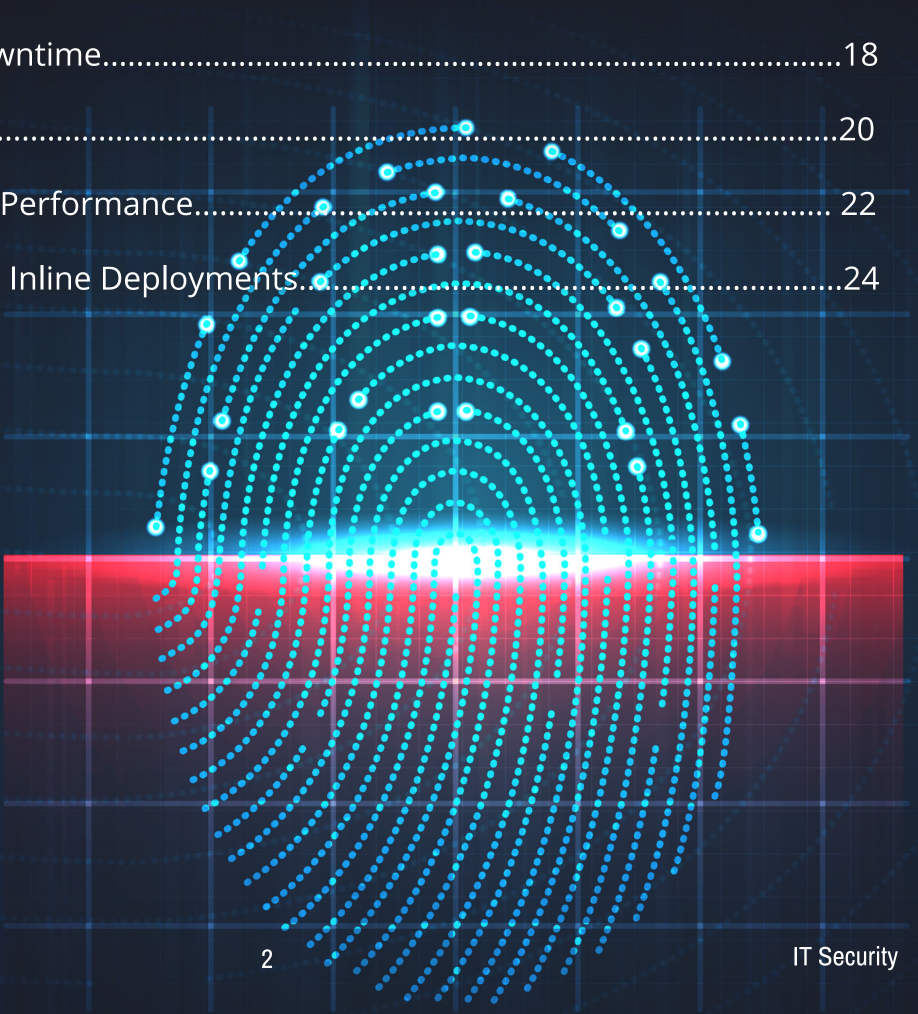
Whitepaper

IT SECURITY

How to Improve Your Threat Detection and Prevention Tool Deployment

GARLAND
TECHNOLOGY
See every bit, byte, and packet®

IT Security | Table of Contents



Introduction

How to Improve IT Security Strategies at the Edge, Data center and Enterprise

IT security, whether deployed at the edge of the network, within a traditional data center or enterprise, all have a common theme — without network visibility, there is no cybersecurity. Or commonly stated — you can't protect what you cannot see.

The ability to detect and remediate cyber attacks pose an existential threat to IT organizations worldwide. A study from IBM and Ponemon found that companies that detect and contain data breaches within 30 days save, on average, more than $1 million compared to organizations that take longer to respond.[1]

Designing a modern security strategy is no easy feat, as it must protect all components of a complex network, while having a limited effect on performance. Today's security strategies incorporate both inline and out-of-band solutions, with a suite of active blocking and passive monitoring tools.

As expected, we get a lot of questions about the differences between an inline and out-of-band security deployment and whether or not network TAPs or Bypass TAPs are needed.

This whitepaper will review how these tools are being used and what industry best practices and use cases may help improve your next deployment.

