Network Critical
The Window to your Network™

# NETWORK VISIBILITY CHECKLIST

Network Critical's Guide to Planning, Selecting and Deploying TAP and Packet Broker Technology

# CONTENTS

# INTRODUCTION

In today's increasingly digital world, the network has become the beating heart of every enterprise. It's expected to operate reliably while other parts of the business – from payroll and sales to customer relationship management and human resources – depend on it to run applications, share information, and more. Simply put, without a healthy network, your business could flatline. That's why managing network performance, security and analytics is a top priority for every savvy IT and network operations team today.

However, as transformational technologies like SD-WAN, cloud, virtualization and IoT are increasingly adopted, networks are becoming more complex. Now billions of bits of information are traversing network links every second, originating from countless sources and directed at all types of destinations. This traffic may be authorized data, malicious code or anything in between.

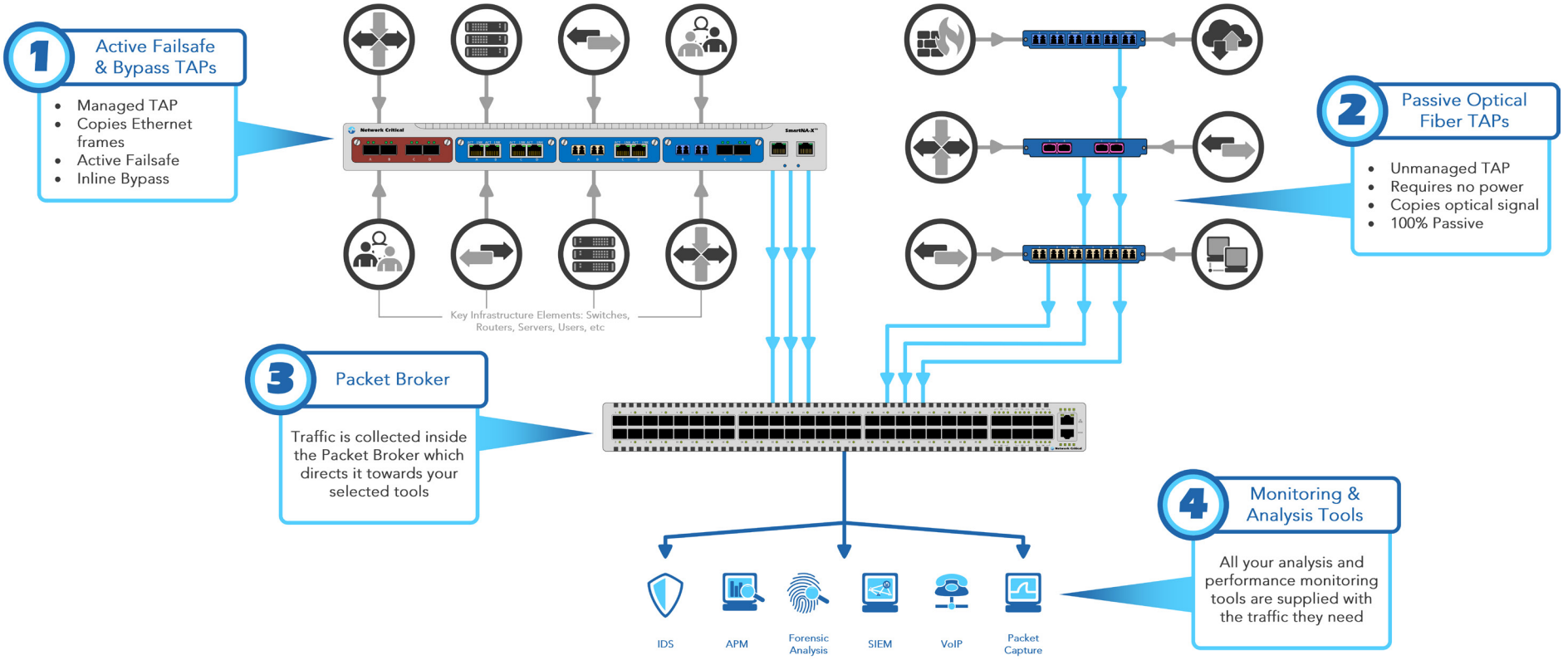
To protect the organization's sensitive information, manage your growing network effectively and support positive end-user experiences, you need visibility. See and understand traffic patterns, root out malware, optimize application performance, protect critical infrastructure, and perform many other critical network management functions using Network Critical solutions.

