a broad range of functions, which include reassembly of fragmented packets, stripping of tunneling or encapsulation protocol headers, and disposal of undesired payload data. nGenius PFS allows for full reassembly of fragmented user packets caused by GTP tunneling and security encapsulation for routing across networks.

Port and time stamping

In the network security realm, security analysts know that accurate and synchronized time stamps are the key to accurate forensics. In order to accurately correlate activities across multiple devices such as servers, IDS, and routers, establishing accuracy is maintained utilizing Network Time Protocol (NTP) services and time stamps. That being said, it must be accurate and ever-present.

One challenge is that many times, network packets are not time stamped because this functionality is not always needed or efficient, depending on the purpose of the protocol. Even if time stamps were in place, for many of the packets, they would likely be in many different formats.

Packet flow switches can introduce date and port stamping to mark traffic with additional metadata. This capability allows the insertion of a single or dual byte at the end of the payload of each packet, immediately before the cyclical redundancy check (CRC) in the packet's trailer.

REMEMBER

This metadata documents the input port of the packet flow switch module where the packet was captured, as well as the time at which it was captured. The CRC is recalculated after the addition of the port stamp to preserve the integrity of the packet, thereby enabling the port-stamped packet to be forwarded to the destination port(s) as a standard Ethernet packet.

REMEMBER

NETSCOUT nGenius Packet Flow Switches are equipped with programmable hardware, enabling them to perform at line rate with no bottlenecks. This high-performance packet processing resource provides hardware acceleration, where the advanced functions are performed, instead of on a CPU, which limits throughput and introduces variable latency.

IN THIS CHAPTER

- » Key use case: Ensuring risk-free and robust inline security
- » Key use case: Deploying security monitoring at scale

Chapter 5 Deploying Security Visibility at Scale: Key Use Cases

Having a network visibility infrastructure that can accommodate not only passive devices, but inline devices, represents a key modern-day requirement. Some companies may require more of an emphasis on prevention, depending on their business model, while others require only detection.

This chapter focuses on two key use cases. The first is a use case where customers need to deploy inline security in a mission-critical environment. The example references an online banking provider that utilizes inline security tools to protect online banking transactions.

The second use case focuses on a provider that must deliver passive security monitoring at scale. This example examines an online services provider hosting web services for numerous companies at global scale.

Key Use Case: Ensuring Risk-Free and Robust Inline Security

Internet Banking Corp. (IBC) is an online financial services provider operating globally with its headquarters and key data centers residing in North America.

As you can imagine, IBC cannot afford a breach of its customer account information. If the wrong users gain access, they can drain customers' bank accounts quickly.

Confidentiality, data integrity, availability, and performance thus stand out as key requirements for IBC.

IBC is also growing through acquisition as well as organically, so its network is growing accordingly. It needs a security visibility infrastructure that allows it to see and prevent any threatening and unauthorized traffic into its datacenter environments. Additionally, IBC needs to maintain availability as it accommodates the increased growth of its network infrastructure, while maintaining inline security throughout the process.

Considerations for inline security deployments

TIP

When designing and deploying a security visibility architecture for active, inline deployments, you must account for agility, scalability, availability, and interoperability.

Key capabilities of an inline packet-flow switching solution include:

- Security service assurance
- Speed/media conversion
- L2-L7 traffic grooming
- Load balancing and asymmetric routing support
- Security service chaining
- High availability for security services
- Thresholds, alerts, and auto-triggers
- Custom security system health checks

- Fault tolerance for security systems and networks
- The ability to deploy new security systems without disruption
- Actionable XML/API integration

Application health checks

NETSCOUT nGenius Packet Flow Switches (PFS) can perform detailed health checks of security systems. These checks can be both “negative” and “positive” in order to intelligently account for that system’s availability as opposed to the rudimentary “up/down” check.

TIP

With layer 7 application-level functionality health checks, nGenius PFS appliances ensure the security application or device is functioning as designed and configured. Health checks can be performed as often as every 100 milliseconds, ensuring that security systems are working properly. This capability decreases the time to detect security system failure. When used in combination with triggers, health checks enable automatic high availability and failover, thus simplifying operations and reducing the security risk.