Out-of-band Security Threat Detection

The term “out-of-band” generally refers to monitoring tools that analyze packet data to optimize network performance. Out-of-band tools sit out of the direct traffic flow and passively process packet data, analyzing specific aspects of the live data streams. In security applications, this analysis is used to improve forensic detection and reduce MTTR (Mean time to resolution) by guaranteeing data quality and integrity, leading to faster analysis and resolution. Common out-of-band security monitoring tools include:

IDS

Intrusion Detection System (IDS) monitors traffic data looking for malicious activity, policy violations and logs events, which trigger reports for IT Admin to respond. Threat detection analyzes the security ecosystem to identify anything that could compromise the network.

SIEM

Security Information and Event Management (SIEM) collects data that is generated from network tools and hardware event logs based on the traffic flowing through the tool and how it reacted, providing real-time analysis of security alerts. For devices that can’t generate event logs, packet decoders on the SIEM can evaluate packet headers, identify errors, and create logs from locations if missing.

DLP

Data Loss Prevention (DLP) is a solution designed to make sure that sensitive files are accessed by only those authorized, as the human element is usually the most vulnerable point in the network. DLP can generate reports on what data is being used, drop connections if sensitive files are being shared incorrectly, and can actively remove sensitive information from the document in real time.

Forensics

Network analyzers and forensics tools capture, record and analyze network packets to determine the source of network security attacks. Forensics tools are designed to collect evidence from the network traffic data, collected from different sites or devices, such as firewalls and IDS.

Top challenges many IT teams face with their out-of-band security tools are ensuring they have no dropped packets or blindspots that may mask threats. It’s this reason most modern IT strategies incorporate a visibility fabric.

For these out-of-band security threat detection tools — providing a cohesive visibility fabric of network TAPs and packet brokers, improves the tool performance tasked with solving various security strategies.

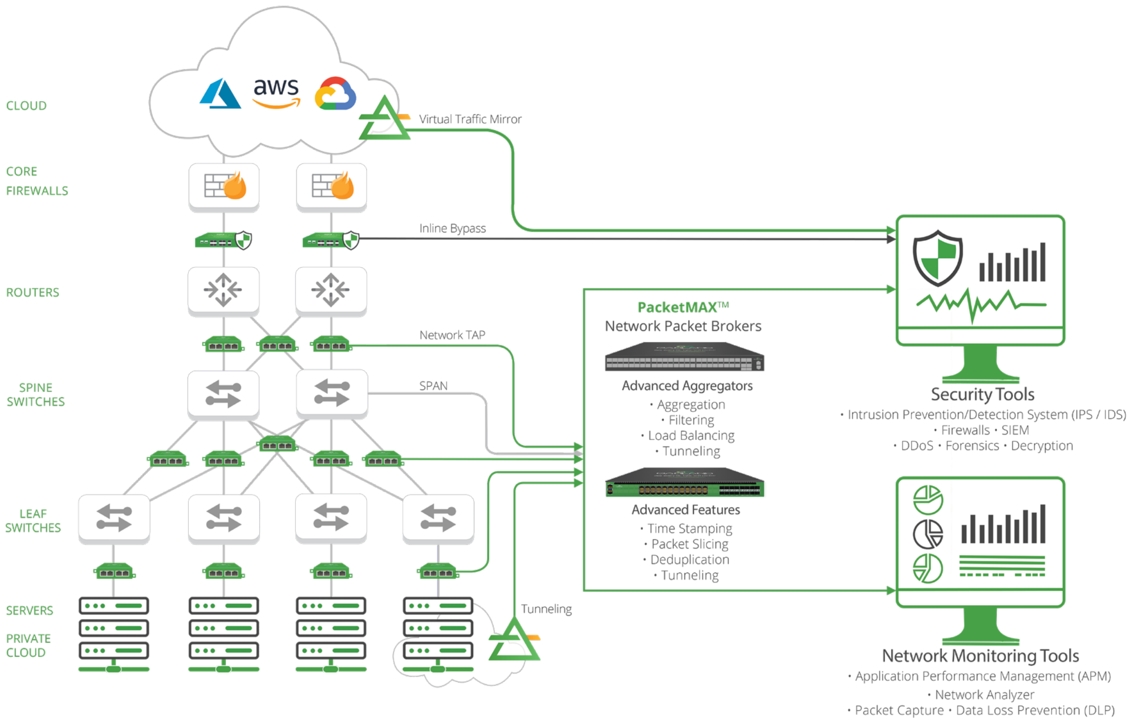


Diagram: Out-of-band visibility fabric

A visibility fabric enhances out-of-band strategies with:

- Improved forensics detection, ensuring no dropped packets and no blindspots masking threats
- Reduce MTTR (Mean time to resolution) by guaranteeing data quality and integrity, leading to faster analysis and resolution
- Improve tool performance — get more out of existing or lower speed tools
- Regain cloud visibility with 1:N traffic mirroring and TLS 1.3 Decryption
- Provide CALEA (Commission on Accreditation for Law Enforcement Agencies) compliant forensics packet capture data in lawful interception cases

Use Cases: How to Improve Out-of-band Security Deployments

1. Eliminate Blind Spots

“Blind spots” refer to the inability to analyze the data between certain segments in a network, and may seem “hidden” to your monitoring tool and can compromise network performance and security. If a network expands without a proper visibility fabric in place, blind spots may become apparent. These blind spots happen for a variety of reasons, including:

- There has been an addition of new network equipment or applications. The additions are not properly architected or the team overseeing this data is not planned out.
- New deployments can lead to network complexity. When new links, new equipment or remote locations are introduced, they can be configured with separate management or teams, making it hard to track what is happening in these segments.
- SPAN ports present a host of opportunities for blind spots – SPAN port contention issues, dropping packets and creating a loss of information, improper SPAN port programming – all resulting in incorrect or missing data captures.
- Introducing virtualization – the migration to a virtualized data center environment is known for introducing blindspots into the network. The evolution of Kubernetes & Containers has created blind spot challenges, along with a maturing industry that is just catching up with proper mirroring technology.

Solution: Network TAPs Guarantee Tools Complete Packet Data Visibility

Network performance monitors (NPMs) can be used to determine areas within a network that aren't performing as they should, letting you know where the visibility problem may be located. Network TAPs, an industry best practice over SPAN ports, create a "foundation of visibility," providing the ability to capture network monitoring data without compromising the network, removing blind spots.

> *Research found that 83 percent of current network visibility fabrics use TAPs for at least half of the fabric access layer.*
>
> *- EMA [Enterprise Management Associates]*

Network TAPs are used to help IT teams easily monitor all network data. A network TAP is a purpose-built hardware device that allows you to access and monitor your network traffic by copying packets without impacting or compromising network integrity.

They are typically placed between any network devices like switches, routers, and firewalls, creating an exact copy of both sides of the traffic flow, continuously, 24/7/365. The duplicate copies can be used for monitoring, security, and analysis, while the network flow continues uninterrupted. TAPs do not introduce delay, or alter the data. They are either passive or "failsafe," meaning traffic continues to flow between network devices if power is lost or a monitoring tool is removed.

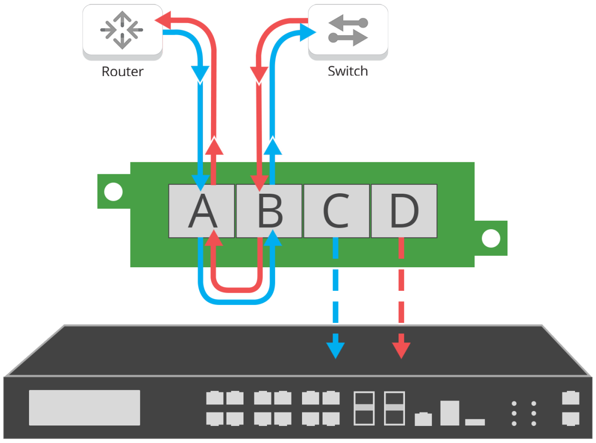


Diagram: Network TAP traffic

2. Improve Tool Performance and Efficiency

Network security tools need packet data to properly analyze and detect any threats. Teams are typically tasked with getting more out of their existing tool investments, which becomes challenging with growing traffic volumes and legacy architecture.

- Network and security tools can themselves be oversubscribed.
- Traffic growth outpaces existing tool capacity leading to reduced throughput and effectiveness.

To get the data to these tools, your options are spanning a port from your switch or utilizing a network TAP. At the same time, it is imperative to not negatively affect the performance of these tools or the connected network.

SPAN ports generally do not affect the performance of the switch, though this varies with different SPAN port features / vendors, but can have an impact on your data and the tools that they are feeding, including:

- Designed for low-throughput situations, SPAN will drop packets if heavily utilized or oversubscribed.
- Can duplicate packets if multiple VLANs are used.
- Can change the timing of the frame interactions, altering response times.
- Will not pass corrupt packets or connection errors.

Solution: Network TAPs Provide Better Data For Tool Performance

Network TAPs are purpose-built to pass 100% full duplex traffic, passing errors, without dropping packets or impacting the performance of the network, enhancing the monitoring and security tools they feed.