But what drives this visibility? While today's network performance monitoring and security tools typically capture the headlines, the real underlying champion of visibility is the data and the aggregation tools, like Network TAPs and Packet Brokers, that deliver it.

To maintain vital business functions and ensure positive user experiences, you must establish a network visibility fabric and be ready to adjust it as your network(s) continue to grow and change over time. This eBook is designed to help you do just that by offering several checklists on best practices for selecting, deploying and maintaining Network TAP and Packet Broker technology.

# TAP & PACKET BROKER OVERVIEW

Refresh your understanding of how TAPs and Packet Brokers work together to give you 100% network visibility.




1 2 TAPs copy the traffic while providing network failsafes

3 Packet Broker aggregates and distributes packets

4 All your analysis and performance monitoring tools are supplied with the traffic they need

# VISIBILITY AND SECURITY STATISTICS

On the left, there are some examples of Gbps and key percentages that your network may have. These figures directly impact the 'Total Potential Savings' you may achieve when using Network Critical solutions, as seen on the right.

| | |
|---|---|
| Average Traffic To Your Tools (Gbps) | 25 |
| Annual Traffic Growth Rate (%) | 15 |
| Capacity Per Tool (Gbps) | 10 |
| Current Tool Utilization (%) | 75 |
| Maximum Tool Utilization (%) | 80 |

**Total Potential Savings**

**$1,643,200**

| | |
|---|---|
| Average Traffic To Your Tools (Gbps) | 50 |
| Annual Traffic Growth Rate (%) | 30 |
| Capacity Per Tool (Gbps) | 25 |
| Current Tool Utilization (%) | 75 |
| Maximum Tool Utilization (%) | 80 |

**Total Potential Savings**

**$5,063,200**

| | |
|---|---|
| Average Traffic To Your Tools (Gbps) | 100 |
| Annual Traffic Growth Rate (%) | 45 |
| Capacity Per Tool (Gbps) | 40 |
| Current Tool Utilization (%) | 85 |
| Maximum Tool Utilization (%) | 90 |

