GARLAND
TECHNOLOGY

”
NEW GENERATION IACS/OT&IT CYBER SECURITY NETWORK VISIBILITY
”

OTD BiLiŞiM
GLOBAL VAD

ICT
OTD
PREFER EXPERIENCE ONLINE
Since 2011

GARLAND
TECHNOLOGY

With Garland Technology

Every Bit, Every Byte, Every Package

OT is a trusted and reliable leader in providing critical infrastructure visibility solutions for enterprises, service providers and government agencies across the world.

We have strong belief that reliable network visibility should be an easy and seamless experience. Since 2011, Garland Technology has been in partnership with OT customers in order to identify unique challenges and requirements for critical infrastructure environments and to offer the most reliable and trusted Network TAP, Data Diode Network Packet Agent and cloud visibility solutions of the world which will provide package visibility while providing the needed secure connectivity

It All Starts
with the Package

Security Solutions Offered

- Real-Time Threat Detection
- Asset Discovery and Management for tools and Software
- Compliance with Compliance Standards
- Operational Visibility and Risk Reduction

Security Solutions Require Visibility You Can't Secure What You Can't See.

- Security solutions are only as good as the data they analyze.
- Blind spots hide threats and anomalies.

Visibility Solutions within OT Environments

- To really on legacy key SPAN ports that are not secure, reliable, or available in terms of visibility
- To face with different media or speed connections
- To experience network spread with the need to reduce network complexity and optimize the traffic
- To have the requirement to provide one-way connectivity
- To have the requirement to produce solution for virtual environments

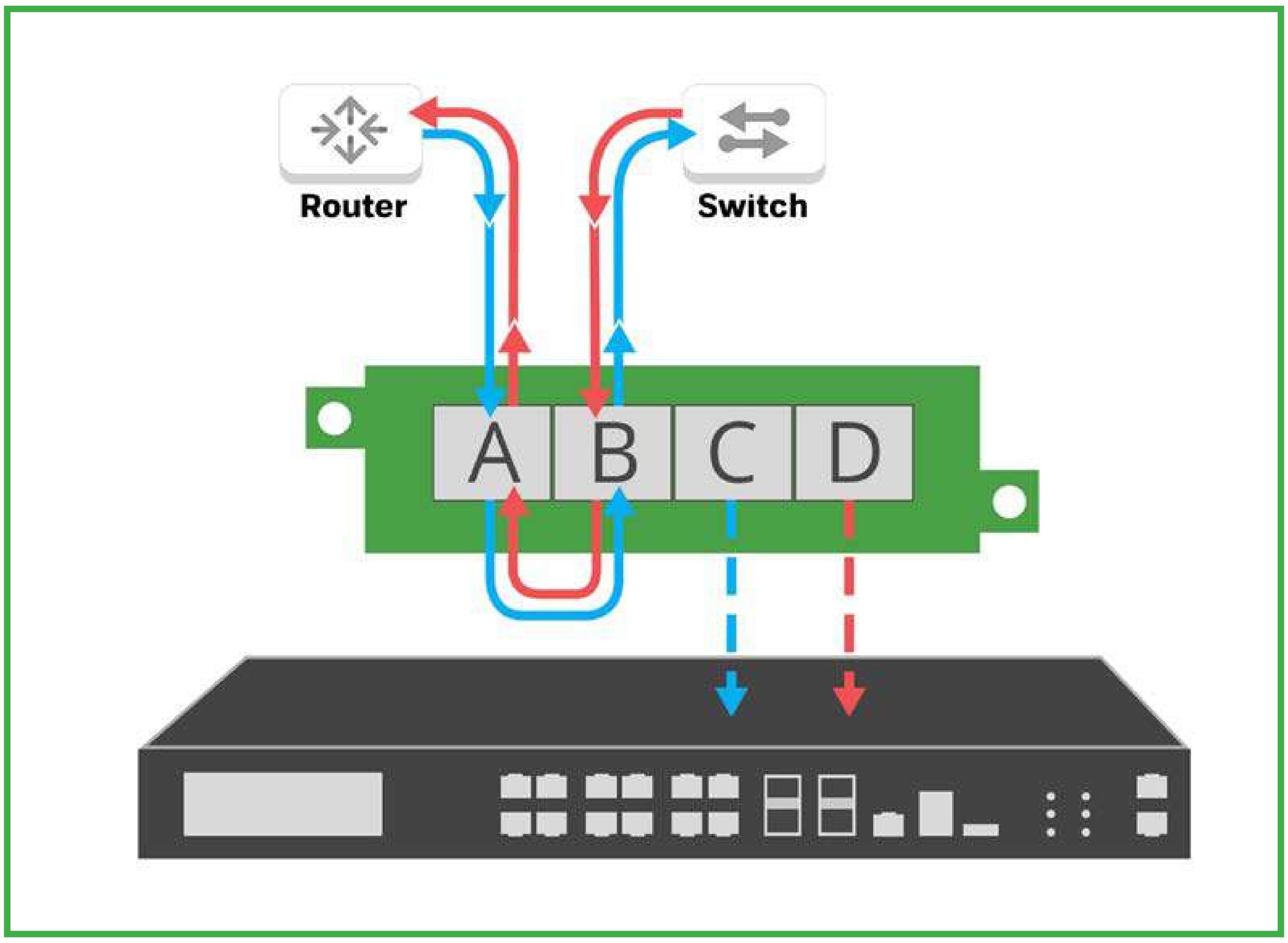
Your Critical IT OT Network
Start Seeing with Garland
Full Package Visibility Solution for Centralized Cyber Intelligence
360° Package Visibility

Garland Technology Produces For These Challenges

- To provide 100% package visibility through ICS Security tools.
- To perform media and speed conversion.
- To facilitate network complexity through traffic aggregation.
- To provide one-way connection with Data Diode TAPs.
- To provide virtual traffic visibility with vTAP solution.

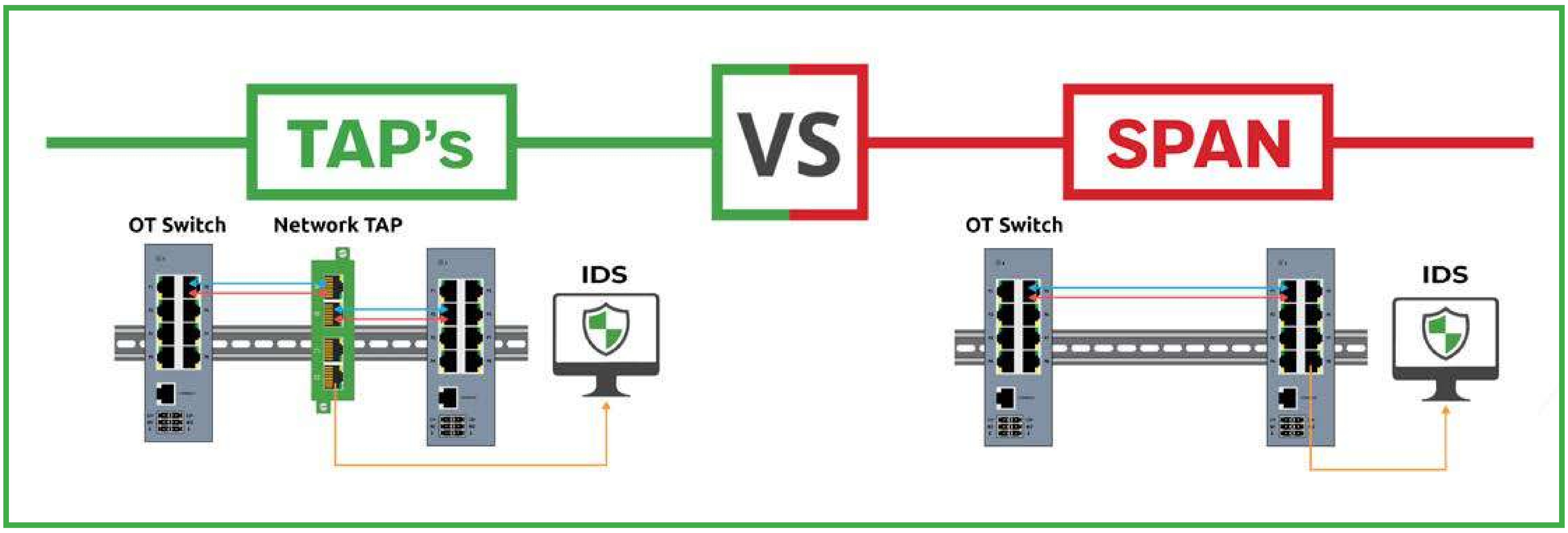
To provide 100% package visibility through Security tools.

To Eliminate Blind Spots and Improve Tool Performance



Network TAPs

- 100% full duplex copy of network traffic
- It is scalable and can perform operations such as single copy, multiple copies (rebuild) or traffic consolidation (aggregation) in order to maximize the performance of your monitoring tools.
- Does not affect the network / It is Passive or failsafe
- Robust and reliable DIN rail DC power converters
- Easy, plug and play

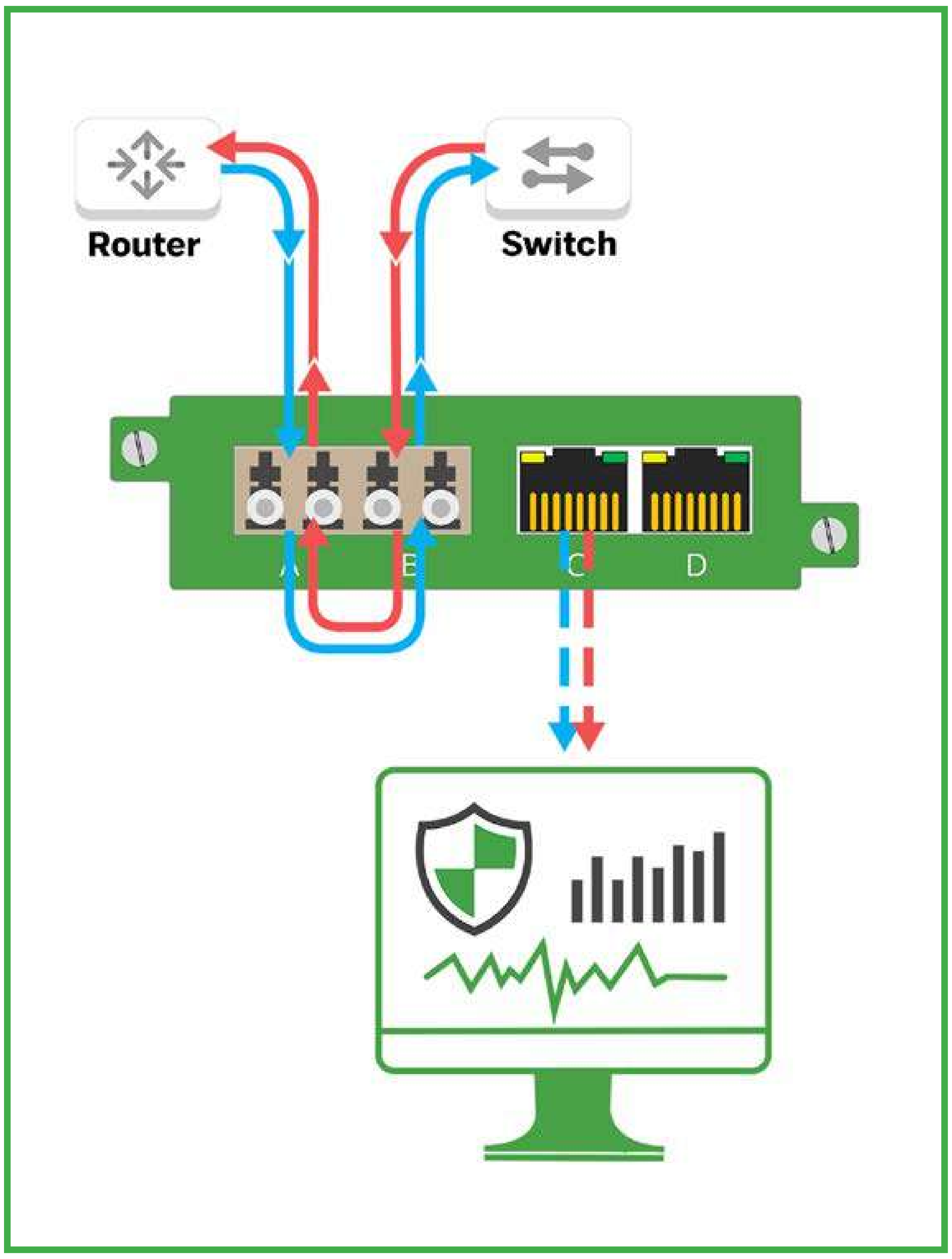


- Ensures dropped packets do not pass through physical errors and supports jumbo frames
- Does not change the time relations of the frames
- Ensures no passive or safe single point of failure (SPOF)
- Data Diode Taps offers one-way traffic to protect against backflow of traffic into the network
- TAPs are reliable but do not contain an IP address or MAC address and therefore, cannot be hacked.
- Can receive high-value ports on the switch

- Some legacy switches do not have SPAN
- SPAN ports can drop packages
- Broken packages and package errors are prevented to pass over SPAN
- Bidirectional traffic opens the backflow of traffic to the
- network, which makes the switch vulnerable to hacking activities
- Costs of management/ programming for SPAN might increase and take longer time

To Adapt to Media Transformation

To Establish a Bridge for the Gap Between Legacy Infrastructure and Modern Security Solutions



Media Conversion TAPs

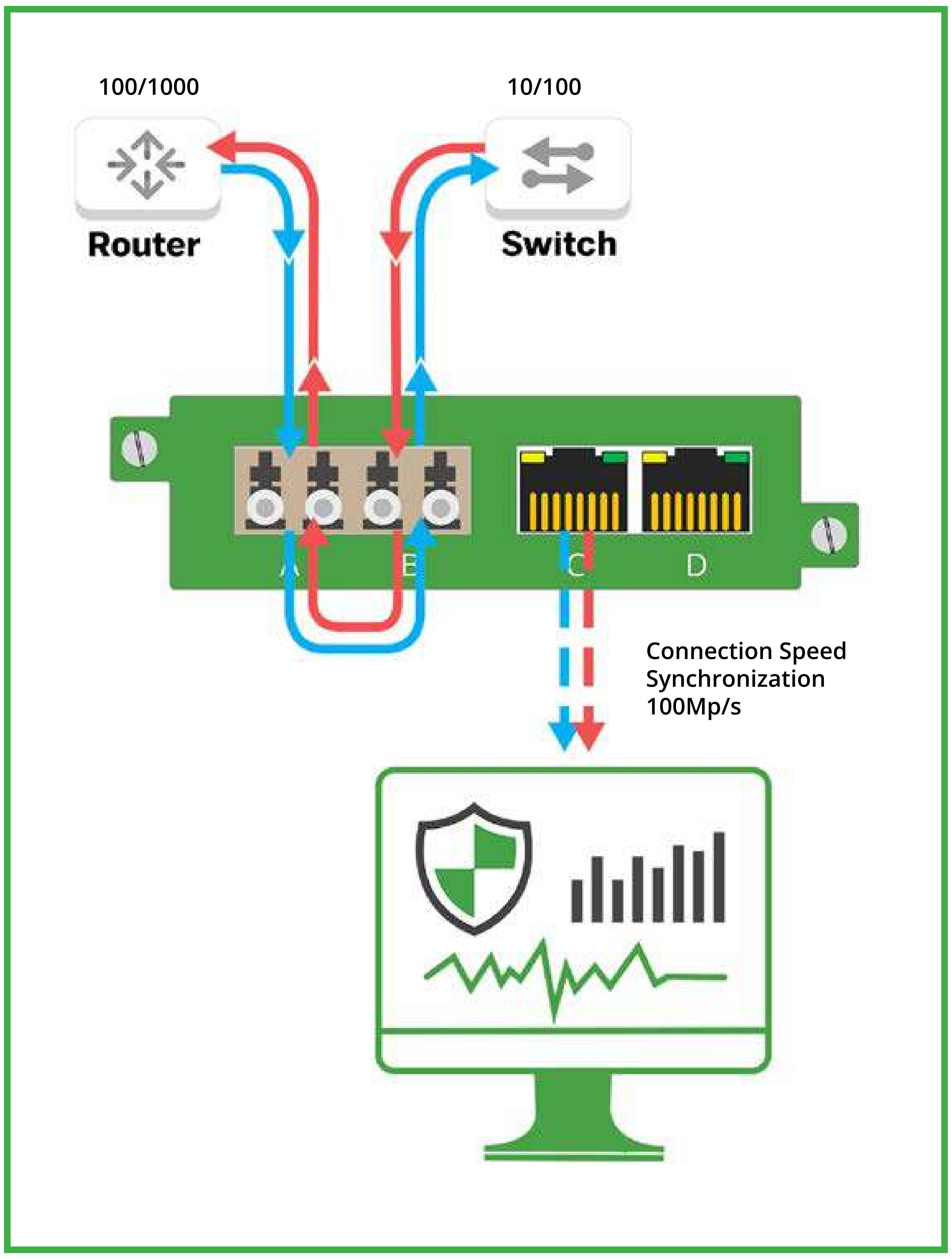
- SX and LX fiber to RJ45 copper or SFP
- 100Base-FX and 100BASE-LX to RJ45 copper

Differs from common media converters with:

- 100% full duplex TAP visibility
- Detecting power outages and automatically reconnects thanks to Failsafe technology
- Reducing critical infrastructure risk with zero impact on operations by achieving 100% network visibility
- Providing additional monitoring ports for future expansions

To Benefit from Speed Conversion

To Establish a Bridge for the Gap Between Legacy Infrastructure and Modern Security Solutions



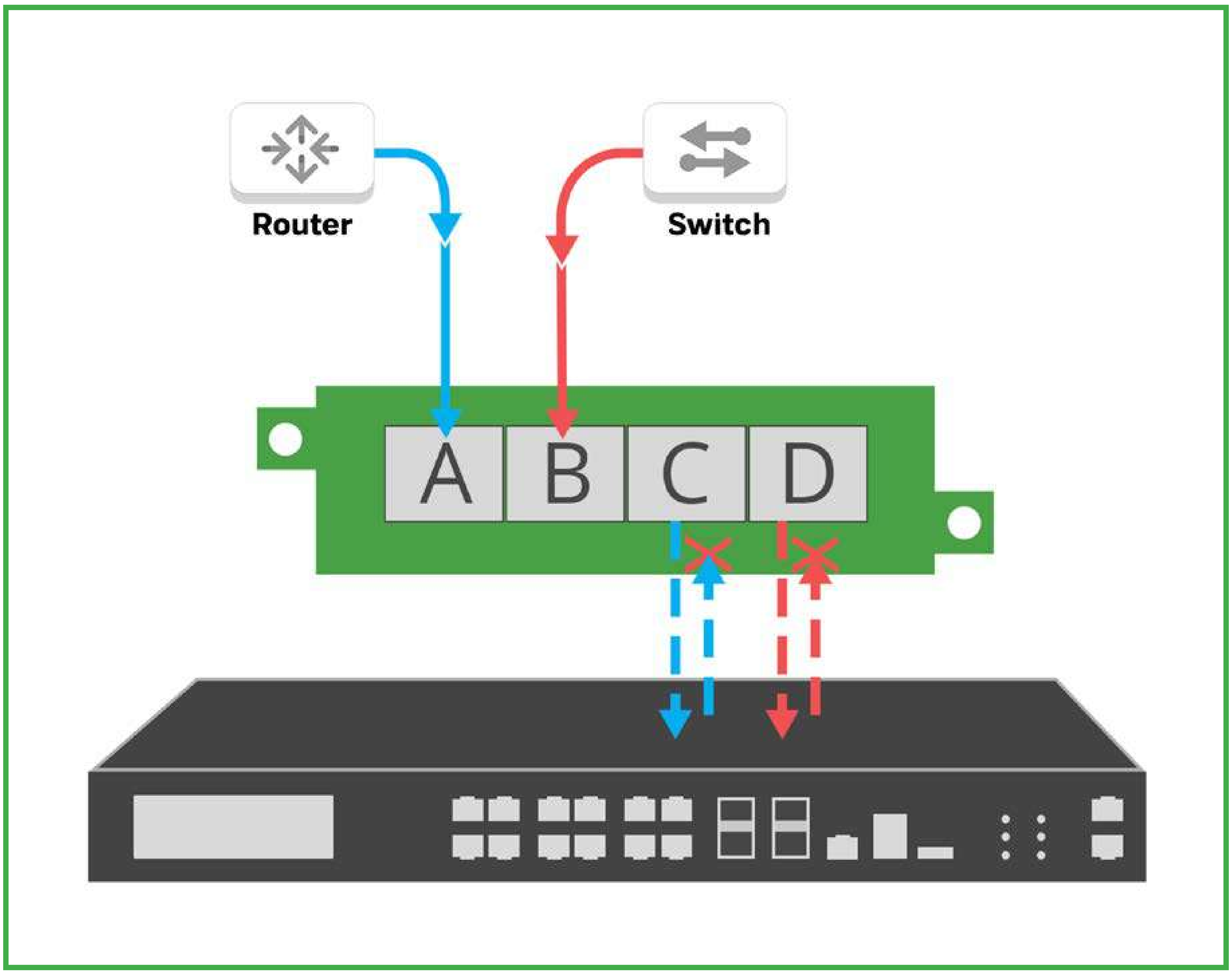
Connection Speed Synchronization is included in Garland's copper network TAPs

To minimize the transfer-related issues thanks to connection speed synchronization:

Auto-negotiation: Automatically connect at highest common speed on all ports. In Synchronization Mode, all ports are automatically placed within Auto MDI/MDIX, Auto Speed and Auto Duplex mode.

Unidirectional Data Diode TAPs

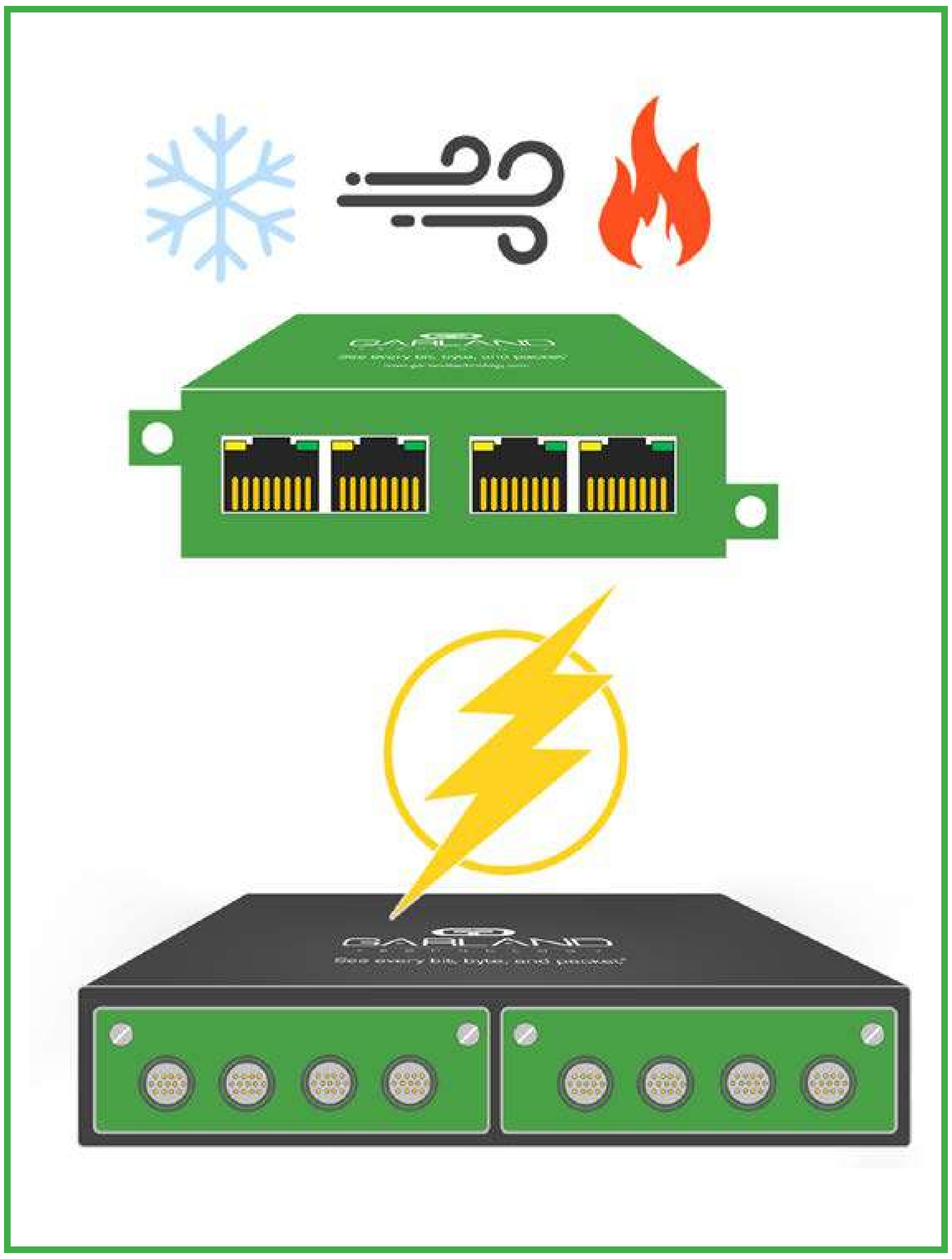
To Provide One-Directional Data Transfer at Hardware Level



- It provides a physically secure one-directional communication path to the monitoring solution.
- Package Injection becomes impossible
- Network traffic control becomes mandatory to be performed at physical hardware level
- Supports 10/100/1000M (1G)
- Supports “Breakout”, “Gathering and Regeneration/SPAN mode”.

Visibility for Customized and Challenging Environments

From Extreme Temperatures to Safe Robust Connections



Robust Metal Construction

Environmental Endurance: Offers resistance to exposure to corrosive, high-temperature and high-pressure air environments.

TAPS designed for extreme temperature changes from -40C to +85C / -40F to +185F.

Also designed in accordance with the specific requirements for electromagnetic interference (EMI).

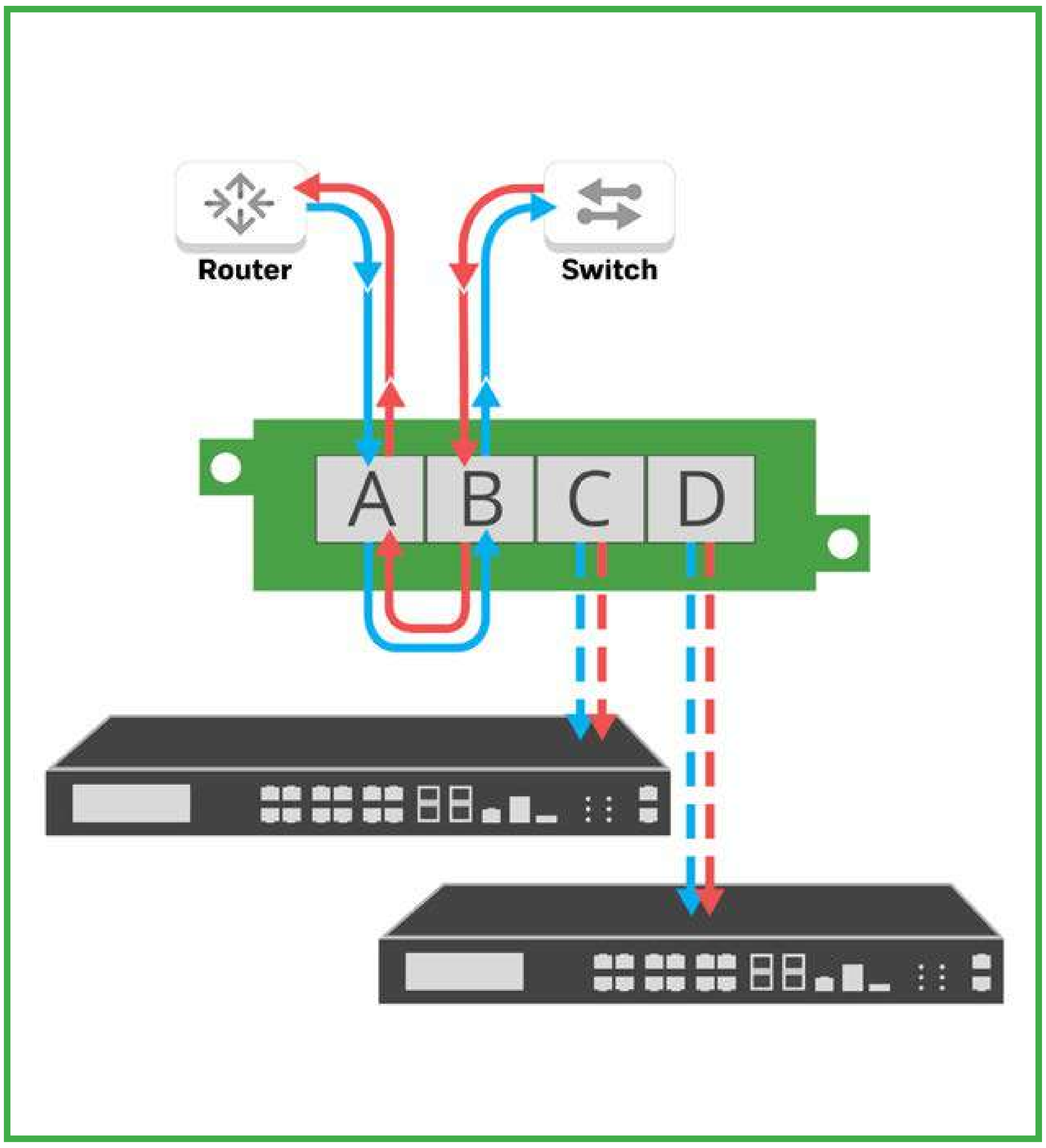
Safe connections and power connectors

-- Mighty Mouse connectors

-- Power Lock connectors

Traffic Concentration Reduces

Facilitate Traffic Flow, Save Budget by Optimizing Your Network & Security Equipment

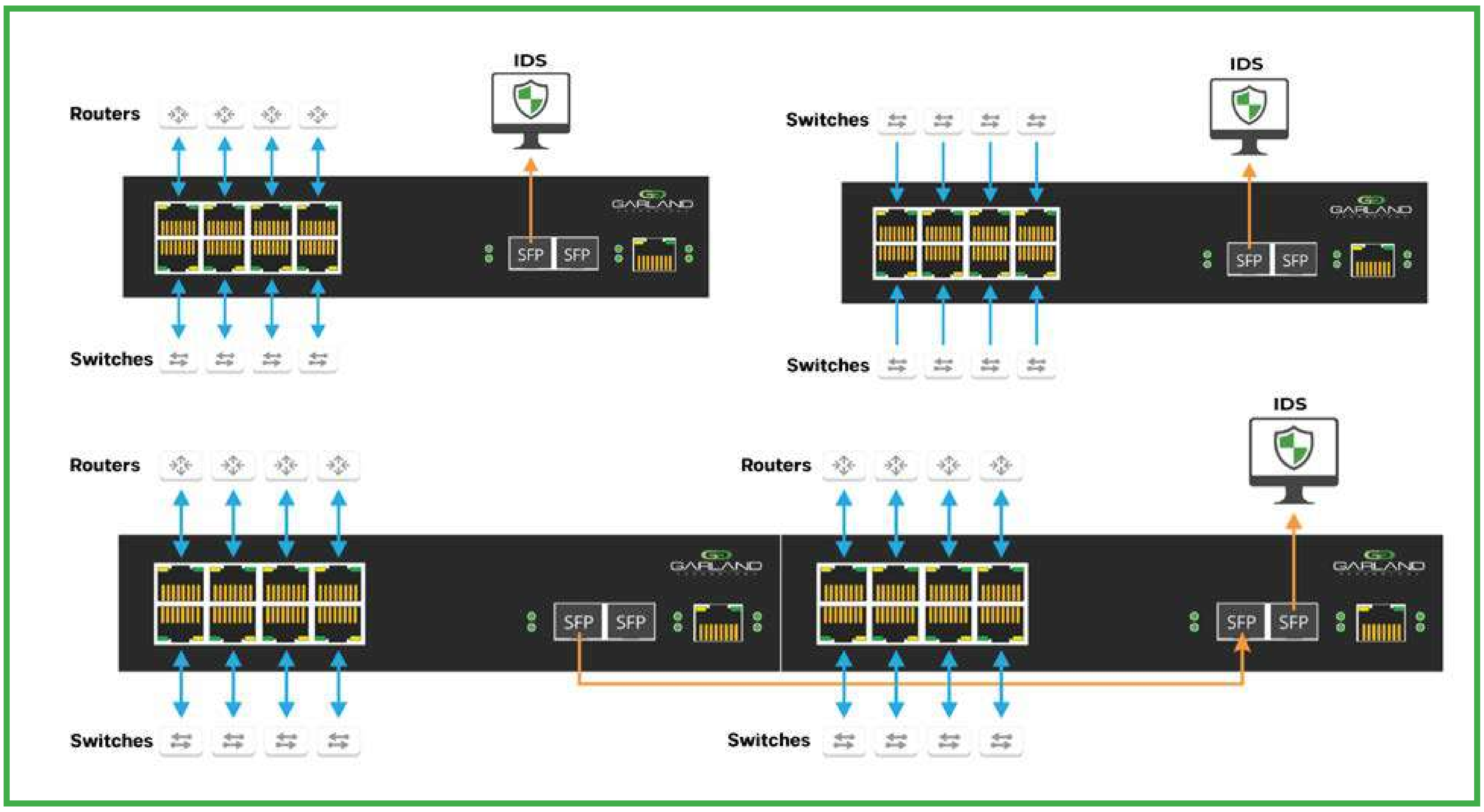


Traffic concentration can be performed by various ways. TAP collection accomplishes two goals:

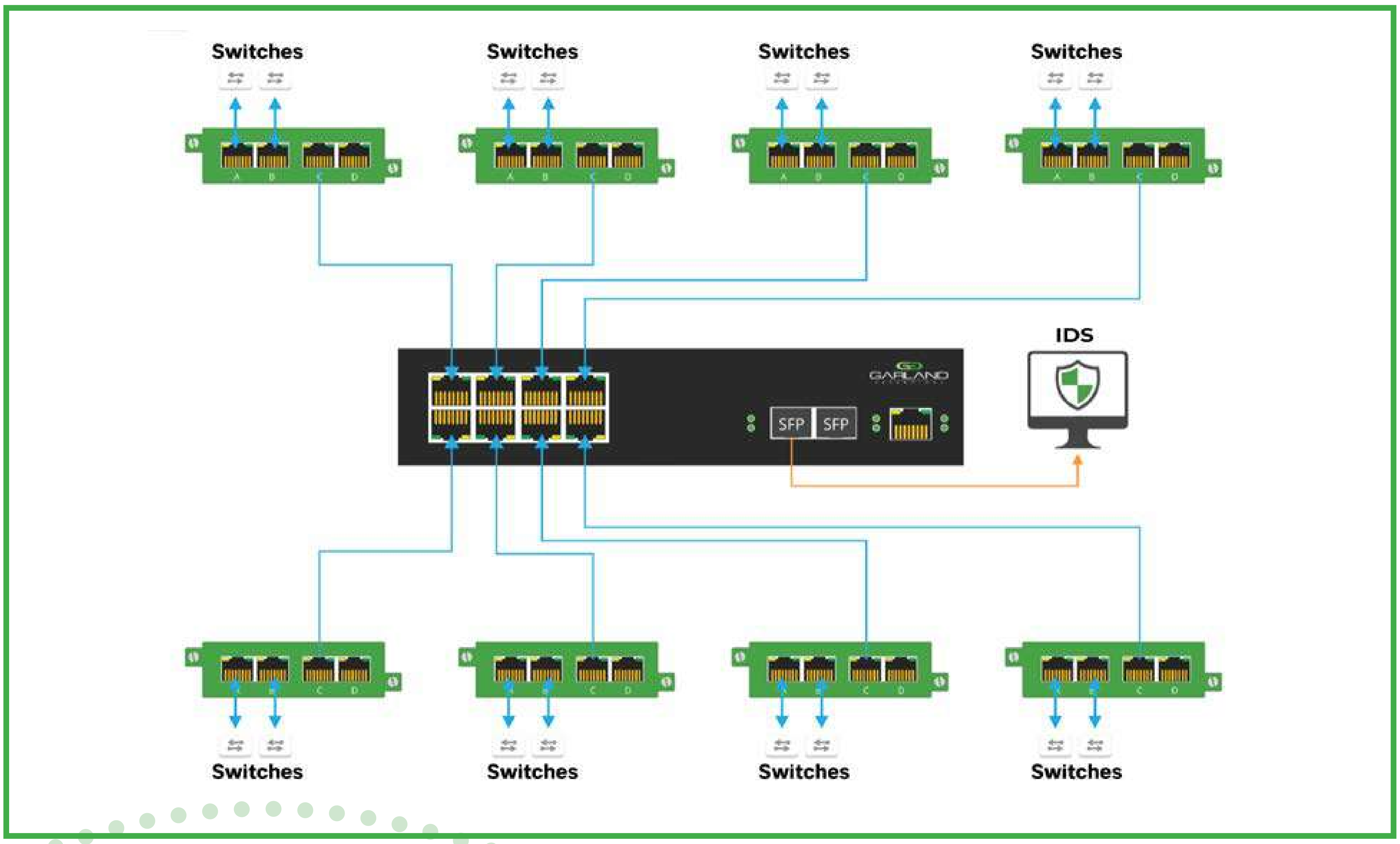
To concentrate traffic so as to ensure that teams can reduce the number of security tools required. To enhance scalability in order to increase visibility and deploy new tools in the future

Usage Example: A single portable TAP can concentrate the traffic to a single monitoring port.

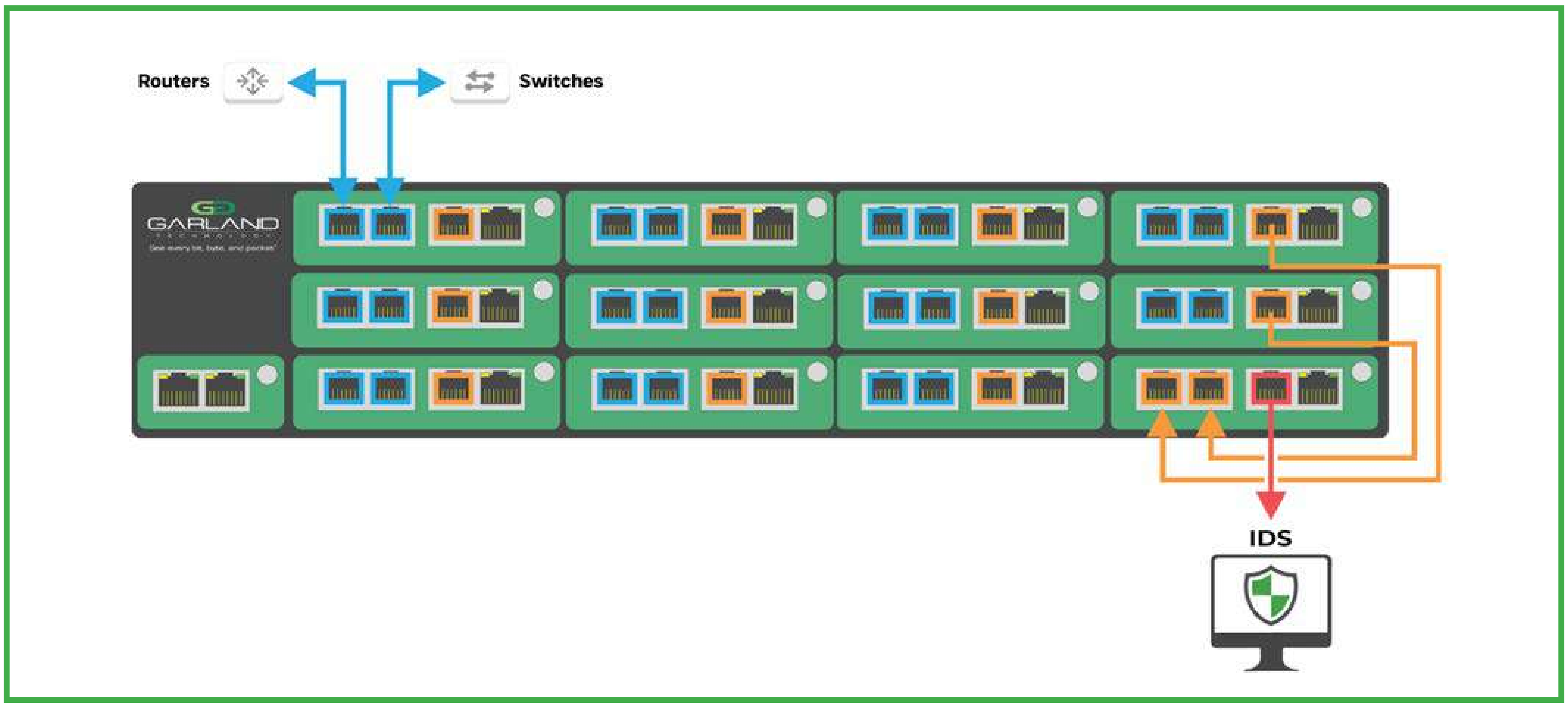
Usage Example: High Density Aggregator TAPs can aggregate traffic 4:1, 8:1 or 8:1 SPAN



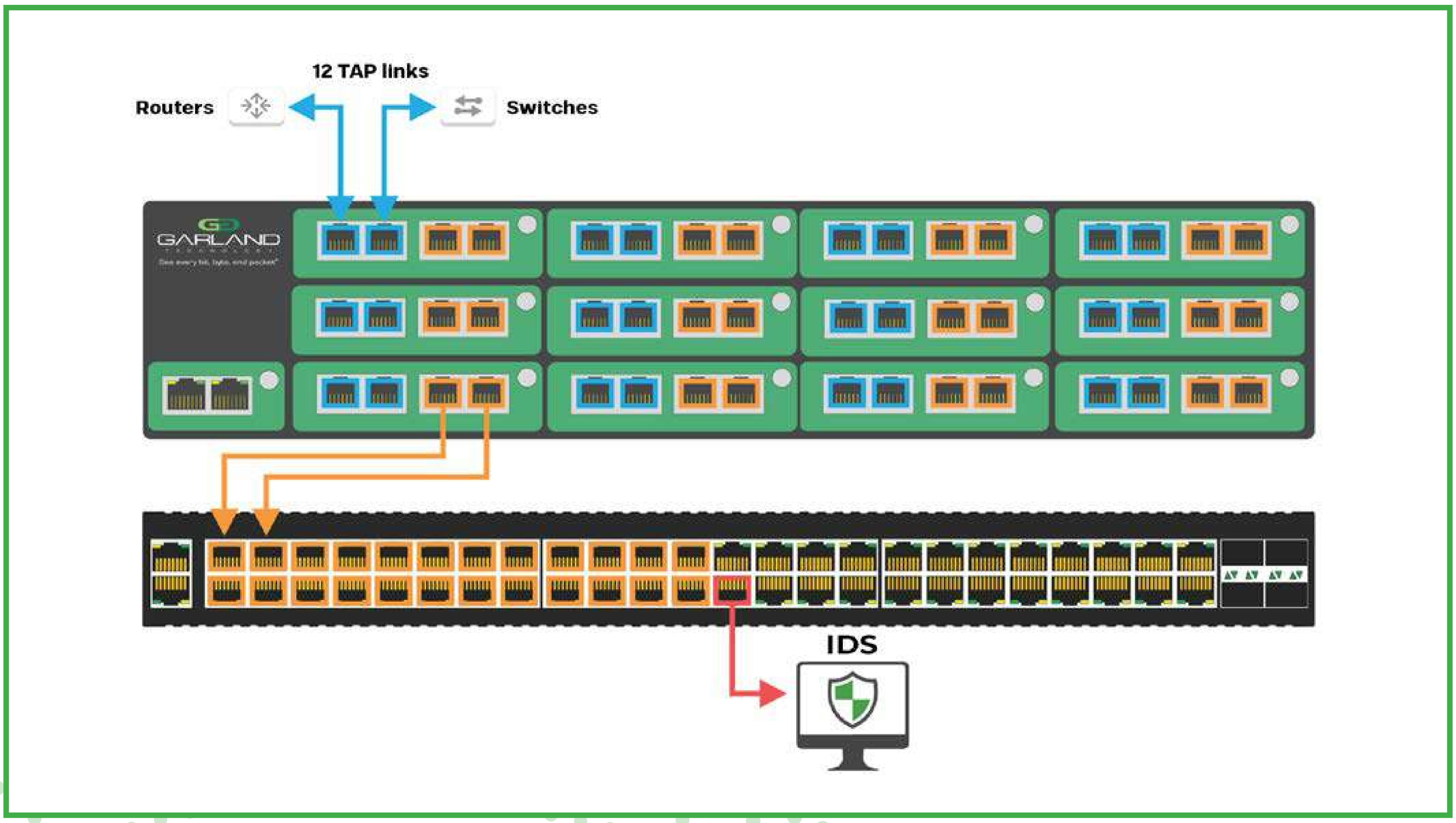
Usage Example: TAP establishes connections at 8 different locations and is aggregated into a single monitoring port.