As we mentioned, network TAPs eliminate blindspots, one key issue monitoring tools face. But TAPs also enhance tool performance by ensuring no dropped packets if oversubscribed and no duplicate packets or altered frames. Network TAPs provide 100% full duplex copies of the traffic you are analyzing. Better data provides better tools performance and added value.

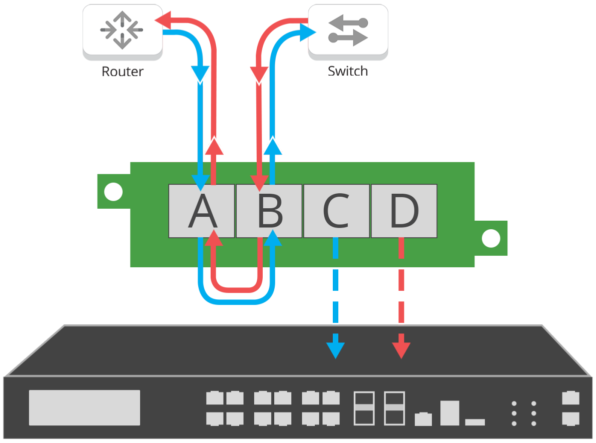


Diagram: Network TAP

Solution: Using Data Filtering to Improve Tool Efficiency

With the growth in network traffic, analyzing this data is not only time consuming but expensive, as it usually includes an extensive number of tools and network segments.

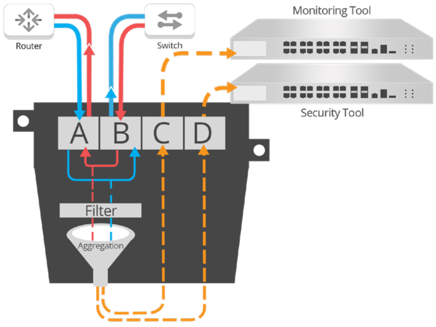


Diagram: Advanced TAP filtering

A more cost-effective technique, that can be used in specifica scenarios, is to isolate data that needs to be inspected, e.g. like VOIP traffic only, or traffic that has a higher risk of being a security threat and focus on analyzing just that data. This unburdens current tools by reducing traffic load, increasing tool effectiveness and performance.

This approach can be accomplished at the TAP level, with Garland's XtraTAP or with a PacketMAX packet broker that is aggegating many links at once.

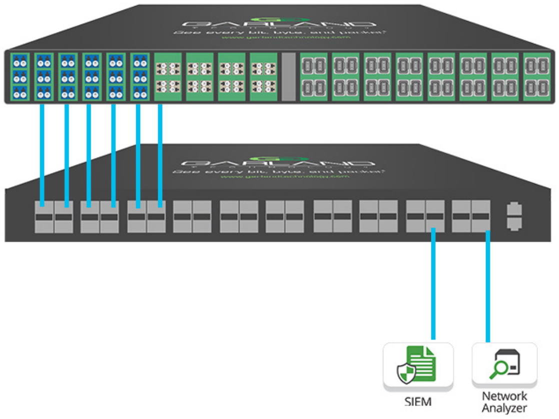


Diagram: Advanced filtering packet broker

3. Overcoming Limited Cloud Visibility

Traditional network monitoring tools weren't designed to monitor cloud traffic, either in public or private clouds. If you have been looking into cloud migration you may have noticed the limitations of VPC-Based Traffic Mirroring from the major cloud providers. The concept of infrastructure-based tap/mirroring solution is superior because it doesn't require host memory or CPU cycles (though it does consume host bandwidth capacity). But there are significant challenges to gaining proper cloud visibility to consider, including lack of legacy VM support (AWS only works with Nitro Hypervisor instances), no support for kubernetes and containers, lack of decryption capabilities and no packet replication - VPC Traffic Mirroring only makes one copy of packets and will only send that copy to one location. And of course, not mentioned, the high costs for full-time monitoring or that traffic mirroring is a low priority feature for their platform.

Companies are running into challenges with their cloud migrations, including:

- Virtualized blindspots and bottlenecks
- Having limited access to packet flows in the cloud
- Existing infrastructure based TAP/mirroring limitations
- Performance degradation
- Aggregation issues, pulling more data than they can handle
- Security risks

Solution: Provide Complete Cloud Visibility with Traffic Mirroring

Today's virtual architecture and applications will not tolerate devices creating traffic bottlenecks and blindspots. Part of the appeal of cloud networking is that you can quickly spin up a new environment to meet new demands. That kind of on-demand scale is great for business agility—but not as great for maintaining 100% traffic visibility.