Policy-based triggers

Policy-based triggers can be configured to initiate actions specific to monitoring and forwarding. IBC can configure triggers that provide specific Simple Network Management Protocol (SNMP) alerts and even force ports into a down state.

IBC has a network forensics infrastructure that captures detailed network data. The company can configure its Syslog server to capture security events as a fail-safe in the event that its network forensics collection appliance goes down.

IBC security engineers are often concerned that denial-of-service (DoS) attacks will flood their security systems, so they decided to configure policy triggers to send overflow traffic that can’t be absorbed by their network forensics appliance to the Syslog server as well. This practice allows IBC to efficiently utilize tools at its disposal automatically without calling system engineers at 3 a.m. to make the change. It can send out a simple alert letting the IBC security operations team know that the Syslog server in its DMZ is capturing overflow traffic during the DoS attack.

IBC's inline IPS appliances can be also affected by the DoS attack load. IBC engineers have configured a traffic threshold trigger using their inline packet flow switching infrastructure to perform conditional packet filtering during the DoS attack, removing duplicate packets. Additionally, the ample buffer space in the packet flow switches helps streamline packet flows during the attack.

Fail-safe active security and integrated network bypass

For IBC, having a proactive security posture is imperative. To prevent attacks, IBC has deployed inline security systems including next-generation firewalls (NGFWs) and intrusion prevention systems (IPS).

IBC also uses passive systems to collect detailed network forensics data for compliance and root cause analysis.

IBC has deployed nGenius PFS using active protection. This type of deployment enhances reliability and simplifies the process of scaling out the company's network security deployments.

If any of IBC's inline security applications fail, they may be bypassed, or traffic can be sent to another system. A unified visibility plane allows IBC to implement multiple security systems and create a defense architecture addressing a wide range of threats.

Addressing security system crashes

IBC has experienced inline security system crashes in the past that resulted in a 3-hour production outage. The company's Internet banking customers were not happy campers. When IBC's staff conducted root cause analysis, they determined that their inline monitoring network did not account for layer 7 abnormalities happening within their IPS device. In particular, the IPS was unnecessarily blocking quite a bit of production traffic. One of the IPS admins accidentally enabled some additional blocking rules that caused the outage. As IBC went about redesigning its security visibility architecture, the company knew it needed a solution that had intelligence at all layers of the stack to account for both man-made issues and device failures.

IBC now performs layer 7 health checks through the IPS to make sure that known-good traffic patterns are not being blocked, and if they are, their packet flow switches are configured to bypass the affected IPS and send an alert to the security operations team immediately. Also, if the IPS hangs, the packet flow switch can initiate a fail-open or fail-closed sequence, or redirect traffic to a standby tool.

Logical service chains

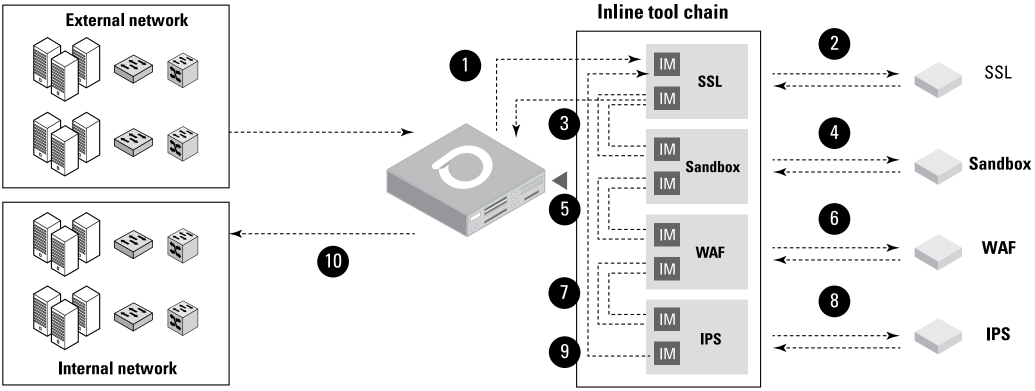
Security threats such as blended DDoS attacks, persistent threats, and ransomware have evolved quickly. Many times, organizations find themselves scrambling to react to the latest tools and technologies. As they incorporate newer technologies, their networks experience downtime and outages during these changes.