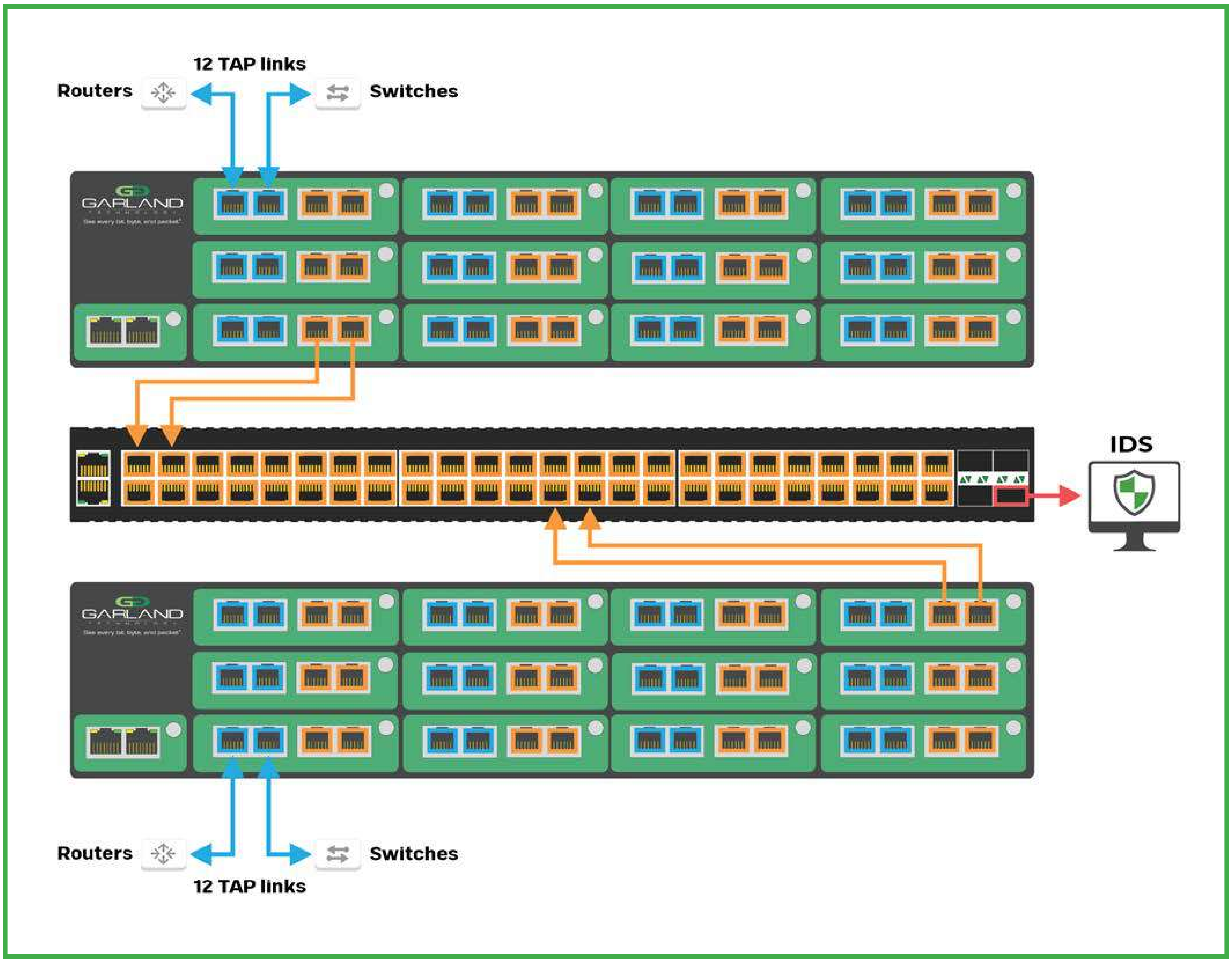
Usage Example: TAP establishes 11 connections and is pooled into a single monitoring port.



Usage Example: TAP establishes 12 connections and is aggregated into a single monitoring port, providing room for possible future growth.

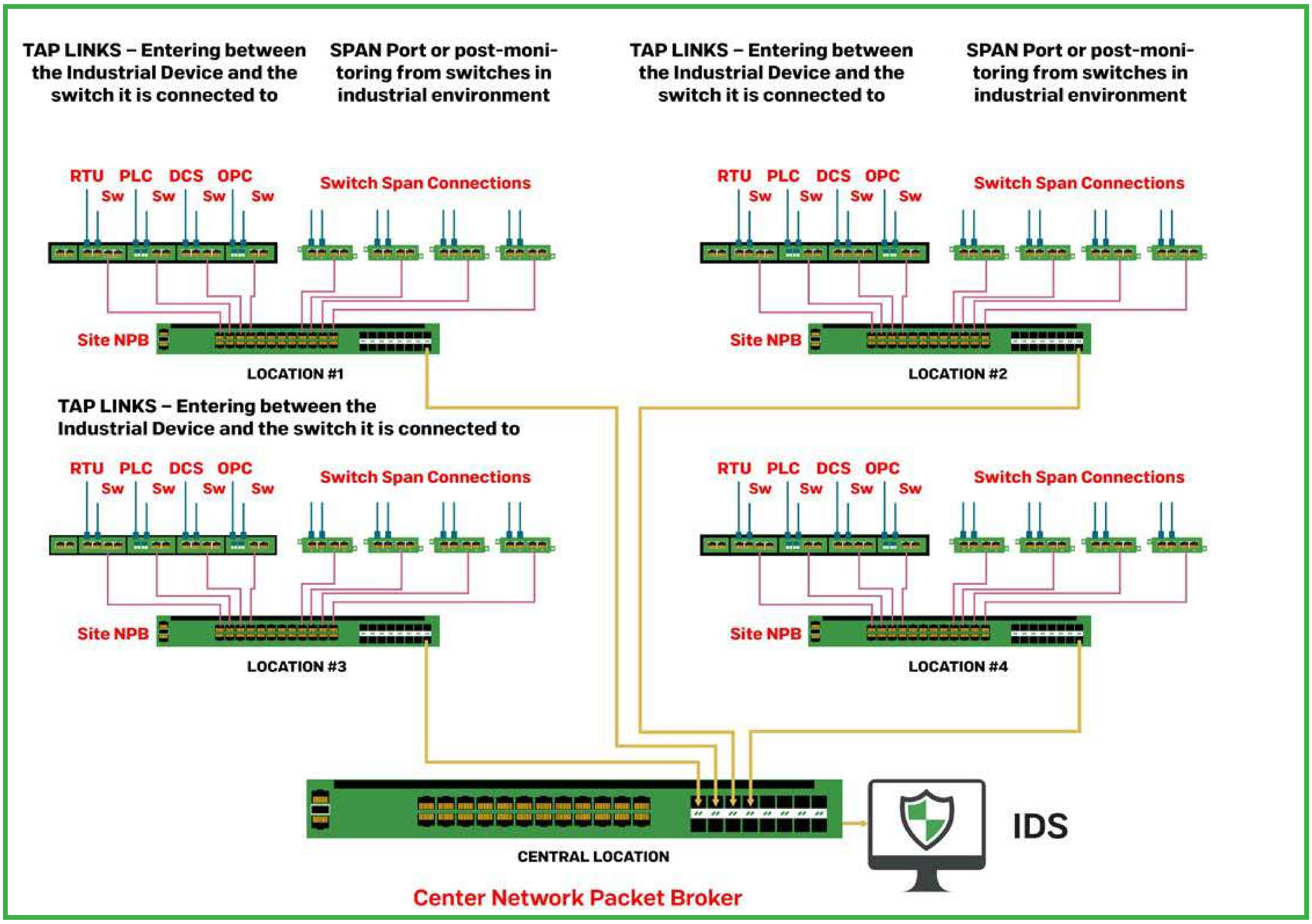


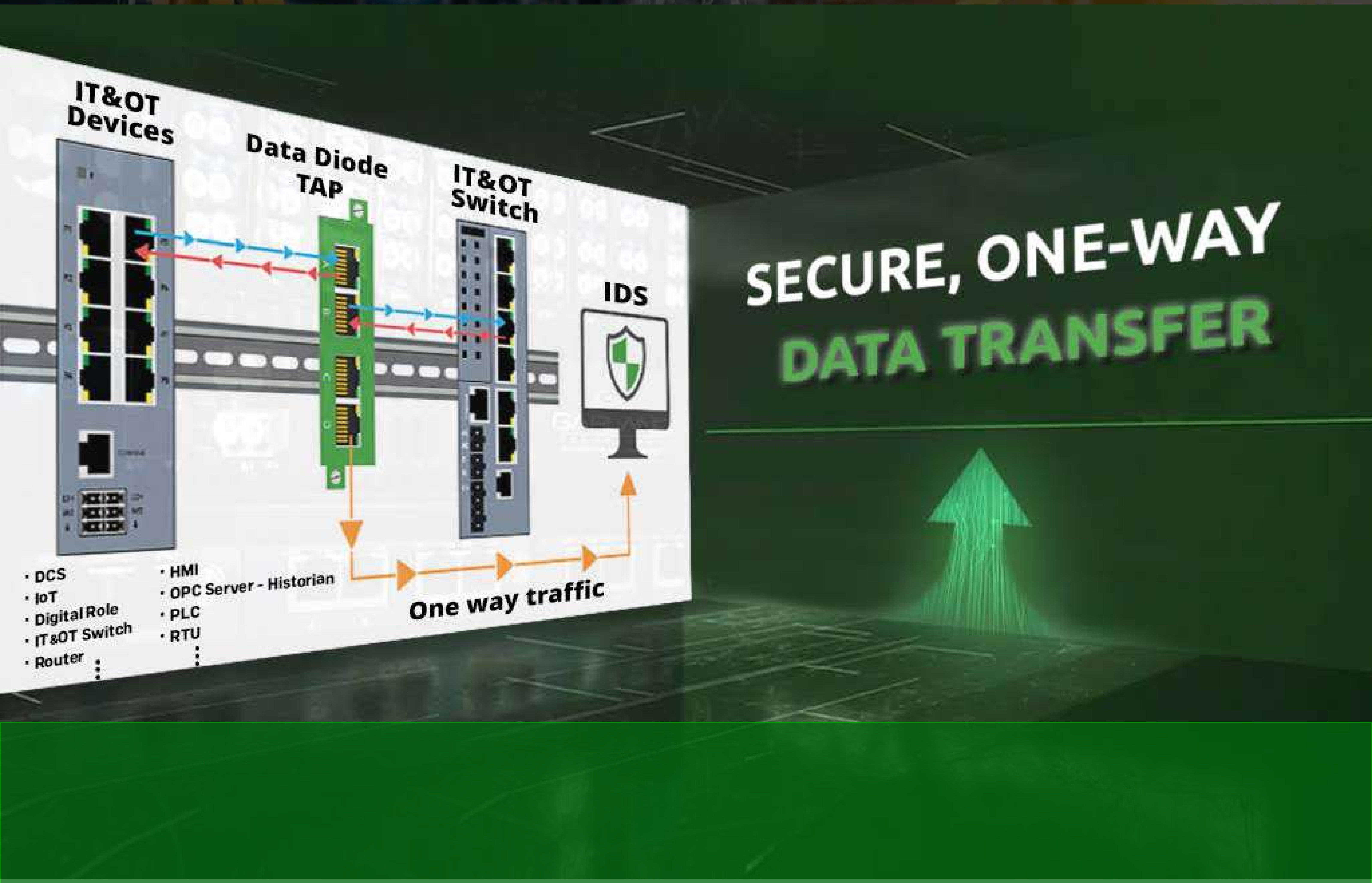
Usage Example: TAP establishes 24 connections and is pooled into a single monitoring port.



Usage Example: TAP and SPAN in various locations

It establishes many connections and connects the center with the GRE Tunnel.

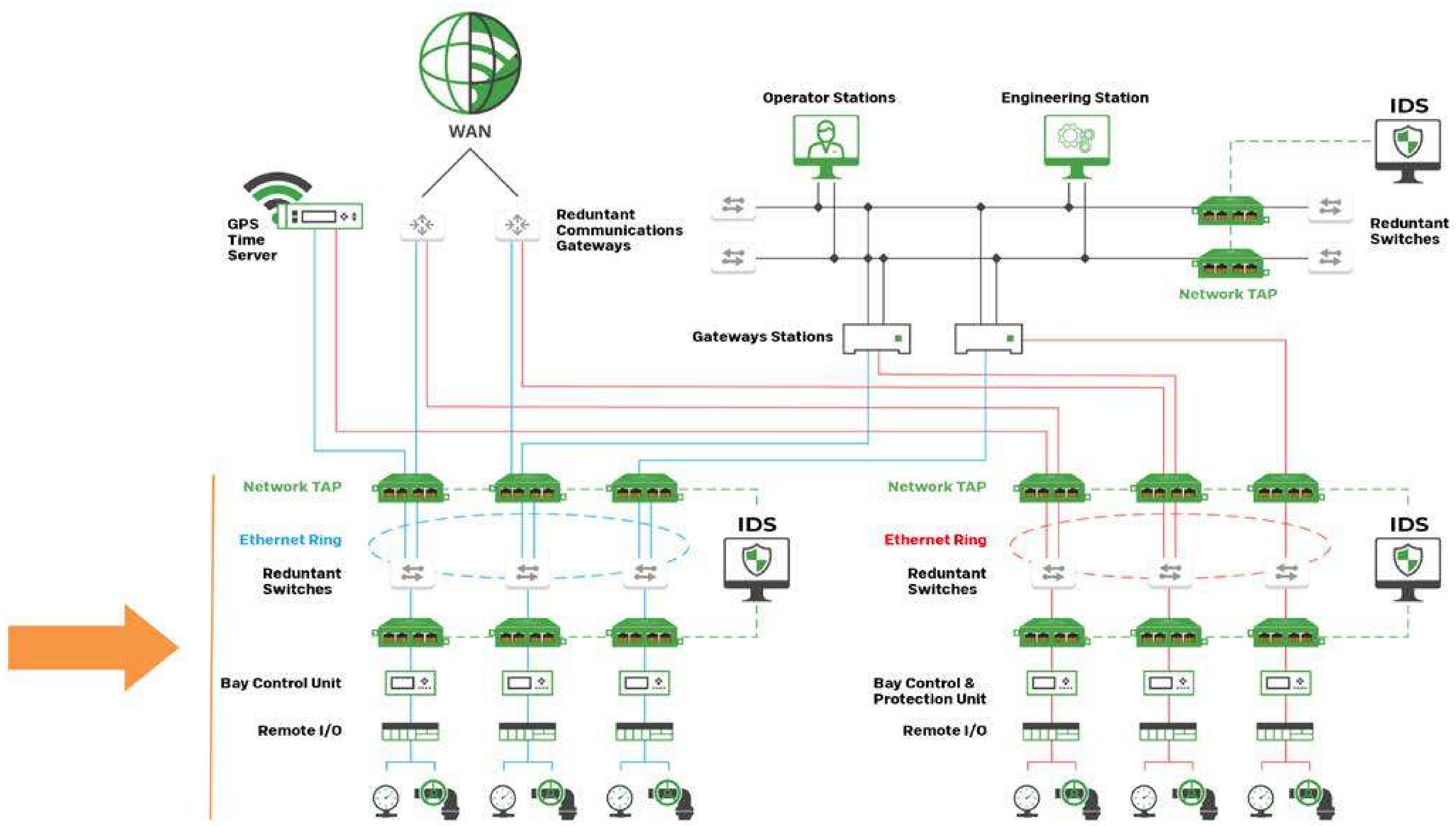

TAP LINKS – Entering between the Industrial Device and the switch it is connected to
SPAN Port or post-monitoring from switches in industrial environment
TAP LINKS – Entering between the Industrial Device and the switch it is connected to
SPAN Port or post-monitoring from switches in industrial environment
RTU PLC DCS OPC
Sw Sw Sw Sw
Switch Span Connections
Site NPB
LOCATION #1
LOCATION #2
TAP LINKS – Entering between the Industrial Device and the switch it is connected to
LOCATION #3
LOCATION #4
CENTRAL LOCATION
Center Network Packet Broker
IDS



ICS Visibility Solutions

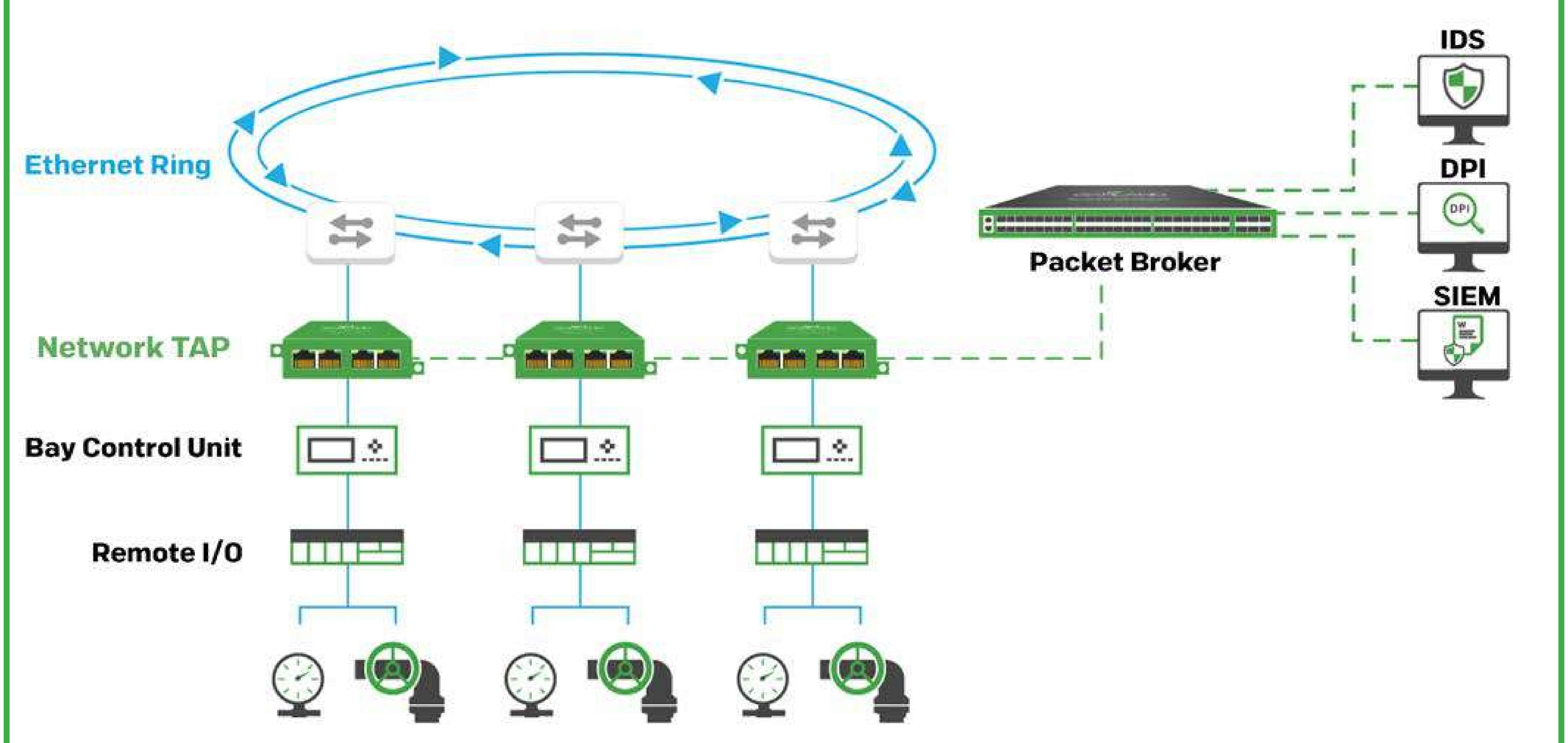
OT Environment Usage Example

Public Services: Energy, Water and Wastewater Network Visibility Structure



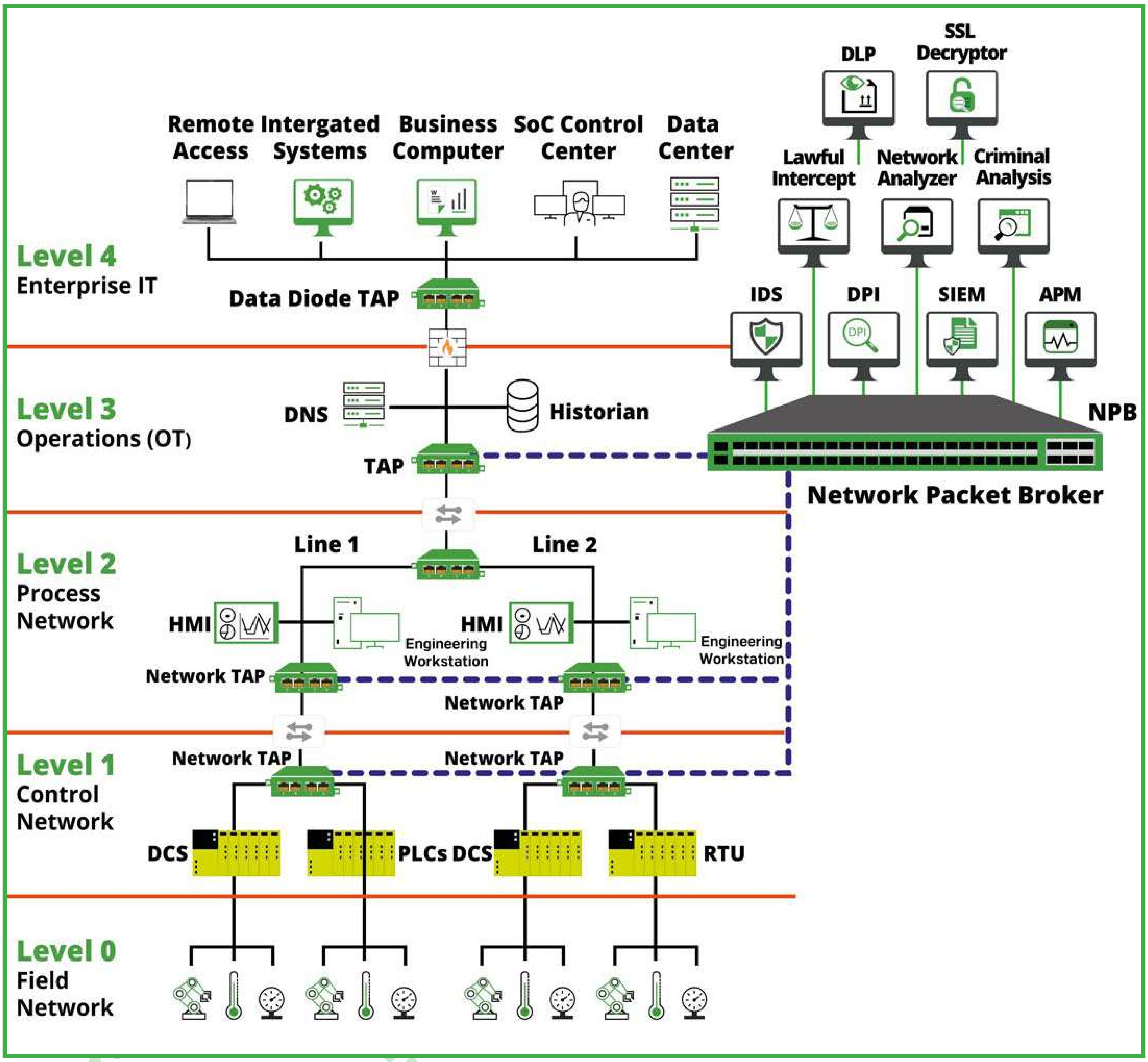
OT Environment Usage Example

Public Services: Energy, Water and Wastewater Visibility Structure



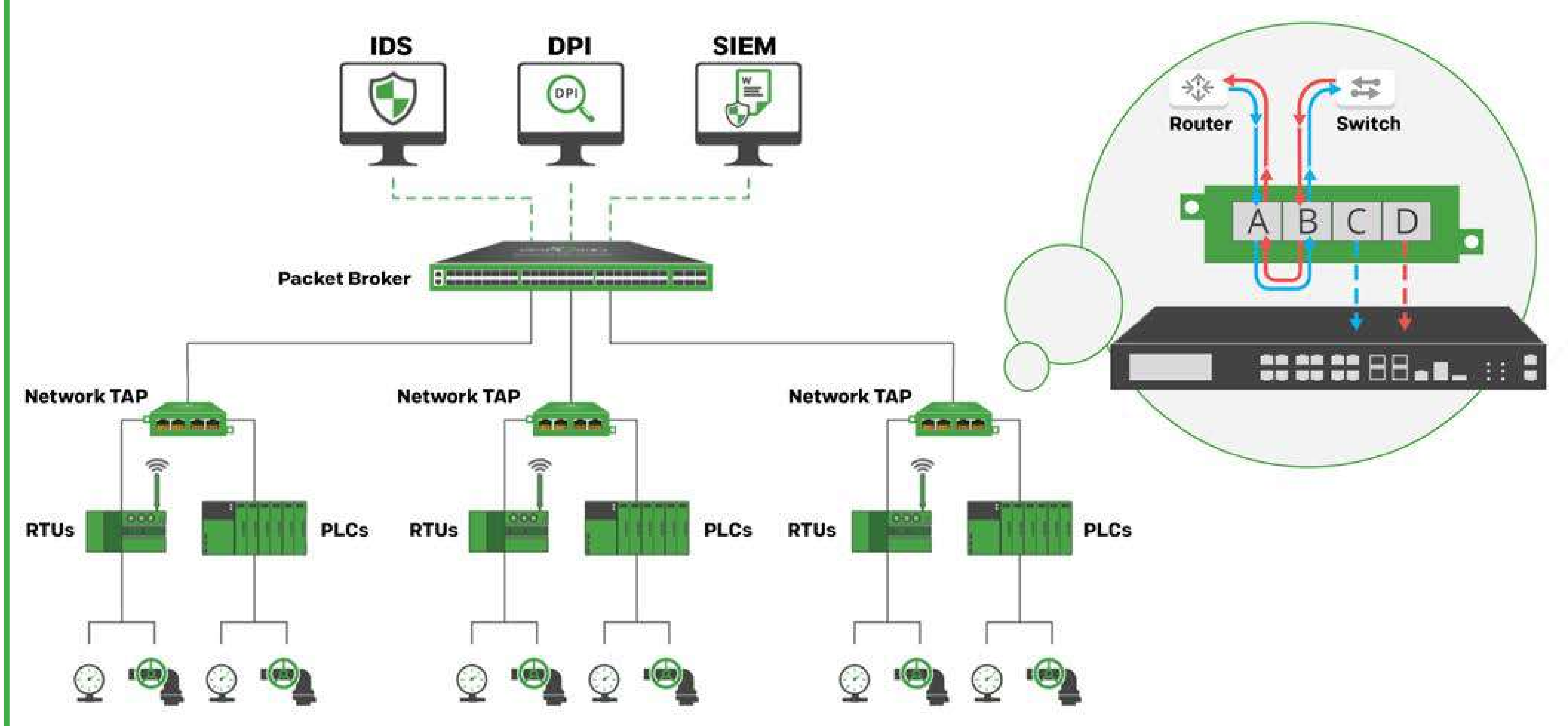
OT Environment Usage Example

Oil and Gas Purdue Model Visibility Structure



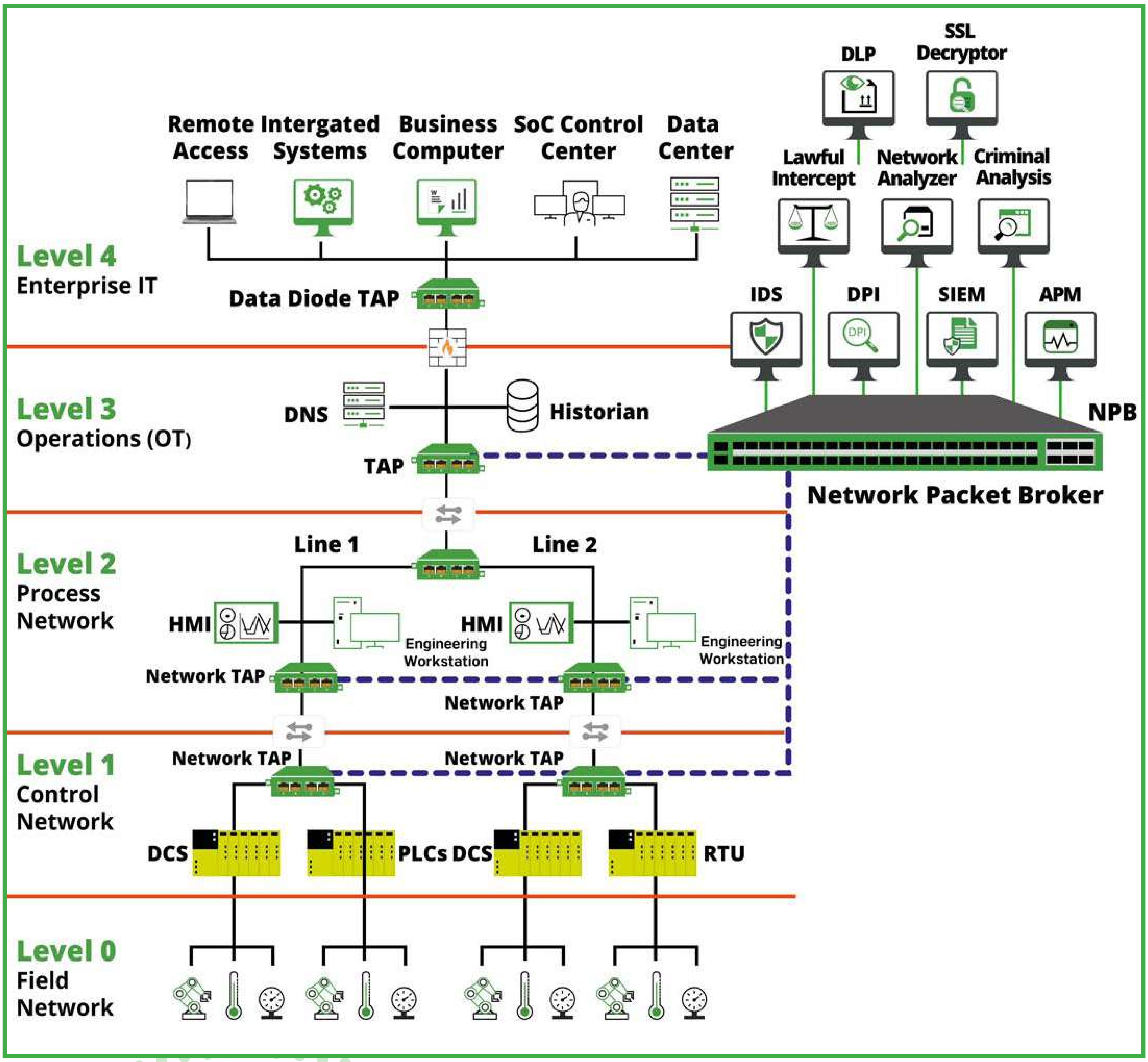
OT Environment Usage Example

Oil and Gas Visibility Structure



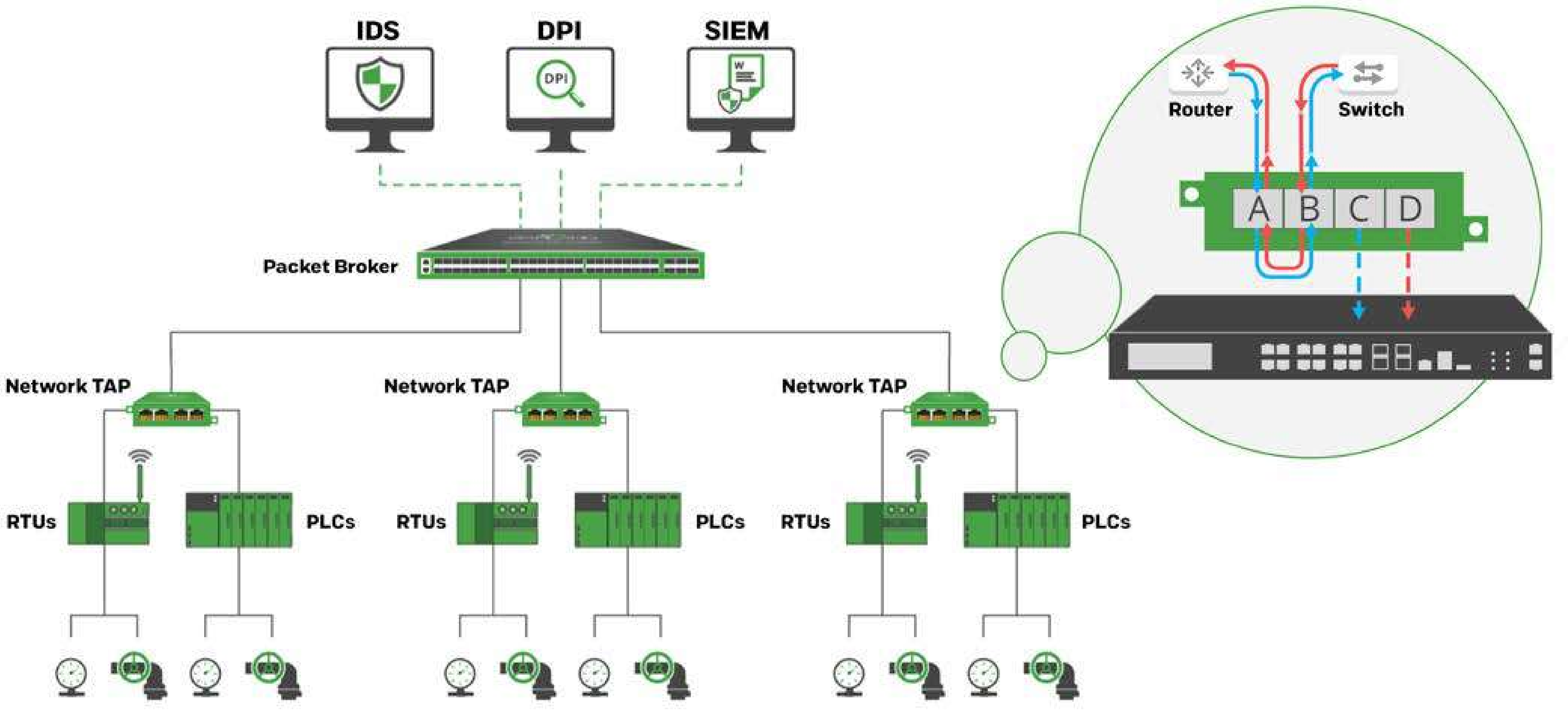
OT Environment Usage Example

Manufacturing and Drug Visibility Structure



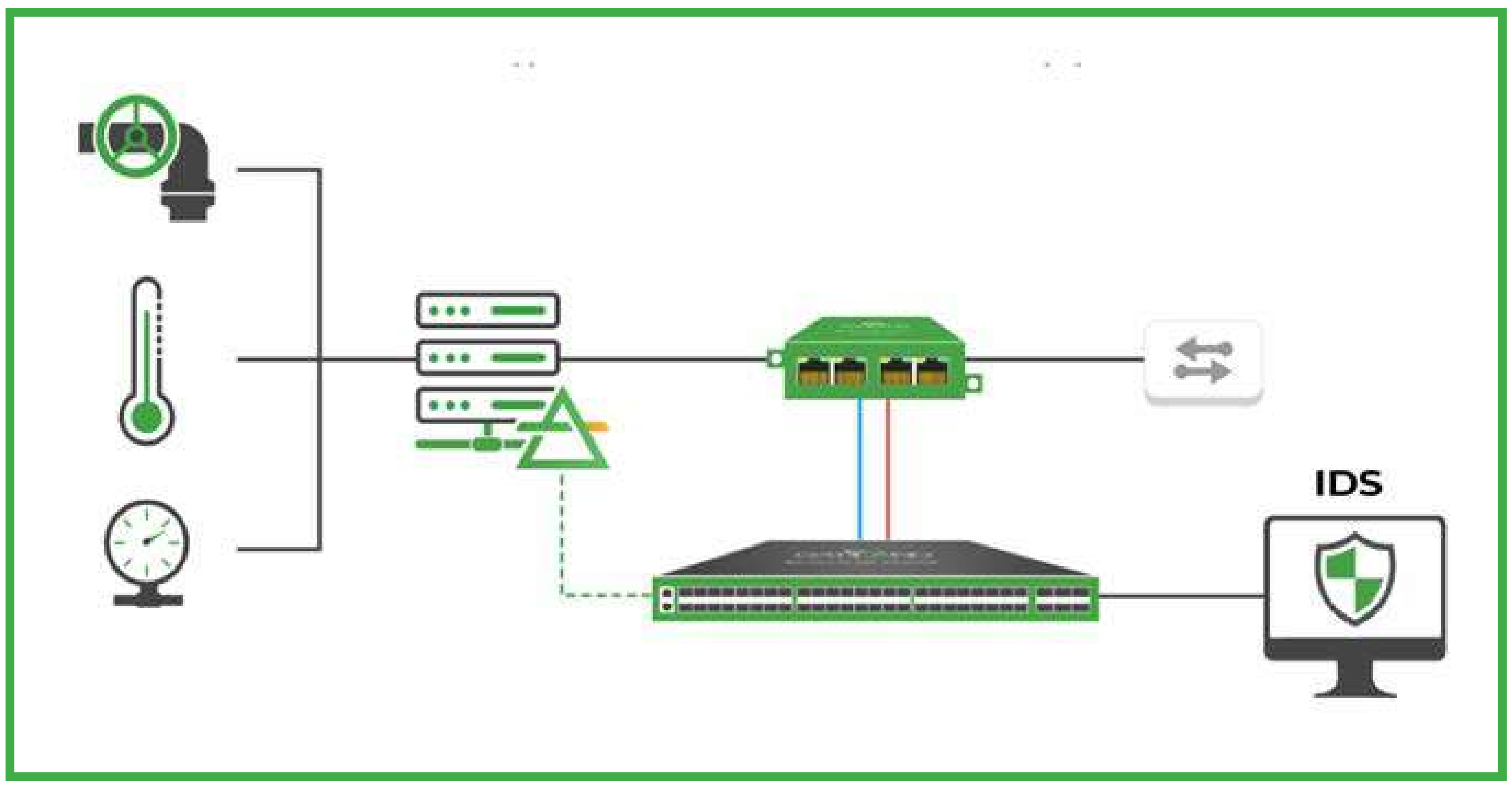
OT Environment Usage Example

Manufacturing and Drug Visibility Structure

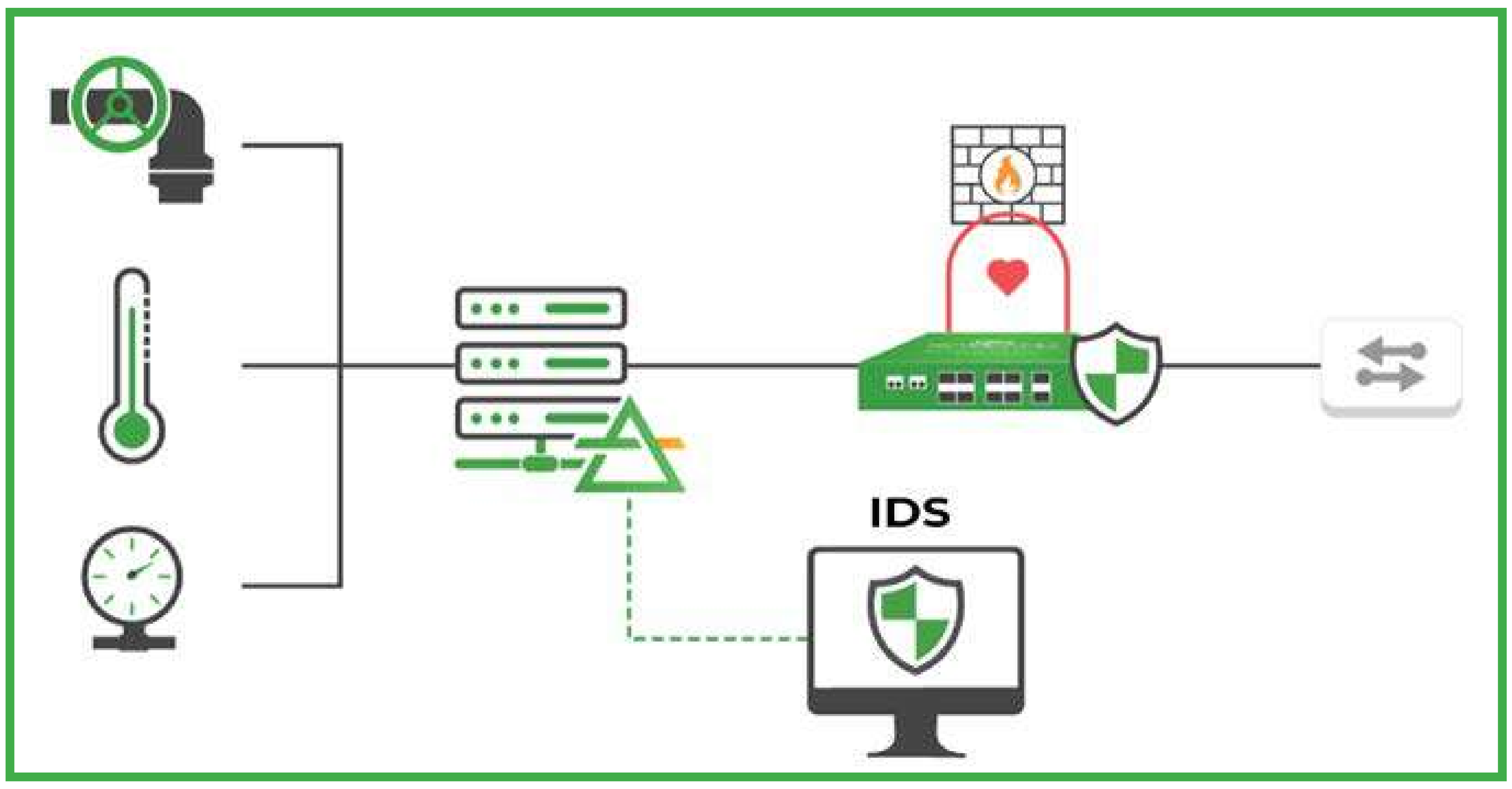


OT Environment Usage Example

Transformer SCADA Virtualization and Firewall Optimization



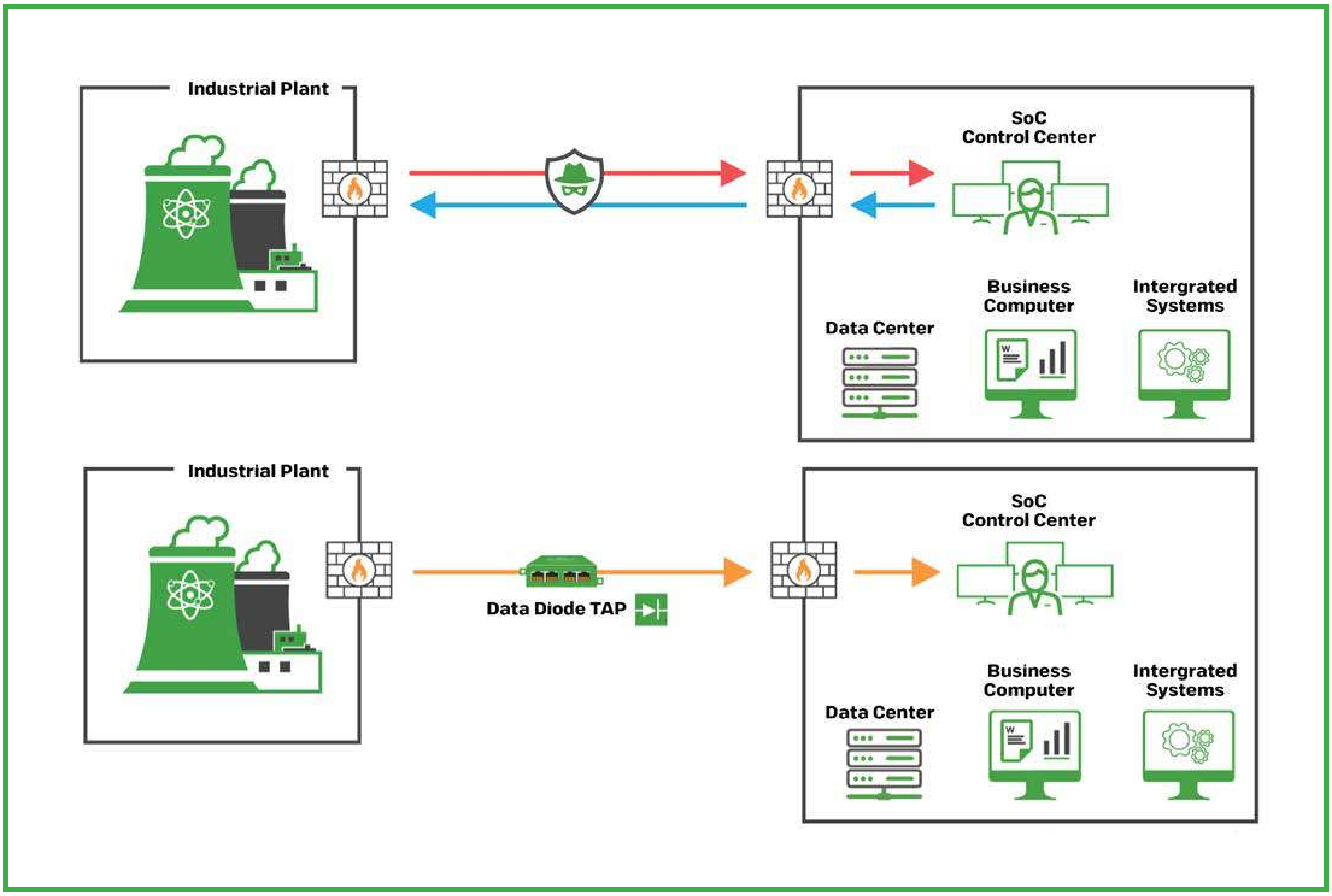
- Captures virtual SCADA packets
- TAP physical interface data
- Collects both physical and virtual data
- Conveys substation data to main data centers
- Offers full transformer data visibility



- SW updates to firewalls result in network downtime
- Loss of transformer center data visibility
- Bypass TAP maintains network availability
- Offers improved visibility during security updates

OT Environment Usage Example

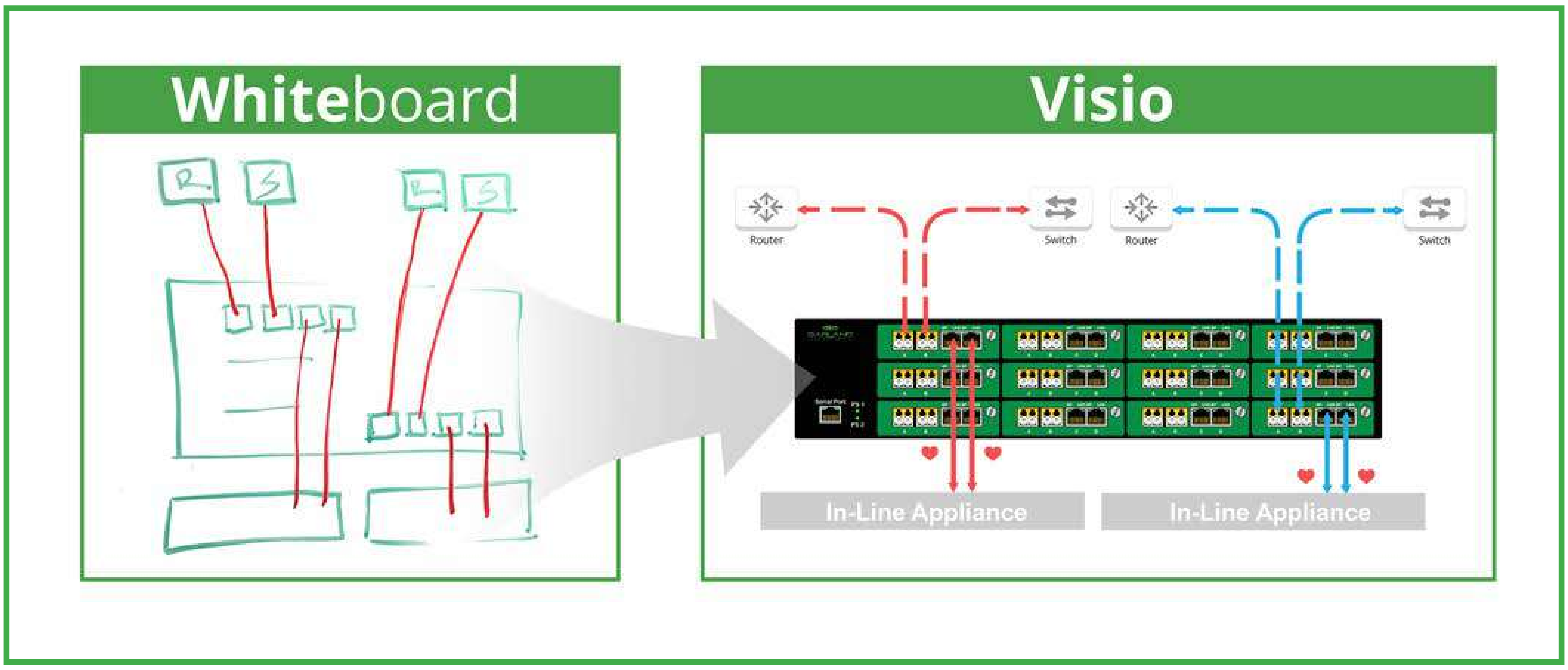
Data Diode TAPs for Secure One-Directional Traffic



Design-IT Demo

Consultancy | Design | Demo

Our engineers will help you in designing your next connectivity strategy



- You can discuss the implementation phase and goals of your project
- You can determine the basic network connection requirements
- You can help our team create whiteboard drawings tailored to your needs
- You can get free Visio diagrams to present to your team
- You can get product demo upon request

Garland Difference

Simple. Scalable. Difference High Quality.