Without total cloud visibility, you risk missing threats that are hidden inside good packet data. That's why, if you want to take advantage of cloud networking benefits, you need to continuously inspect traffic (both east-west and north-south) in these environments

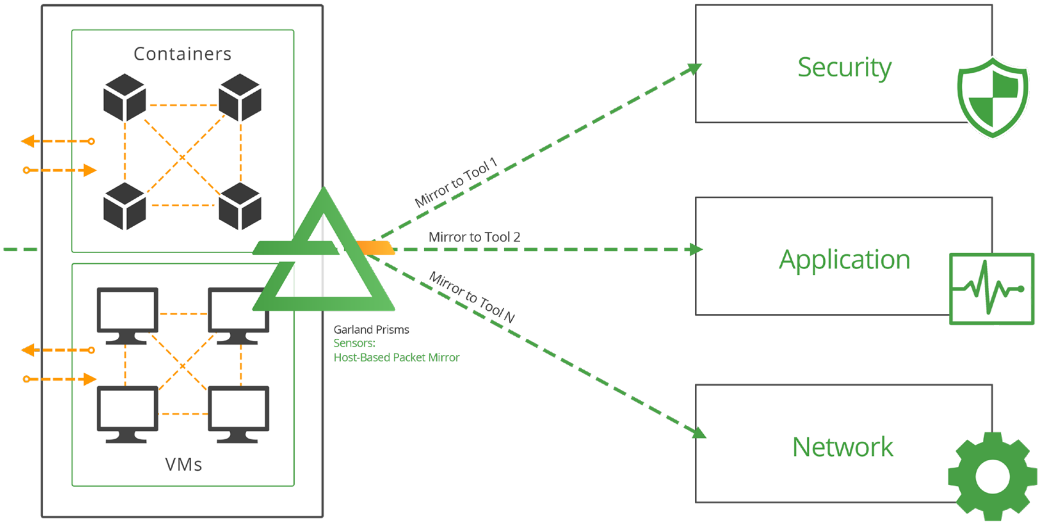


Diagram: Garland Prisms traffic mirroring

Like, their on-prem sibling (TAPs), out-of-band packet mirroring and decryption solutions like Garland Prisms, enables your network-based tools to see deeper into your modern compute environments, providing visibility into Kubernetes and cloud environments without impacting performance or architectures and without modifying your deployment architectures. Acquire traffic from your dynamic workloads, scaling with them so packets are never missed, helping you achieve true network traffic analysis visibility so that you can maintain control over your cloud environments. By guaranteeing 100% packet capture from your clouds, you're able to satisfy your virtualized security strategy

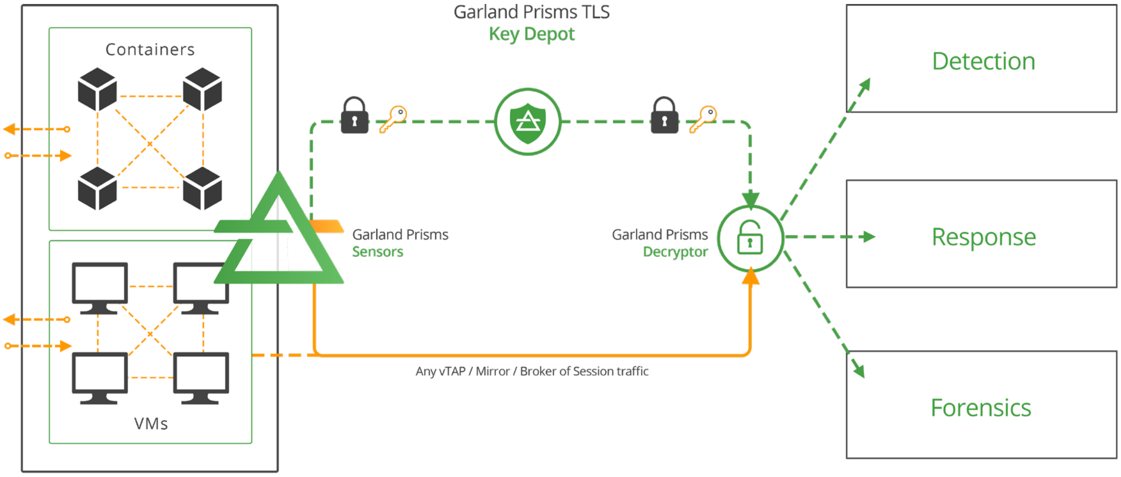


Diagram: Garland Prisms TLS Decryption

Garland Prisms' symmetric key discovery re-enables out-of-band decryption, designed to capture and decrypt traffic at cloud scale.