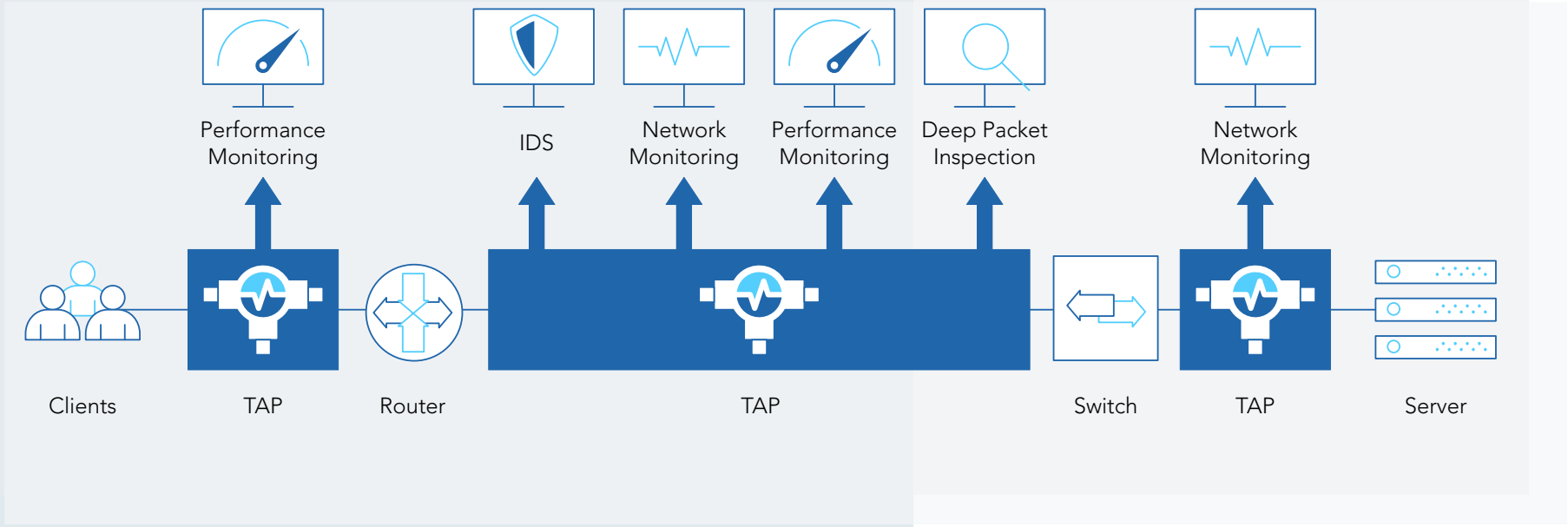
**Total Potential Savings**

**$10,105,000**

# 1

# PRODUCT RECAP

*knowing our products*




Placing Network TAPs into each critical link enables edge to edge visibility

# NETWORK TAPS

Network TAPs (Test Access Points) are stand-alone devices that make a mirror copy of all of the traffic that flows between two network endpoints (nodes). This can then be output to various network or security tools, while the live traffic continues to pass through the network.

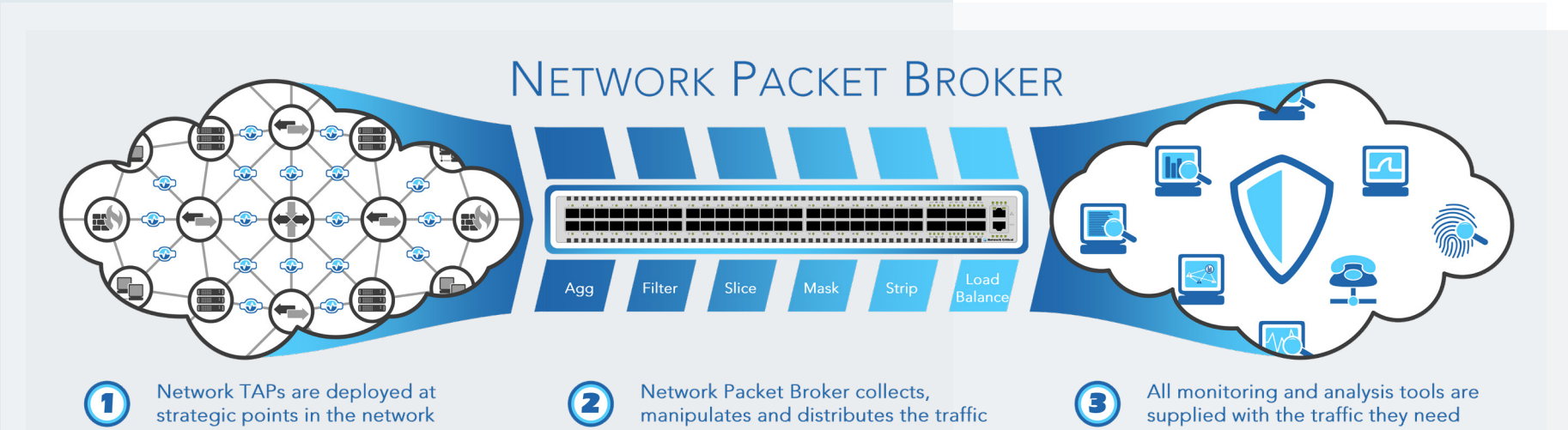
TAPs are independent of the network (and often reside in the access layer) meaning that they are fully configurable. This allows security and/or performance tools to perform complex packet manipulation.