1. Full Solution

360°Visibility
- Industry-leading network TAPs
- purpose-developed package agents
- Innovative inline bypass
- Cloud visibility and TLS decryption

2. Scalability

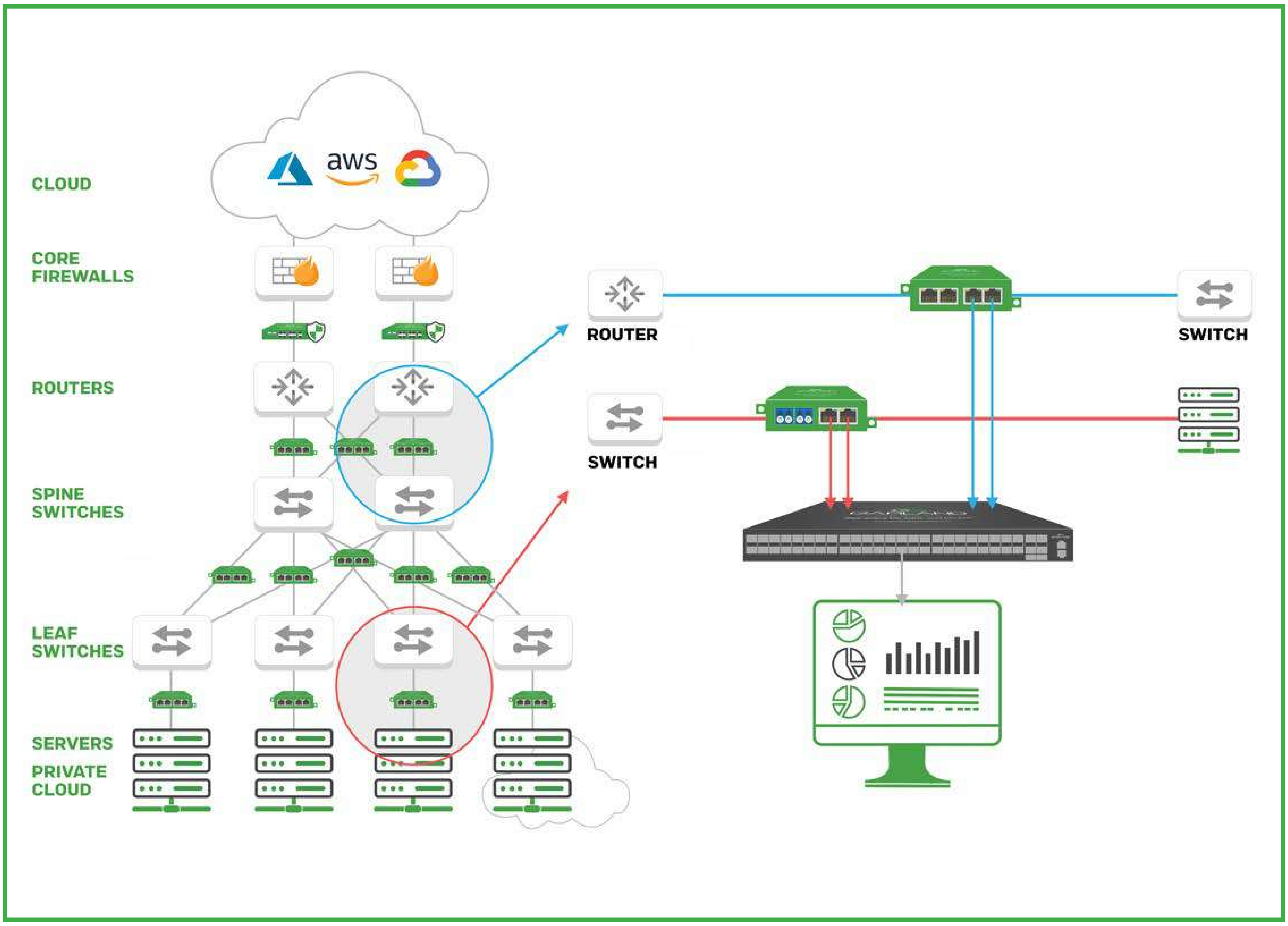
TAP - ToolTM Architecture
- Activation technology
- Unstructured NPB
- Open seller
- Optimized for customer budgets

3. Quality & Performance

Tested and Certified
- Activation technology
- Innovative [OM5, special]
- High density / hybrid
- Durability
- Failover and heartbeat technology
- High availability (HA) designs

Scalable visibility structure for your architecture

You can eliminate network and security blind spots while including flexibility and high performance for both in-line and out-of-band environments.



360º
Your Network Visibility Dock
Starts with Garland Technology

Physical Layer TAPs

- For out-of-band monitoring tools 100% Visibility
- Ongoing development [Customized solutions, First introduction of OM5 debut into the market]

Inline Edge Security

- Reduces the risk of downtime
- Provides flexibility and peace of mind
- Acts as innovative Inline hybrid package agent

Purpose-developed Package Agents

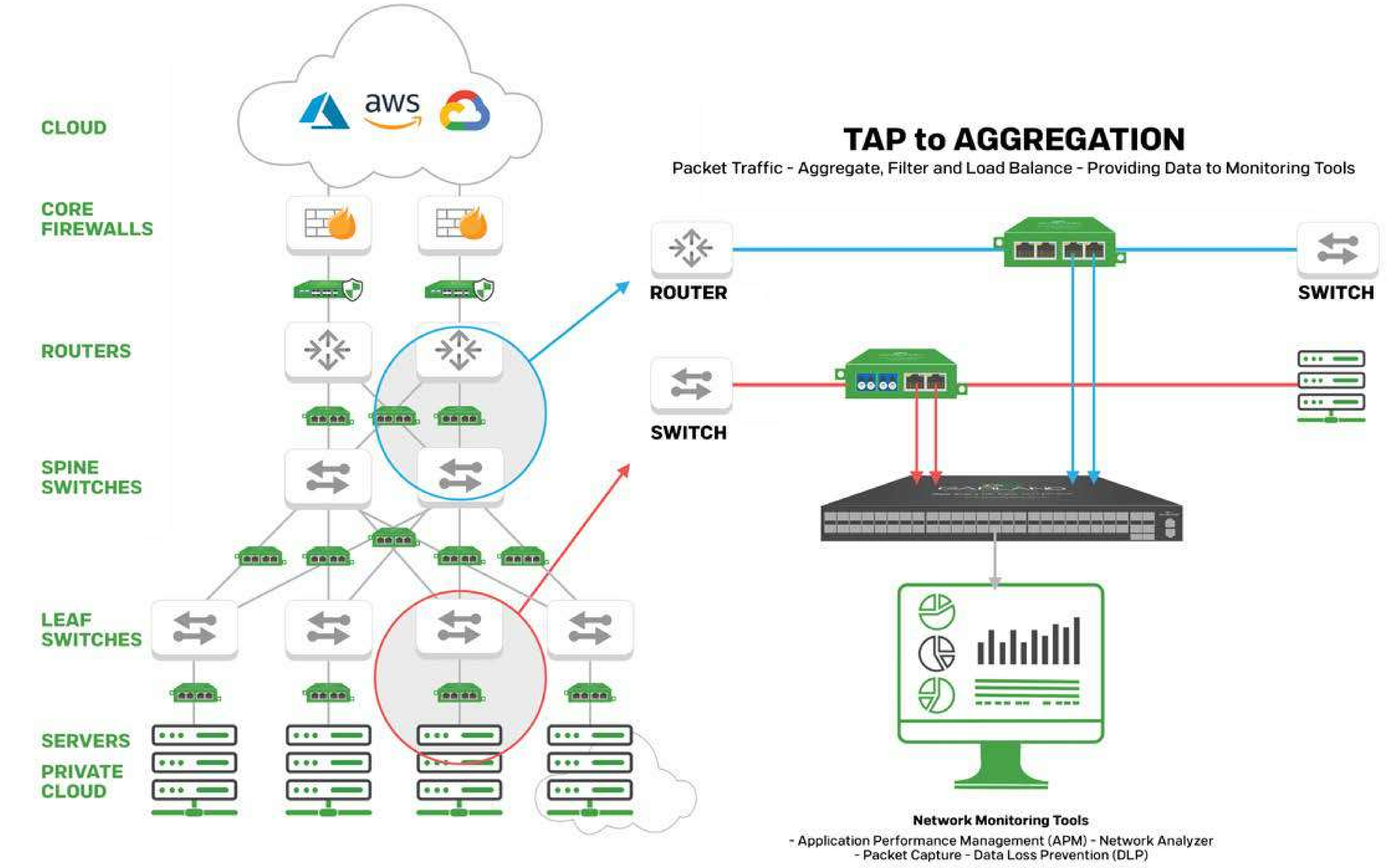
- Concentration layer supports the operations of filtering, concentration and load balancing
- Advanced features support deduplication, package slicing timestamp, and more

Cloud

- Private
- General

To Use the Out-of-Band Visibility Architecture

For Network Monitoring and Security Management


CLOUD
aws
CORE FIREWALLS
ROUTERS
SPINE SWITCHES
LEAF SWITCHES
SERVERS
PRIVATE CLOUD
TAP to AGGREGATION
Packet Traffic - Aggregate, Filter and Load Balance - Providing Data to Monitoring Tools
ROUTER
SWITCH
SWITCH
Network Monitoring Tools
- Application Performance Management (APM) - Network Analyzer
- Packet Capture - Data Loss Prevention (DLP)

Out-of-Band Monitoring and Security

Usage Circumstances

- To receive better network access for vehicles.
- To eliminate the blind spots.
- To increase team efficiency.
- To simplify network complexity.
- To adapt to traffic growth.
- To enhance network performance.
- To produce solution for limited cloud visibility.

Case Studies

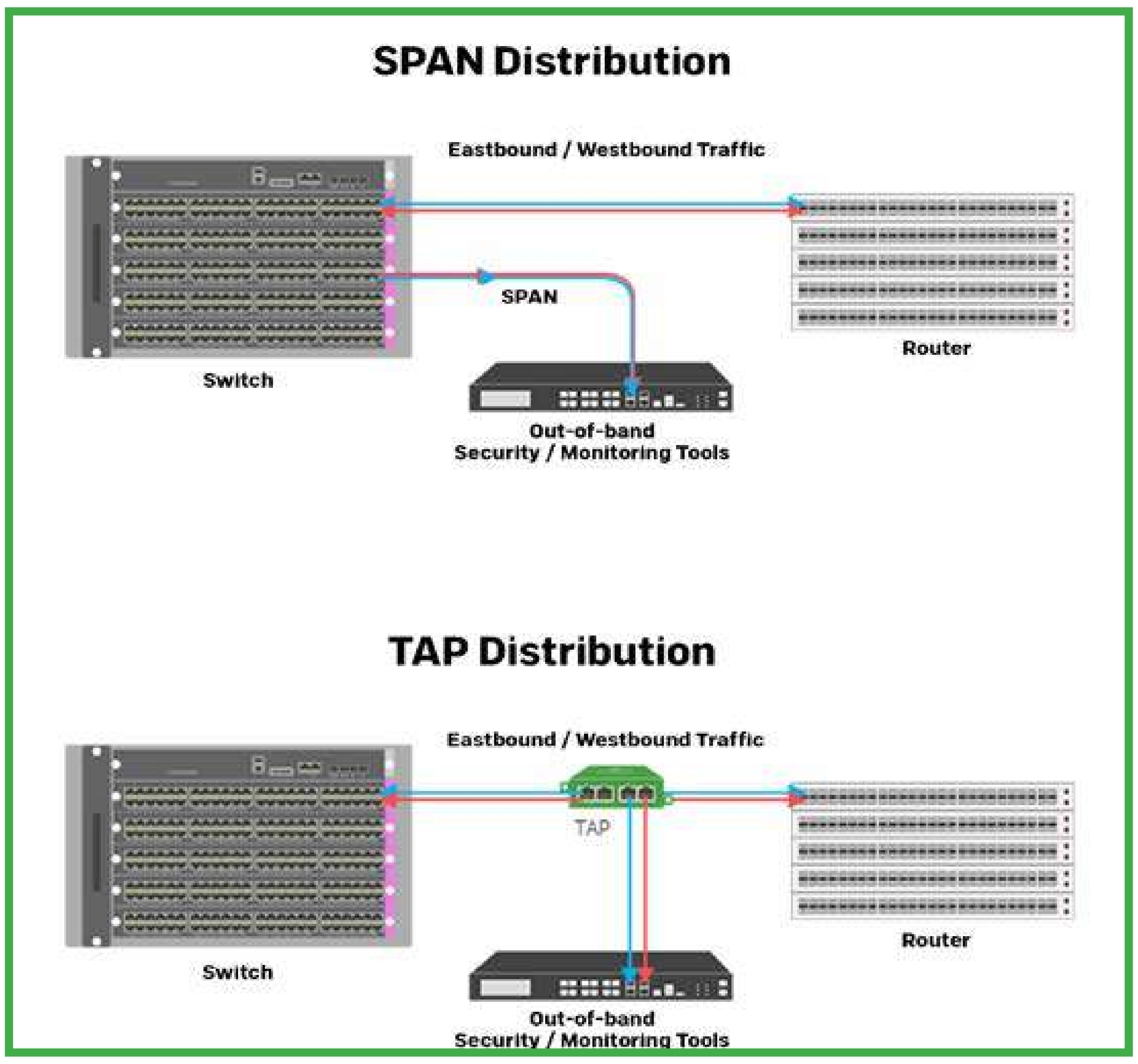
- To provide full visibility in case of an immediate response data breach.
- To provide troubleshooting in user performances in 5G environments.
- To improve visibility in order to improve the fix and fix the vulnerability.
- To provide visibility into industrial infrastructure and to reduce the network complexity.
- To provide additional visibility to one- directional routes.
- To offer tailored solutions to mission-critical data.
- To improve the legacy equipment by means of media and speed conversion.

Better Network Access for Vehicles

Usage Example for Network Monitoring Solutions

- **Difficulty:** There are two ways to access data for network monitoring, which are as follows:
- A mirror/switch port analyzer (SPAN)
- A purpose-developed network test access point (TAP)

- **Solution:** For offering advanges over SPAN ports, TAPS are deemed as the best practice.
- Delivers the 100% full duplex copy of network traffic without changing data or dropping packets.
- It is scalable and can perform operations such as single copy, multiple copies (rebuild) or traffic consolidation (aggregation) in order to maximize the performance of your monitoring tools.

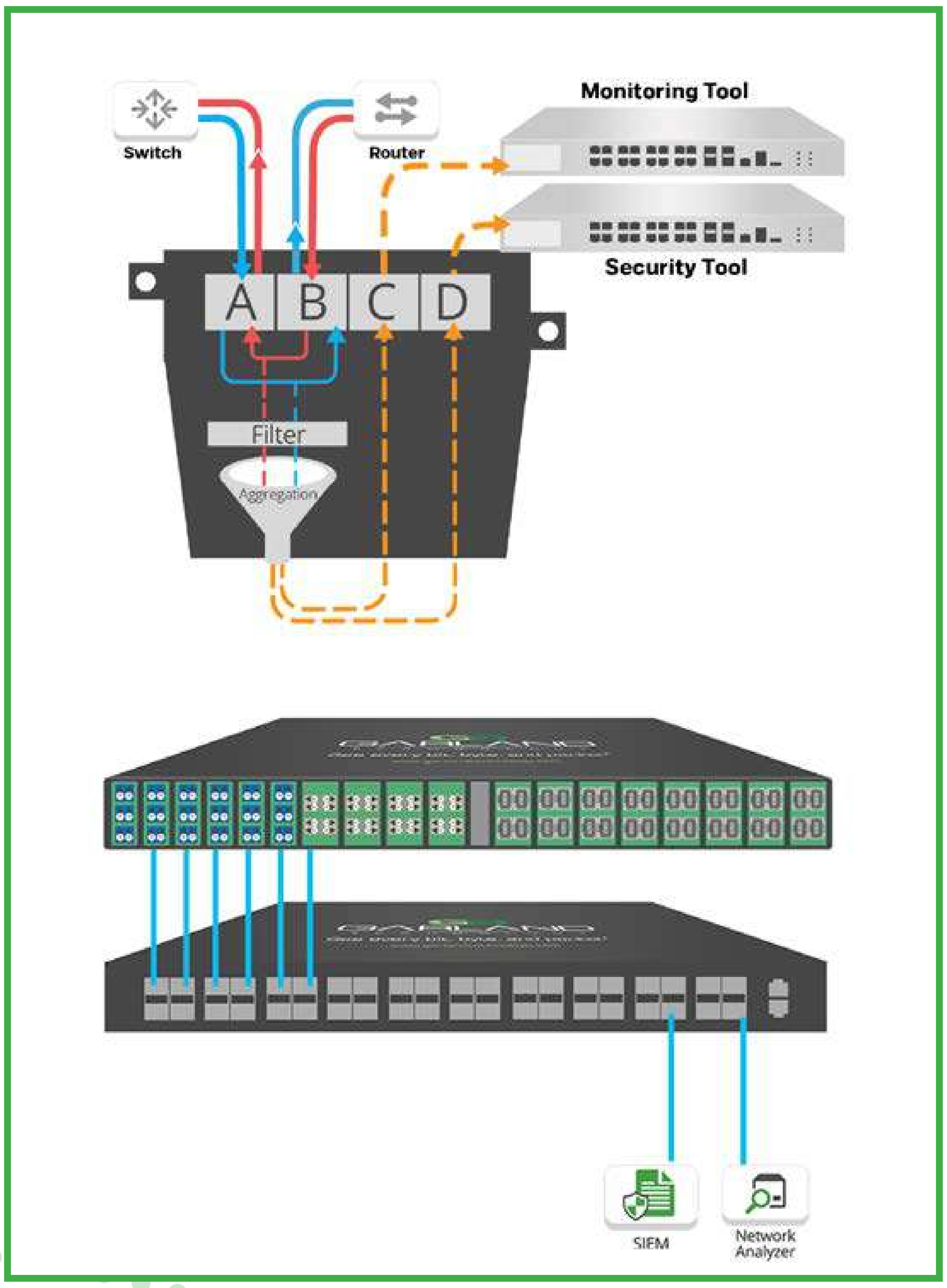

SPAN Distribution
Eastbound / Westbound Traffic
SPAN
Router
Switch
Out-of-band
Security / Monitoring Tools
TAP Distribution
Eastbound / Westbound Traffic
TAP
Router
Switch
Out-of-band
Security / Monitoring Tools

Increase Team Efficiency

Usage Example for Network Monitoring Solutions

Solution 2: Use of data filtering to enhance tool efficiency.

- Cost-effective solution to be used in isolating the data required to be examined
- Eases the load of existing tools and reduces traffic load, and thus, enhances the tool efficiency and performance
- This approach can be applied at the TAP level with the XtraTAP or the PacketMAX packet agents of Garland, which gather many simultaneous connections.



Simplify Network Complexity

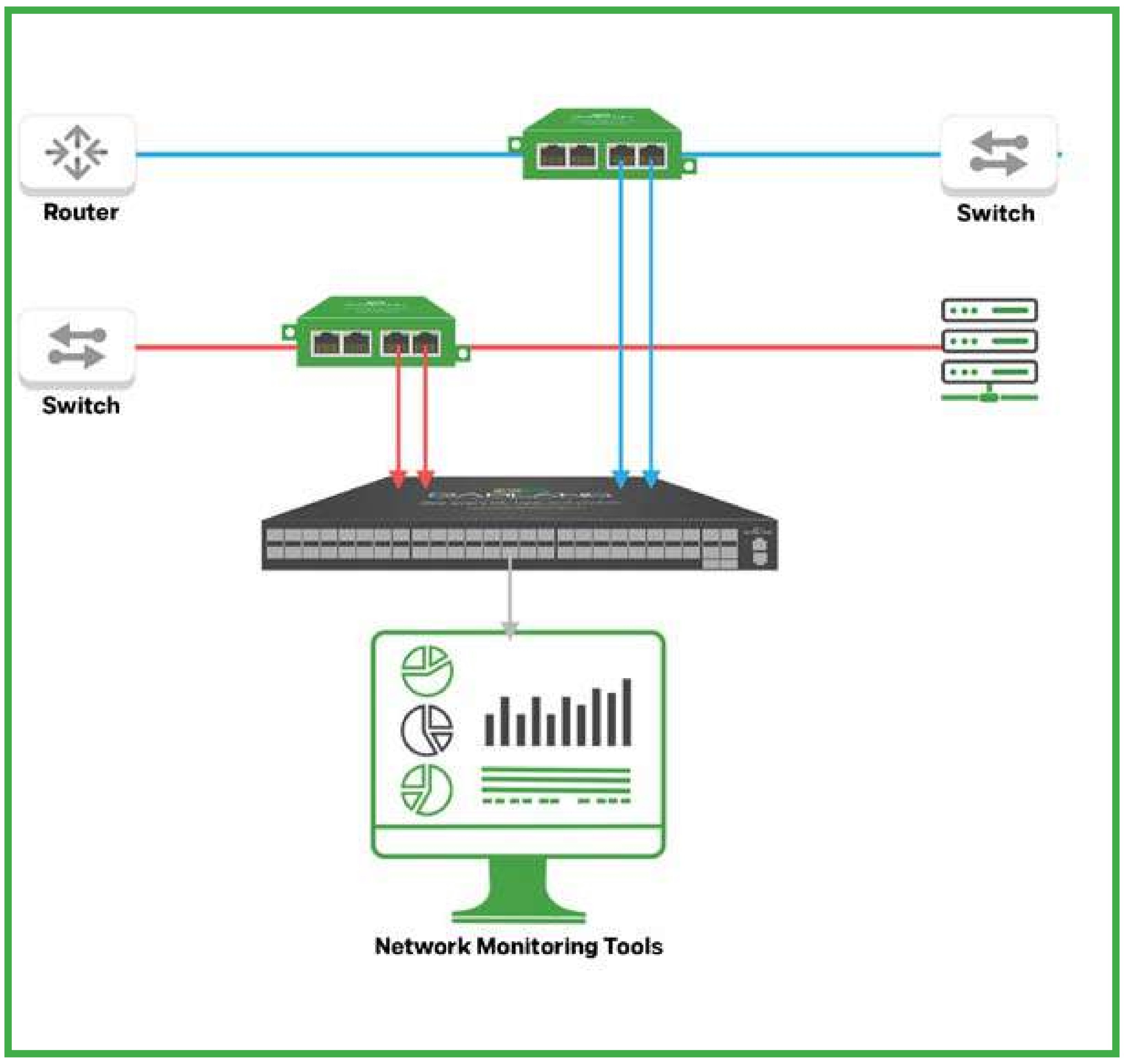
Usage Example for Network Monitoring Solutions

Difficulty: Teams that are using various tools, redundant tools, upgrading for higher speeds, using multi-team access or SPAN access may face with the following situations:

- Slower operational speed
- Data loss and oversubscription
- Slower MTTR and threat detection
- SPAN port maintenance

Solution: Thanks o the visibility structure of network TAPs and package agents, the network complexity can be simplified and the following points can be ensured:

- Better data for better performance and value
- Easy management of network access points to use and deploy new tools
- Bulk and optimized traffic before accessing the tools



Adapt to Traffic Growth

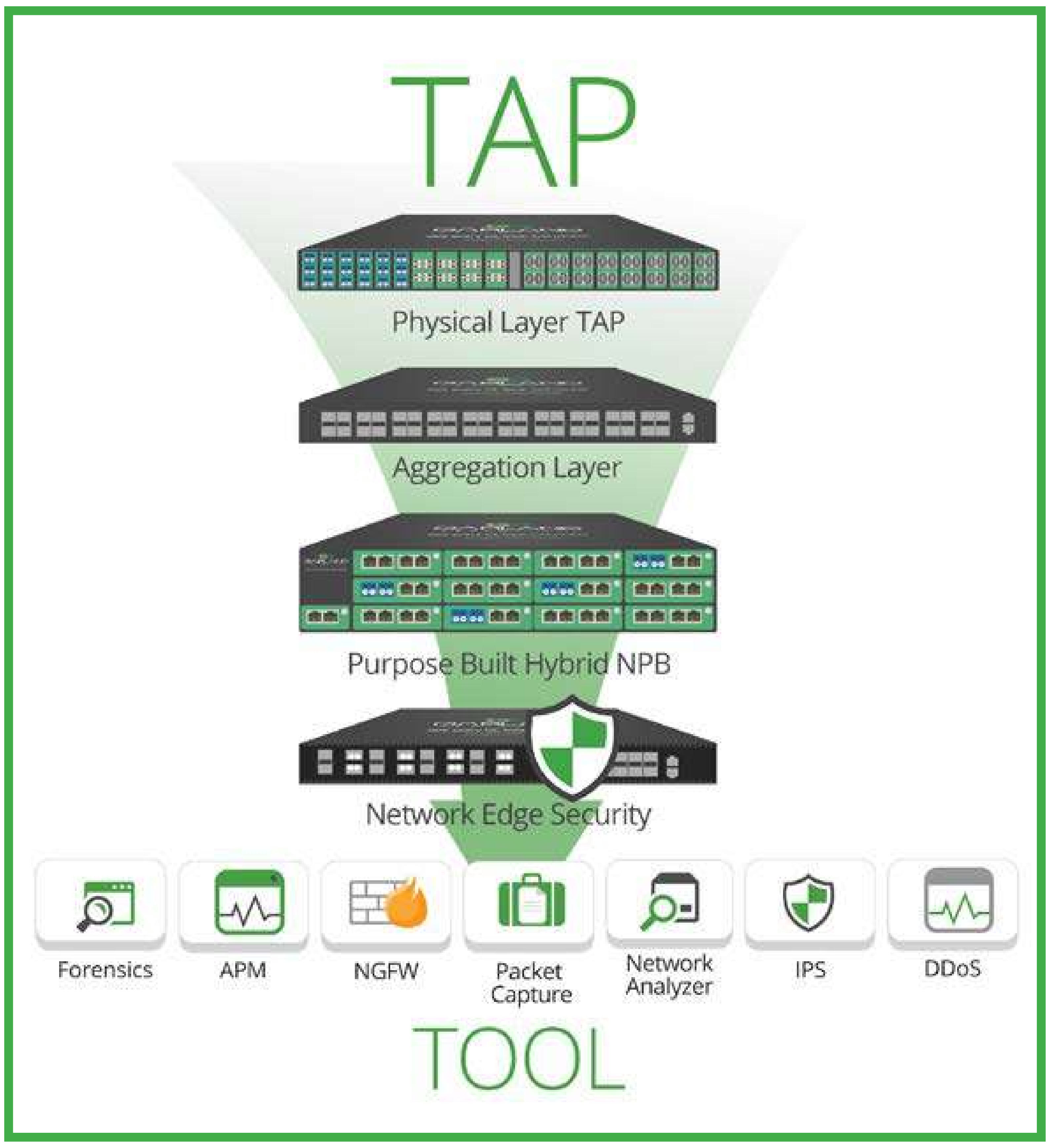
Usage Example for Network Monitoring Solutions

Difficulty: Teams upgrade their network speeds after realizing significant investments in 1G tools or moving from 10G to 25G or 100G.

- Budgets might be tight to accommodate multiple tools at an elevated speed.
- The entire cable infrastructure might be required to be replaced in the process.

Solution1: The modular approach provides scalability and flexibility to deploy what you need exactly when you need it.

- Modular network TAPs provide scalability to include additional TAPs into the same footprint.
- Deconstructed package agents offer cost-effectiveness through no additional port/feature license fees.

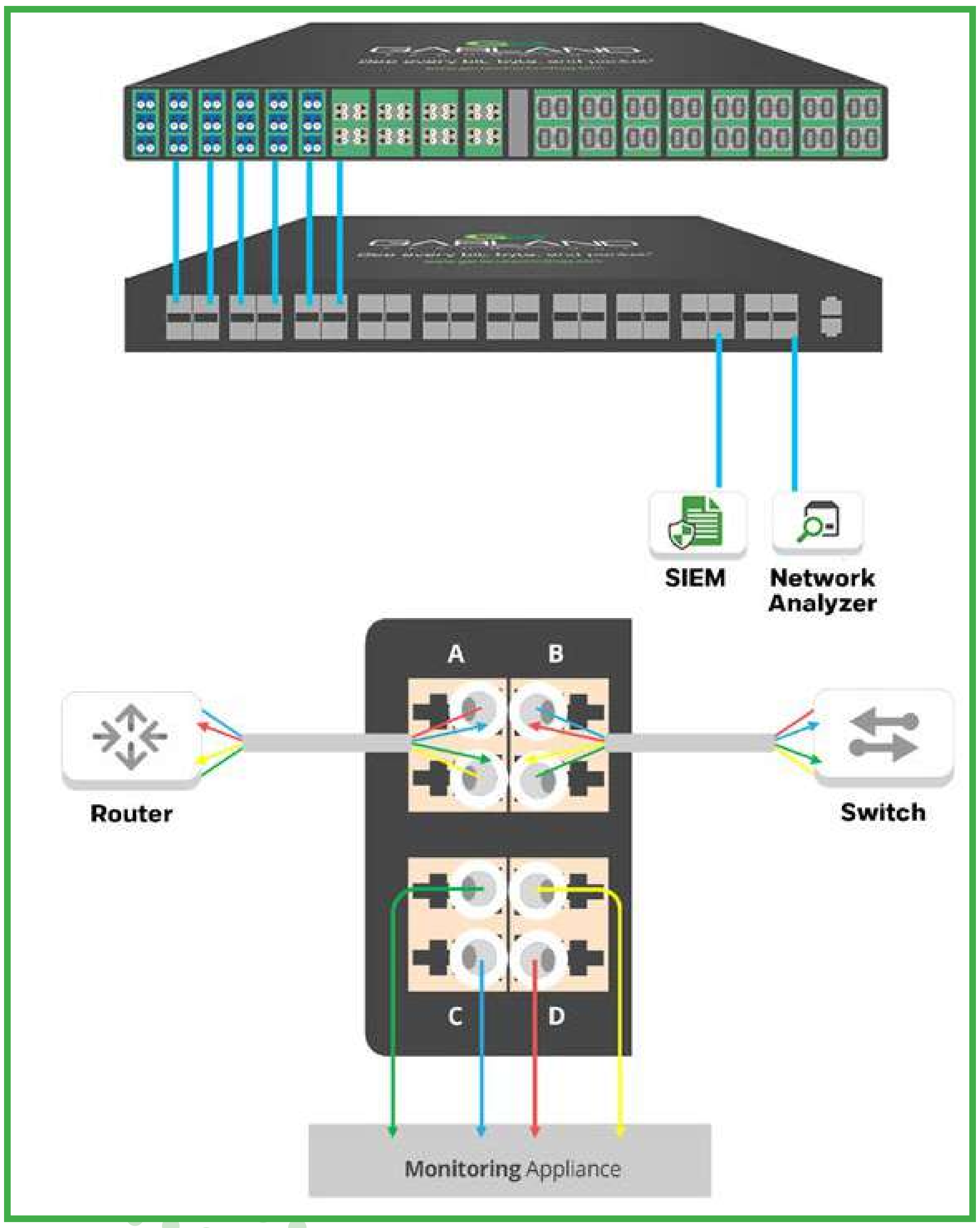


Adapt to Traffic Growth

Usage Example for Network Monitoring Solutions

Solution2: It is a very common situation that network speeds and media that don't match the current monitoring tools when ensuring the necessary compliance with the growth of network traffic.

- Network TAPs offer physical layer media conversion and 1-100G speeds
- PacketMAX packet agents provides the configuration of 1-100G network speeds
- Thanks to BiDi technology, network administrators can achieve
- 100G traffic over existing fiber infrastructure.



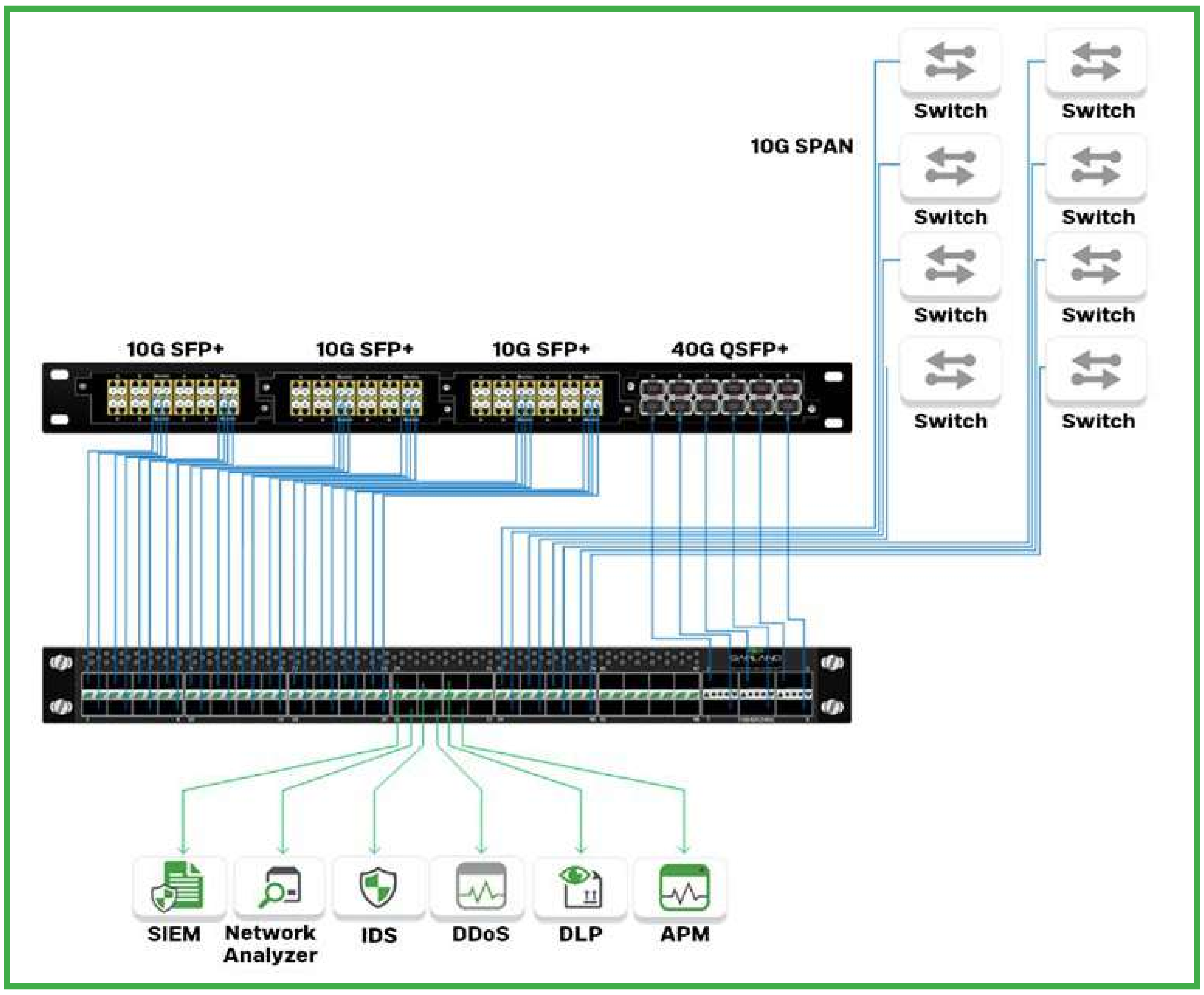
Enhance Network Performance

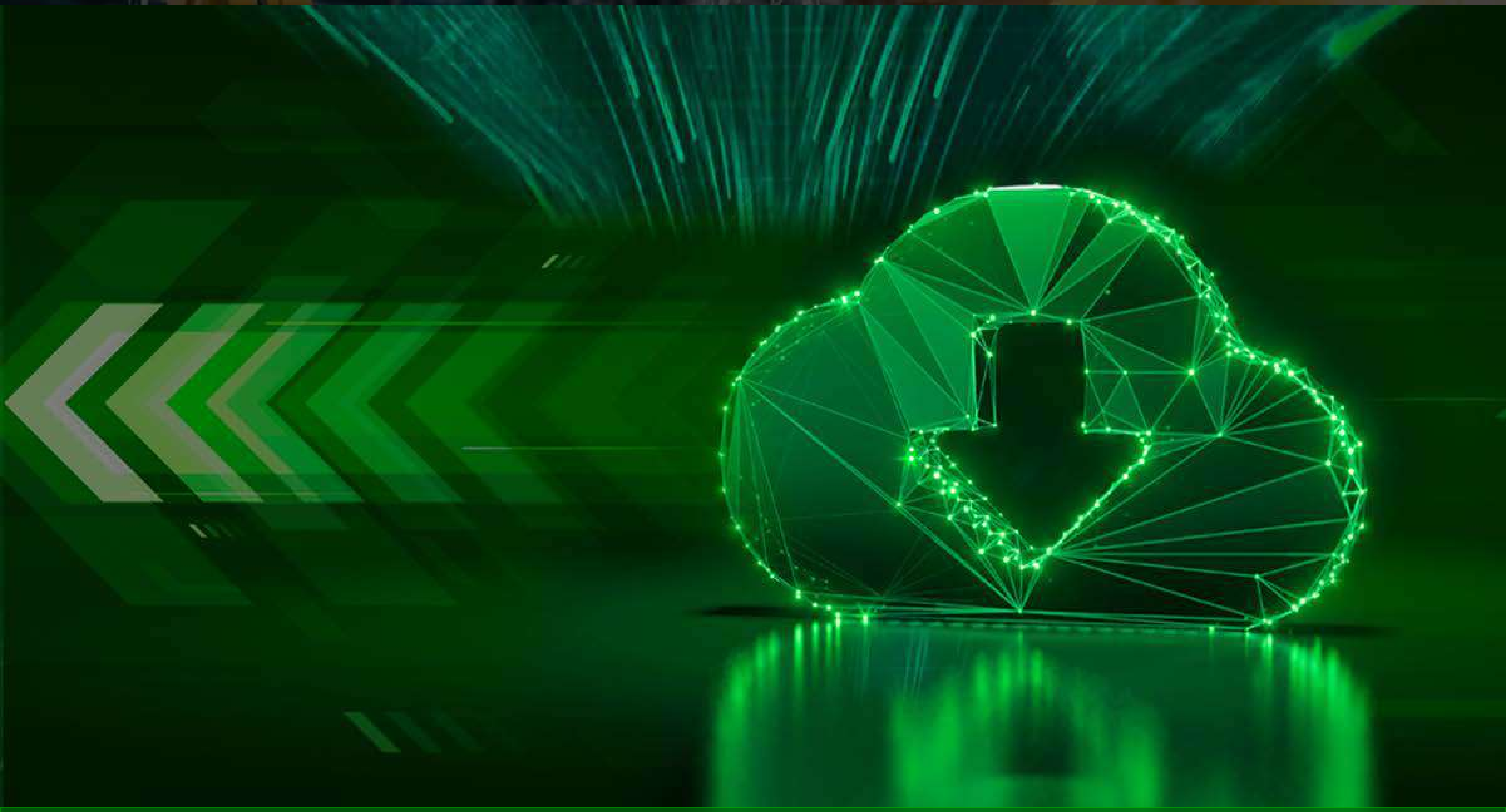
Usage Example for Network Monitoring Solutions

Difficulty: To optimize the network performance in order to troubleshoot and fix the issues.

Solution: Maximize speeds and feeds while keeping tools to offer efficient performance and through non-intrusive TAP solutions.

- Reduce the computational load on switches and tools through network TAPs
- Increase the efficiency and port utilization of NPBs.
- Filter the tool congestion traffic.
- To provide deduplication, package slicing and timestamping to remove the non-relevant parts of packages.





To Use the Out-of-Band Visibility Architecture

CASE STUDIES

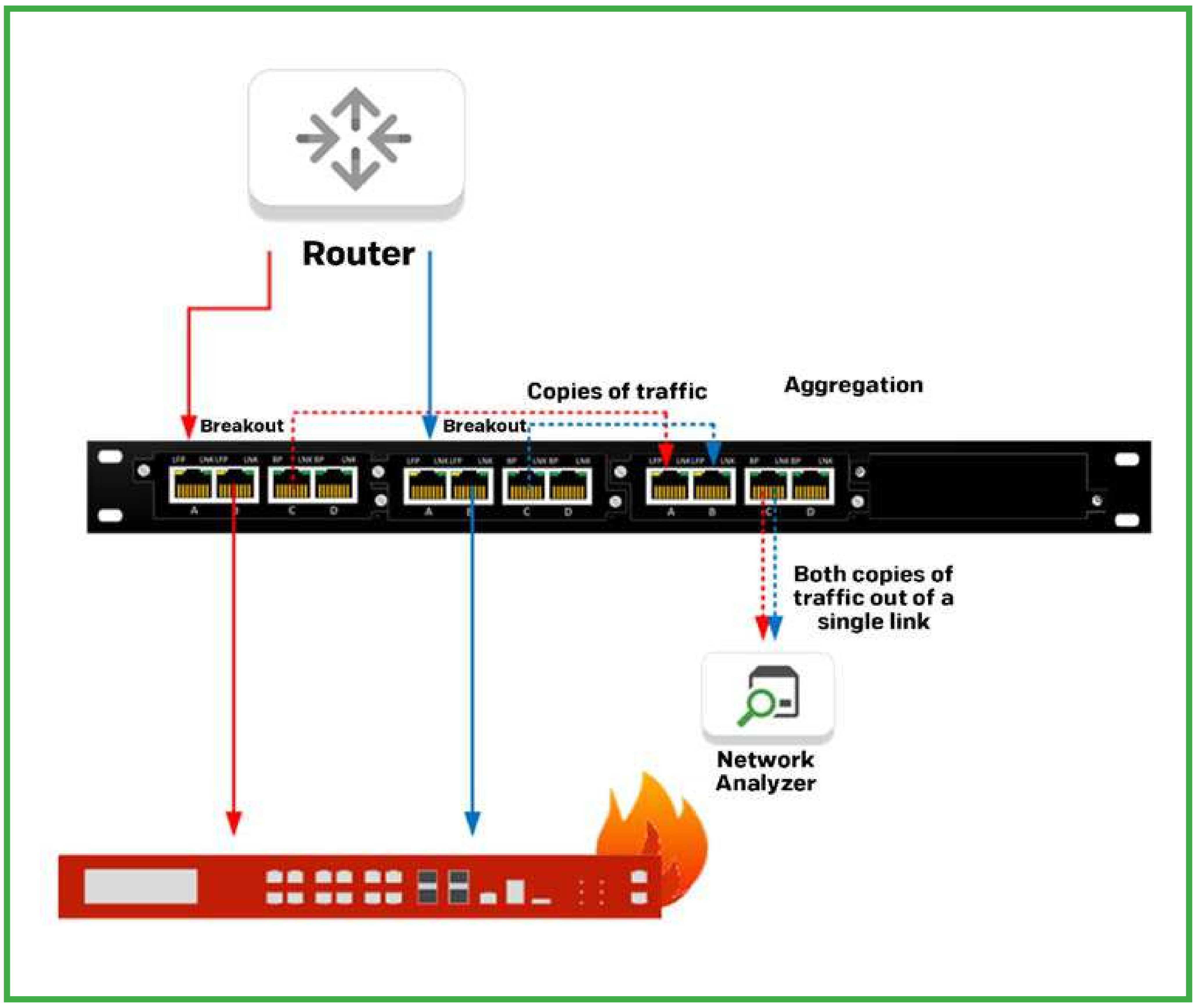
Health IT Security

To Provide Full Visibility in Case ofan Immediate Response Data Breach.

Difficulty: To optimize the network performance in order to troubleshoot and fix the issues.

Solution: Maximize speeds and feeds while enabling tools to provide efficient performance and preventing heavy impact.

- Reduce the computational load on switches and tools through network TAPs.
- Increase the efficiency and port utilization of NPBs.
- Filter the tool congestion traffic.
- To provide deduplication, package slicing and timestamping to remove the non-relevant parts of packages.