IBC security architects have indicated that they need an inline security visibility infrastructure that can accommodate new systems quickly with minimal production impact. Hardwired changes and shuffling of tools in their network is time consuming and represents a rigid and outdated security architecture. IBC decided to deploy an advanced security system chaining solution, as shown in Figure 5-1.

IBC has chosen NETSCOUT nGenius PFS, which enables the company to deploy a comprehensive inline security infrastructure in a virtual chain. Each security system can still receive exactly the traffic it requires, at the speed and in the form that it is designed to accommodate.

In IBC's new architecture, each nGenius PFS provides the assurance of network uptime and continuous monitoring needed in order to maintain uptime and business assurance for the customers.

In recent months, IBC has decided to incorporate an inline cloud access security broker (CASB) solution into its existing NGFWs, IDS, IPS, and network forensic security visibility and enforcement architecture. The company was able to introduce the inline CASB as part of the virtual tool chain in minutes with no additional cabling. IBC also had the option of backing the CASB out of production in seconds, if there were issues, with a simple software-based configuration change.



1. Aggregated traffic is sent to security tool chain where each tool can inspect any or all traffic before next tool
2. SSL receives traffic and decrypts it
3. Decrypted traffic is now available to all systems down the chain
4. Modified traffic is sent to the next tool in tool chain
5. Traffic is sent to the WAF
6. WAF receives HTTP traffic and filters threats
7. Traffic is sent to IPS
8. IPS checks for malicious activity, blocks it
9. Traffic goes to SSL for re-encryption
10. "Clean" traffic can now go to its destination

FIGURE 5-1: Advanced security system chaining allows for flexibility in security tool deployments.

Since IBC deployed its new CASB solution onto the wire, all the traffic flowing through the network is now examined by each security device. Once the inspection is finished, the traffic is sent back to the packet flow switch, which forwards the traffic to its final destination. This "aggregate once, serve many" approach enables every tool to get the type and portion of the traffic the company needs. At the same time, from the network's perspective, there appears to be only a single appliance on the wire.

REMEMBER

Active tool chaining enables deployment of an inline security infrastructure in a virtual chain, rather than cabling each system into a physical configuration. The key advantage of the PFS implementation is the over-50 percent reduction of ports needed and elimination of complex physical cabling configurations. As a result, each device gets exactly the traffic it requires, at the speed and in the form that it is designed to accommodate.

Key Use Case: Deploying Security Monitoring at Scale

Global Services Corp. (GSC) is an online services provider hosting web services for numerous companies at global scale. GSP has a multi-tenant infrastructure. Therefore, understanding traffic origination visibility is one of the company's key requirements. GSC must realize the economies of scale through its architecture so it can pass on those efficiencies to customers in the form of savings and SLA benefits.

GSC has deployed packet flow switches from NETSCOUT that allow its monitoring tools to identify from which links on the network a particular packet flow originates. GSC's switches are configured through customizable virtual local area network (VLAN) tagging. The packet flow switch can set custom VLAN tag ID values as traffic is forwarded to the monitoring tools.

This enables the tools to inspect traffic based on origin, which is critical in multi-tenant environments.

GSC is expanding its services and customer base at an almost exponential rate, so the company needed to have an architecture that could accommodate growth rapidly with virtually zero downtime.

GSC is a data-as-a-service (DaaS) provider, and some of its customers rely on these data feeds for critical operations and forecasting functions. Some of these feeds are large analytical datasets that are streamed in real-time.

With the large amount of traffic that must be inspected from the company's 40GB aggregated links, the processing capability of each security system in GSC's security visibility plane had to be considered to prevent overload and potential failure on any one system. GSC deployed nGenius PFS to support high-capacity (up to 32 instances) session-aware load balancing, providing security visibility and reducing risk by preventing over-subscription and potential failure on any one system. This capability is important because many of GSC's customers are subject to regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act. Therefore, visibility and reporting must always remain available, even during periods of growth and traffic spikes.

Incorporating existing security tools with varying line rates

GSC needed a solution that could address varying line rates between its network infrastructure and its security tools.

Many of GSC's security systems were still operating at 1GB, while their core switching infrastructure was in some areas being upgraded to 10GB. GSC had even forecast that it would need to upgrade to 40GB core switching capacity within the next 12 months or so, designing a security visibility solution that could adapt to upgraded network speeds while preserving investments in existing security appliances.