They deliver maximum visibility with minimal disruption and can be much less expensive and more effective in the long run than SPAN port (switch port analyzer) alternatives.

**Types of TAPs Include:**

| | |
|---|---|
| Passive Fiber TAPs | The most commonly used TAP. It offers visibility into network activity by accurately duplicating all traffic at 100% bandwidth while remaining invisible to all other network components. |
| Active Ethernet TAPs | Used for real-time network threat detection and mitigation, allowing for more complex Inline monitoring and reactive response. Typically feature robust fail-safe mechanisms to protect the live network traffic from disruption. |
| Intelligent Hybrid TAPs | Not only do these perform Passive and Inline TAP functions, but also aggregation, filtering and load balancing. Often utilize a granular architecture for greater control and security. |

Click here to see the Network TAP range




# NETWORK PACKET BROKERS

# NETWORK PACKET BROKERS

Packet Brokers often include the following basic functionality:

Capture 100% of traffic, with zero packet loss.
Aggregate traffic from multiple network TAPs or SPAN ports.
Filter traffic to other solutions, such as security or monitoring tools.
Load-balance of data to various tools.
Application layer visibility and smart filtering rules.
Strip off unwanted payload; reducing critical tool workload
Many to Many connections
Many to Any connections
Any to One connections
One to Many connections

The 'Broker' in Network Packet Broker refers to its ability to combine, integrate, separate, manipulate and process inputs from many sources, delivering the data to a wide variety of appliance and tool destinations.

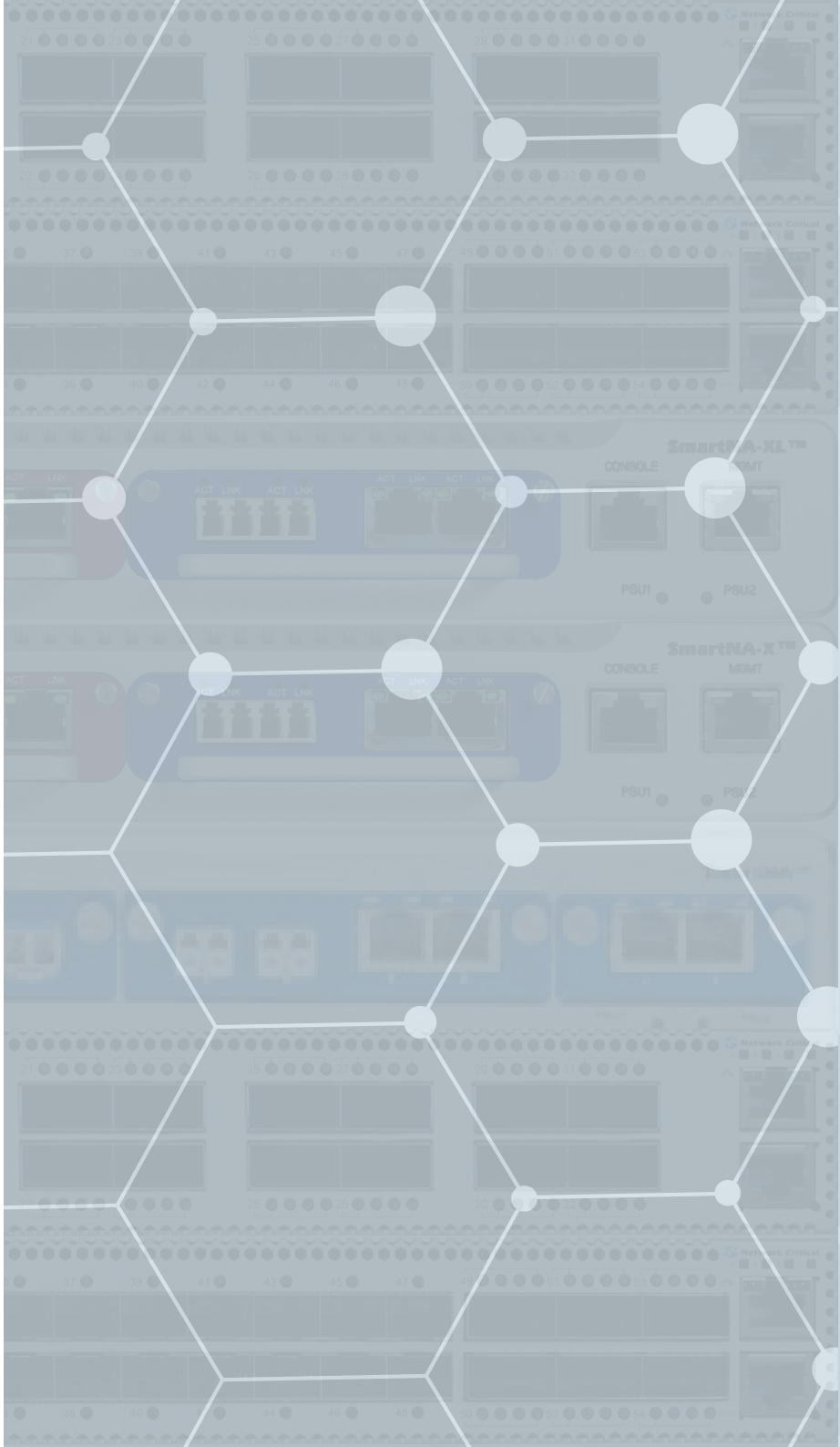
Delivering the right data to the right tool will optimize security and performance. It commonly resides in the control layer of the network.