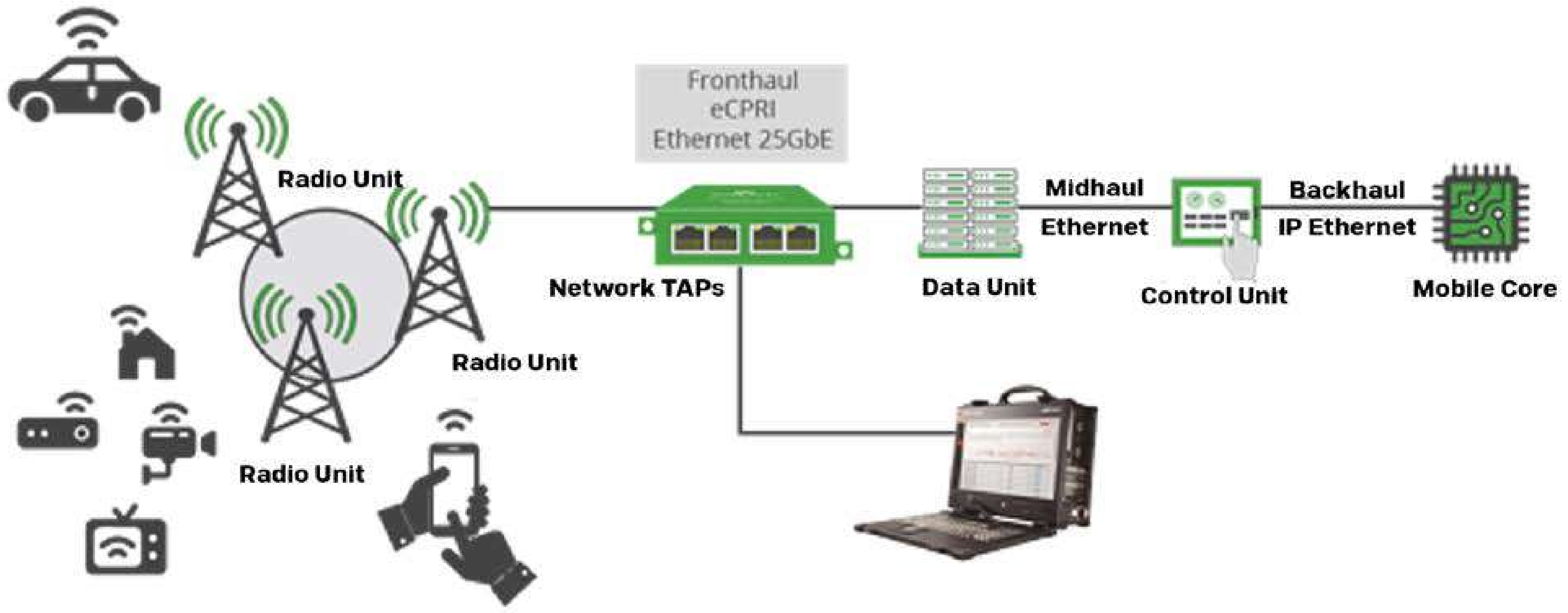
Monitoring 5G Environments

Troubleshooting User Performance Issues in Fronthaul

A mobile wireless provider that has launched a national 5G network has been granted with full package-level visibility for extensive testing and monitoring at high speeds.

Solution: 25G Passive Fiber Network TAPs of Garland which power the SYNESIS 25G Portable has gained instant package capture visibility.

- The current 10G TAPs that cannot adapt to 25G have been replaced
- The need for large space and power requirements compared to rack-mount systems have been eliminated
- Complete "zero packet loss" visibility has provided full reliability for the analysis results
- Reduced CapEx cost for portable high-density equipment
- Reduced OpEx cost for on-site personnel



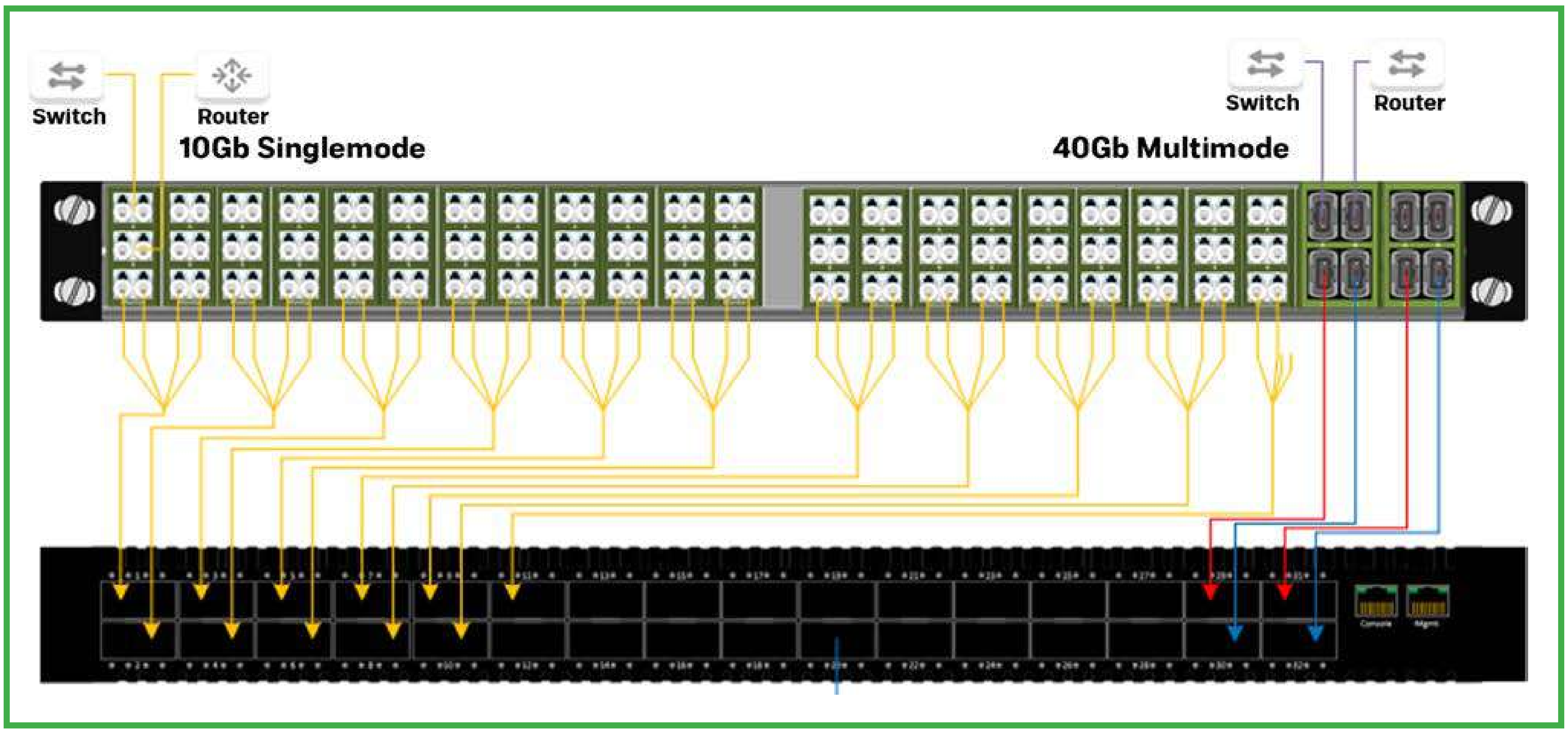
Telecommunications Monitoring

Improve Visibility in Order to Improve the Fix and Fix the Vulnerability.

The Prepaid Wireless Group has included the Garland visibility into its scope in order to enhance its network remediation and to address network vulnerability.

Solution: Distribution of 40G passive fiber SelectTap and PacketMax of Garland that feed the package capture tools of Cirries' PacketPoint.

- Modernize the data collection workflows for analytics during troubleshooting and security incident response.
- Provide improved visibility, network troubleshooting and solution.
- Improve the reduced complexity and network performance.



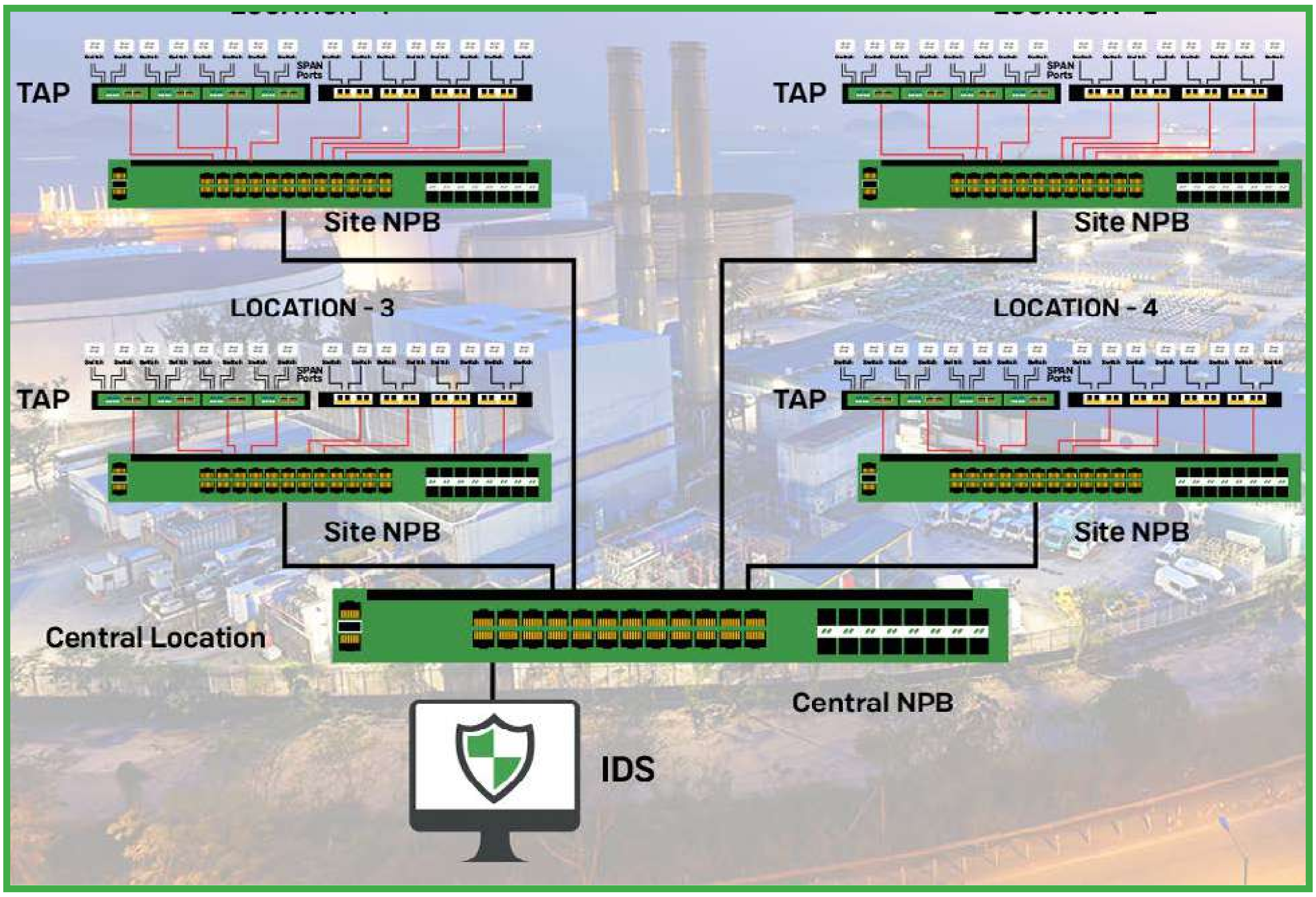
Industrial Infrastructure

To Provide Visibility and to Reduce the Network Complexity.

A leading O&G company intended to reduce the connectivity complexity, to offer higher performance and to establish a bridge OT to IT.

Solution: Distribute the AggregatorTAPs and PacketMAX package agents all together across the network that provide feedback to the central location.

- Reduce complexity and management burden.
- Enable infrastructure upgrades.
- Enhance Network performance.
- Increase the effectiveness of team performance.



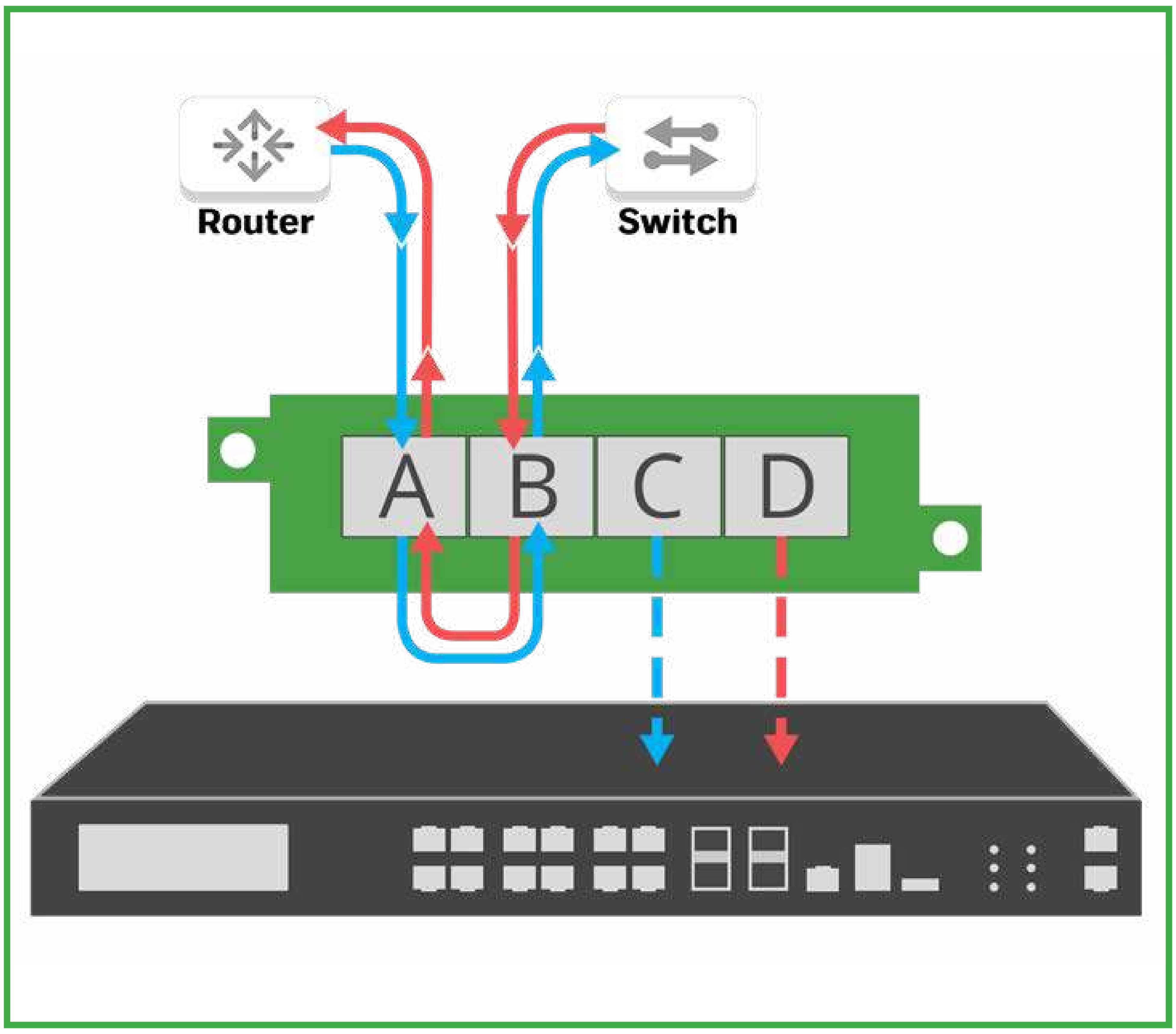
Industrial Infrastructure

To Provide Additional Visibility to One-Directional Routes.

A leading multinational O&G company has taken additional measures against cybersecurity risks.

Solution: Data Diode TAPs

- Avoids the bi-directional traffic in order to protect against backflow of traffic into the network.
- Secure- TAPs do not contain any IP address or MAC address and are not vulnerable to attacks.
- Protects the additional data flow resources such as switch SPAN ports and network connections.
- Network traffic control becomes mandatory at physical level.



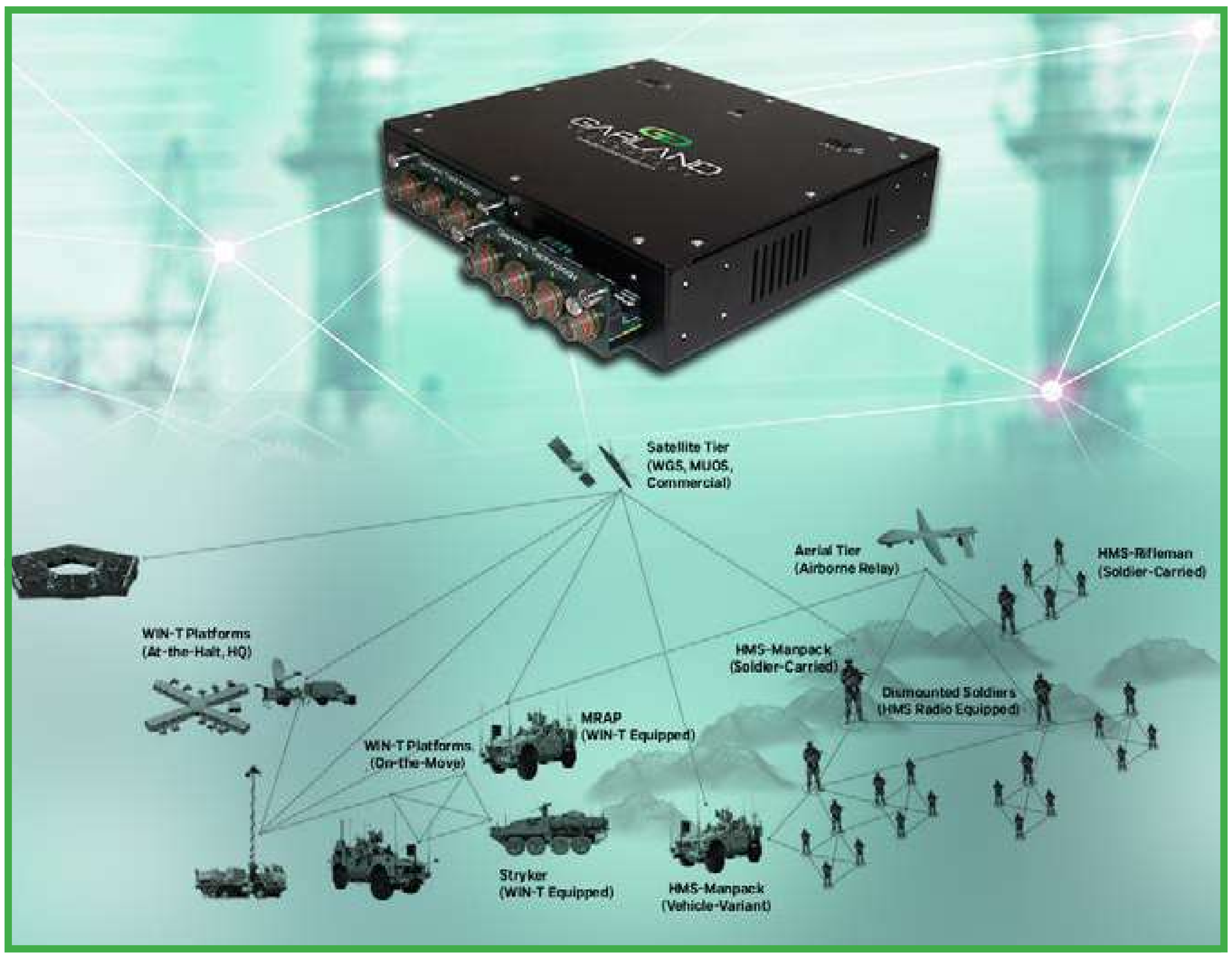
Federal Full Package Capture

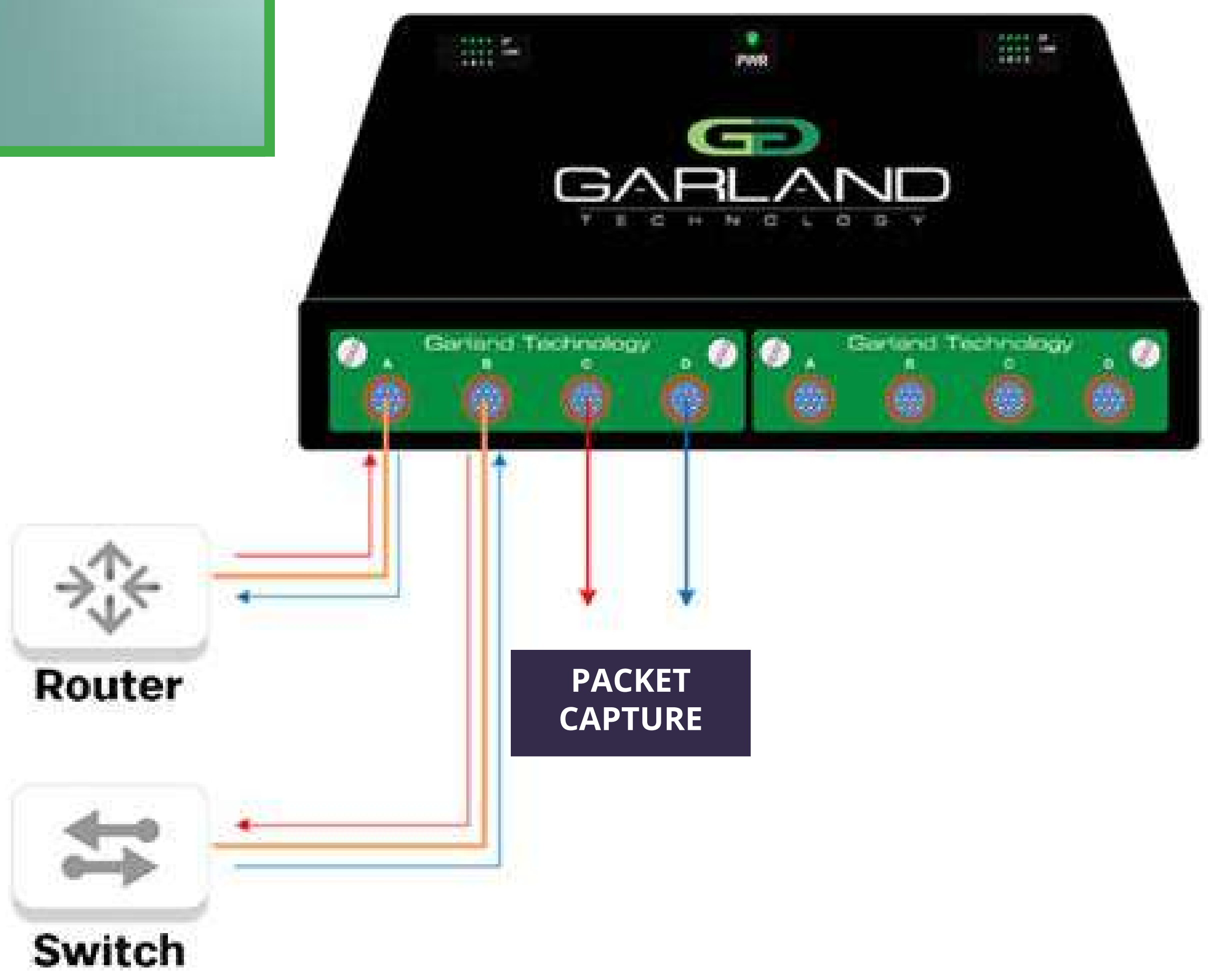
Tailored Solutions for Business Critical Data.

The Ministry of Defense relies on Garland for custom, durable, high quality, fast turnaround.

Solution: Special TAPs for Extreme Environments

Garland has developed a tailored TAPS to resists against environmental and durability- related concerns and feed the operational data to a package capture tool and hard drives, enabling the collection of 100% complete mission-critical data.





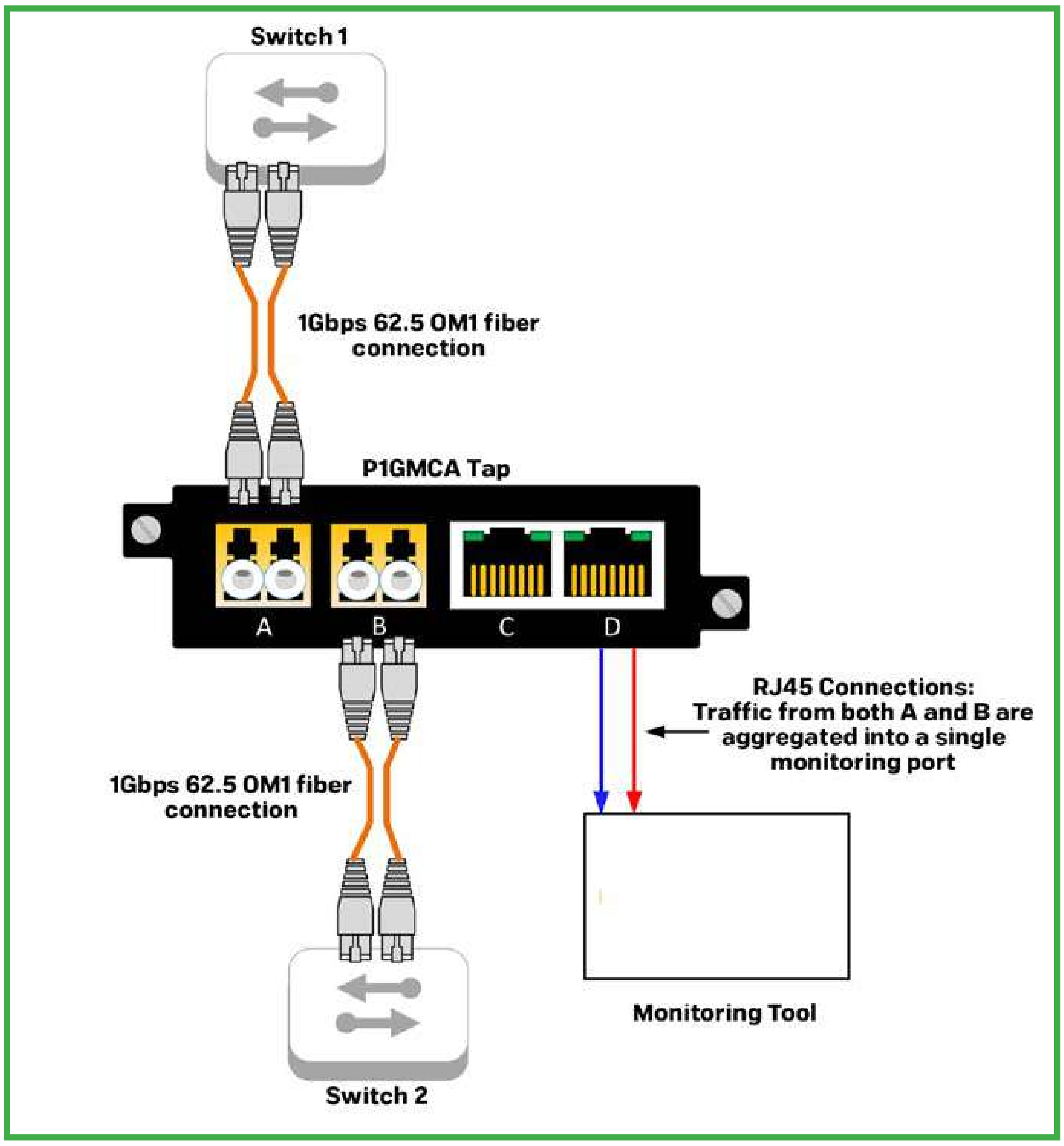
Industrial Infrastructure

To Improve the Legacy Equipment by Means of Media and Speed Conversion.

A leading US utility company needed to to build and manage a security platform.

To produce network visibility solutions through media conversion, and accordingly, to minimize the critical infrastructure risk with legacy connections.

1G Aggregator TAP of Garland was used, which resulted in 100% network visibility, and critical infrastructure risk was enabled to be reduced with zero impact on operations

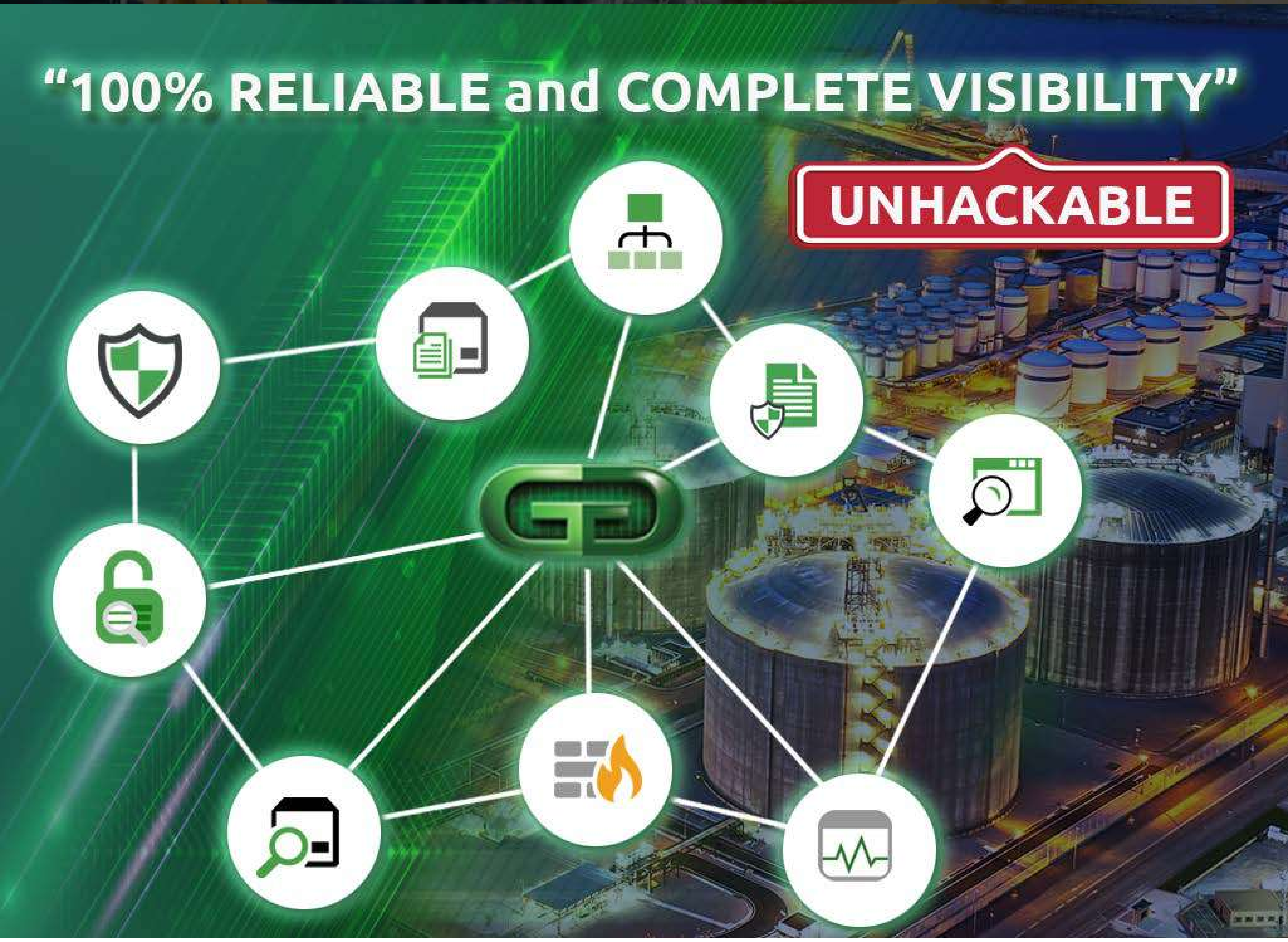

Switch 1
1Gbps 62.5 OM1 fiber connection
P1GMCA Tap
A
B
C
D
RJ45 Connections: Traffic from both A and B are aggregated into a single monitoring port
1Gbps 62.5 OM1 fiber connection
Monitoring Tool
Switch 2

Network TAPs and Package Agents increase the effectiveness of security and monitoring technologies and reduce overall risk.

Advantages to be Offered:

- To Simplify Network Complexity
- To enable infrastructure upgrades
- To increase the effectiveness of team
- performance
- To facilitate traffic growth
- To reducing compliance violations
- To offer improved uptime
- To increased security team productivity

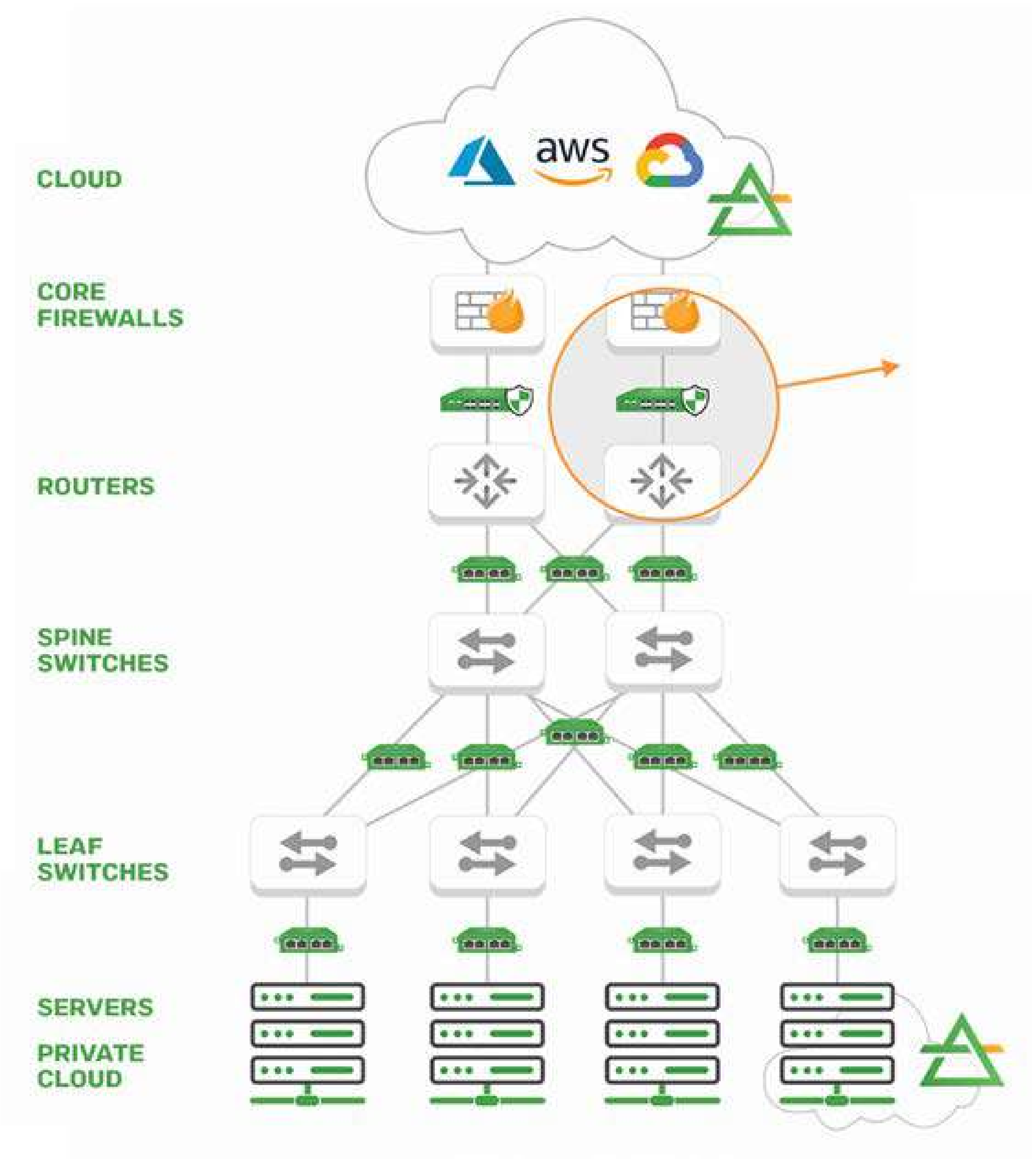
GARLAND TECHNOLOGY

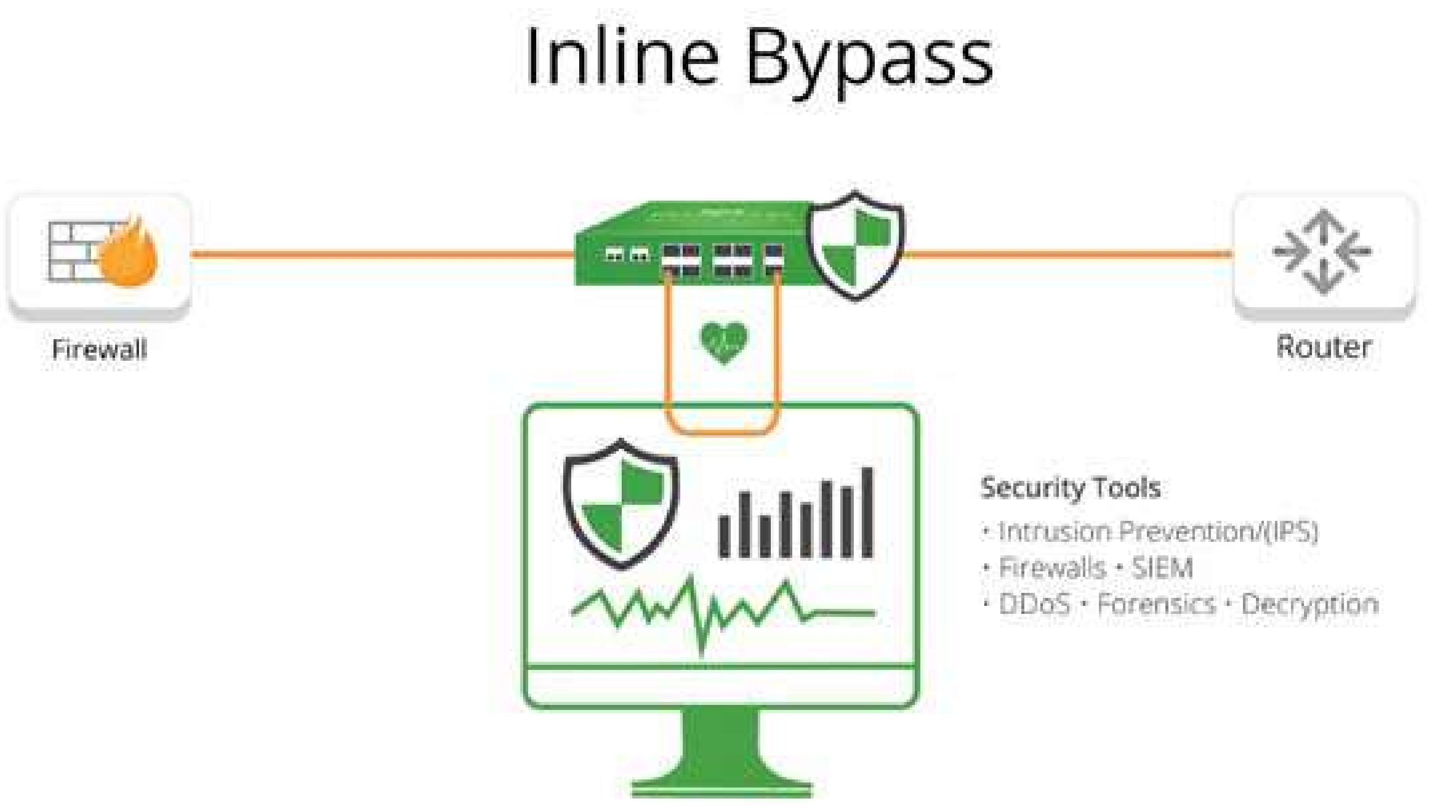


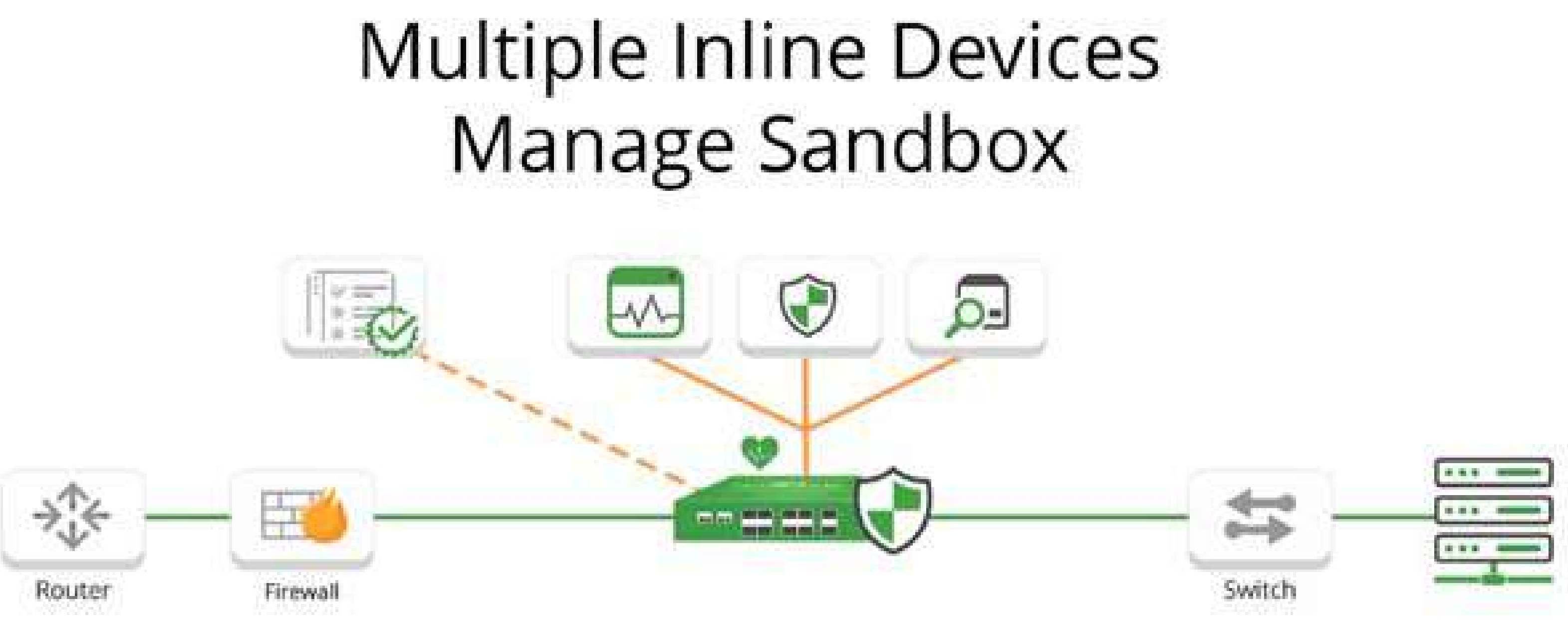
How to Improve IT Security Threat Detection and Prevention Deployments?

To Use Inline Visibility Architecture

Inline Edge Security







Inline Security

Usage Example:

- Reduce Network Downtime
- Eliminate Single Point of Failure
- Manage Multiple Inline Tools
- Optmize Inline Tools Performance
- Include Backup HA Solutions

Case Studies:

- Provide Inline Threat Prevention Optimization and Analysis
- To Offer Full High Availability (HA)
- Redundancy for Critical Connections

Reduce Network Downtime

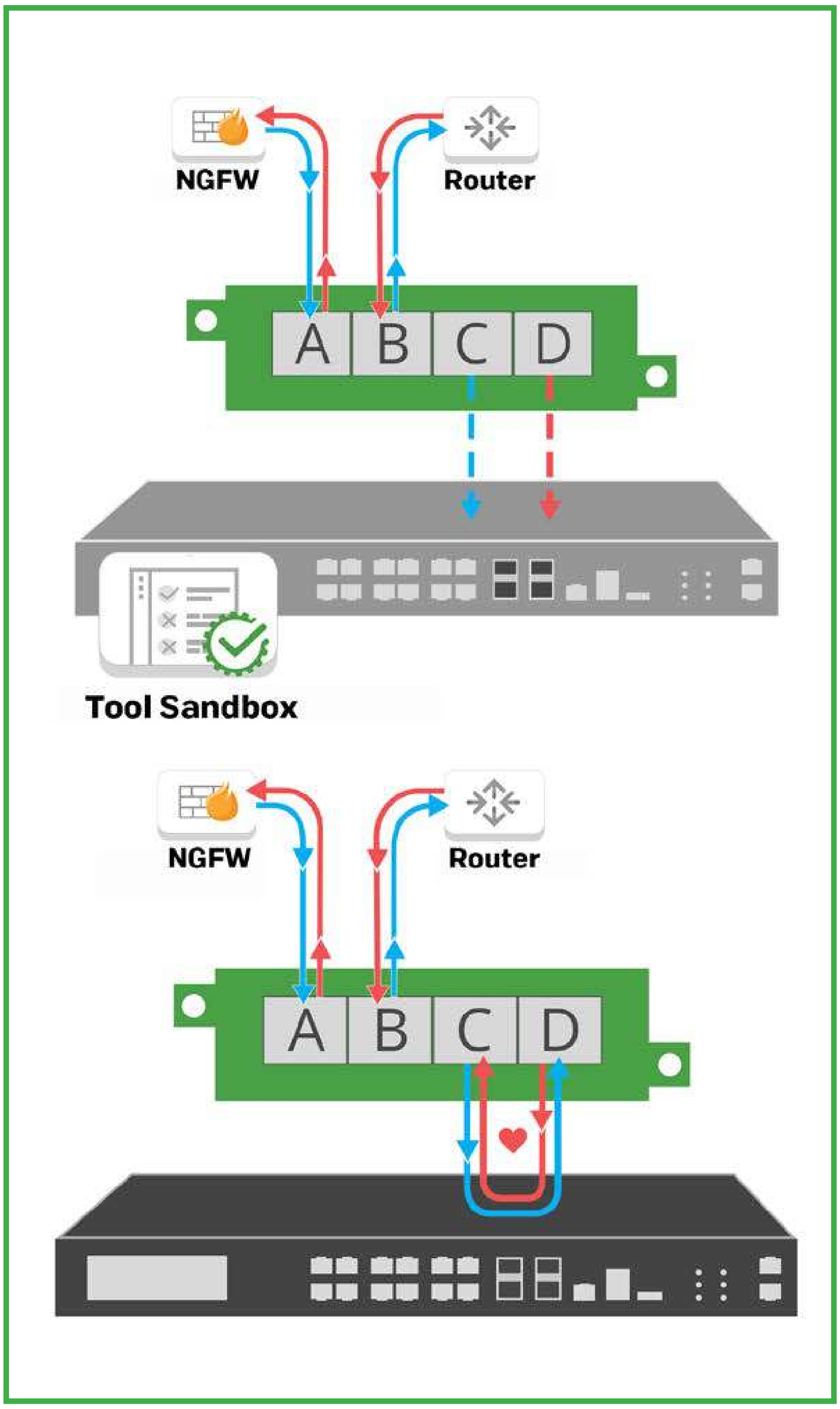
Usage Example for IT Security Solutions

Difficulty: To manage the risk of downtime is a critical issue in deploying the security tools.