4. Lawful Intercept

Lawful Intercept (LI) is a term used to describe a scenario when a government Law Enforcement Agency (LEA) is granted the legal means to obtain communications network data pursuant to lawful authority for the purpose of analysis or evidence.

Challenges arise over how to provide certified forensics packet capture data. To ensure the quality of evidence, the agency has to adhere to specific regulations providing clear access to all data without any loss of information or impact on the network being monitored, while adhering to warrant parameters, including time span, types of communications, and many more.

In these cases a network packet capture utilizing SPAN will not hold up in court for these simple reasons:

- Monitoring tools may miss dropped packets due to SPAN port oversubscription
- Will not pass corrupt packets or errors (bad packets) and are dropped
- SPAN can change the timing of the frame interactions, altering response times
- The timestamps are can read different but the packet contents are the same
- Can duplicate packets if multiple VLANs are used.

Solution: Network TAPs Provide 100% Certified Data

Network TAPs pass every packet, including physical errors, supports jumbo frames and does not alter or duplicate packets. This provides a complete picture for the monitoring and security tools to complete analysis on this traffic. Network TAPs are CALEA (Commission on Accreditation for Law Enforcement Agencies) approved for use in Lawful Intercept cases for this reason.

Network TAPs ensures:

- 100% Full duplex packet capture, without loss, at full line rate
- Passes physical errors, supports jumbo frames
- No altered or duplicate packets
- No dropped packets
- CALEA approved

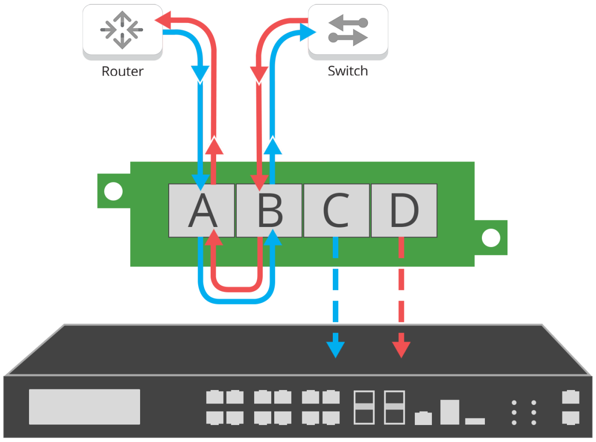


Diagram: Network TAP traffic

Solution: Look-back Forensics

For inline deployments, Garland's EdgeLens® Inline security packet brokers, not only offers bypass resilience but also additional use cases like "Look-back Forensics" which provides visibility to out-of-band packet capture, storage and analysis tools for inspecting the traffic from your inline IPS, Firewalls and WAFs tools. If active blocking failed to stop a threat, you have traffic storage for post breach forensics.

Look-back forensics ensures:

- 100% Full duplex packet capture, without loss, at full line rate
- Provide easy to correlate events generated by IPS/NGFW PCAP data
- Facilitate the time-critical workflow for security incident response.
- Enables forensic timelines of days/ weeks/months
- Extracted PCAP data may be presented as evidence in court as "chain of custody"

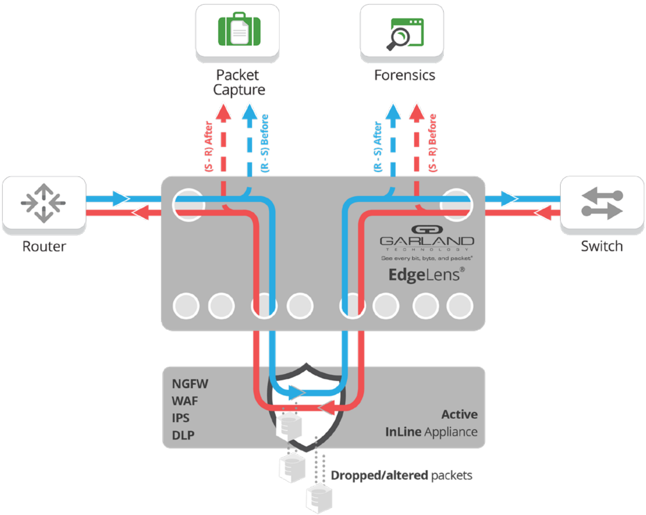


Diagram: Collecting out-of-band analysis from an inline link

Inline Security Threat Prevention

The term “inline” refers to network devices like routers, switches, and firewalls that are considered critical to the function of an enterprise network and are directly connected. Any failure or performance degradation of these devices typically results in dropped packets or errors in the computing programs and processes, leading to network downtime, which can turn into disruption of services, revenue loss or impacting the company reputation.