Click here to see the Packet Broker range

# 2

# CHECKLISTS

*doing things right*



# EVALUATING THE SITUATION

Visibility is important and you're ready to jump in and deploy Network TAP or Packet Broker technology to help fuel your monitoring tools with the data required. What are some of the key considerations before you get started? Use this thorough checklist to help eliminate errors down the road and have a better understanding of the pre-game requirements.

- Do you understand the tools you are deploying? The type of data you need to capture? And what other tools might already exist on the network (and could impact your deployment)? It sounds basic, but often times IT professionals do not have a thorough understanding of the monitoring tools being deployed or configured.
- Does your network fiber, copper, single mode, multi-mode TAP and Packet Broker technology match the topology?
- Do you have a complete network map and do you understand the digital and physical elements? This is critical in understanding a variety of elements, including whether or not there are existing TAPs and Packet Brokers already deployed, which you could leverage or, which could impact traffic duplication and negatively impact network Performance.
- Have you isolated your aggregation points? Understanding where TAPs and Packet Brokers will be deployed is key to selecting the best options and features.
- Evaluated rack space and cable length. This is important as these solutions take space.
- If deploying to aggregate data to a security solution, do you fully understand the data requirements from the security team?
- Have you evaluated the data load so tools can be properly load balanced (and tools can be added in the future)?
- Are you working within any compliance mandates? Packet Brokers can help mask and encrypt data, often helping meet compliance standards or guidelines.
- Checked whether you should you be combining your TAP and Packet Broker technology. Depending on the deployment scenario, you could save space and cost on a hybrid solution.
- Do you have an understanding of the flow of traffic across your network? This is essential for successful deployment of visibility products.

# ASKING THE RIGHT QUESTIONS & PICKING THE RIGHT TECHNOLOGY

Pre-game is complete and it's time to buy. But, what questions should you be asking your vendors or consultants? What features should you care about? Use this checklist to ensure you're prepared when making your purchasing decision for TAPs and Packet Brokers.