- Tools with a high number of subscribers cause a decrease in the network performance
- tool failures might crash the network
- To include new technologies into the network
- To project the planned downtime

Solution: Thanks to Bypass TAP Inline lifecycle management:

- You can easily take the tools out of band in order to perform the operations of updating, patching, maintenance or troubleshooting for optimization and validation purposes.
- Administrative isolation - Zero maintenance window
- Tool Sandbox - Pilot or deploy new tools



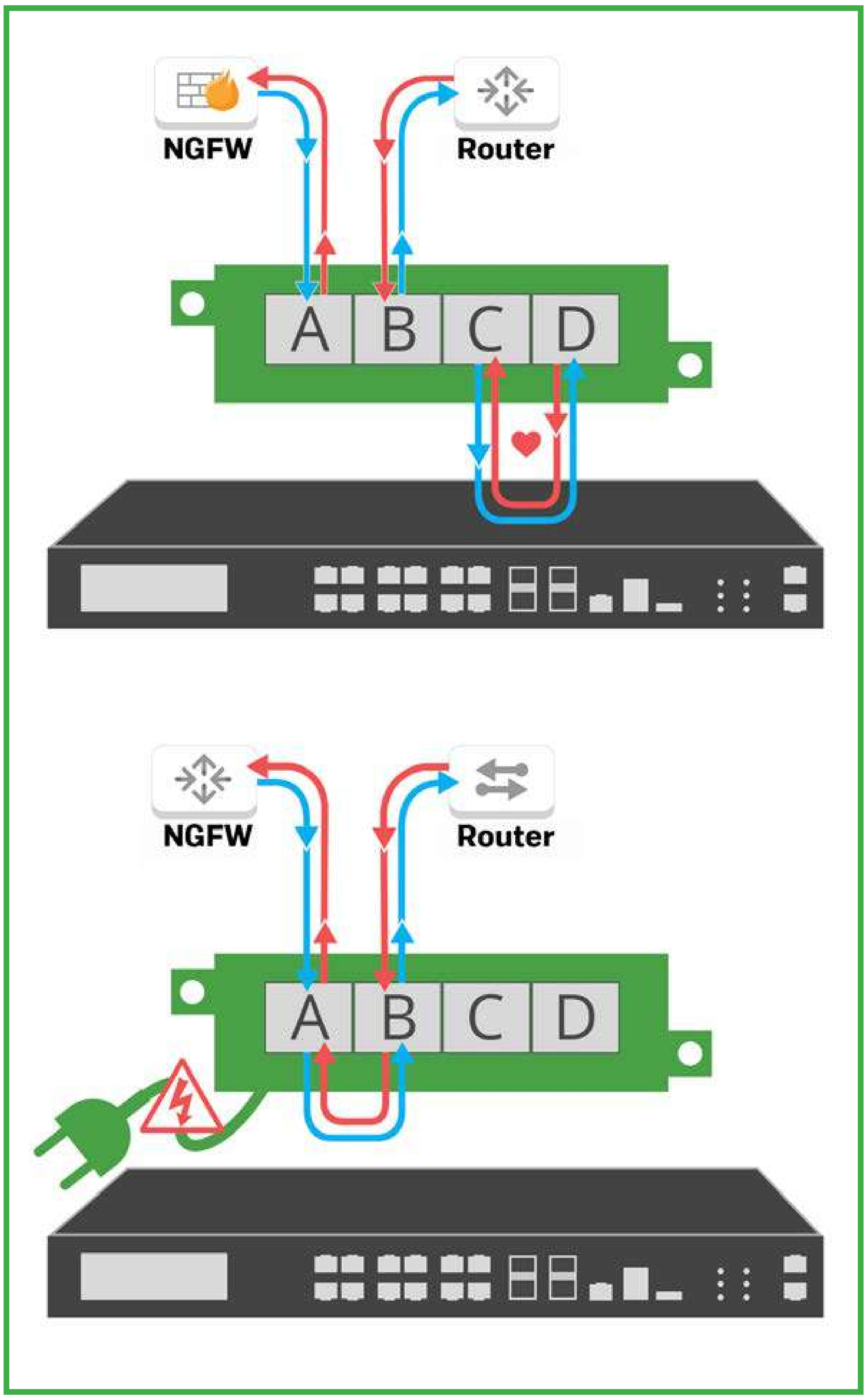
Multiple Inline Tool Management

Usage Example for IT Security Solutions

Difficulty: To deploy and manage the evolving list of security tools, including IPS, WAFs, firewalls, SIEM, DDoS and SSL encryption.

Solution: You can manage inline and out-of-band vehicle availability thanks to Inline Tool Chaining.

- You can pass traffic through multiple inline tools.
- You can monitor the health of each inline tool independently with bypass heartbeats.
- Load balance to other tools 1:1 or 1:N tools
- You can also send traffic to out-of-band monitoring tools.

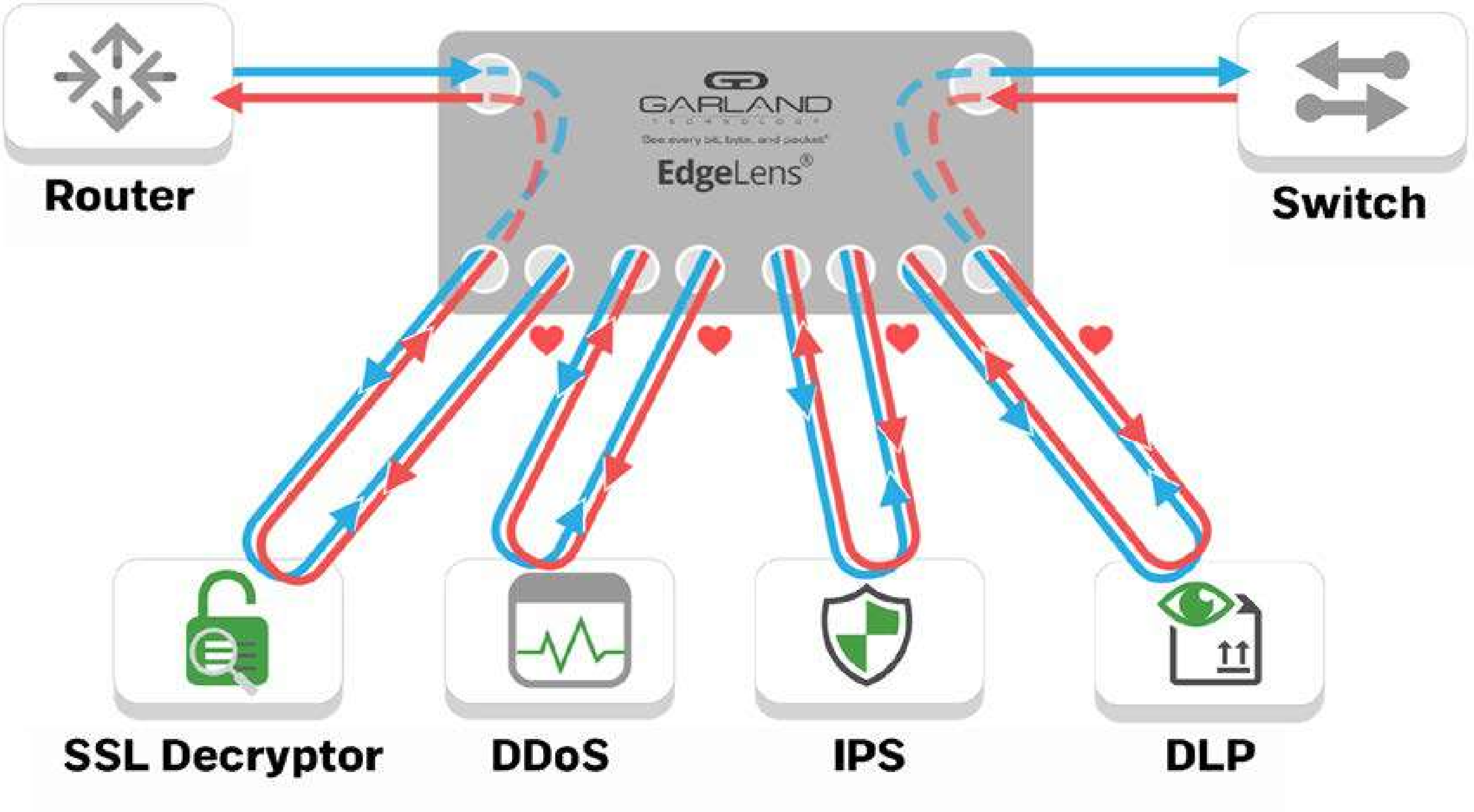


Multiple Inline Tool Management
Usage Example for IT Security Solutions

Difficulty: To deploy and manage the evolving list of security tools, including IPS, WAFs, firewalls, SIEM, DDoS and SSL encryption.

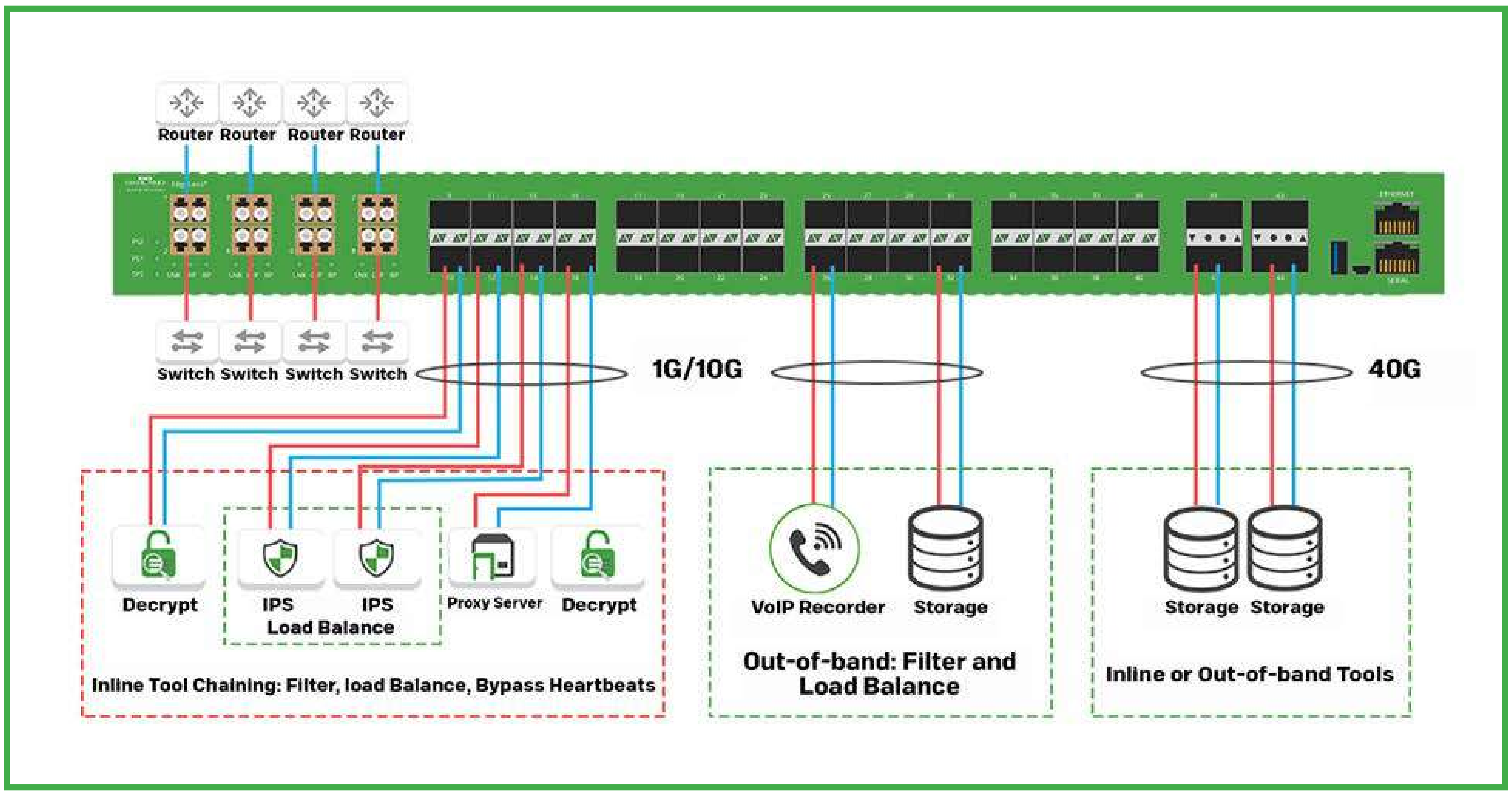
Solution: You can manage inline and out-of-band vehicle availability thanks to Inline Tool Chaining.

- You can pass traffic through multiple inline tools.
- You can monitor the health of each inline tool independently with bypass heartbeats.
- Load balance to other tools 1:1 or 1:N tools
- You can also send traffic to out-of-band monitoring tools.



Multiple Inline Tool Management

Usage Example for IT Security Solutions


Router Router Router Router
Switch Switch Switch Switch
1G/10G
40G
Decrypt
IPS
IPS
Load Balance
Proxy Server
Decrypt
Inline Tool Chaining: Filter, load Balance, Bypass Heartbeats
VoIP Recorder
Storage
Out-of-band: Filter and Load Balance
Storage
Storage
Inline or Out-of-band Tools

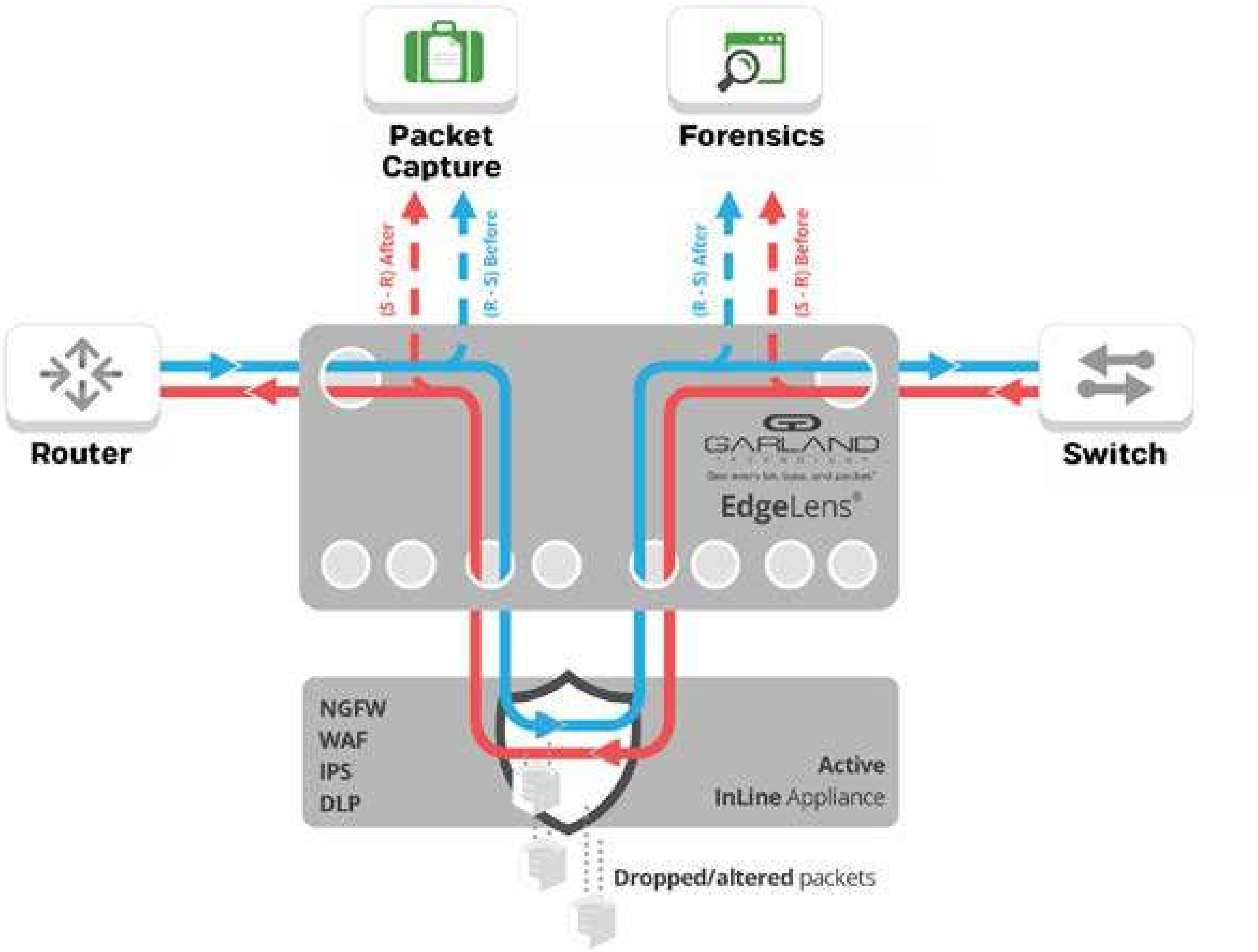
Difficulty: To deploy and manage the evolving list of security tools, including IPS, WAFs, firewalls, SIEM, DDoS and SSL encryption.

Solution: You can manage inline and out-of-band vehicle availability thanks to Inline Tool Chaining.

- You can pass traffic through multiple inline tools.
- You can monitor the health of each inline tool independently with bypass heartbeats.
- Load balance to other tools 1:1 or 1:N tools
- You can also send traffic to out-of-band monitoring tools.

Optimize Inline Tools Performance

Usage Example for IT Security Solutions



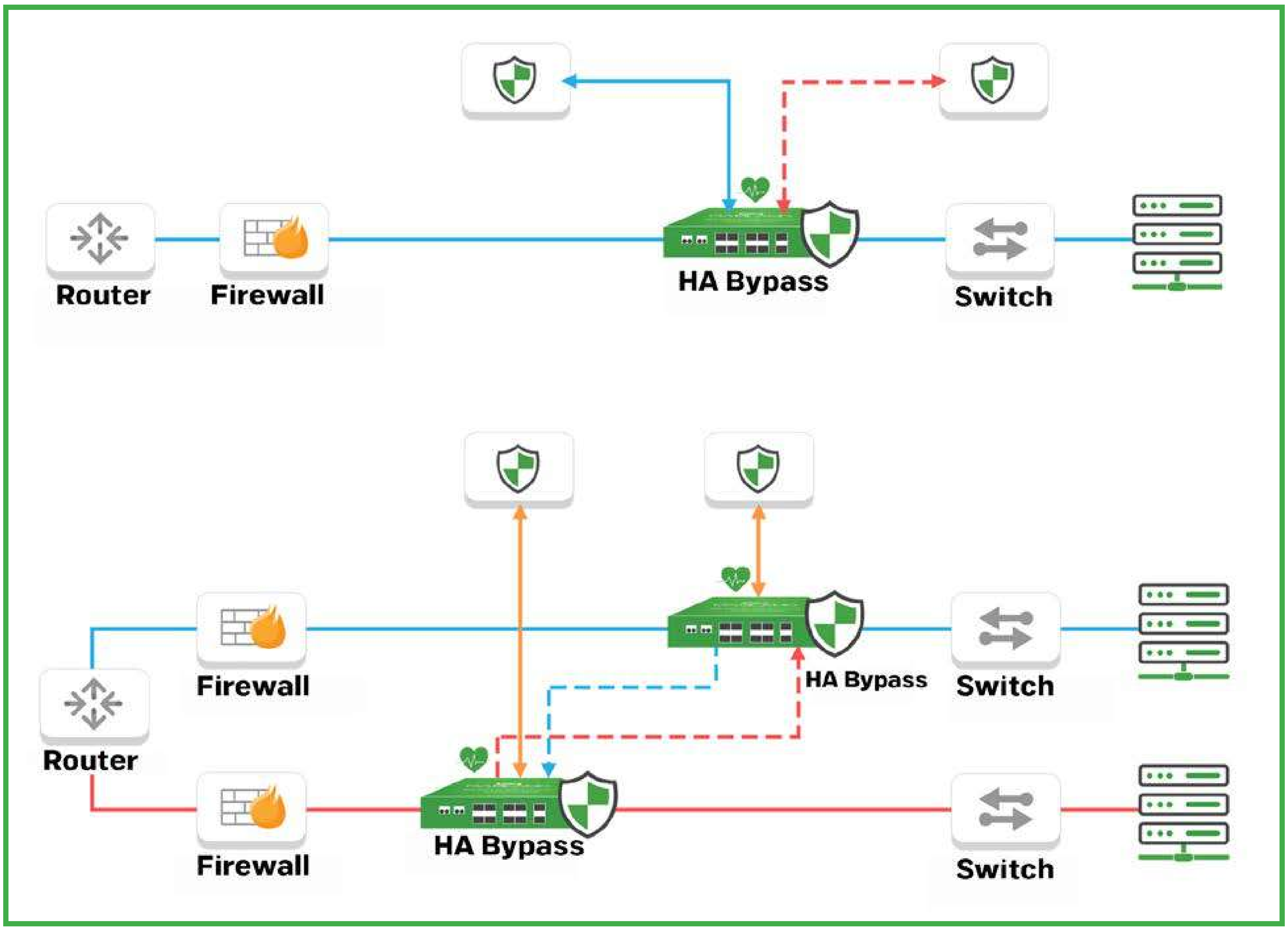
Difficulty: How to fix a problem if inline tools (IPS, firewalls) are not properly configured and optimized?

Solution: Before and after the optimization and approval processes, you can obtain visibility for your out-of-band package capture, storage, and analysis tools.

- Analyze packet data before and after your inline tool in order to get the best tool performance when verifying any updates or identifying and resolving the cause behind the failure to block the threats.
- Enable real-time proof-of-concept assessments without affecting the network.
- Verify changes or updates that your tool is configured properly.

Including Extra HA Solutions

Usage Example for IT Security Solutions



Difficulty: To design Intrusion Prevention Systems (IPS) for critical connections with High Availability (HA) or redundant designs.

Solution: Garland offers two options for incorporating High Availability (HA) solutions into your network:

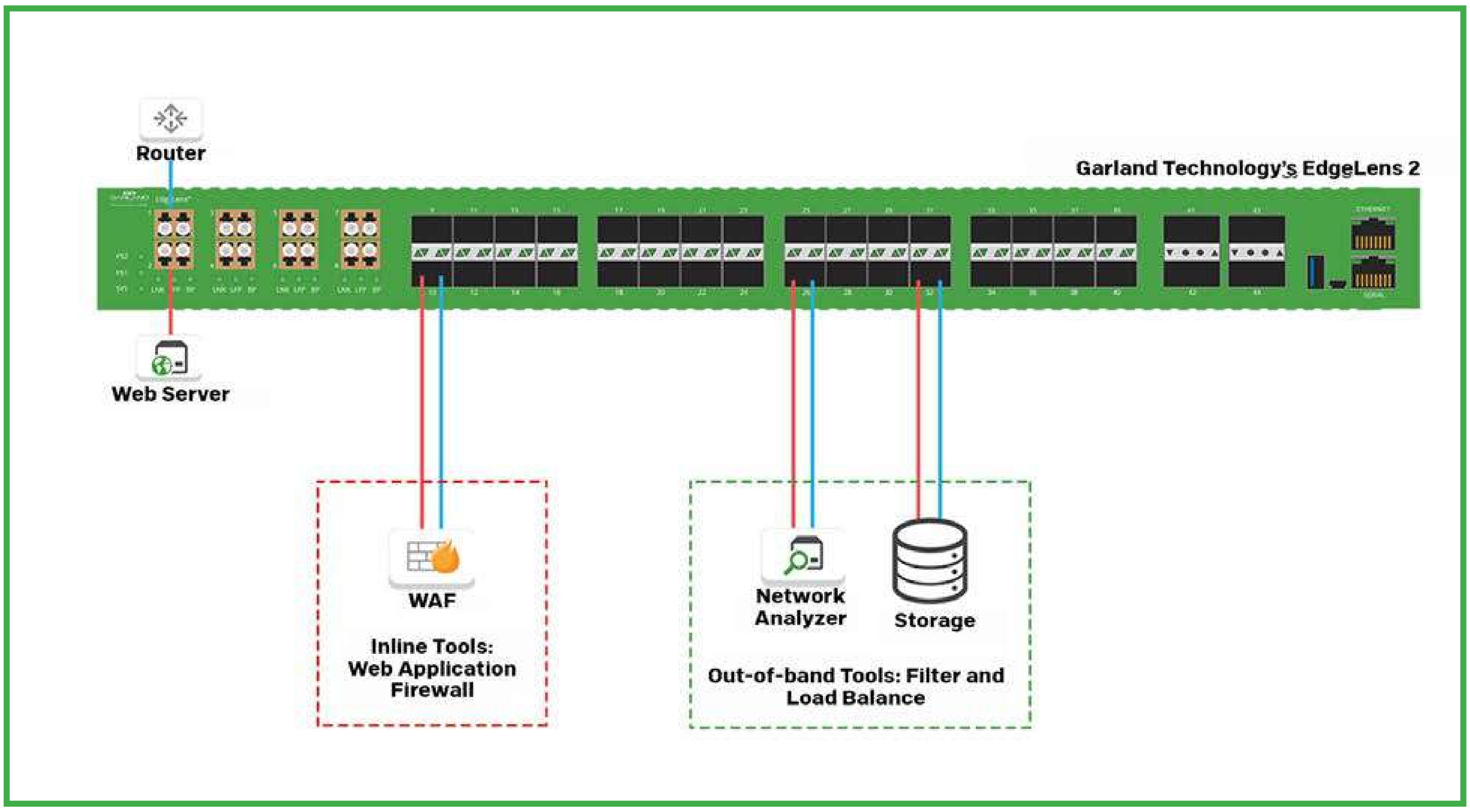
- Active Standby (Active/Passive) provide failover from the primary tool to the backup tool by being deployed into a secondary appliance.
- The Design of Active/Active Crossfire covers a secondary means and redundant connections to provide ultimate failover in case of any active tool’s failure.

To Use Inline Visibility Architecture

CASE STUDIES

Financial Services

Provide Inline Threat Prevention Optimization and Analysis


Router
Garland Technology's EdgeLens 2
Web Server
WAF
Inline Tools: Web Application Firewall
Network Analyzer
Storage
Out-of-band Tools: Filter and Load Balance

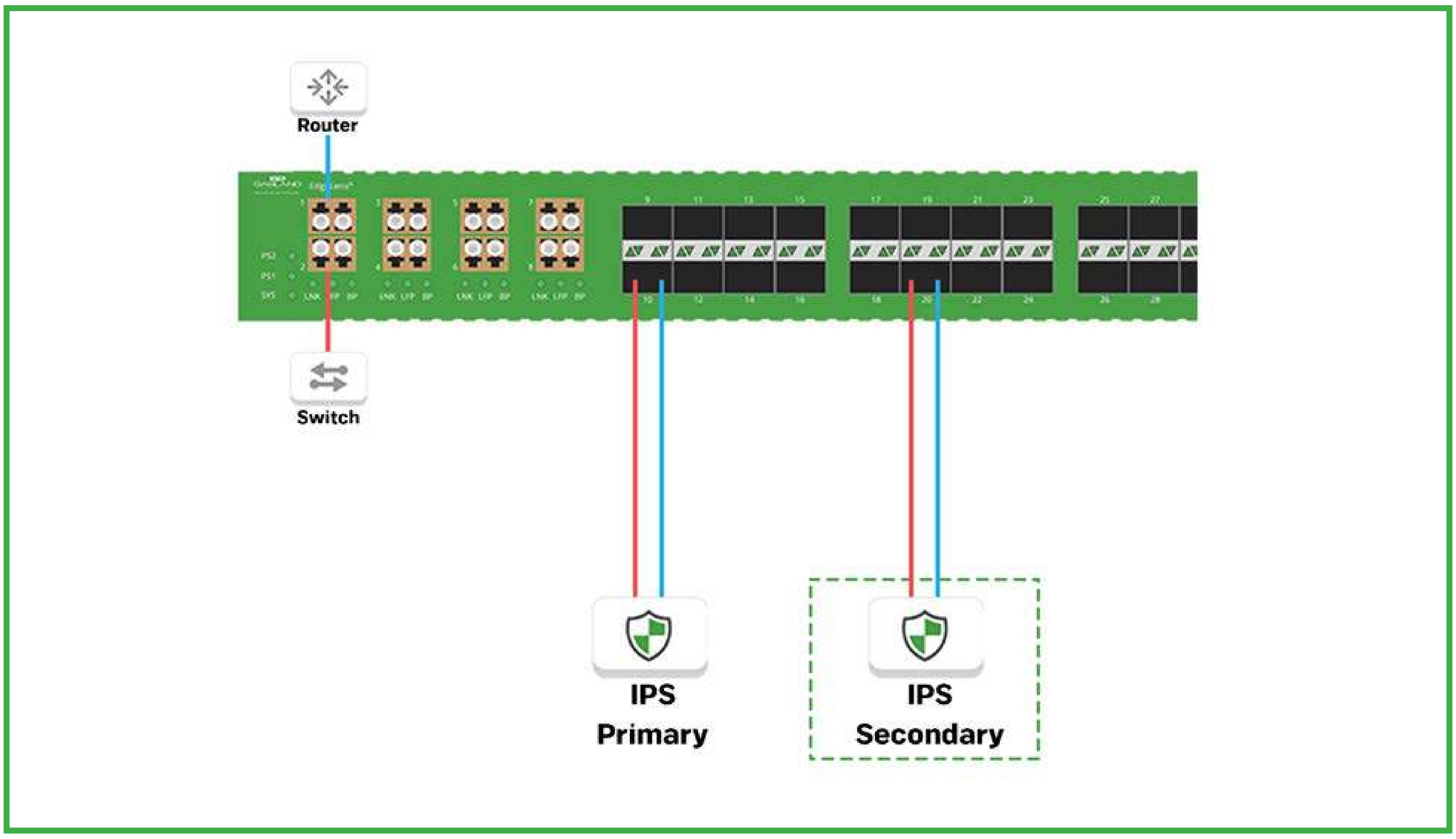
A major-scaled investment company intended to optimize threat prevention strategies with inline tool analysis

Solution: Garland's EdgeLens has transformed network security capabilities with its "Look Back" solution.

- They are enabled to analyze WAF performance to see whether configured properly or the threat is missing or not.
- Analyze package data before and after inline tool to get optimum tool performance.
- Verify all updates or ask the causes of failure to block threats.

Financial Banking

To Offer the Full High Availability (HA) Redundancy for Critical Connections



A large financial company has secured all of its critical connections through Garland's HA redundancy to ensure to have zero downtime or interruptions while protecting the sensitive data.

Solution: Garland's EdgeLens used the redundant IPS tools in an active standby scenario.

- A primary or "active" IPS
- And a secondary or "passive" IPS

If a primary tool is disabled, the secondary tool is automatically enabled over the primary tool.

Bypass function is required to prevent inline security tools from causing any network performance degradation and downtime.

Advantages to be offered:

- Ability to update/repair/replace inline security tools without interruption
- Reduced risk of unplanned downtime
- Warning/reporting on inline tool failure/ performance
- Cost reduction in security tools
- Reduced network complexity
- Tool Sandbox - piloting or deploying new tools
- Deployment efficiency - extend the access ability of the same tools across multiple network segments

TAP - VEHICLE TM Architecture

To secure and monitor your network is of the most significant goal.

Garland is a technology of convenience. Our philosophy is not to compete with the tools, but to follow and achieve this goal by designing the tool.

TAPs

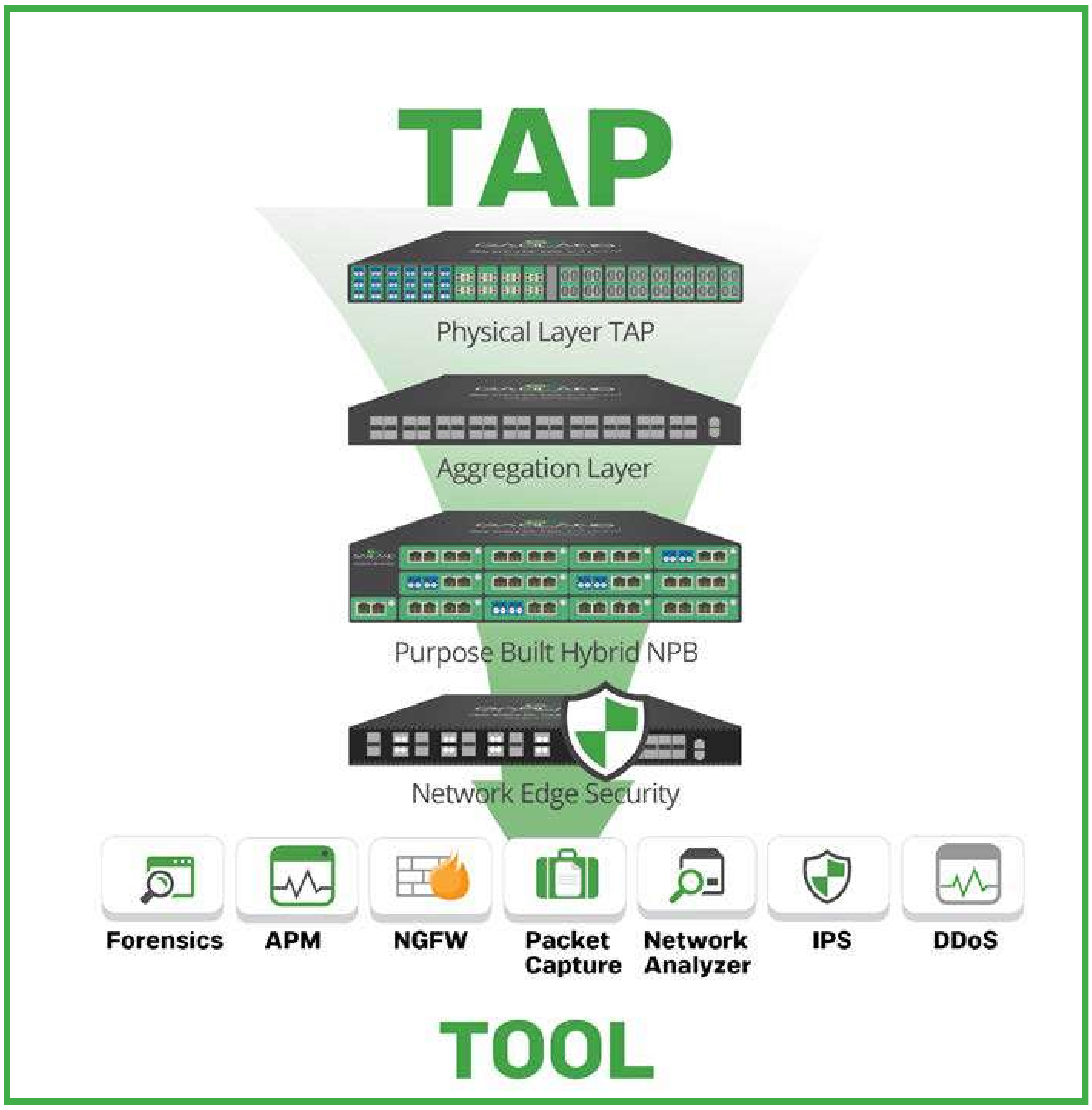
Basis of Visibility: Starts with network TAPs

- Offers 100% raw package data
- Collection, regeneration, bypass functions

Network Package Agent
Deploy what you need

- Advanced Concentration-Filters, Aggregation and load balancing
- Advanced Features - Deduplication, package slicing, timestamping, etc.
- Hybrid - Integrated TAPs with bundle agent functionality

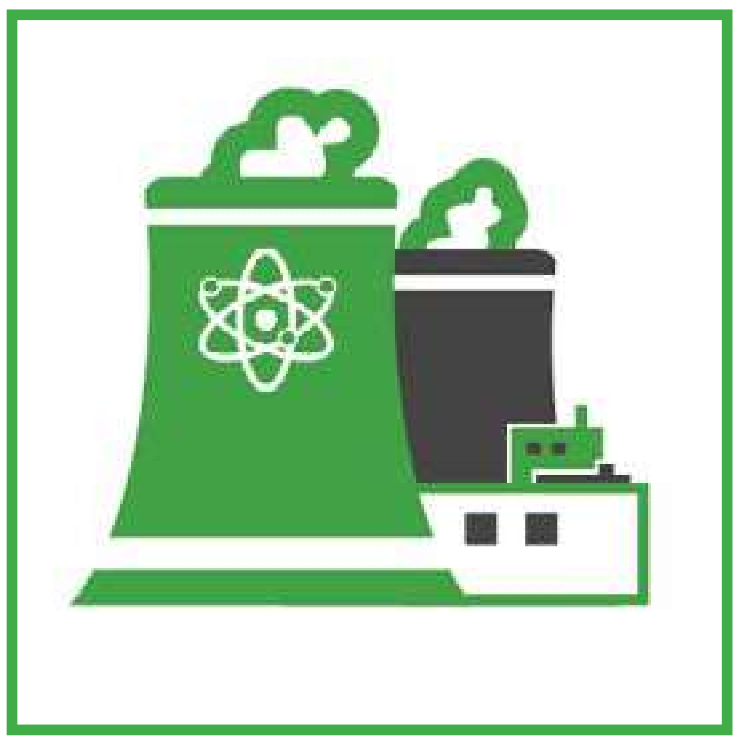
Tools| They feed: Network Analyzers, IDS, SSL Decryption, NGFW, Packet Capture, APM, IPS, DDoS.



VISIBILITY

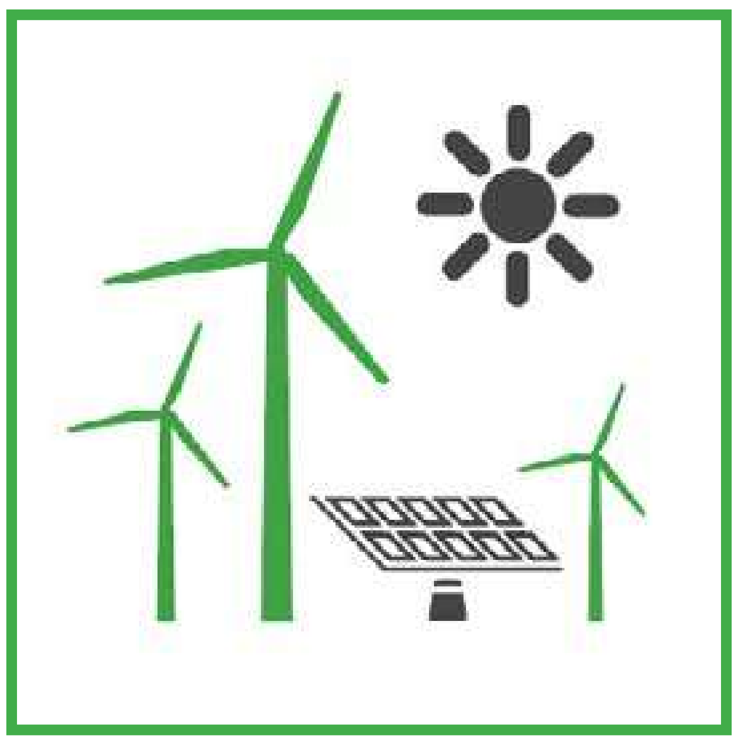
COAL

NATURAL GAS



NUCLEAR POWER PLANTS

HYDROELECTRIC PLANTS



RENEWABLE RESOURCES (SOLAR, WIND & GEOTHERMAL)

OIL

ICS VISIBILITY

APPROACH OF OT AND IT ENVIRONMENTS

For decades, OT systems were based on proprietary protocols and software that were manually managed and monitored. These obsolete critical infrastructure systems were considered relatively unimportant targets for terrorists because access to the terminals required physical breach of the facility.

Of course, IT networks are experiencing steady growth in the complexity of computer systems, hardware, software and networks to facilitate the processing and distribution of data.

Considering that we are in the 21st Century, there is little question as to why digital transformation is being implemented for these previously unconnected systems. Industrial control systems have been brought online to deliver big data and intelligent analytics to embrace new capabilities and enable integration to improve efficiency.

This application; It has been driven by new requirements for enterprise connectivity and remote access, pushing IT solutions for ease of use, integration and lower costs.

This IT-OT approach provides organizations with a complete view of both industrial systems and process management solutions. To better manage accurate information about users, machines, switches, sensors and devices in real time.

Unfortunately, OT infrastructure remains vulnerable because they tend to have poor protection against cyber attacks and much of it in use today was developed decades ago. Facing companies with OT/IT challenges:

- Most IT security solutions are not suitable for protecting legacy control systems such as SCADA.

- How to ensure the security of emerging technologies such as cloud computing and the internet of things (IoT)

5 NETWORK CHALLENGES FACED BY ENERGY AND UTILITIES

Utility networks, including Energy (Electric, Nuclear), Water and Wastewater, provide services in operational technology (OT) environments that commonly include Supervisory Control and Data Acquisition (SCADA) Systems and Distributed Control Systems (DCS). These systems reliably manage the numerous functions performed by industrial equipment, assets, processes and events.

Systems ranging from substations to Power plants are based on a range of equipment that generates thousands of real-time processes. The task of analyzing and monitoring this massive volume of data to detect threats and anomalies can seem like an insurmountable task. But combining infrastructure visibility best practices and modern security solutions is the key step.

1 - Hierarchical Power Systems

For power plants, systems and networks covering large geographical areas, managing and monitoring activities pose obvious logistical challenges. Today's control systems are tasked with monitoring large volumes of operational data for each substation and must monitor the status of many devices and assets for each in real time.

The architecture of monitoring and security strategy for modern power systems must have appropriate visibility and connectivity fabric to easily manage substation deployments, installation, configuration and maintenance.

Hierarchical architecture best practice should also include visibility and monitoring tools in substations that communicate with the computer-mediated communications (CMC) layers above them. Architects should try to group substations and device distributions to improve system management. In this way operators can obtain substation and system-wide views of data and analytics.

2 - Substations Interoperability

Electric utilities typically have hundreds to thousands of substations that are used to step down power from the transmission grid to the distribution grid and consumer infrastructure.

Substations are extremely important in facilitating the efficiency and adaptability vision of the smart grid, which should send data on consumption and operations to a central point for analysis through energy management systems and substation automation systems.

Smart grid architecture includes two-way data communication between substations and corporate management, which was not possible in the past. Modern substation systems, It must now support interoperability, ensure high reliability and availability, and offer protection against potential cybersecurity threats.

3 - Transformer Bandwidth Blind Spots

Low bandwidth causes monitoring difficulties in the substation. The bandwidth of traffic flowing between the various substations and the main control center is generally low, but is sometimes active only or when necessary.

Appropriate network infrastructure, including Quality of Service (QoS) policies, integrated IEC 61850 process buses and network TAPs (test access points), optimizes network traffic under various conditions to guarantee sufficient network resilience.

The aim here is to ensure that communication between substation monitoring devices and CMCs is optimized for bandwidth in a way that does not create network blind spots or oversubscription.

4 - Accurate Time Synchronization

Control network equipment requires time synchronization to less than a microsecond accuracy to perform its tasks. These include IEDs (intelligent electronic devices), control units, combining units and Ethernet devices. Time synchronization makes it possible to repeat events by specifying in detail which situation occurred when on which equipment. These:

The IEEE 1588 protocol and the use of a master clock or global positioning system (GPS) are considered the preferred and secure timing system.
SNTP (simple network time protocol) is widely used but may provide relatively less accuracy and was created for IT environments.

Malicious actors target IEEE 1588 / SNTP communication or master clock/GPS to maliciously try and disrupt operations. Security monitoring solutions at this level are required to detect any changes in communication trunks or device state to enable the prevention or remediation of threats related to time synchronization and to identify specific attacks against SNTP resources. Network TAPs TAPs enable monitored traffic to be delivered without modification in real time.

5 - Ensuring Compliance with Standards and Communication Protocols

Organizations follow the NIST (National Institute of Standards and Technology) Cybersecurity Framework to evaluate IoT and security programs and controls. Compliance efforts are designed to improve cybersecurity and operational reliability, including:

ISC standards
North American Electric Reliability Corporation (NERC) CIP standards
EU NIS Directive for critical infrastructure organizations (NISD)
ISA 99/IEC 62443

These compatibilities are taken as a basis when managing the data added from serial communication to Ethernet when upgrading the network of a substation.

Communication protocols and their monitoring have improved. Distributed Network Protocol (DNP3) is widely used in electrical and/or water and wastewater treatment facilities. Despite the substations
IEC 60870-5-104, DNP3 and Modbus communication protocols are rapidly evolving. Although the packets covered by these protocols are simple, data endpoints sent over the cable can be monitored via Wireshark.

Many today's substations consist of a mix of equipment, some using IEC 61850 communications and others using serial communications schemes (standardized in IEC 60870-5-101). Proper evaluation of 61850 protocols has proven to be a much more complex process, which
It has resulted in Deep Packet Inspection (DPI) being a best practice method. In this process, DPIs manage complex payloads with multiple layers (ACSI over MMS) by managing the consistent state of each IED, even if controlled by commands from multiple protocols (GOOSE and ACSI) or SV (Sample Values). manages.

IN THE FIELD OF ENERGY AND PUBLIC SERVICES CYBER SECURITY THREATS

As utilities and energy companies invest in digital transformation to improve operational efficiency, cyber risks have increased significantly, causing unplanned outages, negative corporate brand perception, and data and security concerns.

Before power grids adopted the Ethernet and TCP/IP-based method of connecting IT communications to external systems, cybersecurity came down to communication protocols and network isolation. Today, industrial control systems face the same cybersecurity risks as IT networks, but also have potentially disastrous consequences.

As threats to the energy sector increase, these facilities are now recognized as fundamental risks to social and economic stability.

Threats enable lateral movement within the organization, often targeting the entryway to adapt to a system. This pathway is used across large and disparate infrastructures that connect various systems, equipment, devices, and assets, making it easy to hide even when in plain sight.

To help companies develop modern security strategies to combat such threats, both CISA3 and NIST4 promote a 5-step Cybersecurity Framework.
These 5 steps are: Identify, Protect, Detect, Respond and Recover.

1 - Identification

To form the basis of an Asset Management program, identify the physical and software assets located within the organization, the business environment the organization supports, including their role in the supply chain, and
Identify organizations' place in the critical infrastructure sector.

2 - Protect

The ability to limit or restrict the impact of a potential cybersecurity incident to ensure the delivery of critical infrastructure services, including Identity Management and Access Control protections within the organization, including physical and remote access.

3 - Detect

Ability to identify the occurrence and potential impacts of cybersecurity anomalies and incidents.

4 - Reply

The ability to act on a detected cybersecurity incident, along with the competencies to cover the impact of a potential cybersecurity incident.

5 - Recover

Maintaining resiliency plans by supporting timely recovery to normal operations to mitigate the impact of a cybersecurity incident and repair any capabilities or services damaged as a result of a cybersecurity incident.

ICS VISIBILITY

FOR ENERGY AND PUBLIC SERVICES ICS SECURITY SOLUTIONS

In addition to solving network and security problems, ICS security solutions are designed to enable you to effectively respond to and manage threats. To properly identify, protect, detect, respond to, and recover from threats, many ICS security solutions focus on visibility, threat detection, compliance, and asset management.

Threat and Network Visibility

A key ICS security best practice is to have real-time visibility into cyber attacks, risks, and events. This focuses on having appropriate access to all traffic flowing through the network and those analytics to identify assets, network communications and activities, including protocols and equipment status. The aim here is to know the factors and people in your network.