Inline tools are designed to protect these critical links and devices within the network. To do this, instead of passively analyzing copies of the data like out-of-band monitoring, these tools sit directly in the traffic to actively process original live data to block threats before they get to devices or other parts of the network.

NGFW

Firewalls typically sit at the front line of a network acting as a company’s main network connection to the outside world, this “critical link” acts as a liaison between devices in the network. The firewall is designed as a policy enforcer to prevent unauthorized access to data, ensuring network confidentiality. Only traffic defined by firewall policy is allowed on the network – any other traffic attempting to access is blocked. Next-Gen Firewall (NGFW) have additional features beyond a traditional firewall, such as IPS, Anti-virus, and URL filtering capabilities.

IPS

Intrusion Prevention System (IPS) is a network security and threat prevention technology, that provides real-time inspection of network traffic to detect and prevent threats. The IPS is designed to block break-in attempts that cause data theft, ensuring network integrity. Any suspicious or malicious packets are dropped from the live network stream.

WAF

While a firewall protects the network, a Web Application Firewall (WAF) protects web applications running on the servers by applying rules to HTTP traffic to protect against attacks like cross-site scripting and SQL injections. The WAF is a device designed to stop web-based application attacks.

SSL Decryptor

SSL Decryption is deployed inline to encrypt packets so that sensitive information cannot be gathered as it travels over the network or internet, protecting information like passwords, credit card information, bank account information, etc. In order for security tools to do their job, they need access to traffic in an unencrypted state.

DDoS

DDoS (Distributed Denial of Service) protection actively mitigates a targeted server or network from a distributed denial-of-service (DDoS) attack, ensuring network availability.

Top challenges many IT teams face with their inline security strategies are ensuring network uptime and availability, without creating single points of failure, as well as managing and maintaining the growing number of inline tools.

Inline security appliances sit either at the edge of a network or between network segments and inspect traffic. The network Edge is the specific boundary of WAN to LAN connectivity and ownership in a network. The Edge protects the critical assets of a corporation and is typically the demarcation point of local connectivity to wider Internet connectivity.

In today's modern IT security strategies — inline bypass TAPs and packet brokers are used to manage the availability of these inline security tools, safegauding the network from a SPOF, while ensure the performance, optimization and resilience.

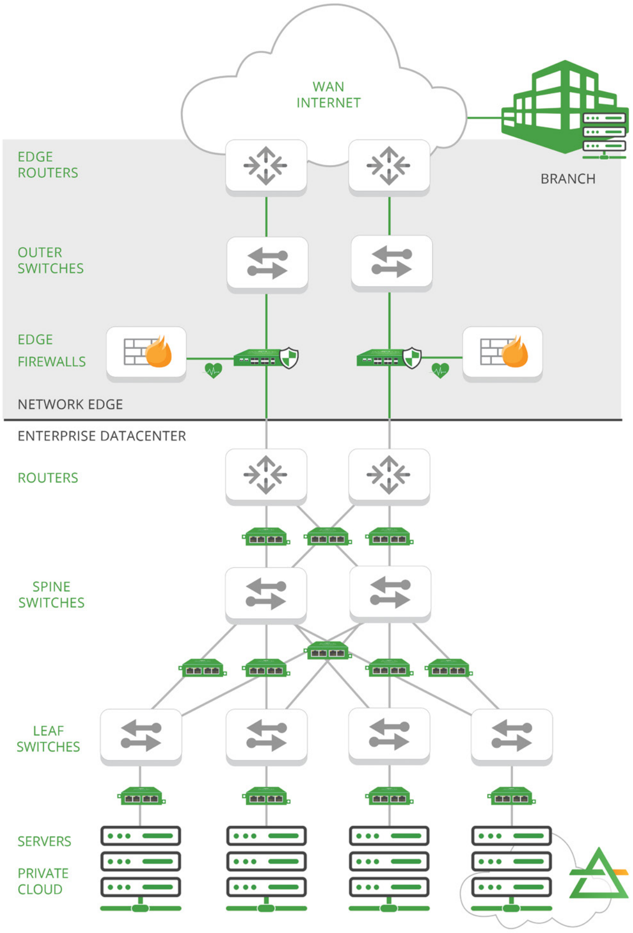


Diagram: Inline edge network topology

Use Cases: How to Improve Inline Security Deployments

1. Eliminate Single Points of Failure

Teams tasked with adding active blocking inline tools such as an IPS or firewall throughout their network on all critical links, want to ensure they aren't adding additional risk into their security strategy.