- Does the device have the proper port density? Can I send data to a variety of tools, and is it scalable for future additions? A good guide can vary from 16 to 64 ports.
- Does the TAP or Packet Broker process data at full line rate under full load? If not, your tools could be operating on incomplete data.
- Can your Packet Broker perform deduplication at line rate speeds? If not, this can result in missed duplication events.
- Can deduplication work concurrently with other PB features enabled, such as filtering? If not, you could have performance problems.
- Does the Hybrid TAP or Packet Broker have an intuitive management interface and good deployment features? Does it make things like rules generation, aggregation, filtering, deduplication, header stripping, payload slicing and GRE tunnels, easy to manage?
- If you plan to place tools Inline, does your TAP have a bypass option with fail-over capability that allows the network to survive if the network fails?
- Does the TAP or Packet Broker have a variety of split ratios to meet your needs? If you deploy without the correct split ratio you could face potential network outage problems.
- Before sending data on to a tool, you'll likely want to filter the data, this can be a tedious process. Check if your Hybrid TAP or Packet Broker offers filtering features.
- Does the Packet Broker offer burst protection to help with traffic management and eliminate lost traffic in the case of congestion?
- If you plan to have visibility into virtualized environments (like a data center), you will need to deploy virtual TAP solutions and may need tunnelling technologies for aggregation/filtering of data traffic. Be sure to evaluate the best options and look at hypervisor support and performance impacts.

# AVOIDING PITFALLS & USING DEPLOYMENT BEST PRACTICES

You have the tech, now it's time for rollout. What pitfalls should you avoid, what advice should you heed? Use this detailed knowledge checklist to help avoid landmines, and ensure your deployment goes as smoothly as possible.

- Understand the light budget. When deploying Passive Fiber Optic TAPs, you need to perform end-to-end light budget calculations to ensure that all elements will receive adequate signal power.
- Will you be aggregating data from multiple TAPs (or SPAN ports) through a Packet Broker and on to a tool? If so, be sure that you understand the line rate processing capabilities of your Packet Broker or you could lose data.
- Are links too fast for old equipment? Changing link media does not necessarily require replacing all legacy monitoring tools. Your Packet Brokers can load balance to allow high-speed network links to evenly distribute the traffic among a number of lower-speed tools.
- Don't confuse packet slicing for packet manipulation. The latter provides privacy compliance, accurate traffic management and a wider range of user-defined options for traffic analysis.
- Be sure that you understand port mapping. Some TAPs require that specific ports are used for network traffic and others are used to connect monitoring tools. Flexible port mapping allows any port to be utilized for any type of traffic, giving ultimate flexibility.
- Move past hierarchical filtering and utilize independent filtering, which eliminates traffic that is not relevant to the mission of the connected monitoring tool. It helps tools run faster, more efficiently and allows them to monitor more links.
- Configure TAP fail-safe parameters correctly to minimise interruption in the case of system failure.

**PRO TIP:** Future proof your investment by purchasing technology that scales up, not out. What does that mean? Click here to find out.