Threat Detection and Monitoring

Threat detection retrieves network visibility (packet data and devices) and provides complete IT-OT monitoring essential to protect the availability, integrity and security of energy operations. Many threat detection and monitoring solutions include MITER ATT&CK Framework and ICS Matrix, which serve as a database and overview of the tactics and techniques used by threat actors when attacks against industrial control system networks occur.

Asset Discovery and Management

Part of providing full visibility is expanding security and monitoring activities across all your assets. This includes utility companies as well as large, geographically dispersed sites with a very complex network of devices and equipment. It is critical to correctly identify and manage all assets in OT environments. Today's solutions provide asset discovery and network visualization to monitor those devices and activities, including firmware updates and availability.

Ensuring Compliance Standards

While adding visibility, threat detection, asset management solution coverage, adding a whole new layer of complexity, networks must adhere to industry compliance and standards. With solutions such as Advanced Deep Packet Inspection (DPI), various protocols and compliance, such as NERC CIP requirements, can be determined to ensure operational reliability and cybersecurity standards.

These security solutions and techniques are often deployed alongside Firewalls, SIEMs (Security information and event management), SOARs (Security Orchestration, Automation and Response), and NACs (Network Access Controls).

ENCOUNTERED IN WEED ENVIRONMENTS ICS VISIBILITY CHALLENGES

Securing and monitoring your network is the most important goal. However, OT teams face complex challenges when it comes to architecting connectivity across this large and sometimes aging infrastructure that was not originally designed with network security in mind. These challenges include:

- Relying on legacy switch SPAN ports for visibility that are not secure, reliable, or usable.
- Encountering different media or fast connections between the network and various devices
- Network sprawl with the need to reduce network complexity
- One-way connection requirement for monitoring tools
- Need for a secure, air-gapped solution for virtual environments

Fortunately, there are solutions to these difficulties. Optimized security and performance strategies start with 100% visibility into network traffic. Visibility starts with the package.

While the common access point for network visibility in OT environments consists of SPAN ports on network switches, engineers will often provide connections directly to intrusion detection systems (IDS) or network monitoring tools.

However, there are currently two options for accessing network packets for security and monitoring solutions to accurately analyze threats and anomalies, performances and regulatory conditions: network TAPs and SPAN ports. We will examine these options in detail in the next section.

Legacy Networks and Switches

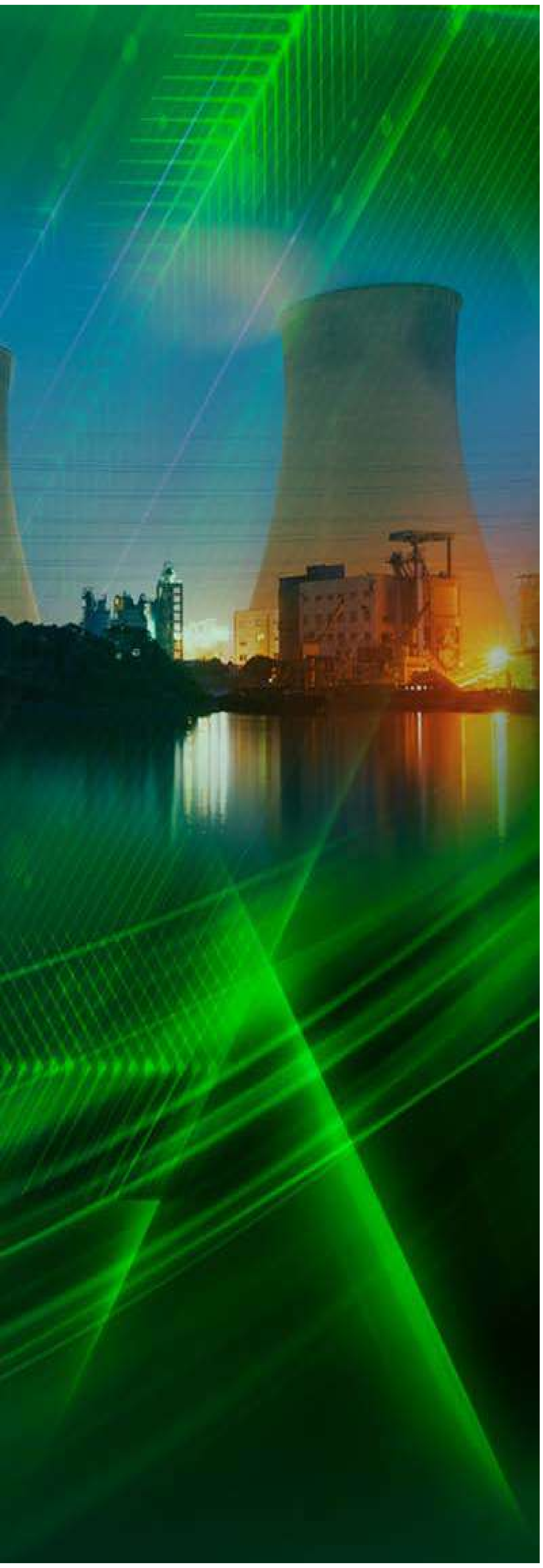
Legacy OT networks pioneered the concept of redundancy. Born from the need to ensure that these critical infrastructure networks do not collapse, redundant network segments are designed to remain in use for decades and provide production and infrastructure maintenance windows for any issues or upgrade activities.

Even with redundancy in many OT environments, the fact remains that aging technology is a continuing challenge for many legacy networks:

- Many networks still operate at 10M or 100M with 100BaseFX or 100BaseTX cabling.
- Many networks run older operating systems such as Windows 95 and Windows XP due to security concerns, even though the older operating systems no longer support them.
- Complying with static generation traffic regulations. Re-certification and calibration are required for many changes to the machine environment.

Major legacy switch providers have been the cornerstone of OT network infrastructure for decades. Since these environments are built to last 20+ years, it makes sense that these switches are still in use. Many older switches use very little data, usually up to 10M, 100M, 1G.

ICS VISIBILITY



Connectivity Challenges Encountered in OT Environments

Engineers face two connectivity-related challenges when bridging the gap between legacy infrastructure and modern security solutions:

- Speed variations - Vehicles must connect at a different speed than the live network
- Media incompatibility - Connecting devices with different media connections than network devices must

Many security solutions may not support legacy 1Gbps OM1, 100Base-FX fiber, or 10/100M copper connections. How do you connect a security platform using 1Gbps copper links to enable faster detection and response to SCADA risk?

Ensuring One-Way Data Compatibility

Some utility and energy environments face challenges to protect their network segments from incoming threats through network infrastructure designed to provide protection. These situations require a one-way data transfer between segments or facilities. Single axis or unidirectional
The data flow is designed to protect the OT network from external threats and maintain business continuity by adhering to the following US power transmission and distribution cybersecurity compliances:

Application of Air Gap Networks

While providing connectivity to enterprise IT environments such as OT systems and infrastructure, cloud computing, big data analytics, artificial intelligence (AI) and the internet of things (IoT). With the added benefit of efficiency and computing power comes additional vulnerabilities and expanded threat vectors.

One way to bring OT and IT closer is to implement an air-gapped network where necessary. This security measure physically isolates a secure network or device from unsecured networks, such as the public Internet or an unsecured local area network. This ensures that the network does not have network interfaces connected to other networks, providing the benefits of digital transformation while reducing the security threats brought by the connection.

ICS VISIBILITY BEST PRACTICES

This is a common mantra in security circles because:

Security solutions are only as good as the data they analyze
- Blind spots hide threats and anomalies

The goal of network, security, compliance and application administrators requires complete visualization of the network and the packets within it. True visualization is everything. How will you understand and solve a problem such as attack, misuse, inefficiency if it is not visible?

Many modern strategies therefore include a visibility fabric.

By providing a cohesive visibility fabric for security threat detection or monitoring tools – network TAPs and packet brokers – the tool performance tasked with solving various security strategies is improved.

When you implement a visibility engine in an OT environment, you can perform the following steps:

Protect uptime: Ensure minimal network downtime for deployment and upgrade windows and protect against unwanted downtime due to a breach or outage

Improve Risk Assessment: Makes it easier to detect vulnerabilities and manage changes to the protection surface to provide full visibility into your network traffic and data flows.

Reduce Network Complexity: Network TAPs and NPBs make it easy to maximize vehicle utilization through traffic aggregation load balancing, packet filtering, and other features. These features minimize the number of tools you need to deploy to maximize visibility while reducing complexity in expanding OT environments.

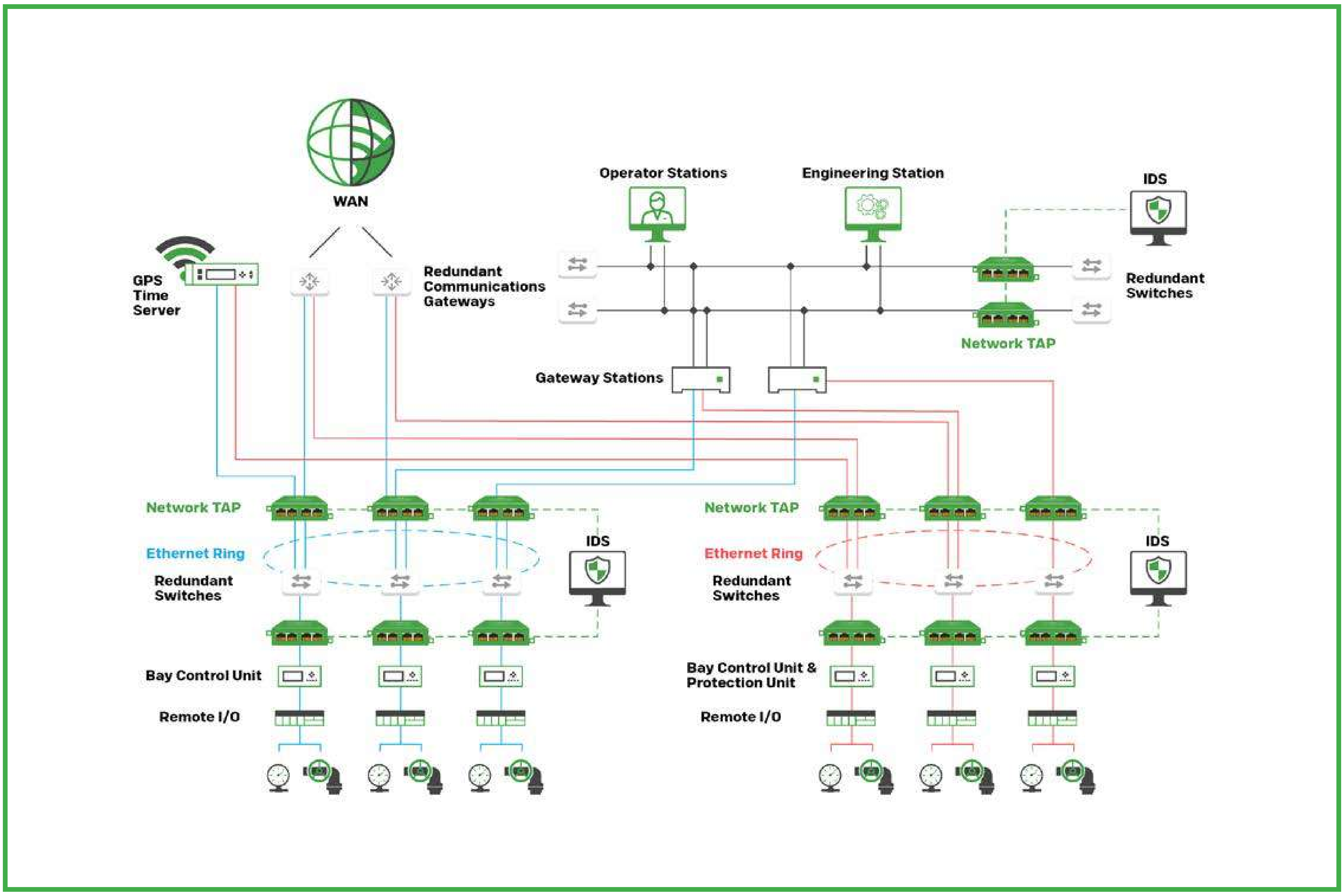
Simplify Infrastructure Upgrades: Creates a layer of visibility, more access points to your network, and the ability to implement in-line or out-of-band security and monitoring tools. Instead of keeping the network down for long periods of time to upgrade infrastructure components, you can maintain data flows while making changes to the architecture.

Better Vehicle Performance: The only way your security and monitoring tools will deliver the best results is if they see every necessary traffic packet. Your network visibility layer is fed with whatever data each tool needs.

Reduce Compliance Violations: When your monitoring and security tools can see all data packets, you can prevent problems that would otherwise occur until the network becomes non-compliant.

ICS VISIBILITY

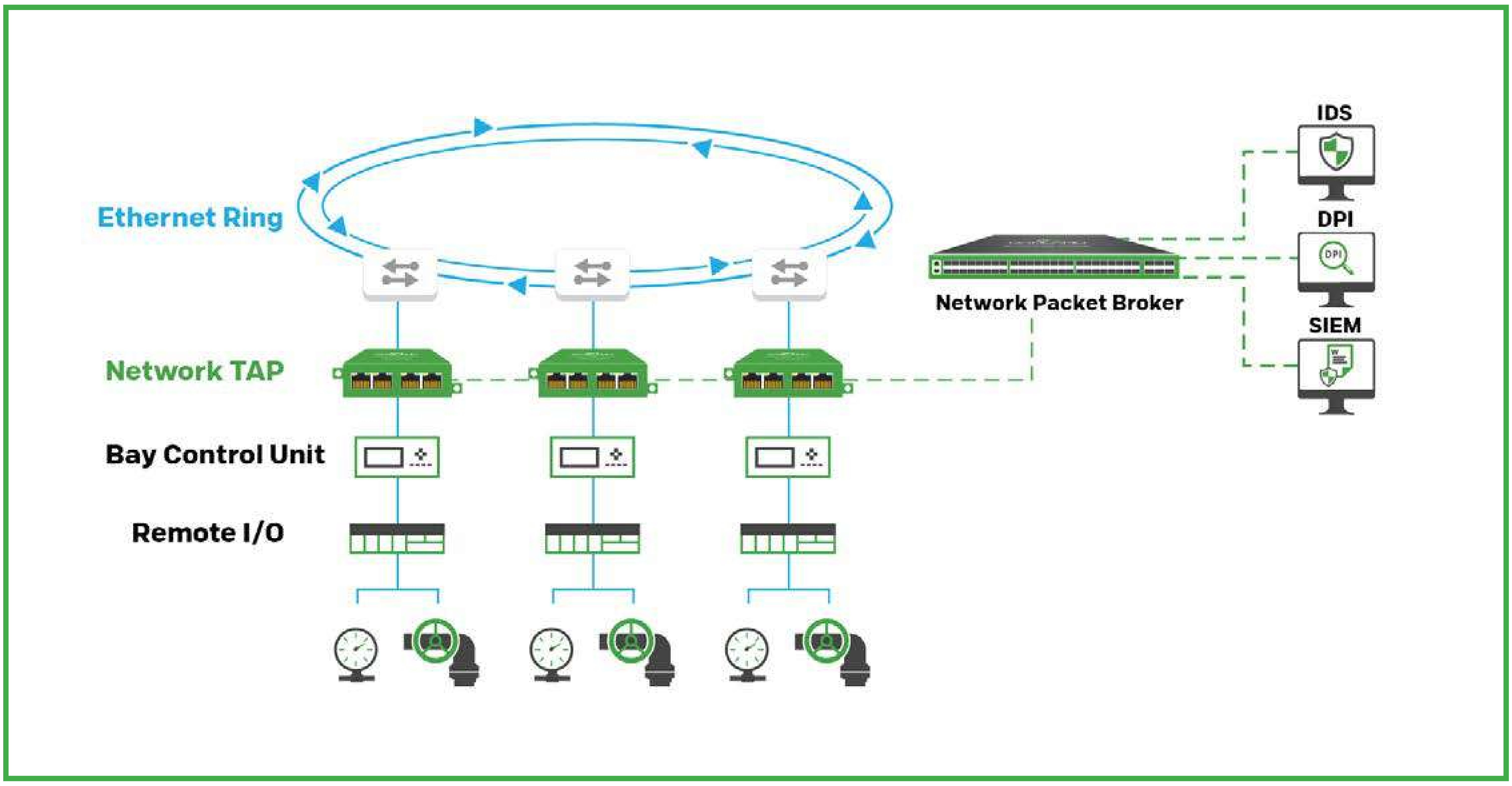
Today's ICS network requirements require full, real-time access to packets flowing through your network for security, monitoring, management, compliance and control of your networks.



In this high-level network scheme, power companies provide convenient access to network visibility with TAP technology, which is the most suitable and reliable technology for this job, as SPAN ports are exposed to many challenges and extra security risks.

VISIBILITY

For larger deployments with many network TAP and SPAN connections, the addition of network packet brokers provides a scalable visibility solution with advanced aggregation, filtering, and load balancing to streamline traffic flow, reduce network complexity, and improve security and monitoring agent performance.



Using network TAPs and packet brokers in the TAP architecture also eliminates many of the visibility issues engineers face, including:

- Ensuring 100% package visibility with security tools.
- Eliminating blind spots
- Improving vehicle performance.
- Perform media and speed conversion
- Reducing complexity with traffic aggregation
- Provide one-way connection
- Providing a secure air gap solution for virtual environments.

Let's look at various visibility use cases.

HOW TO ACHIEVE 100% PACKAGE VISIBILITY WITH ICS SECURITY TOOLS?

Often times, ICS teams face several challenges when connecting packet visibility to security solutions. It is likely that your IDS security or asset management tools will need to eliminate blind spots before they cause any problems. It is also very important to optimize the investment in security, monitoring and compliance tools where necessary.

1- Eliminate Blind Spots

“Blind Spots” refer to failure to analyze data between certain segments within a network, which may appear “hidden” in your monitoring tool or pose a threat to network performance or security. These blind spots occur for a variety of reasons, including:

• New network tools, equipment or applications have been added. Either the additions are not properly designed for visibility or security tools cannot access the packages needed in the segment.

• SPAN ports present the opportunity for blind spots – SPAN port mismatch issues, packets being dropped or information lost, programming of inappropriate SPAN ports – all resulting in incorrect or incomplete data capture.

2 - Improve Team Performance and Productivity

Network security tools need packet data to properly analyze and detect any threats. Teams are tasked with getting more out of their current vehicle investments, which is often made difficult by increasing traffic volumes and legacy architecture.

• Network and security tools may be oversubscribed.
• Increased traffic exceeds the current vehicle capacity, causing a decrease in efficiency and effectiveness.
• Dropped packets also pose a risk to security and regulatory solutions because they cannot obtain a complete picture of the packet data.

ICS VISIBILITY

SOLUTION

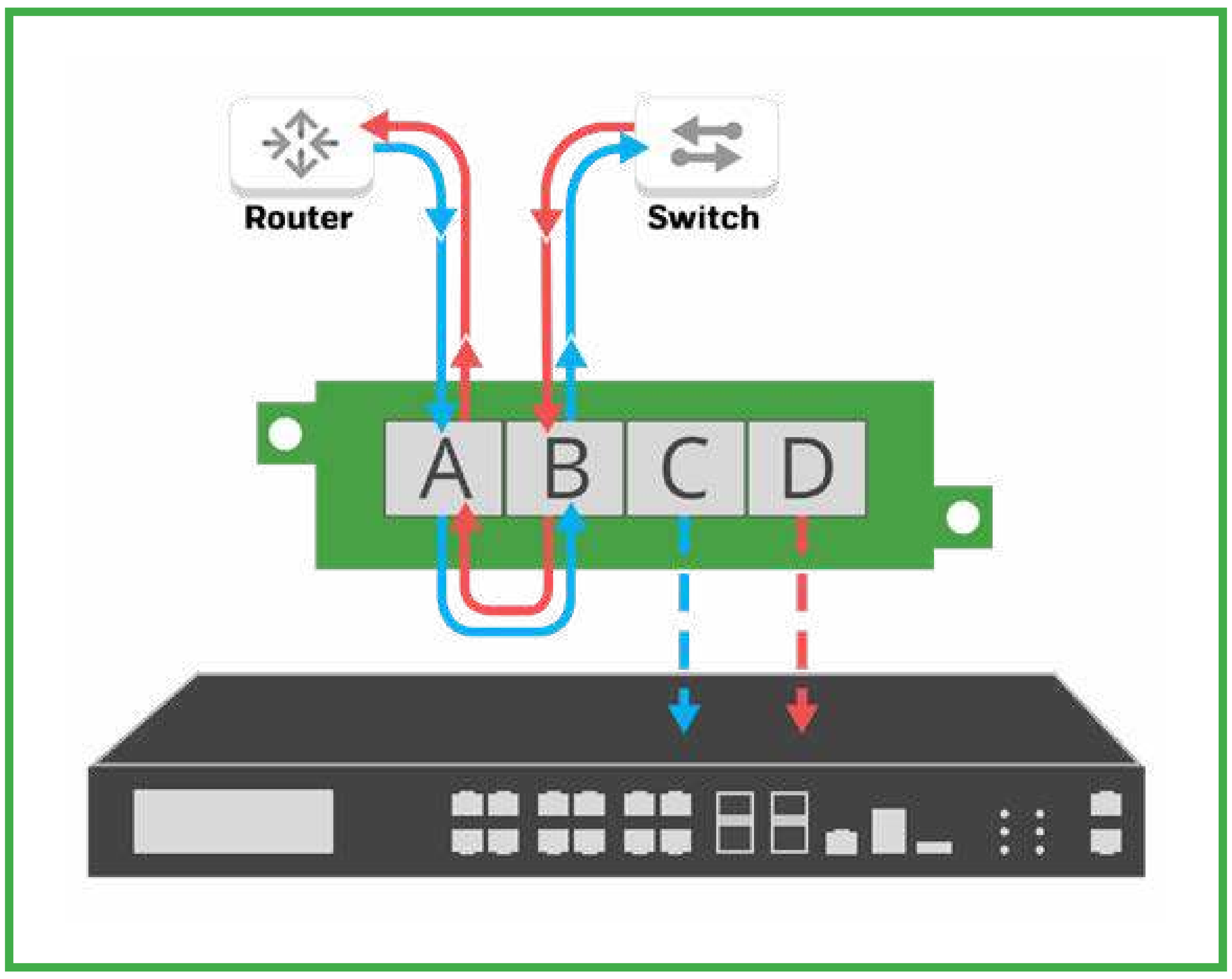
NETWORK TAPS GUARANTEE FULL PACKET DATA VISIBILITY

Industry best practice network TAPs over SPAN network connections provide the ability to capture network monitoring data without compromising the network and eliminating blind spots.

ICS teams use Network TAPs to easily monitor all network data. A network TAP is a purpose-built hardware device, usually placed between network devices such as a switch and router, that constantly creates an exact copy of both sides of the traffic flow 24/7/365. While network flow continues uninterrupted, duplicate copies can be used for monitoring, security and analysis. TAPs do not cause latency or modify data. TAPs are either passive or have a “failsafe” feature. This means that in the event of a power outage or removal of the monitoring tool, traffic continues to flow between network devices, ensuring that it does not become a single point of failure.

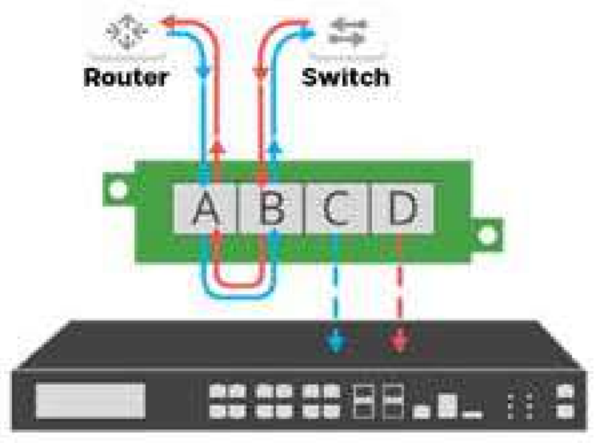
TAPs improve vehicle performance by ensuring that packets are not dropped in the event of oversubscription and by preventing duplicate packets or modified frames.
Network TAPs provide 100% full-duplex copies of the traffic you analyze. Better data leads to better team performance and added value.

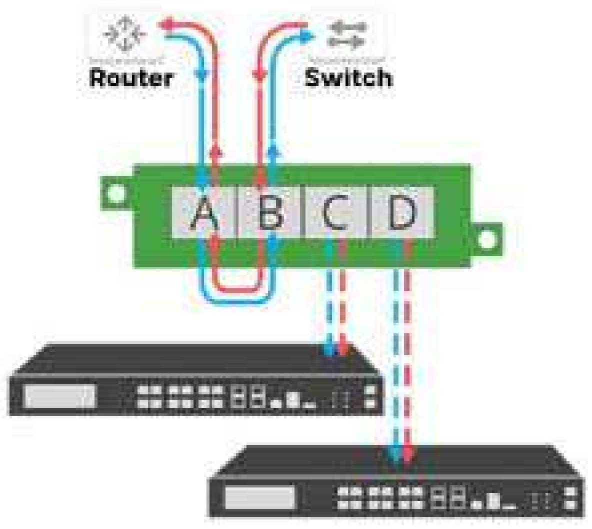
Network TAPs can perform a variety of functions designed to provide flexibility for traffic optimization. These functions include:

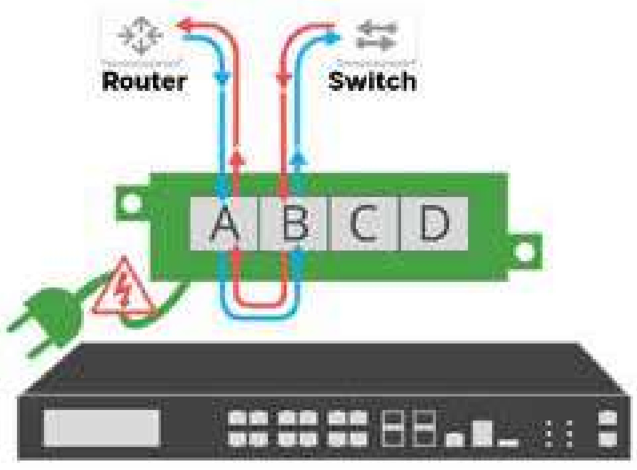


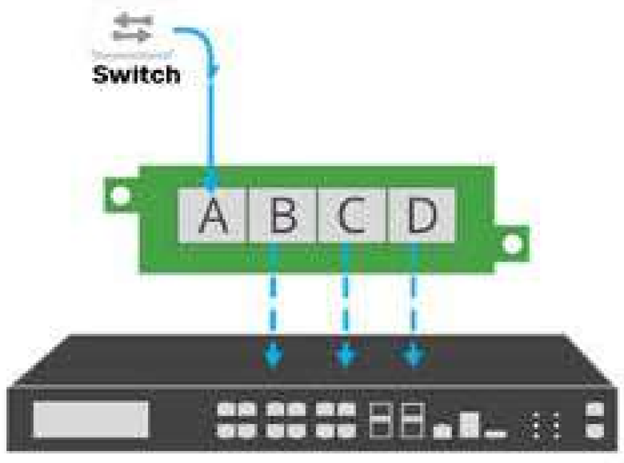
Recommended Products

Copper Network TAP
10M/100M/1000M (1G) | Portable |
Breakout Model # P1GCCB
Copper OT Network TAP
10/100/1000M (1G) | Portable Breakout |
Constant DC power Model # P1GCCB_OT
designed for temperature variations from
-40C to +85C / -40F to +185F


TAP 'Breakout' Mode


Collection Mode


Failsafe


TAP 'Breakout' Mode

ICS VISIBILITY

HOW TO USE MEDIA AND SPEED CONVERSION?

Teams facing connectivity issues in OT environments while bridging the gap between legacy infrastructure and modern security solutions sometimes need to connect devices with a different speed or media types than the live network.

What do you do if your network analyzer or IDS uses copper gigabit and you need to perform a 100Base-FX connection? 100Base-FX NIC cards are not available for your security or performance monitoring device.

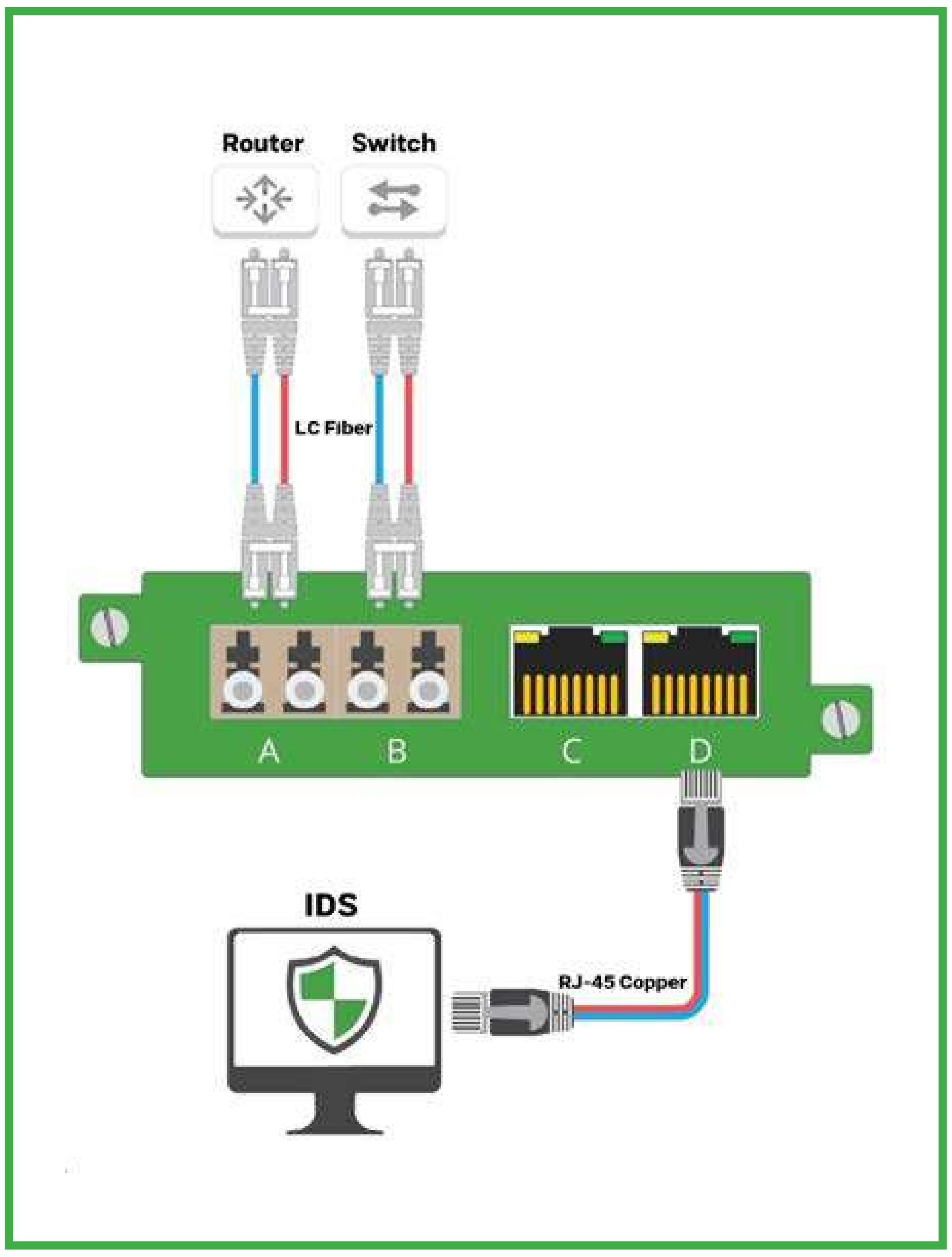
SOLUTION

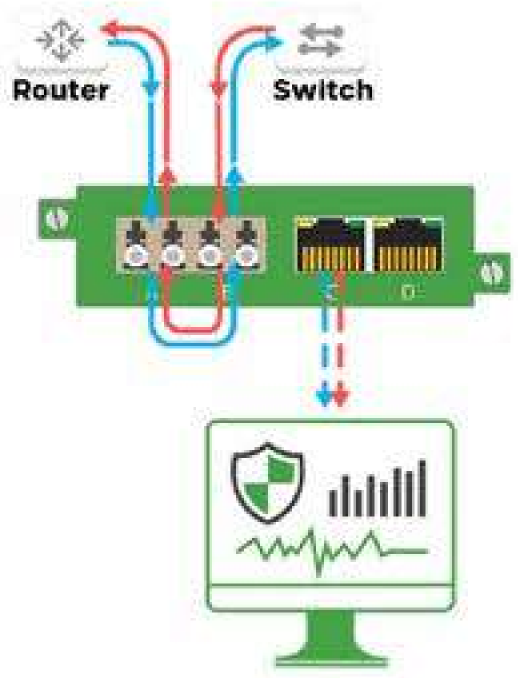
NETWORK TAPS OFFER VARIOUS MEDIA CONVERSION OPTIONS

Network TAPs not only bridge the gap between various media types but also solve connectivity issues without the need to upgrade existing infrastructure. But network TAPs provide something other media converters cannot: enable full packet data to perform at peak performance without causing packets to be dropped by security platforms.
• Media conversion from SX and LX fiber to RJ45 copper or SFP
• Media conversion from 100Base-FX and 100BASE-LX to RJ45 copper

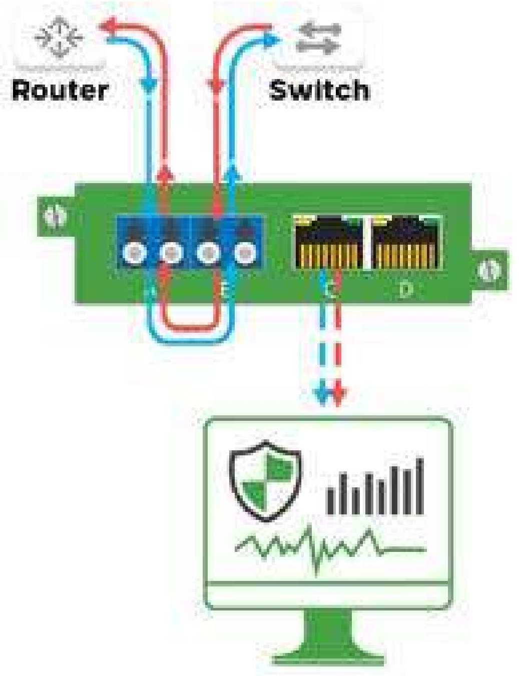
Unlike common media converters:

• Failsafe technology detects power outages and automatically reconnects
• Traffic from two sources is collected and aggregated into a single connection
• Reduce critical infrastructure risk with zero impact on operations by achieving 100% network visibility
• Additional monitoring ports for future expansion

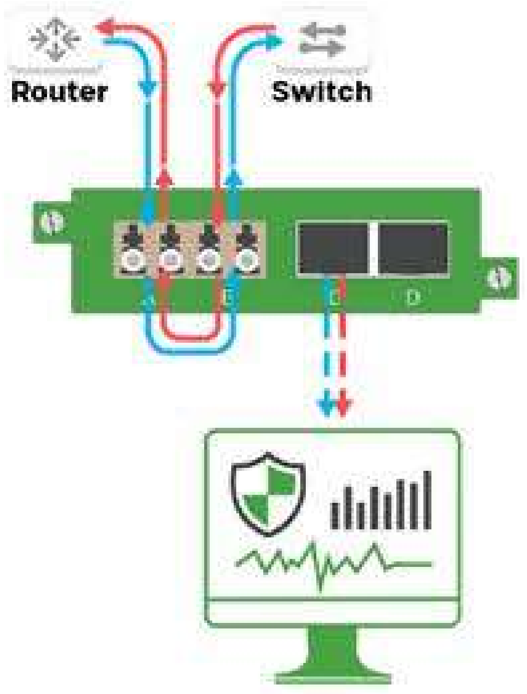




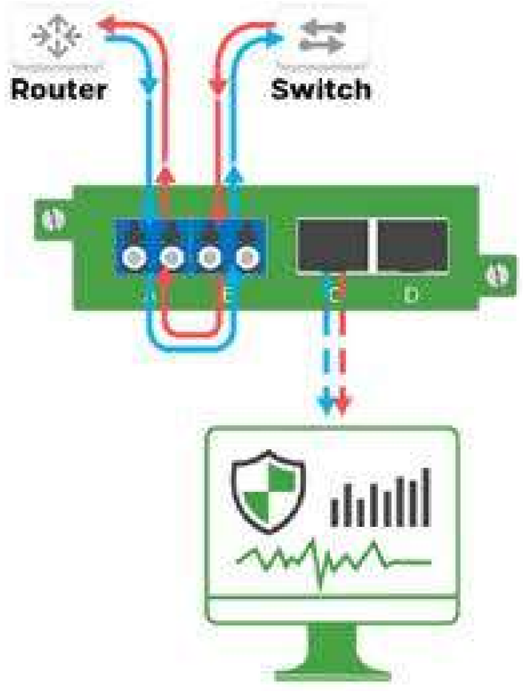
From multimode fiber to Copper single mode fiber,



Copper multimode fiber



SFP to single mode fiber



SFP to SFP single mode fiber

ICS VISIBILITY

SOLUTION

MINIMIZING TRANSMISSION PROBLEMS WITH CONNECTION SPEED SYNCHRONIZATION

Link speed synchronization is built into Garland's copper network TAPs, enabling the TAP to automatically address issues with copper-based network traffic flows to deliver the best possible throughput between all connected devices. With auto-negotiation, two devices can establish an automatic connection at the highest common denominator by announcing all communication parameters (port speed and duplex status).

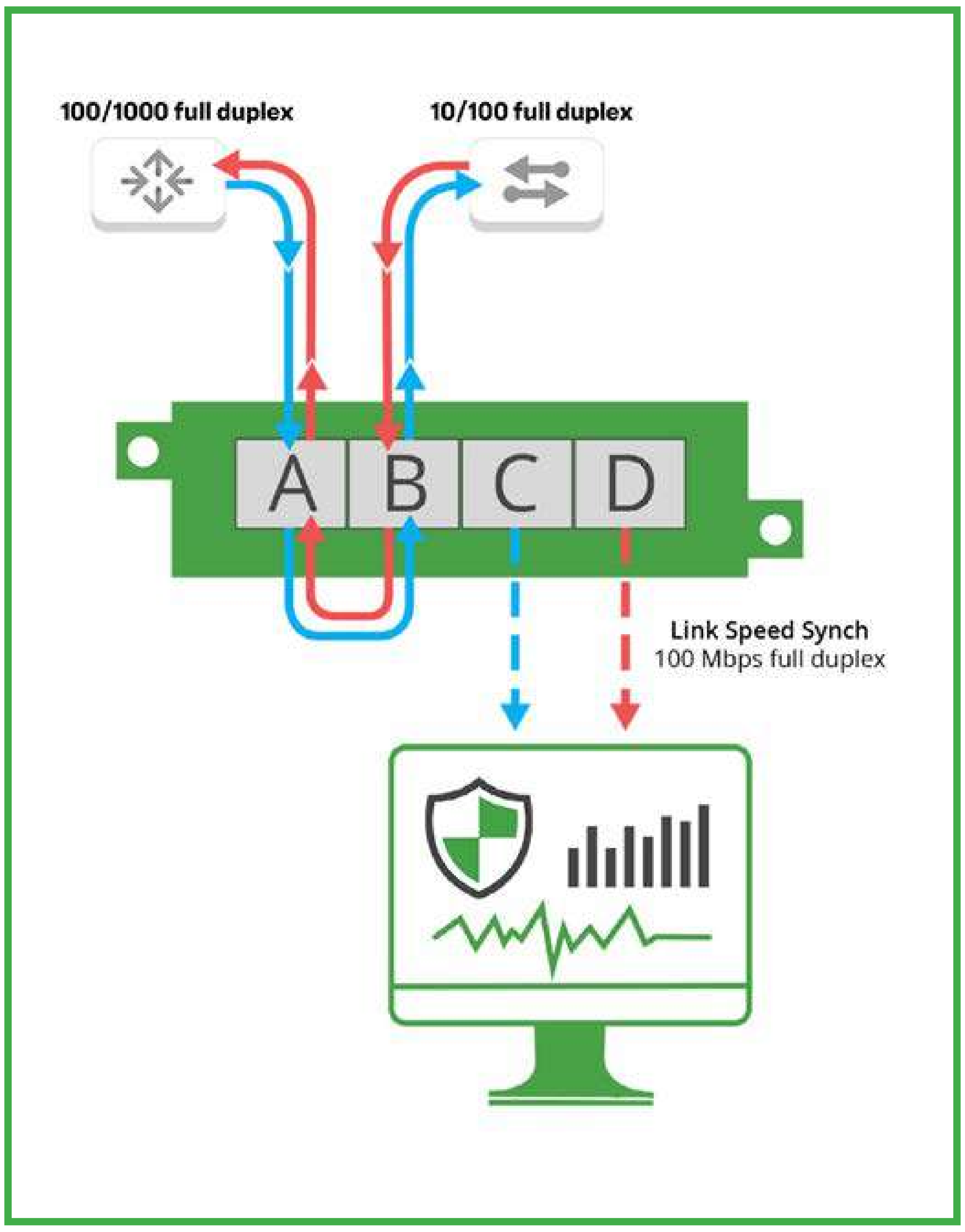
• Auto-negotiation: Automatically connects at the highest common speed on all ports

This means that a switch advertising 10/100/1000 full duplex and a router advertising 10/100 full duplex will communicate at 100 Mbps in full duplex because TAP is smart and will know the highest speed the switch and router will choose if they are connected to each other.

TAP uses autonegotiation to query both connected devices to determine their individual capabilities and maintains a data table to automatically determine the best transfer speed for each connection.

Ex: In case someone breaks into the router and changes the notification of 10/100 full duplex to 10/100/1000 full duplex.

The Garland Link Speed Sync function will ensure that transfers occur in full duplex at 1000 Mbps without any manual intervention.



Recommended Products

Copper Network TAP
110M/100M/1000M (1G) | Portable | tap 'Breakout' mode Model #P1GCCB

AggregatorTAP: Passive
100 million | Portable | Collection mode Model # P100CCA

AggregatorTAP: Copper
10/100/1000M (1G) | Portable | Gathering, tapping and regeneration/SPAN modes Model#P1GCCAS

Copper Modular OT Network TAP
110/100M and 10/100/1000M | 1U or 2U | tap 'Breakout' mode Model # M1GCCB

Military Grade Industrial Network TAP
10/100/1000M(1G) | Modular 1/2 rack Portable Chassis Tap "Breakout" mode Model#M1GCCBm

HOW TO REDUCE NETWORK COMPLEXITY WITH TRAFFIC AGGREGATION?

Expanding industrial networks that use a variety of tools, multiple systems, and devices within legacy infrastructure often find themselves experiencing complexity and network sprawl. Many companies that run the majority of traffic over SPAN ports often see a complex network to manage, which can lead to SPAN port incompatibilities that can potentially result in the following situations.

- Slower processing speed
- Data loss and oversubscription
- Slower MTTR and threat hunting
- Data silos

SOLUTION

COLLECTING TRAFFIC FOR VISIBILITY OPTIMIZATION

Collecting traffic can be accomplished in a variety of ways

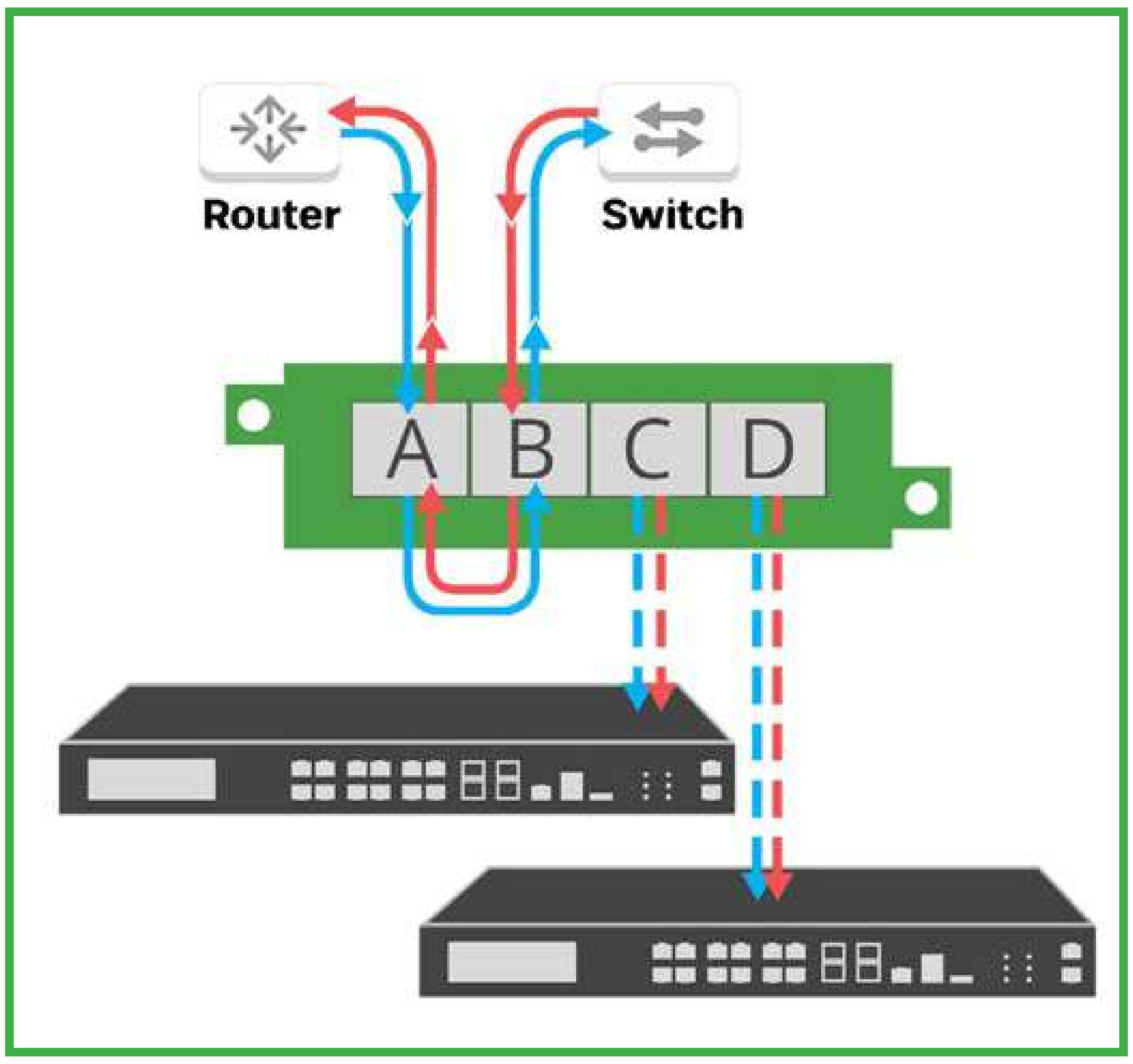
TAP collection fulfills two goals:

- Teams must determine the number of security tools required.
enabling it to reduce
regulates traffic.
- Improves scalability to increase visibility and deploy new devices in the future

A single portable TAP can provide full duplex traffic on a single connection or even reduce three SPAN connections into one.