GSC took advantage of the high buffer capacities of nGenius PFS to address the varying line rates between its core network and its security appliances. In addition, the company took advantage of several other key capabilities of the solution to further minimize the impact of the line rate discrepancies.

GSC used the nGenius PFS conditional filtering capabilities in order to reduce the traffic to ports that are being oversubscribed. The company also balanced the traffic across more monitor ports and tools to ensure optimal usage and scale using the architecture shown in Figure 5-2.

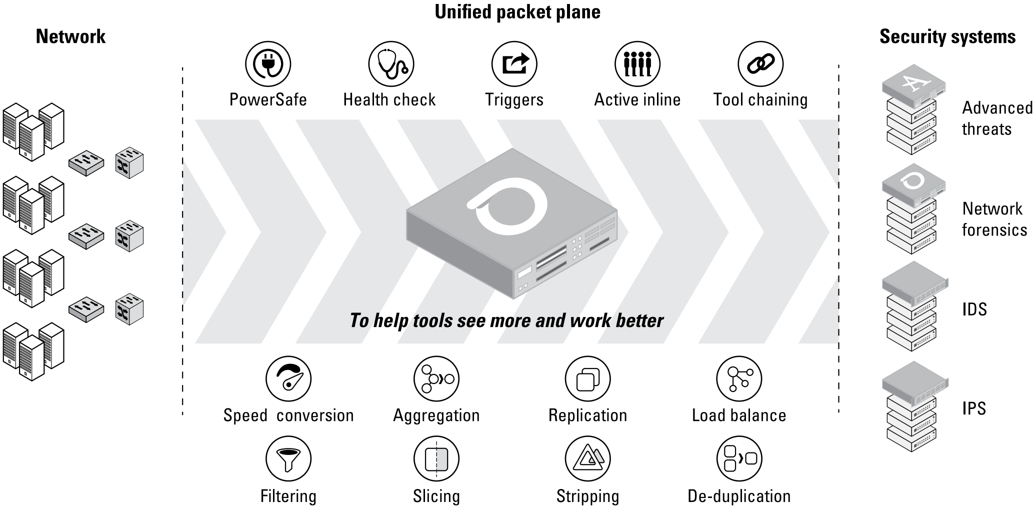


FIGURE 5-2: Unified packet plane with conditional filtering and traffic balancing.

Applying advanced packet conditioning

As a multi-tenant provider and sourcer of data-as-a-service (DaaS), GSC sources and distributes datasets to from and to networks all over the world. As a result, the company has many WAN layer tunneling protocols in place as part of this architecture.

GSC leveraged advanced protocol conditioning and de-encapsulation capabilities for various protocols, including GRE/NVGRE, GTP, MAC-in-MAC, MPLS L2/L3, TRILL, VLAN, VN-tag, and VXLAN traffic.

IN THIS CHAPTER

- » Security visibility at scale
- » Inline performance

Chapter 6
Ten Things to Ask Your Network Security Visibility Vendor

Now that you have a better understanding of the challenges associated with network visibility, you can ask more informed questions when talking to your security visibility solutions vendor. Here are some questions you should ask before pulling the trigger on your next investment:

» **How does your solution help achieve operational simplicity?**

As everyone knows, change is the only constant. Network designers always strive to design environments that are agile and flexible, and high performance.

Packet flow switches offer operational simplicity by:

- Increasing the reach of existing tools
- Avoiding costly and disruptive upgrades
- Simplifying change management

- **How does your solution handle advanced packet conditioning scenarios?**

  A robust packet flow switch solution should operate at line speed, using purpose-built hardware that is specifically designed to deliver customized traffic to each monitoring system.

  The solution should deliver advanced packet conditioning capabilities such as protocol de-encapsulation, conditional protocol slicing, time stamping, and speed conversion with microburst mitigation.

- **Does your solution handle microbursts using hardware acceleration?**

  Different applications and network protocols tend to exhibit bursts and be jittery in nature. These microbursts often happen at sub-second intervals.

  In order to prevent packet loss in microburst situations, you must have hardware with ample buffering capacity. Ample buffering allows for the traffic to be normalized, relative to the speed of the receiving devices.