# ONGOING MANAGEMENT & MAINTENANCE (LOOKING AHEAD)

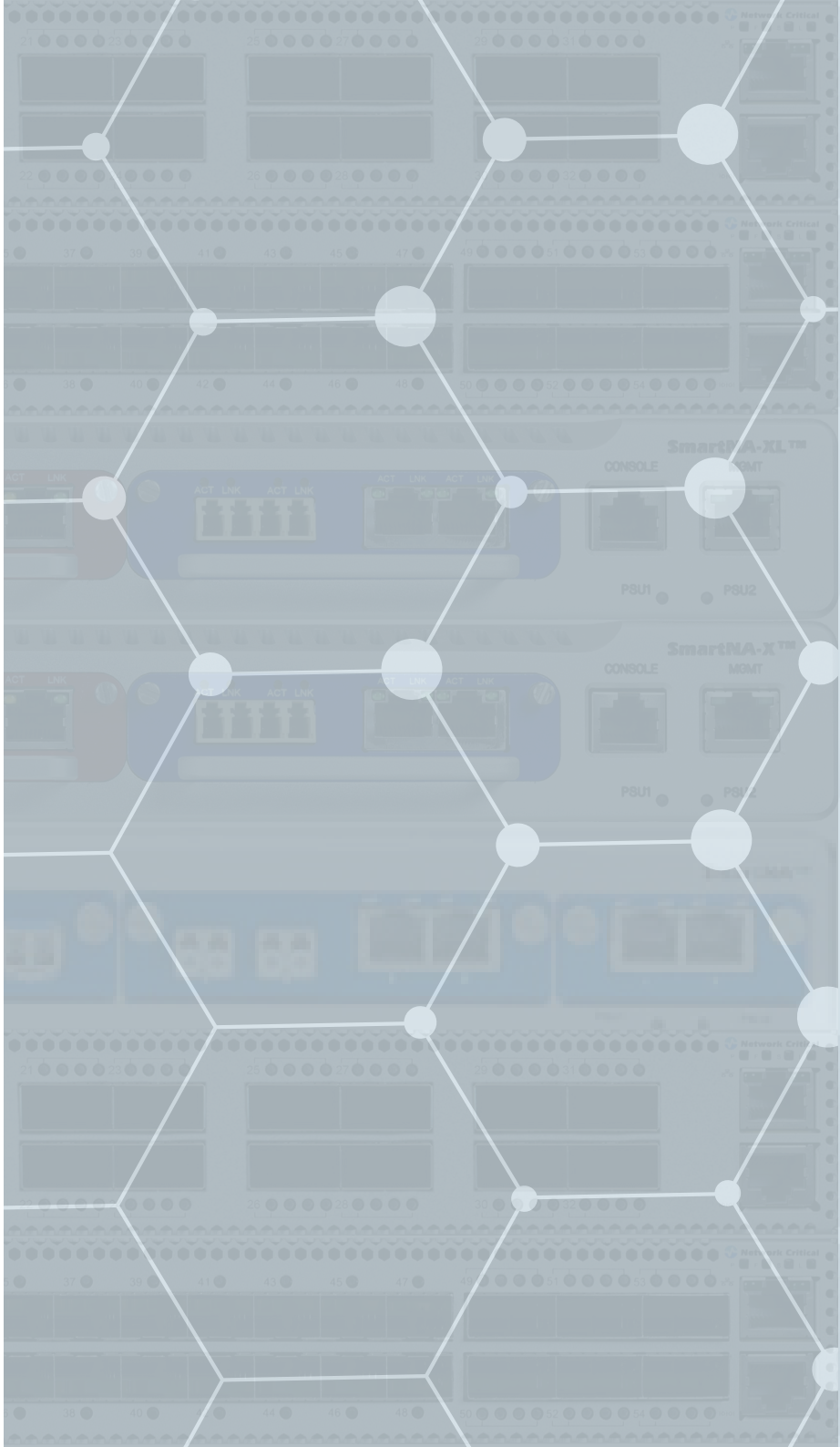
Congratulations, deployment is complete. But your work is never done! Many people think that Network TAPs and Packet Brokers are a "set-it and forget-it" technology. However, the reality is a well-managed TAP and Packet Broker can help ensure network performance and security monitoring meets organizational expectations long after initial deployment. Follow this maintenance checklist as a reminder to remain vigilant.

- Network Utilisation changes over time so be sure that you can see this.
- Understand every products' latest updates
- Regularly check that load-balanced groups are still working
- Always ensure Packet Broker configs remain up to date
- Enable SNMP for active management
- Periodically validate that you are running the latest firmware

# 3

# FINISHING TOUCHES

*networks are evolving*



# SEE YOUR DATA. ALL OF IT.

As networks evolve, companies struggle with the insight needed to maintain tight control, hardened security and service-level performance requirements. Network Critical's scalable and persistent visibility layer feeds tools and systems the crucial network data that is needed to optimize, monitor and control the changing network infrastructure without compromising operations or security.

**Check out our variety of Network TAP and Packet Broker technology here, or schedule a demo.**

# CONTACT US


sales@networkcritical.com

Head Office, UK +44 (0) 118 954 3210
US Office, GA +1 (470) 554 7170