A half-rack 1U TAP can collapse four full duplex links or eight SPAN links into 1, and a 2U chassis can bundle 11 TAP links into a single link.

The network packet broker scales traffic collection as needed, reducing 24 TAP connections to one.



Recommended Products

AggregatorTAP: Copper
10/100/1000M (1G) | Portable | Gathering, tap "Snatch" and Regeneration/SPAN modes
Model#P1GCCAS

AggregatorTAP: Fiber
Portable | Gather, tap, 'Burst' and Refresh/SPAN modes Model # P1GMCA | P1GMSA | P1GSCA | P1GSSA

AggregatorTAP: 100Base-FX
Portable | Gather, tap "Burst" and Refresh/SPAN modes Model # P100FXCA

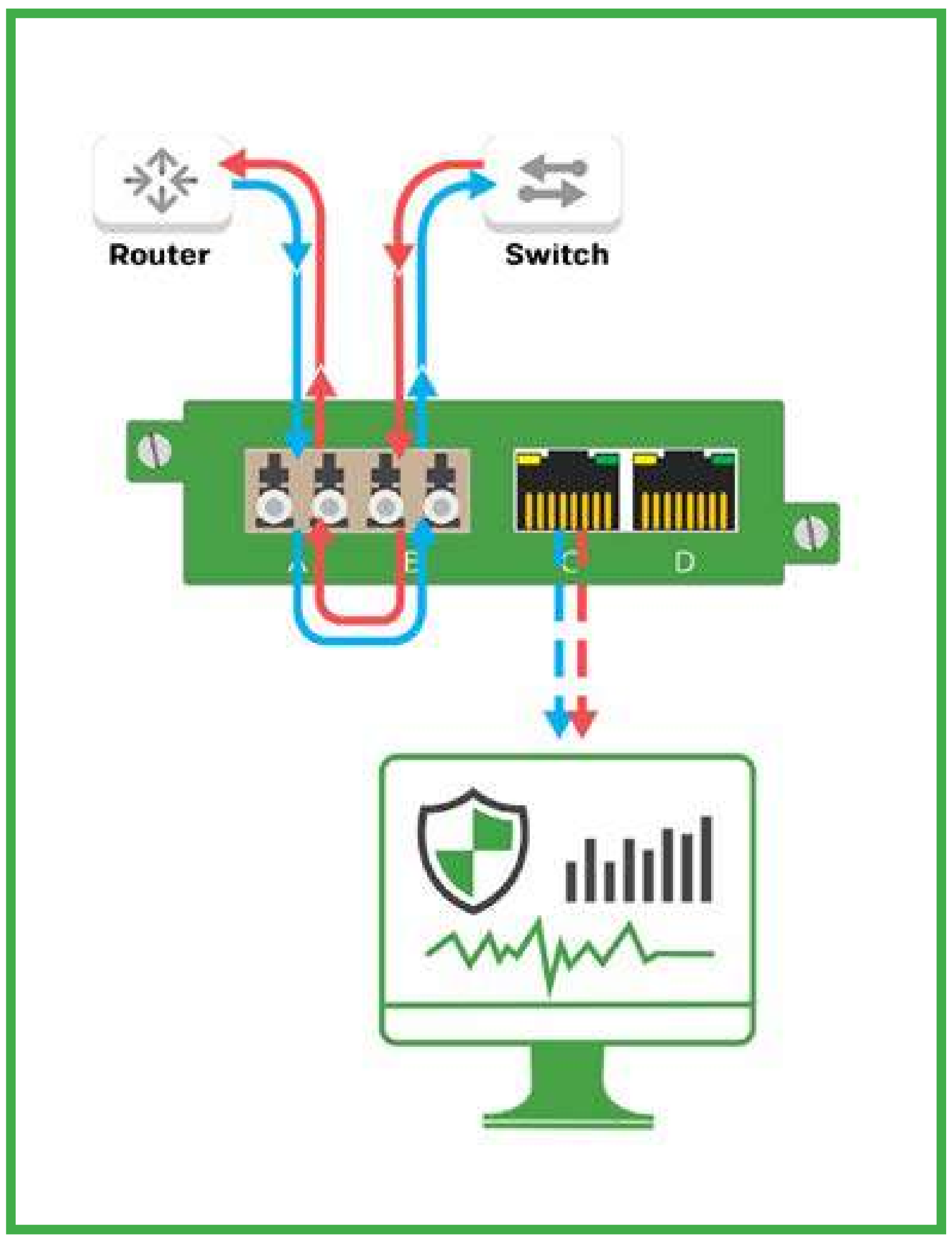
AggregatorTAP: Copper High Density
1G | 1U 1/2 rack | Collection & Regeneration / SPAN modes One-way data | Diode Circuit Design Model # INT1G10CSA | INT1G10CSA-DC | INT1G10CSASP INT1G10CSASPDC

XtraTAPTM: Modular Package Broke
10/100/1000M (1G) | 1U or 2U modular chassis | Remote Management Filter, Aggregate, Break and Refresh/SPAN modes
Model #M1G1ACE | M1G2ACE | M1GC | M1GCCF

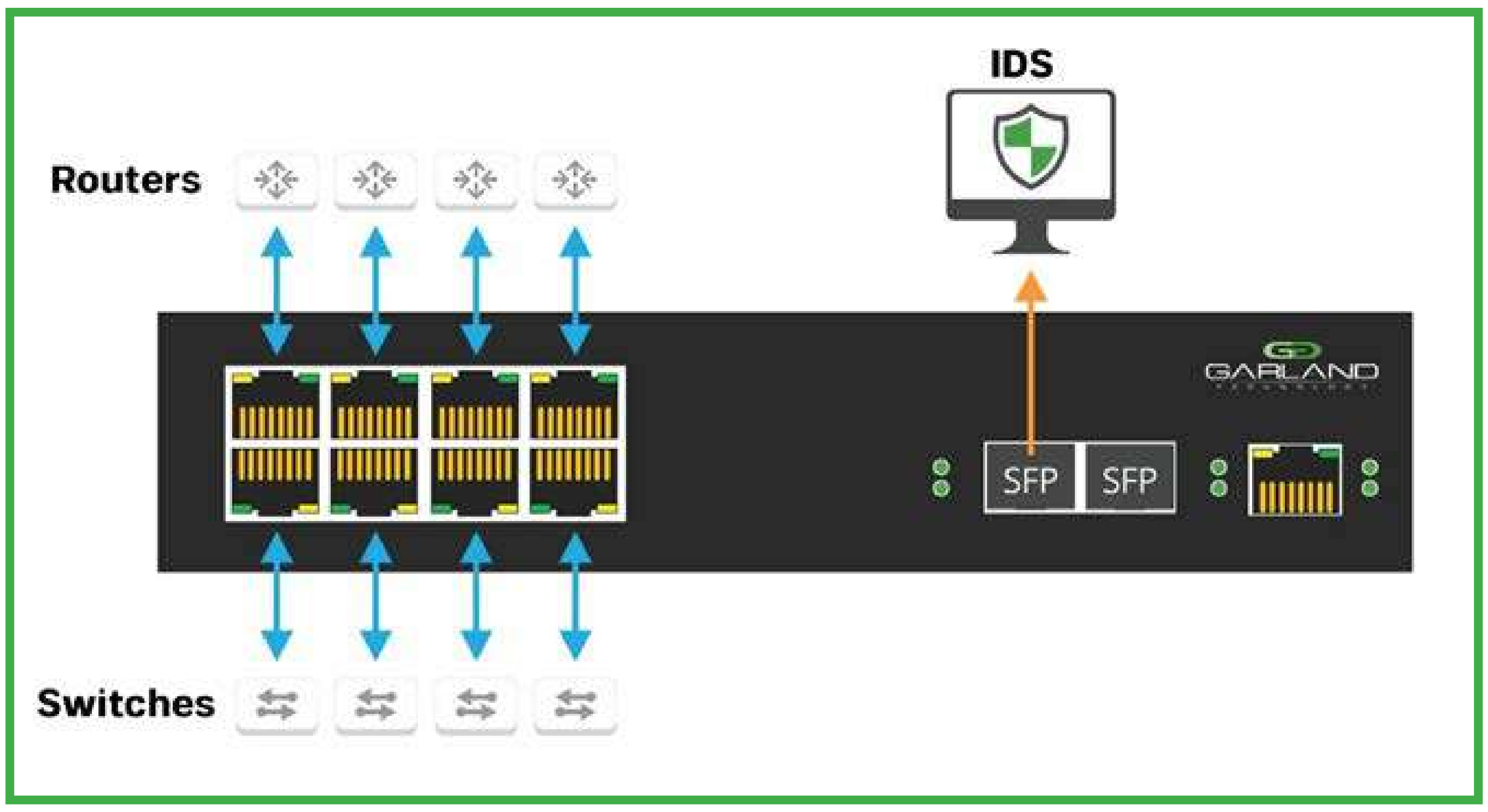
PacketMAXTM: Advanced Collector
1G | High Density Collection | Filtering | Load Balancing Model # AA1G52ACv2

PacketMAXTM: Advanced Features
1/10G | High Density Collection | Filtering | Load Balancing Tunnel Encapsulation [GRE, L2GRE] Tunnel Decapsulation [GRE, L2GRE, ERSPAN, VxLAN] Model # AF1G40AC | AF1G40DC

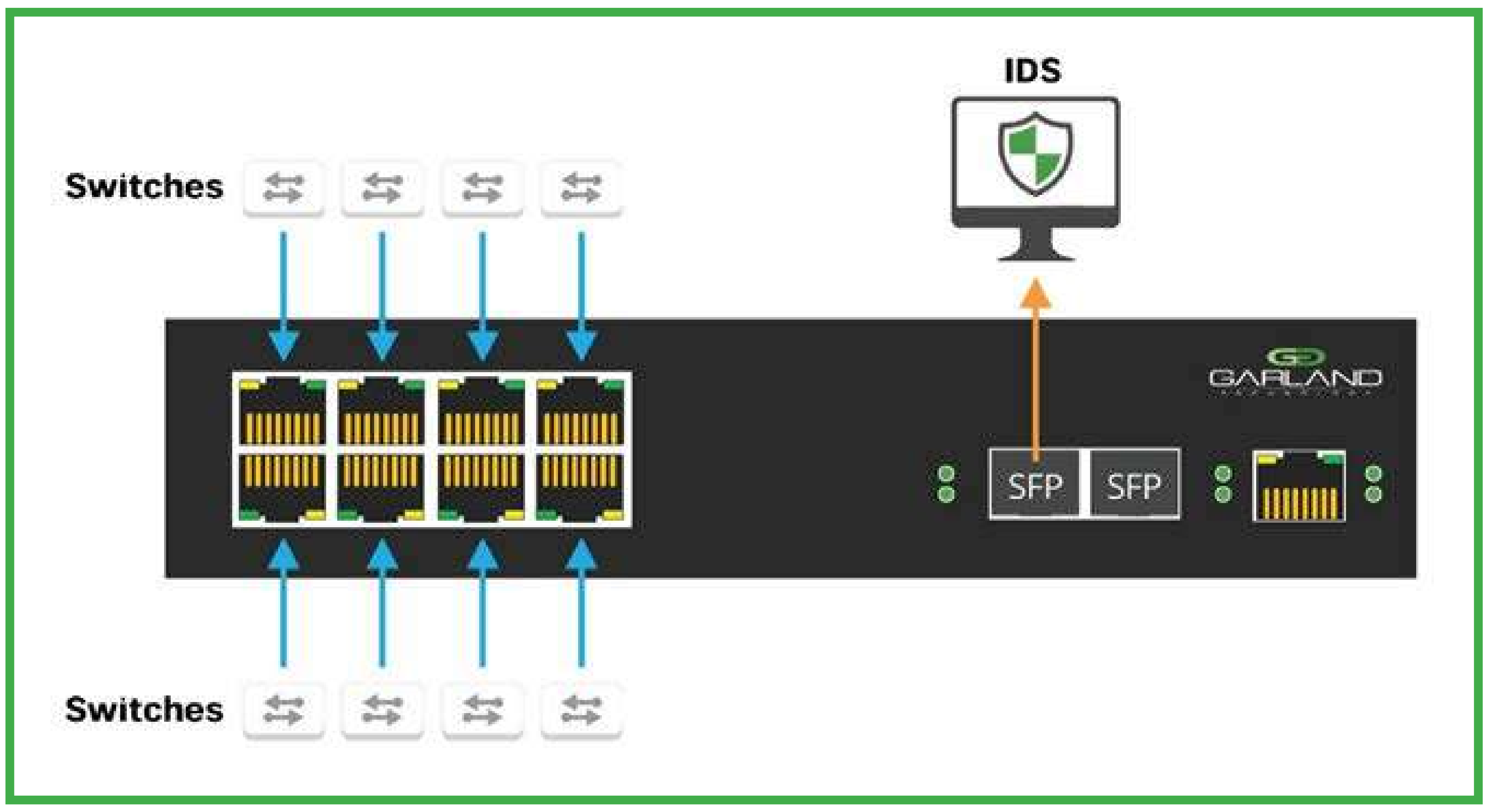
TAP COLLECTION USE CASES



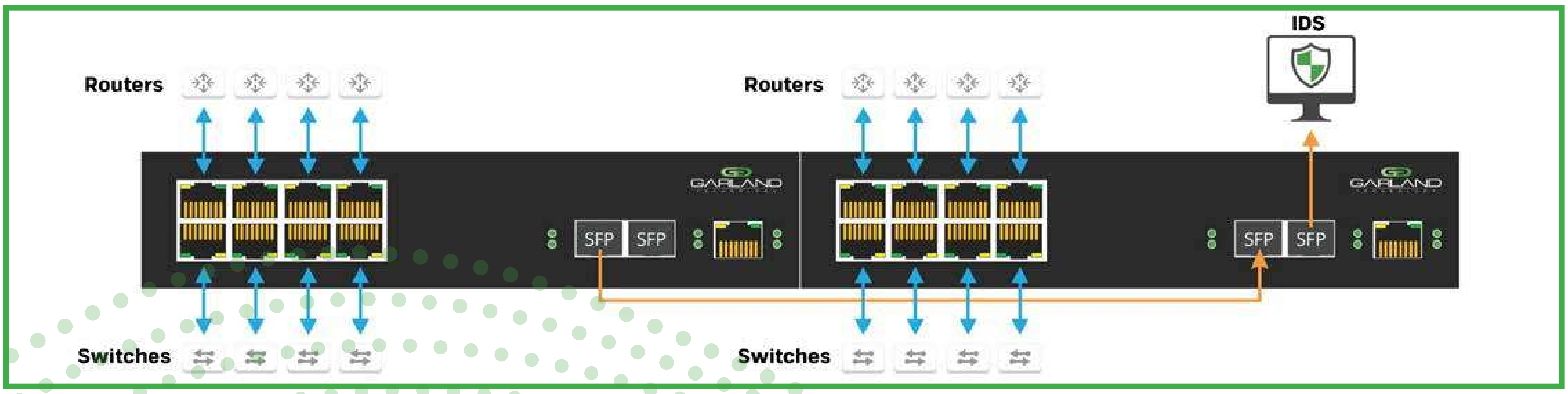
In this scenario, you can tap a connection and aggregate it down to a single tracking port



In this scenario you can tap 4 links and aggregate them into a single tracking point.

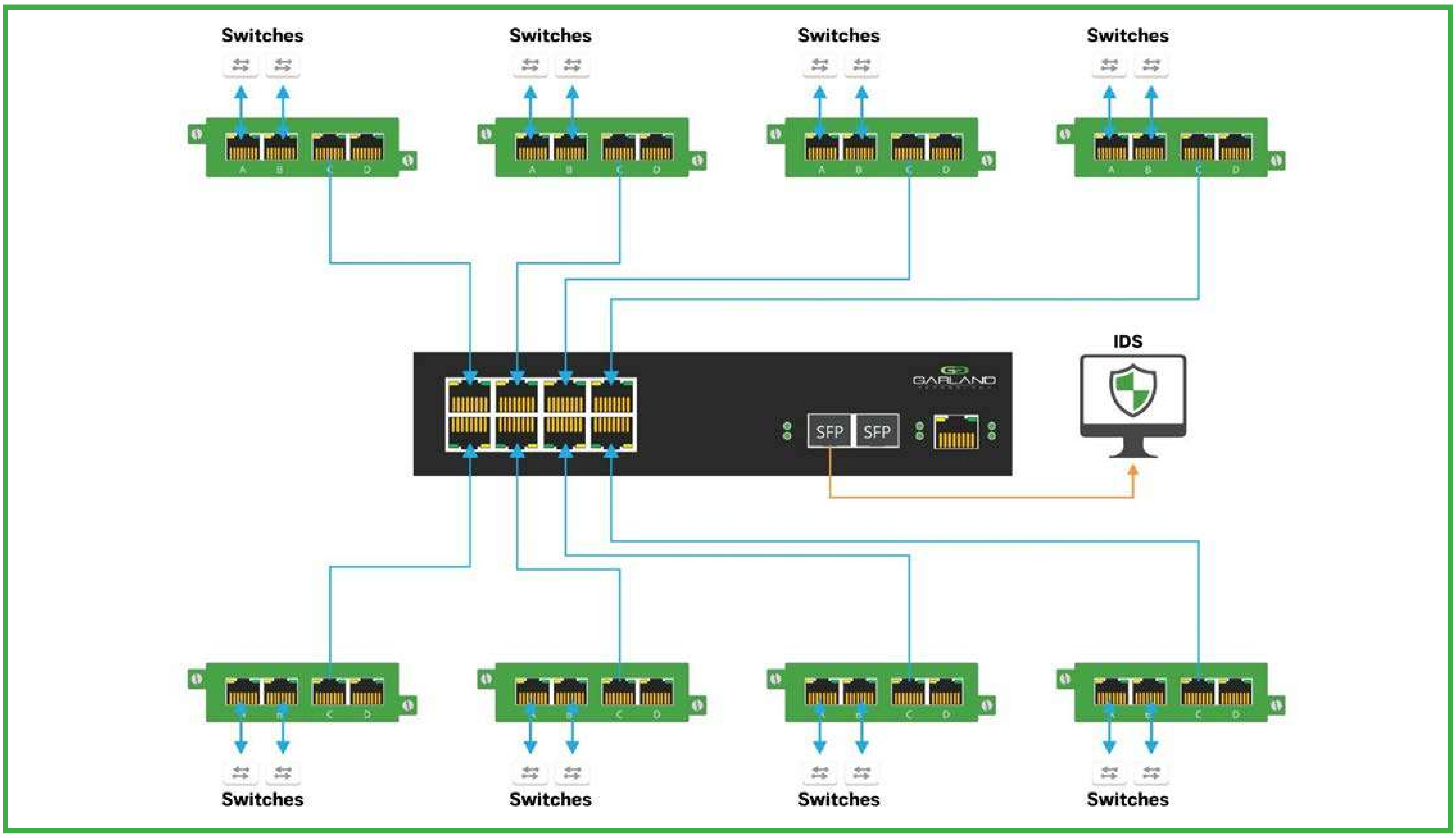


In this scenario, you can combine SPAN 8 connections and roll them up to a single monitoring port.

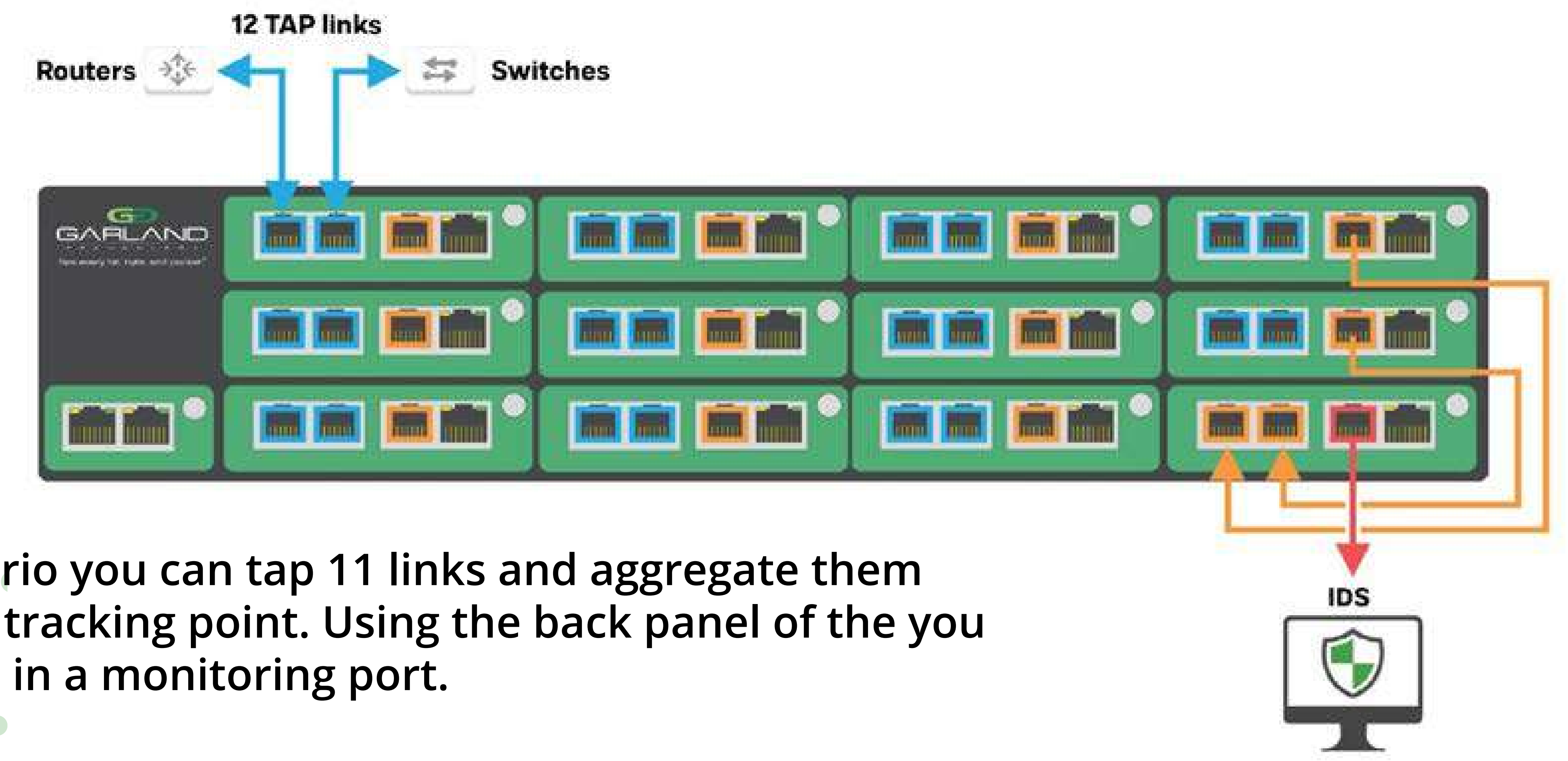


In this scenario you can tap 8 links and aggregate them into a single tracking point. By combining two units you can reduce the first four connections to the second unit's 4 connections and a single monitoring port.

TAP COLLECTION USE CASES SCALING

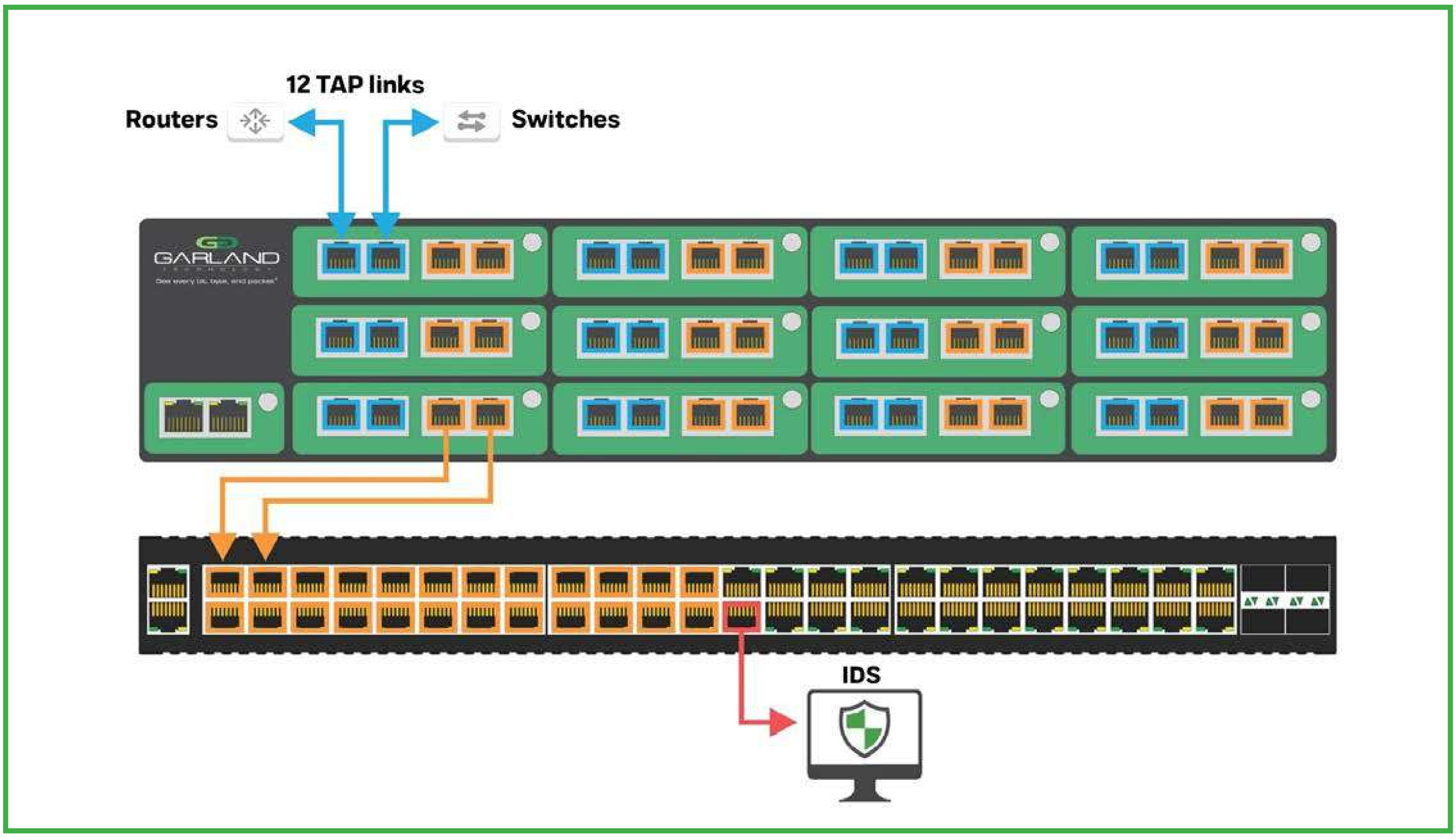


In this scenario, you can tap 8 connections in different locations and sum them up to a single monitoring port. Using 8 passive 10/100 portable TAPs (P100CCA), you can aggregate various locations into a single monitoring port with the AggregatorTAP aggregator.

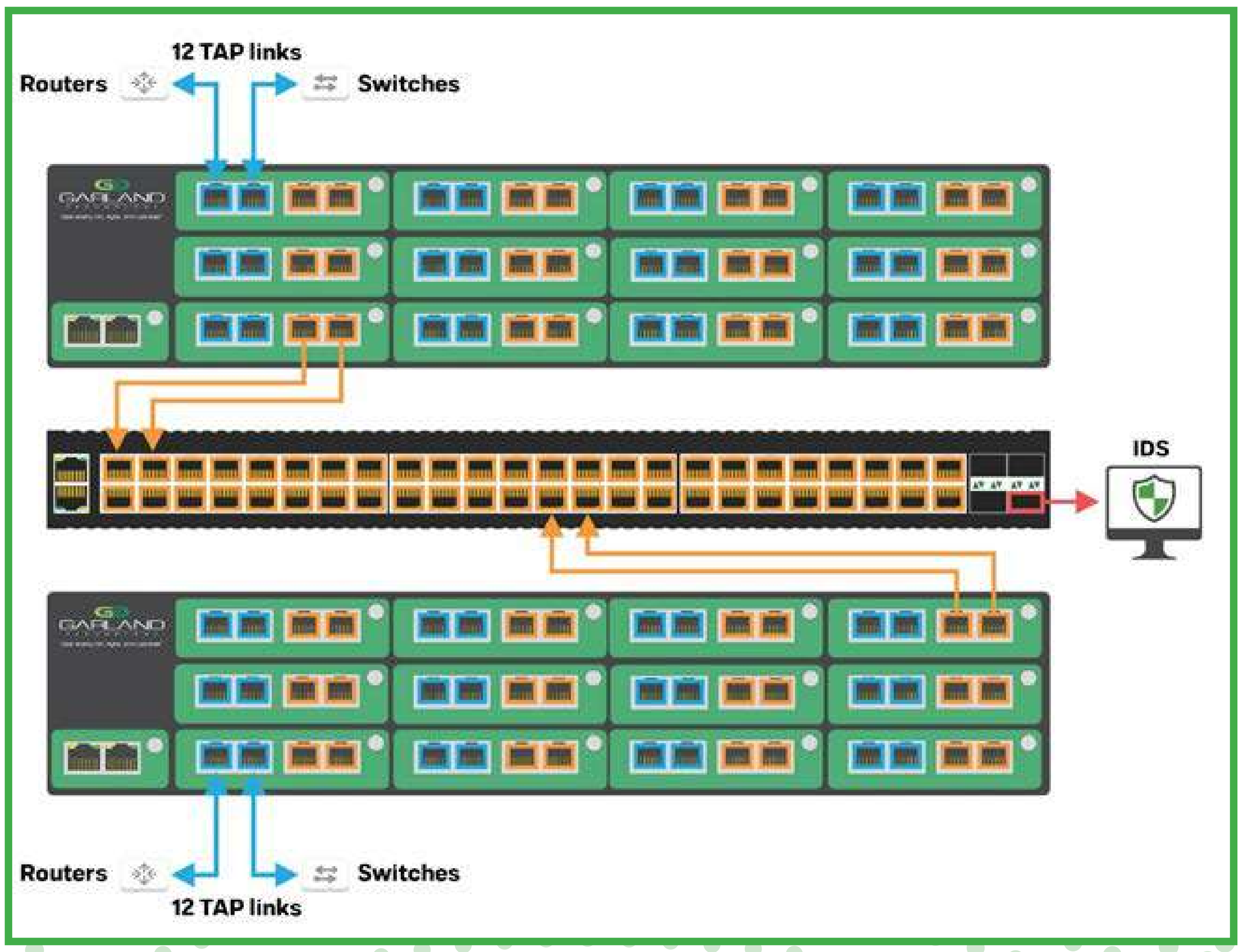


In this scenario you can tap 11 links and aggregate them into a single tracking point. Using the back panel of the you can collect it in a monitoring port.

VISIBILITY

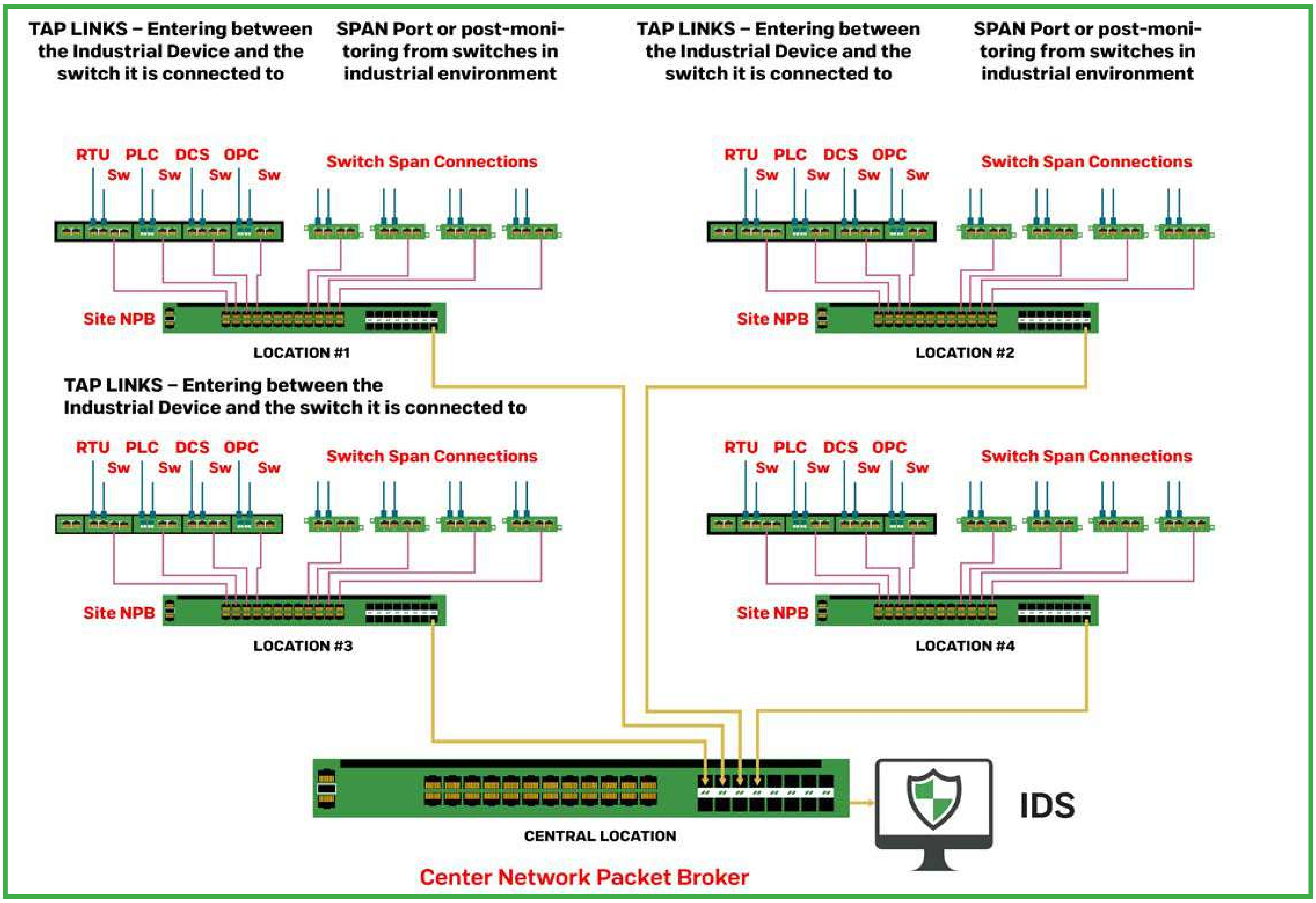


In this scenario, you can aggregate 12 'breakout' TAP connections into a single monitoring port. You can reduce 12 TAPs to one using PacketMAX Advanced Aggregator. This high-density unit has over 25 ports, enabling future growth.



In this scenario, you can aggregate up to 24 “breakout” TAP connections and one monitoring port using the additional ports on the PacketMAX Advanced Aggregator.

VISIBILITY


TAP LINKS – Entering between the Industrial Device and the switch it is connected to
SPAN Port or post-monitoring from switches in industrial environment
TAP LINKS – Entering between the Industrial Device and the switch it is connected to
SPAN Port or post-monitoring from switches in industrial environment
RTU PLC DCS OPC
Sw Sw Sw Sw
Switch Span Connections
Site NPB
LOCATION #1
RTU PLC DCS OPC
Sw Sw Sw Sw
Switch Span Connections
Site NPB
LOCATION #2
TAP LINKS – Entering between the Industrial Device and the switch it is connected to
RTU PLC DCS OPC
Sw Sw Sw Sw
Switch Span Connections
Site NPB
LOCATION #3
RTU PLC DCS OPC
Sw Sw Sw Sw
Switch Span Connections
Site NPB
LOCATION #4
CENTRAL LOCATION
IDS
Center Network Packet Broker

In this scenario, you can use PacketMAX advanced features to connect to many connections in various locations.
You can perform TAP and SPAN and restore the GRE Tunnel to a central location.

ICS VISIBILITY

ONE-WAY TRAFFIC TO SECURITY AND MONITORING VEHICLES HOW TO PROVIDE?

Some service environments face regulations such as NERC CIP v5 regulations and NRC guidelines that require one-way data transfer to implement physical unidirectionality to protect network segments from threats between segments or facilities.

The use of SPAN is unacceptable in these network deployments. The process of SPAN, or network connection mirroring, over a network switch is bi-directional, creating the opportunity for device deployment and hacking for monitoring or security purposes.

SOLUTION

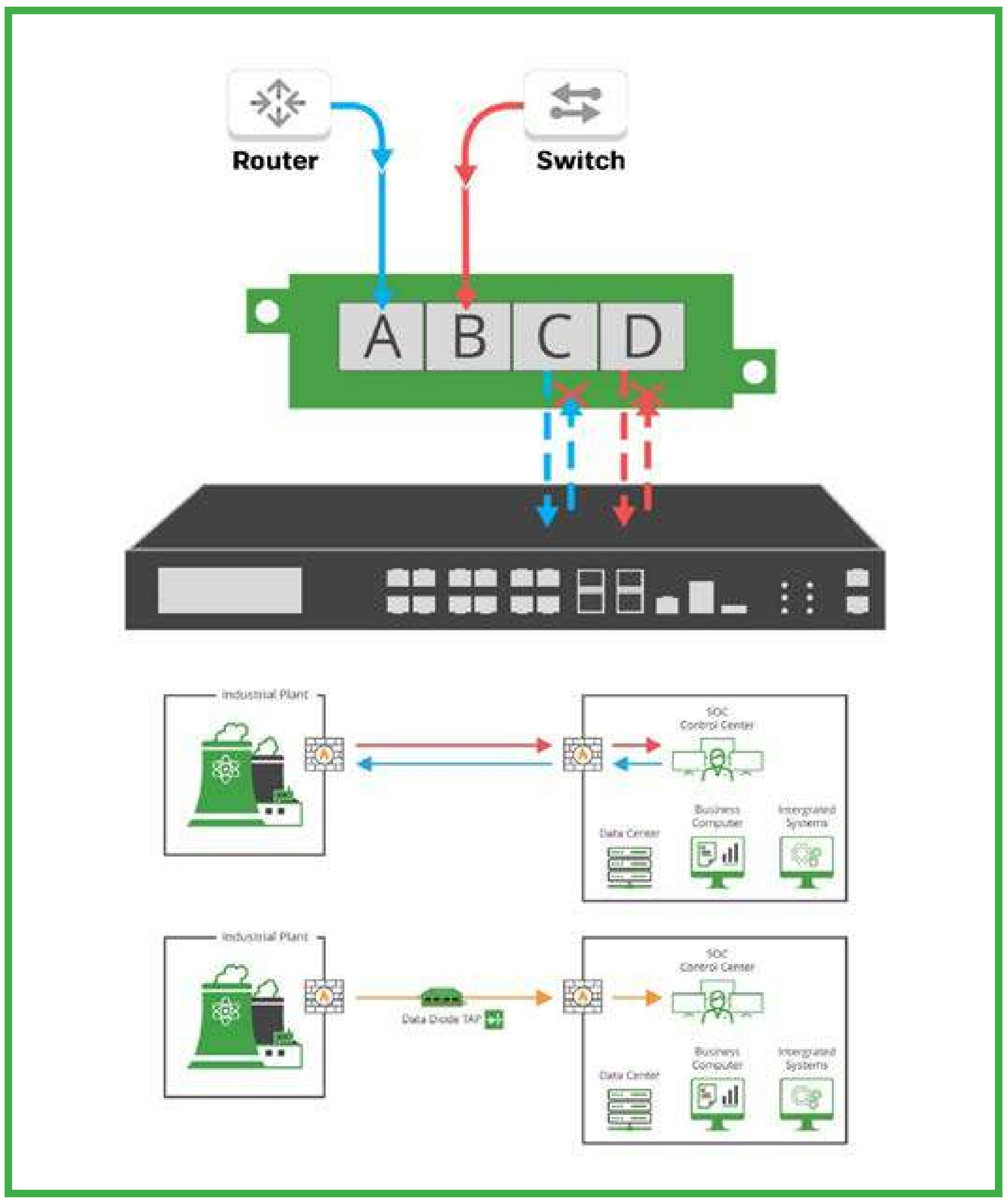
DATA DIODE TAPS OFFER ONE-WAY SAFETY

Data diode TAPs are a purpose-built network hardware device used as a traffic enforcer that allows raw data to travel in one direction only, ensuring information security or the protection of critical digital systems such as industrial control systems against incoming cyber attacks.

Data Diodes are specifically designed not to send traffic back to the network. Data diodes can most commonly be found in high-security environments such as federal defense and Industrial IoT, where they act as connections between two or more networks with different security classifications. This technology is used for security purposes such as nuclear power plants, energy production and railway networks.
It can be found at the industrial control level for facilities such as critical systems.

Garland Technology Data Diode TAPs offer "injection-free" tap collection for 10/100/1000M copper networks. This prevents any Ethernet packets from being physically forwarded to the Live Network Tap Ports or SPAN ports.

It creates one-way monitoring solutions that capture every bit, byte and packet and prevent copied packets from bouncing back and disrupting the industrial network – all in a purpose-built shielded package.



Recommended Products

Data Diode Network TAP
10M/100M/1000M (1G) | One Way Data Diode Circuit Design Model # P1GCCAS-Custom | CTAP-P1GCCREG
AggregatorTAP: Copper High Density
1G | 1U ½ rack | Collection and Regeneration One-Way Data Diode Circuit Design
Model # INT1G10CSA | INT1G10CSA-DC | INT1G10CSASP | INT1G10CSASPDC

Data Diode TAPs secure SPAN connections by providing a physically secure one-way communication path to the monitoring tool.

ICS VISIBILITY

HOW TO PROVIDE A SECURE AIR GAP VISIBILITY SOLUTION FOR VIRTUAL ENVIRONMENT MONITORING?

With performance demands and progress in innovative industry 4.0 use cases for IoT devices, artificial intelligence, machine learning and other advanced technologies, fully air-gapped networks have become visible in very limited numbers.

At this point, many people state that with the widespread connectivity offered by industrial network components, air gap is no longer a valid security tactic. Connectivity, along with the increasing use of cloud-based solutions, has led industrial network architects to seek more modern answers to cybersecurity problems.

This points to greater challenges facing industrial network architects. When you start using public and private cloud environments, how can you maintain visibility of all packets entering and leaving the network in a way that provides full control of security? It has always been important to design industrial networks with passive network TAPs and data diodes. However, new cloud environments and air-gapped networks require a more specialized solution.

SOLUTION

VIRTUAL AIR GAP PACKET VISIBILITY FOR ADDITIONAL SOLUTION SECURITY

Thanks to Garland Prism, you can reflect your out-of-band virtualized traffic to your monitoring tools from an air-gapped platform.

Garland Prisms Private Controller, manages virtual Prisms sensor deployment activities from on-premises environments that are “air-gapped” or without Internet connectivity for security purposes

Garland Prisms Private Controller is built from the Garland Prisms Cloud-based SaaS controller platform that Garland customers use to monitor application workloads on the public cloud. To extend virtualized visibility capabilities to air-gapped networks, Garland Prisms also includes on-premises management options to secure industrial environments without compromising cloud capabilities.

Recommended Products

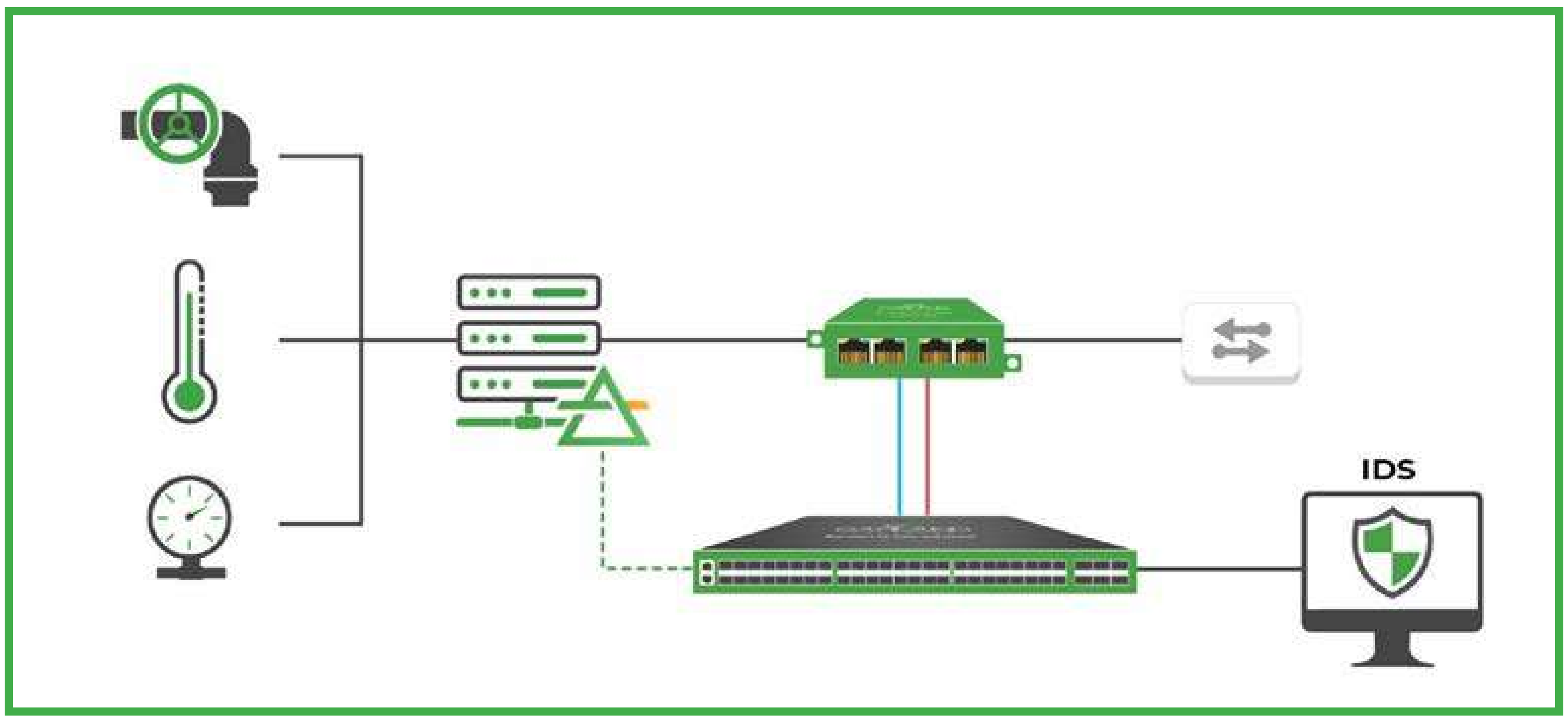
GTVTAP1YRA
1 Year License Single Prism Intelligent vTAP Agent for Public and Private Clouds 'A' Price Level valid for 10 licenses.