- **How do you handle active security?**

  Test Access Points (TAPs) — physical network access points — only support passive deployments and can't be used for inline systems such as firewalls or intrusion prevention system (IPS) installations. Traditionally, bypass switches have been used for inline devices to ensure that in the event of the failure of the inline device, the device can be bypassed altogether.

  Bypass switching is a basic and coarse approach; it doesn't apply any logic to incoming or outgoing traffic. Bypass switches are an on-and-off-only approach that essentially does nothing more than pull the security system out of the path if it is not responding.

  Packet flow switch-based load balancing can take sessions and packet flows into account, and enables administrative control of traffic distribution to security systems, increasing output capacity while maintaining session integrity and performance.

- **Does your solution handle hybrid active/passive security visibility scenarios?**

  A flexible security visibility solution should allow for both passive (copies of traffic) and active (production) traffic to be sent to the same monitoring tool port. This feature allows security systems with a hybrid port capability to receive both passive and active traffic on the same port.

  Systems such as intrusion detection services (IDS) and intrusion prevention systems (IPS), which can perform both active and passive functionalities, are becoming more commonplace. A security visibility architecture should be able to handle both at the same time.

- **What about active application-level health checks (positive and negative)?**

  The solution should be able to perform an assessment of a security system's functionality with both "negative" and "positive" health checks. It is not enough to ping a security system for a "heartbeat" to see if it is on.

  If a security tool "hangs" and is neither "on" nor "off," you need to be able to automate failover accordingly.

- **How does your solution handle varying line speeds and active inline aggregation?**

  When you're aggregating active inline traffic, the importance of keeping every packet and ensuring that the respective inline security systems can handle the flows can't be understated. Aggregation places stress on inline tools such as firewalls and IPS devices when used to combine traffic from multiple sources. When multiple ports are aggregated, the potential for microbursts compounds itself, so expanding buffering becomes an increasingly critical requirement. In addition, your packet flow infrastructure should be able to aggregate traffic without the need for additional virtual local area network (VLAN) tags.

- **Does your solution support logical chaining of security services?**

  When using TAP or bypass switch-based architectures, you are required to physically couple these devices inline with your production network architecture.

This requirement introduces rigidity into the architecture. What if you need to upgrade your switch architecture? How will that affect your inline and passive security systems? Will you need to upgrade them simultaneously as a result? How much downtime will that introduce?

Make sure your security visibility solution will allow you to create logical chains for your security devices without any modifications to physical connectivity. This capability virtually eliminates the downtime associated with security system upgrades and environmental modifications.

- **Do you support a self-organizing mesh architecture?**

  A mesh architecture for packet flow switching is only as capable as the packet flow switch technology that you choose to deploy. Because of the potential complexity of mesh configurations, the best practice is to leverage packet flow switches that can self-organize their topologies with minimal administrative intervention.

  If any of the links or devices fail, traffic must be automatically redirected through available packet flow switching links in order to maintain traffic visibility and ensure security rule enforcement for both inline and passive architectures.

- **How does your solution help scale and manage security visibility for multi-tenant environments?**

  Having a unified packet visibility architecture allows you to scale out and scale up. Packet flow switching should support traffic density of 40GB to 100GB and be able to support line-rate buffering that utilizes hardware to minimize the latency that is specific to active security tool deployments such as intrusion prevention systems.

Achieve complete security visibility

As security threats grow in scope and volume, network architects and business leaders increasingly face the need to ensure complete and timely security visibility down to the packet level. This book shows you how architecting a modern security visibility network infrastructure can help your business adapt to new threats, lengthen the usefulness of your current security system investments, and enhance uptime and availability to drive business assurance.

Inside…

- See the entire threat landscape
- Understand security visibility basics
- Create deep packet flow visibility
- Support both inline and out-of-band systems
- Optimize packet flows
- Explore security visibility use cases
- Ask the right questions about visibility

NETSCOUT.

Chad Russell has been in the cybersecurity industry for more than 15 years. He leads and conducts security risk assessments for customers throughout North America. Chad has held numerous certifications including CISSP, CCNP, MCSE, and MCDBA.

for dummies®
A Wiley Brand

ISBN: 978-1-119-37962-1
Not for resale