GTVTAP1YRE
1 Year License Single Prism Intelligent vTAP Agent for Public and Private Clouds 'A' Price Level valid for 10 licenses.

GTVTAP1YRH
1 Year License Single Prism Smart vTAP Agent for Public and Private Clouds Price Level 'H' is valid for 1000 licenses.

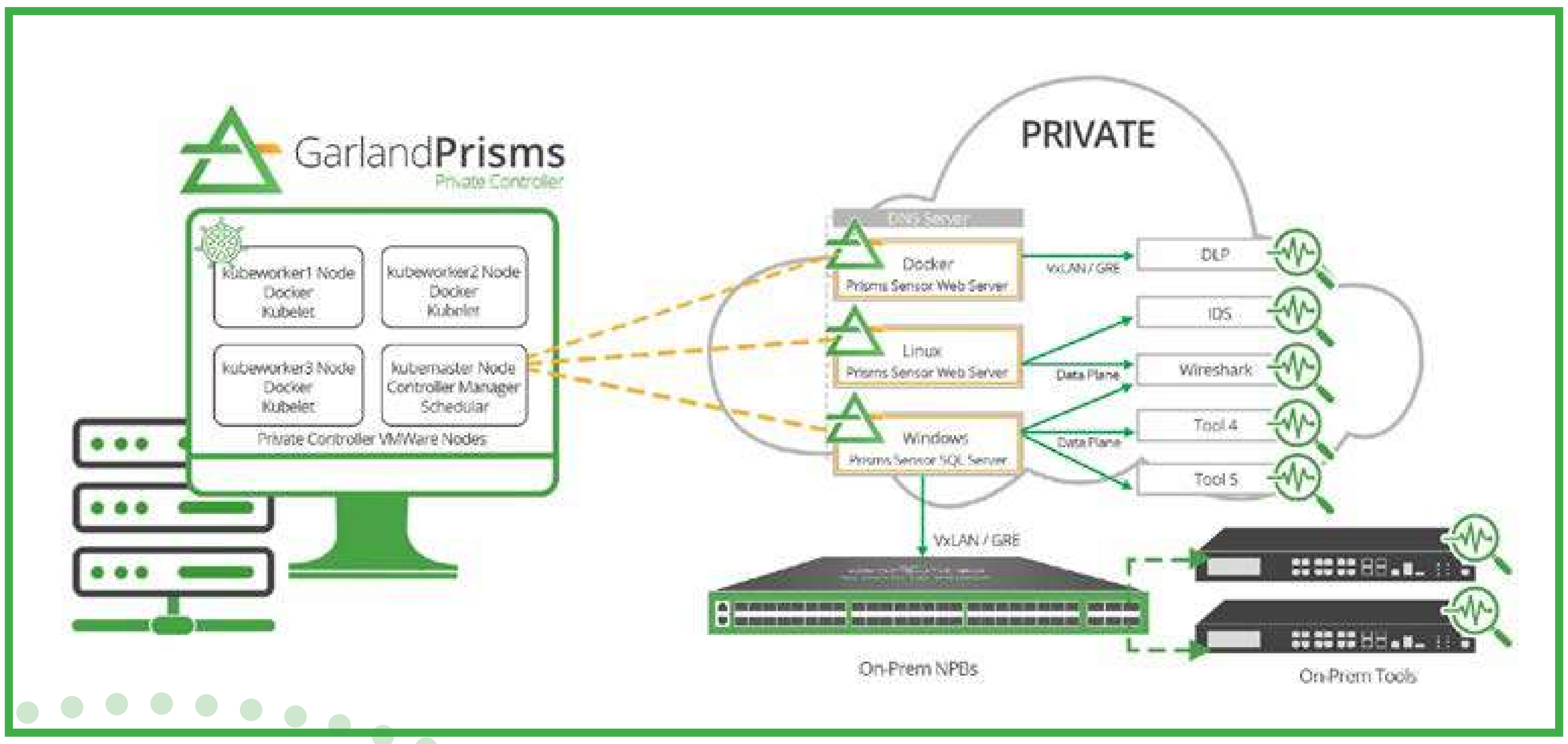
ICS VISIBILITY

HOW TO PROVIDE A SECURE AIR GAP VISIBILITY SOLUTION FOR VIRTUAL ENVIRONMENT MONITORING?



Migrating a utility substation design to a virtualized SCADA deployment offers many benefits, including hardware server consolidation, high availability, migration capabilities, and easy backup and retention processes. However, virtualization of SCADA deployment comes with many challenges, such as having to reconfigure resource allocation, conflicts with network operating system activities, and reduced visibility into the substation.

By deploying Garland Prisms traffic mirroring with substation hypervisors, cloud data blind spots can be eliminated and all other connected systems are provided with access and visibility. By integrating this virtual packet into physical layer network TAPs and packet brokers, a complete end-to-end visibility structure is provided for the substation.



- Dedicated vTAP controller for air gap architectures
- Containers support Linux and Windows Server
- Integrates with Garland physical TAPs and packet Brokers for complete end-to-end visibility

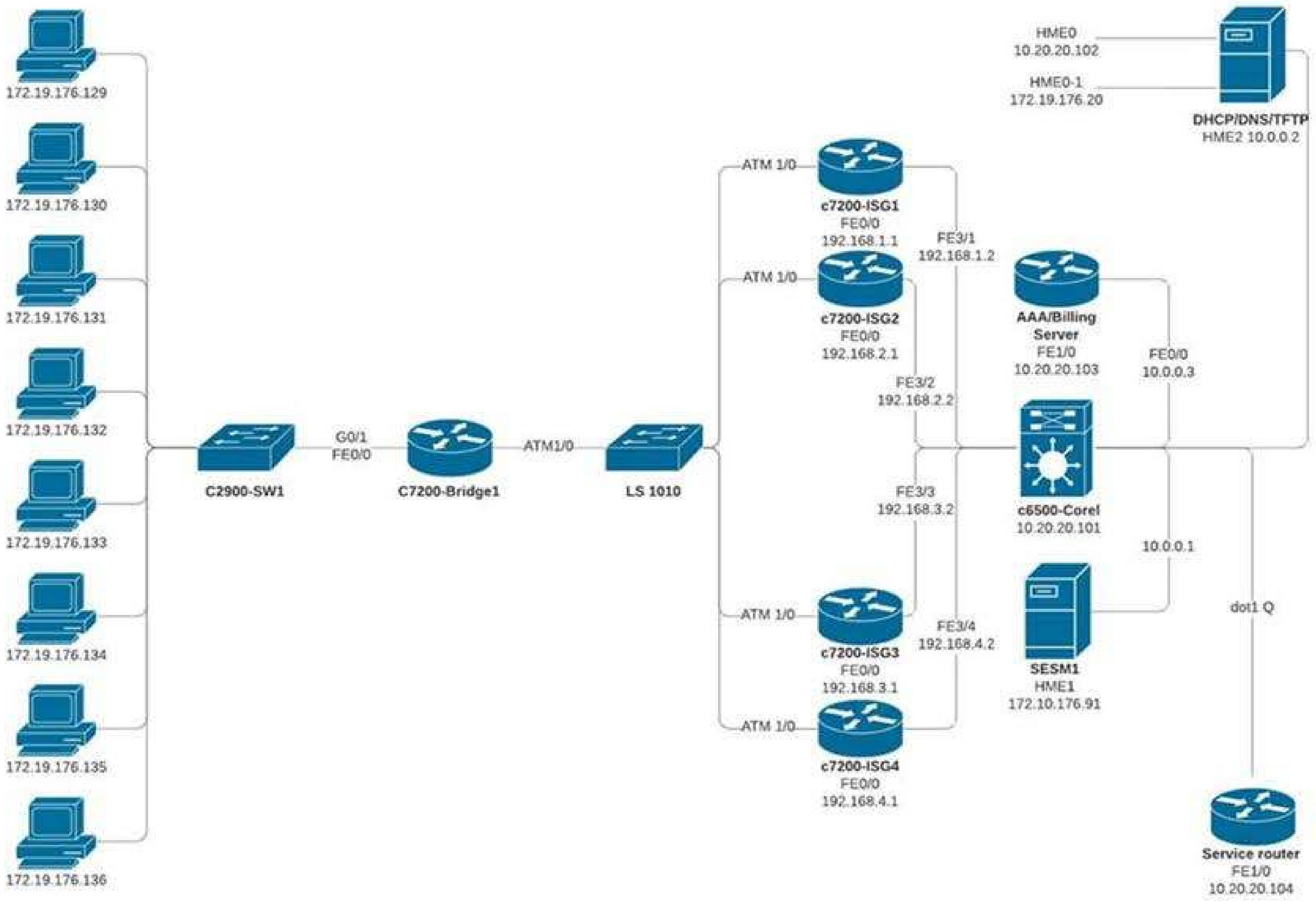
Functional Solutions

Access and Visibility

FUNCTIONAL

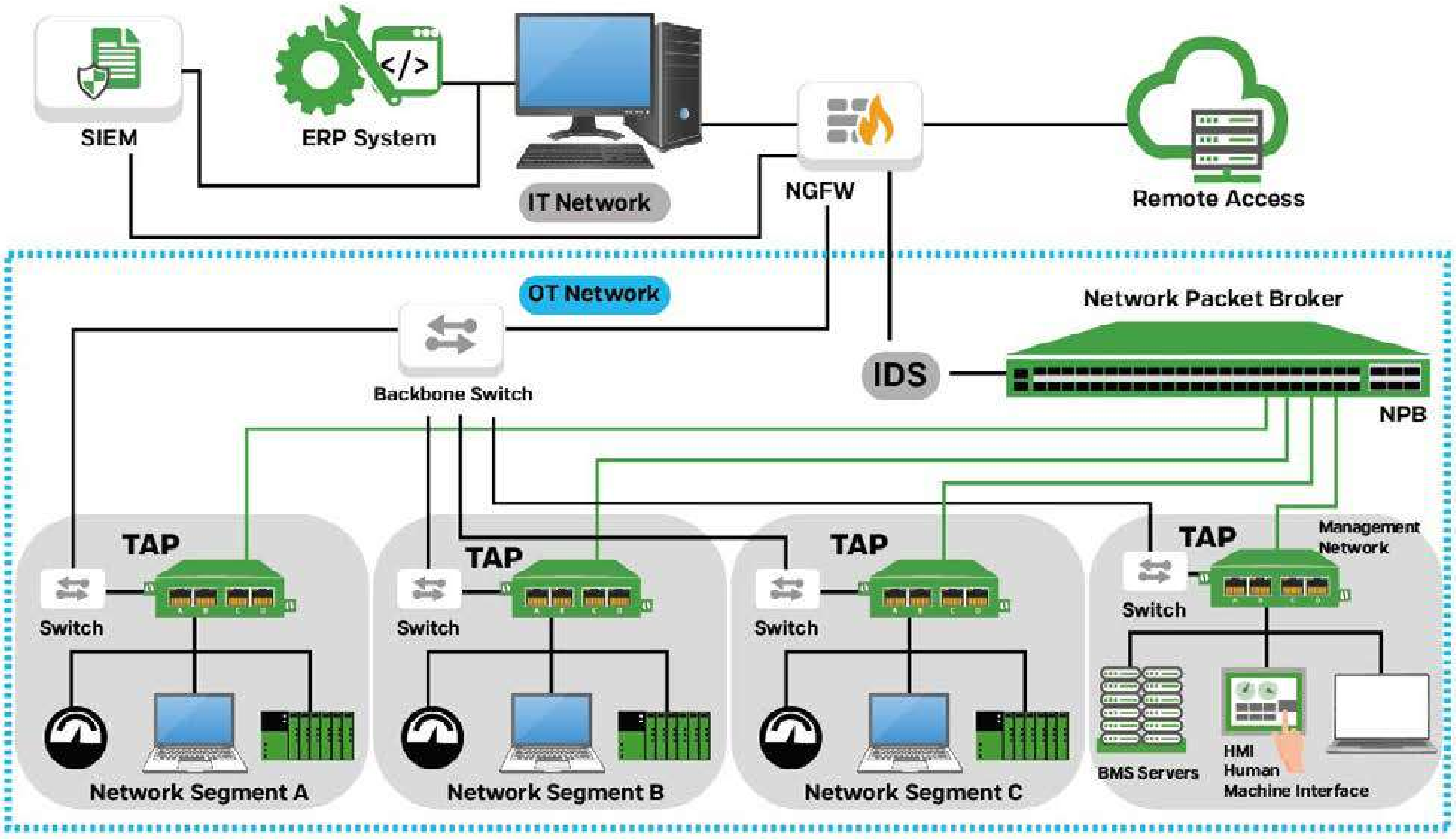
Security/Monitoring Structure

Visibility to Ensure Performance & Security



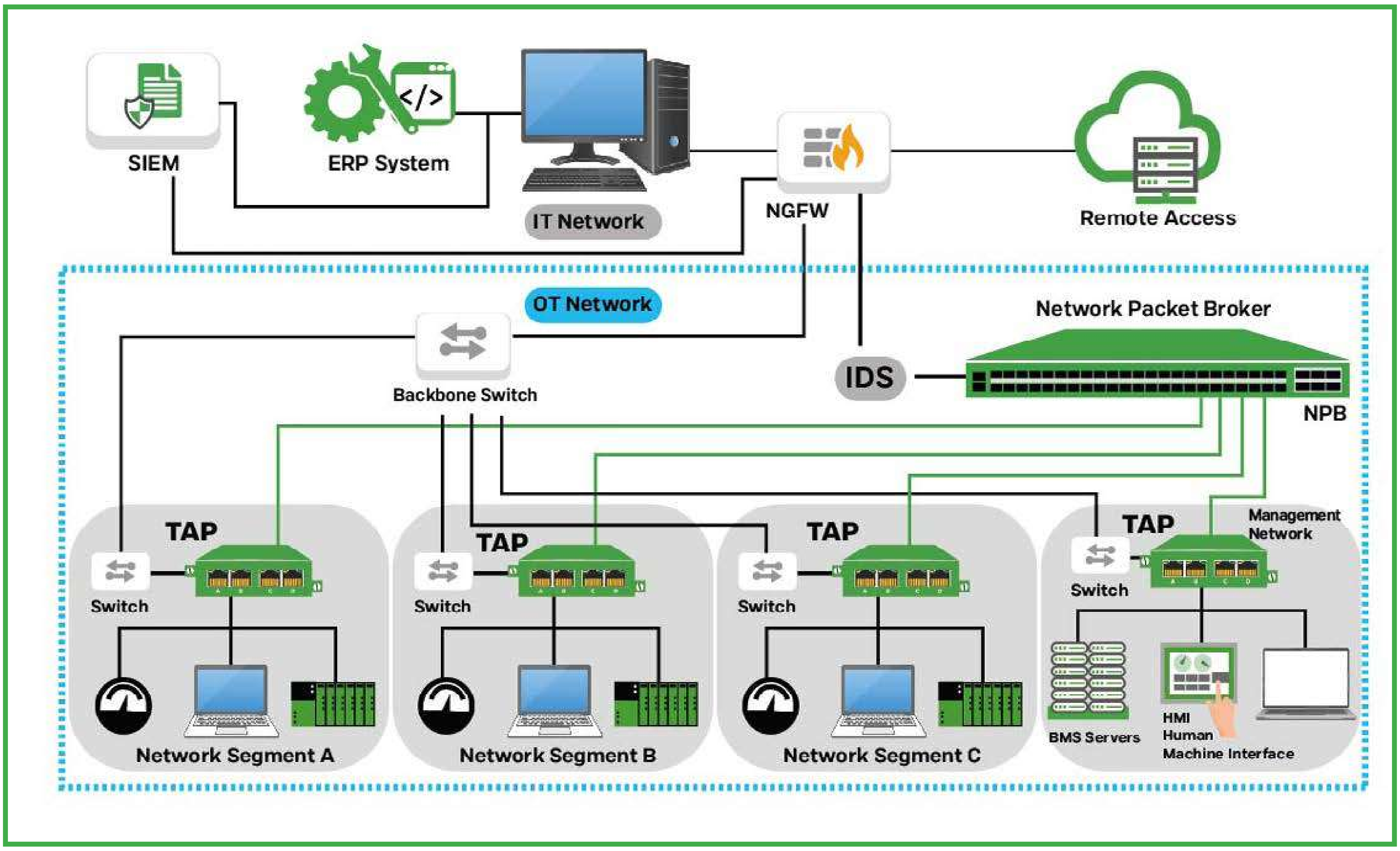
Security/Monitoring Structure

Visibility to Ensure Performance & Security



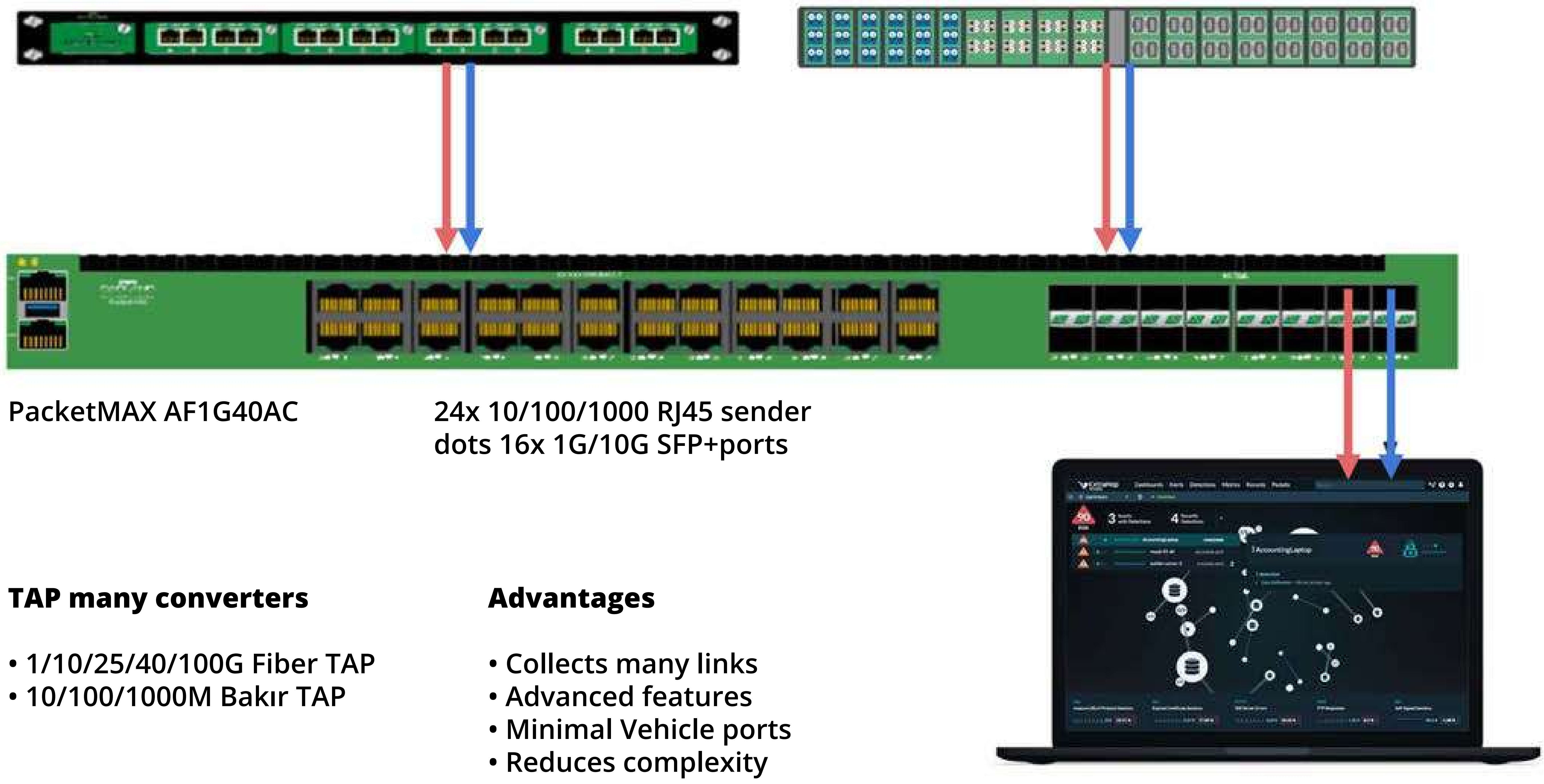
SCADAfence

Uninterrupted Monitoring for Industrial Environments



Medium-Scaled Websites

TAP + Concentration 1-100G Tracking



M1G1 with Copper Breakout Module

SelectTAP FMC with Optical TAP Modules

PacketMAX AF1G40AC

24x 10/100/1000 RJ45 sender
dots 16x 1G/10G SFP+ports

TAP many converters

- 1/10/25/40/100G Fiber TAP
- 10/100/1000M Bakır TAP

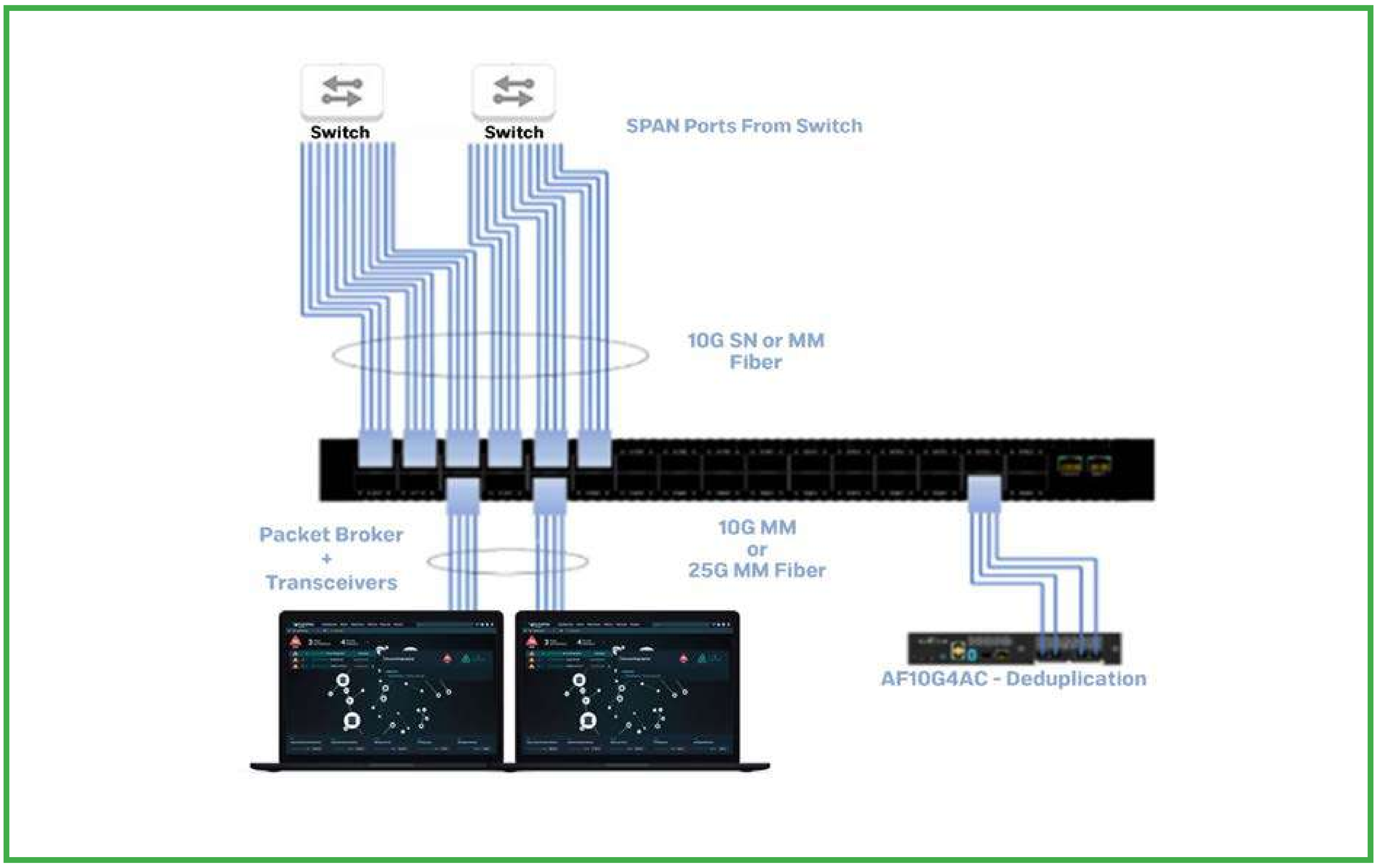
Advantages

- Collects many links
- Advanced features
- Minimal Vehicle ports
- Reduces complexity

FUNCTIONAL

Large-Scaled Websites

TAP + Concentration 1-100G Tracking

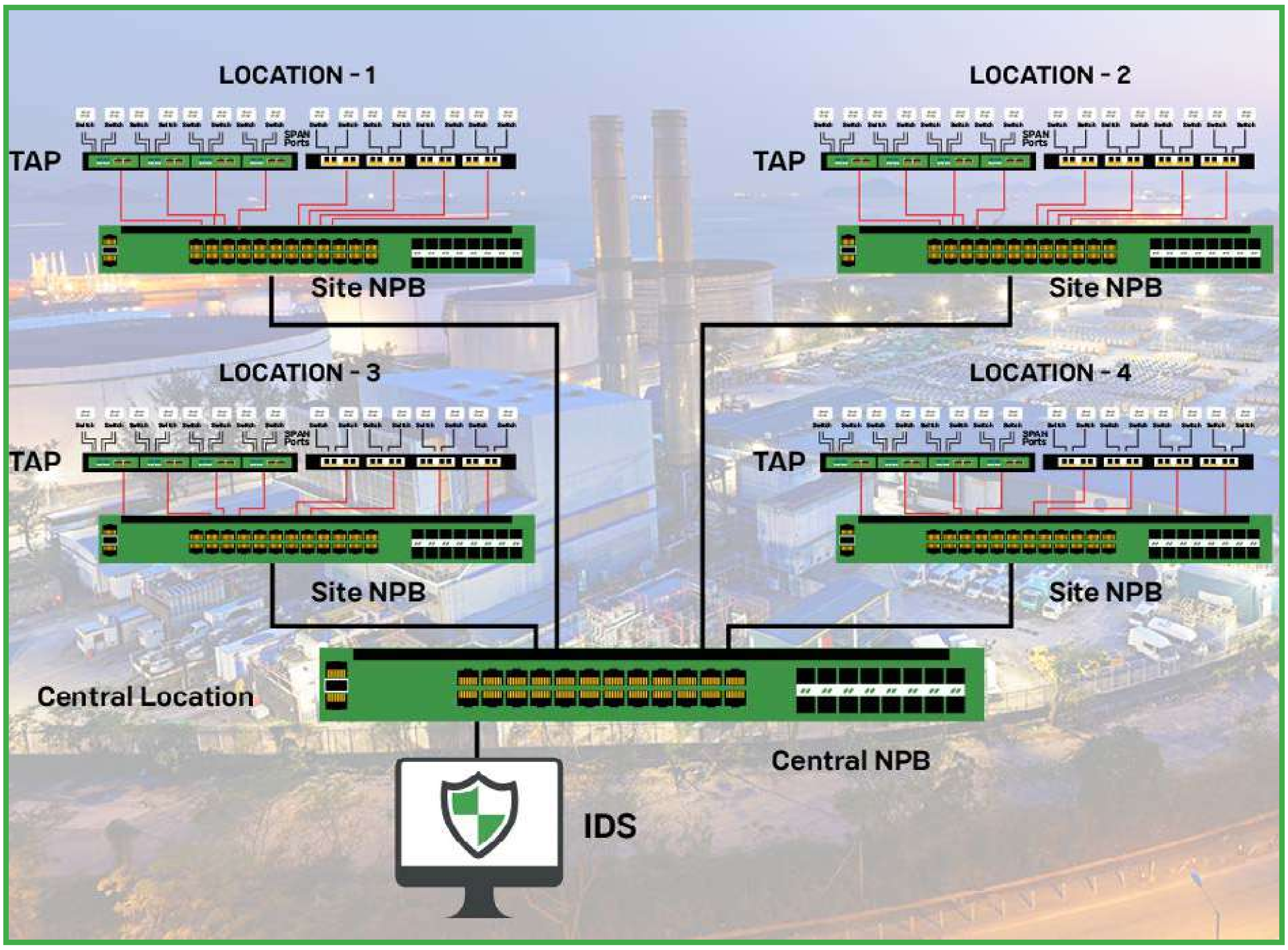


10G Connection
- Concentrates many TAP connections
- Concentrates many SPAN connections

Advantages
- 100% wired data visibility
- Advanced concentration and load balancing
- Deduplication
- Balancing the 25G connections of tools
- Media conversion

Multi-Location Intrusion Detection Solution

To provide visibility and to reduce the network complexity.



An examplary solution with a single IDS that tracks multiple locations

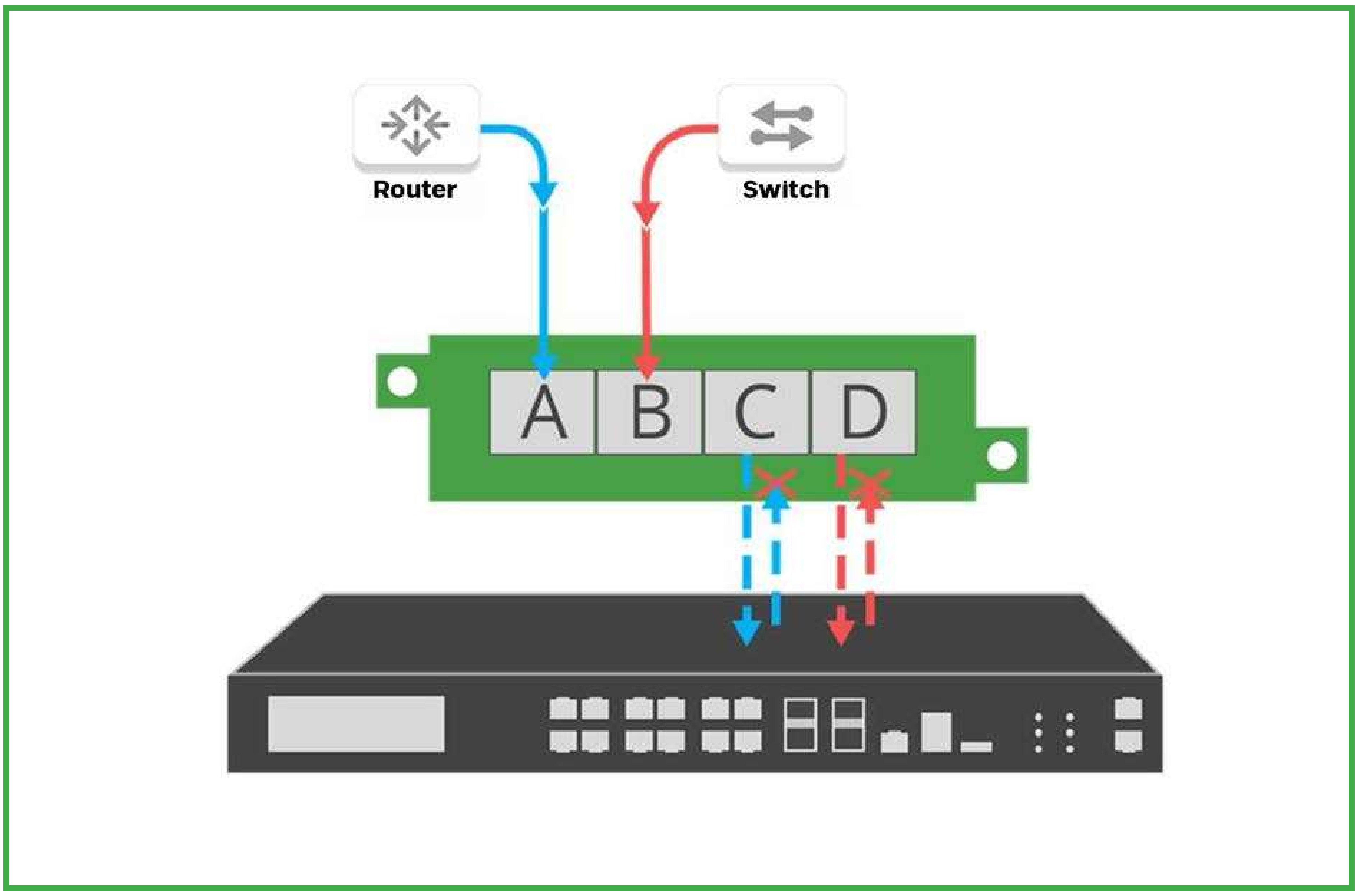
Solution: Distributing the Network TAPs and PacketMAX package agents together within the network, which provide feedback to the central location.

- Reduce complexity and management burden
- Enable infrastructure upgrades
- Increase the effectiveness of team performance

FUNCTIONAL

Infrastructure Protection

To Provide Additional Visibility to Air-Gapped One-Directional Routes.



Secure out-of-band analysis

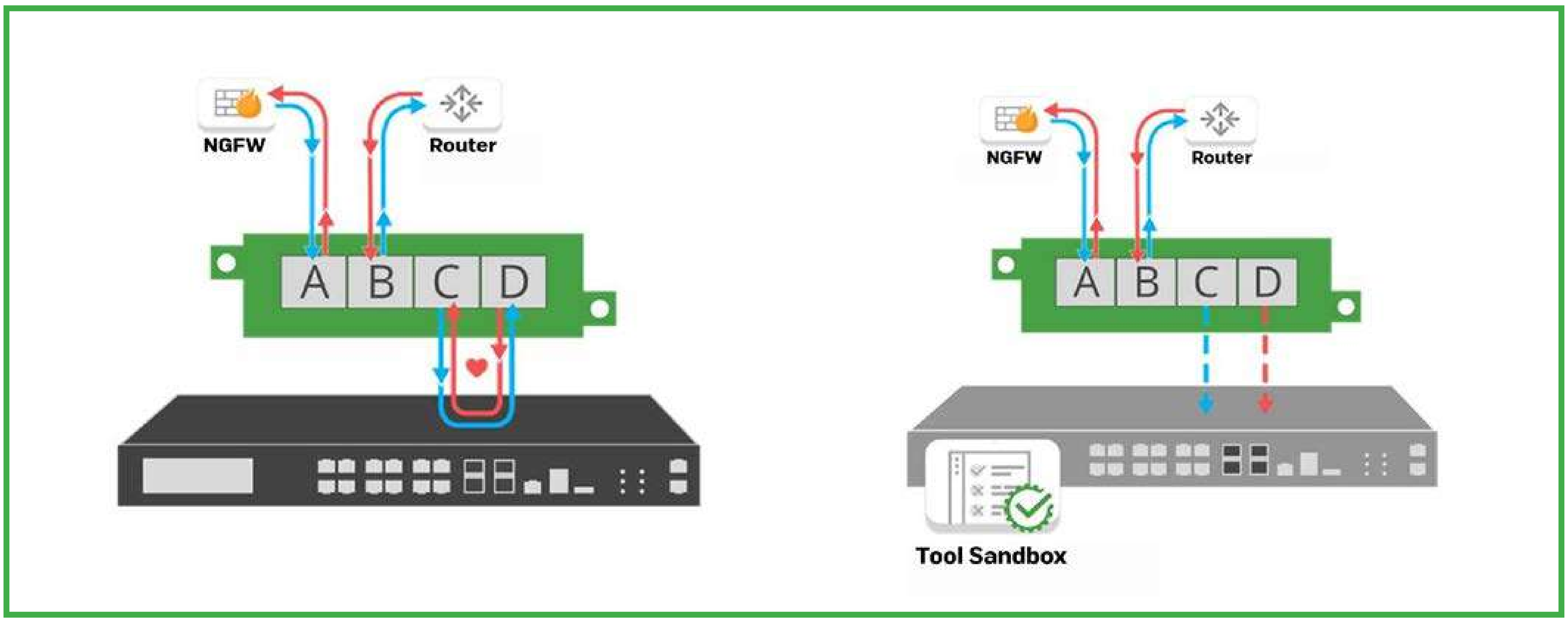
Solution: Data Diode TAPs:

- Avoids the bi-directional traffic in order to protect against backflow of traffic into the network.
- Secure - TAPs do not contain any IP address or MAC address and are not vulnerable to attacks.
- Protects the additional data flow resources such as switch SPAN ports and network connections.
- Network traffic control becomes mandatory at physical level.

FUNCTIONAL

Establishes Connection to In-Line Security Tools

Usage Example for IT Security Solutions



Difficulty: To manage the risk of downtime is a critical issue in deploying the security tools.

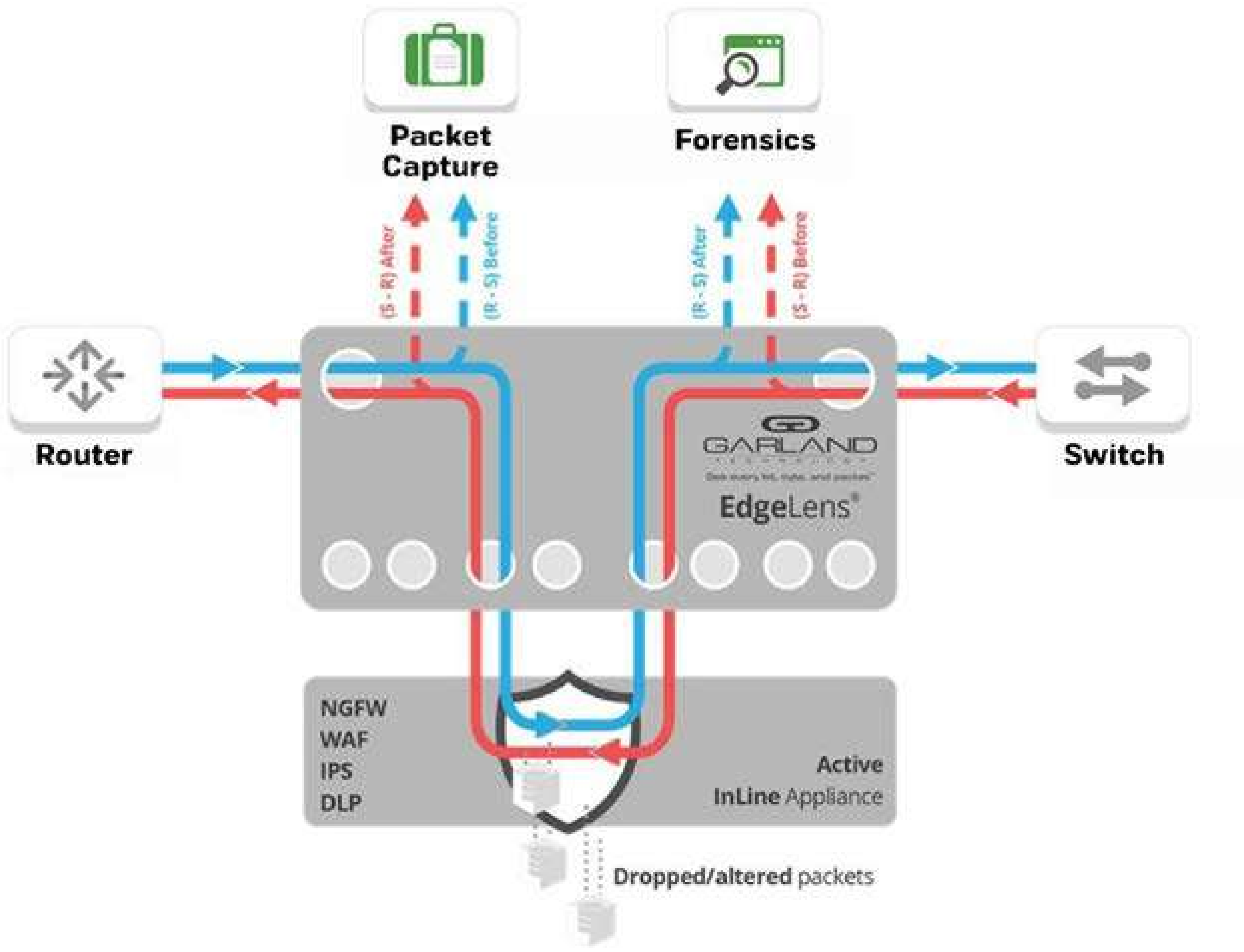
- Tool failures might crash the network
- To include new technologies into the network
- To project the planned downtime

Solution: Bypass TAP Inline lifecycle management

- You can easily take the tools out of band in order to perform the operations of updating, patching, maintenance or troubleshooting
- Tool piloting and deployment processes are simplified
- Administrative isolation
- Zero maintenance window
- Reduced network impact and downtime

Optimize Inline Tools Performance

Usage Example for IT Security Solutions



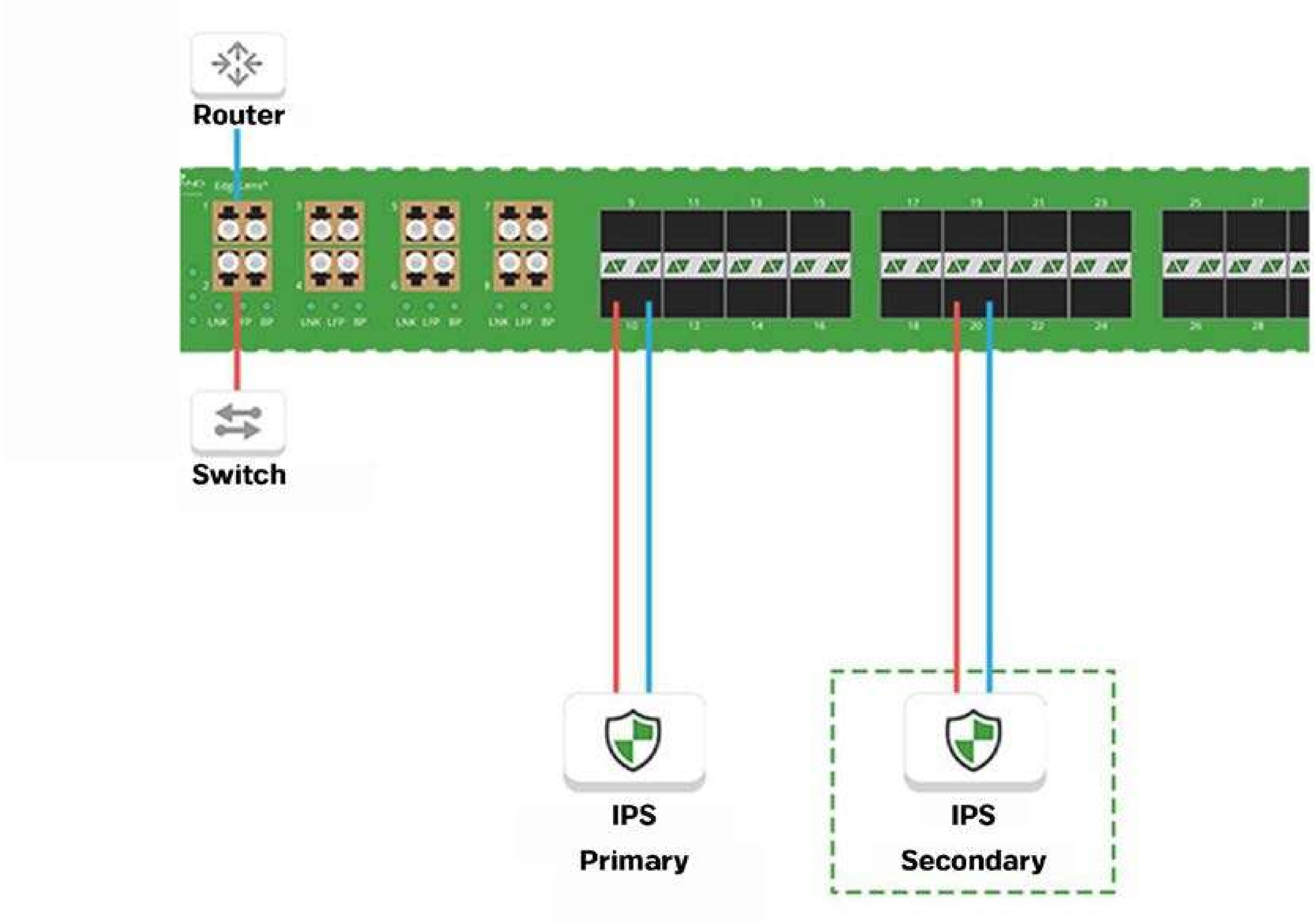
Difficulty: Troubleshooting in-line tools (IPS, firewalls, etc.) is properly configured and optimized.

Solution: Before and after the optimization and approval processes, you can obtain visibility for your out-of-band package capture, storage, and analysis tools.

- Analyze packet data before and after your inline tool in order to get the best tool performance when verifying any updates or identifying and resolving the cause behind the failure to block the threats.
- Enable real-time proof-of-concept assessments without affecting the network.
- Verify that tool changes and updates are configured properly.

To Ensure Availability

To Offer Full High Availability (HA) Redundancy for Critical Connections



A large financial company has secured all of its critical connections through Garland's HA redundancy to ensure to have zero downtime or interruptions while protecting the sensitive data.

Solution: Garland's EdgeLens used the redundant IPS tools in an active standby scenario.

- A primary or "active" IPS
- And a secondary or "passive" IPS
- If a primary tool is disabled, the secondary tool is automatically enabled over the primary tool.

YOU CANNOT SECURE!
"What You Cannot See"

GARLAND
TECHNOLOGY

OTD BiLiŞiM
GLOBAL VAD

ICT
OTD
PREFER EXPERIENCE ONLINE
Since 2011

CENTER OFFICE

Atakent District 221st Street Route
Office Site Block A No. 3 / 1 / 17 34307
Küçükçekmece İstanbul / TÜRKİYE

HALKALI OFFICE

Atakent District 223. Cadde Elit City
Site Door No. 2 Block A1 APT: 83
Küçükçekmece İstanbul / TÜRKİYE

GEBZE OFFICE

Mevlana District Soma Maden Şehitleri
Boulevard Elmas Plaza No. 4 / 1 Floor: 5
APT: 33 Gebze - Kocaeli / TÜRKİYE

MARYLAND OFFICE

7620 Old Georgetown Rd Apt 202
Bethesda, MD 20814 Maryland / USA

T: +90 216 912 10 05   F: +90 216 912 10 07   otd.salesgrp@onlineteknikdestek.com