Because these Inline tools sit in the live network, the challenge of deploying these tools is to not create a possible single point of failure (SPOF) in the process. SPOFs arise if any of the inline tools become unavailable for any reason such as power loss, traffic congestion or degradation, software or processing errors, which will bring down the link or even the network.

The core challenge is that these inline security tools create a constant tug of war between network security and downtime. Deploying advanced security solutions to inspect and block threats in real time seems like an obvious component of network design. However, each tool you deploy on the live network circuit becomes a new single point of failure for your data center.

> ***“Extensive use of external bypass devices is a best practice. Organizations that are successful with inline security deployments were more likely (55%) to deploy external bypass devices everywhere.***
>
> *- EMA [Enterprise Management Associates]*

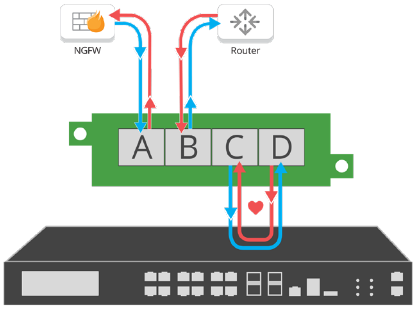
Solution: Inline Bypass

When architecting inline security tools into your network, incorporating bypass and failsafe technology together with network redundancy are three fundamental best practices to avoid costly network downtime, eliminating single points of failure in your network.

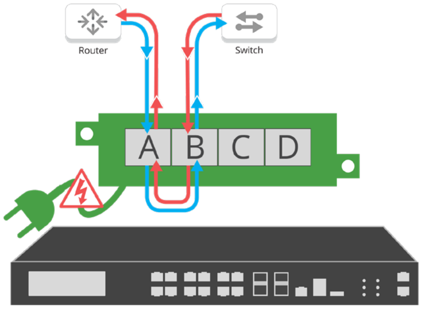
Incorporating a bypass TAP provides the ability to manage your inline tool any time without having to take down the network or impact business availability for maintenance or upgrades — ensuring this inline security tool is not a point of failure in the network.

In the case of a failure, a bypass TAP offers flexibility to either bypass the tool and keep the network up, failover to a redundant link, or leverage an HA solution.

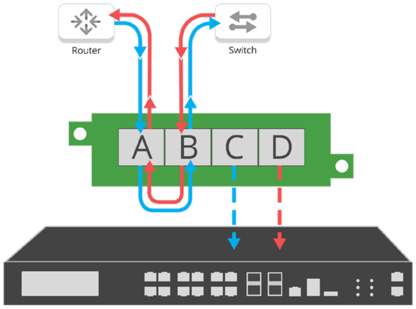
Bypass TAPs offer the flexability to take the tool in and out-of-band as shown here:



Inline Bypass Heartbeats



Failsafe - Power Loss



Out-of-band Breakout TAP

Inline Bypass provides:

- Failsafe deployment of inline tools
- Configurable security tool heartbeats
- Eliminates single points of failure within your network
- Reduce network downtime, with inline lifecycle management
- Operation isolation and tool sandboxing (updates, installing patches, maintenance or troubleshooting)
- No maintenance windows
- High availability (HA) inline deployments adds additional layers of resiliency and reliability

2. Reduce Network Downtime

As inline security devices sit between network segments, managing the risk of downtime is a critical consideration when deploying security tools. Downtime, whether planned or unplanned, can not only impact the functionality of the network but also impacts availability and lost revenue to the company. When deploying inline security tools, security teams commonly face:

- Oversubscribed devices, degrade network performance
- Device failures can bring down the network
- Deploying new technologies into the network
- Scheduling off hour planned downtime for deployments, maintenance and troubleshooting

Solution: Inline Bypass

Bypass functionality is essential to preventing inline security devices from causing network performance degradations and downtime. Many appliances have internal bypass capability, but external bypass devices are considered more reliable and offer more features. Extensive use of external bypass devices is a best practice.

Bypass TAP “inline lifecycle management” allows you to easily take tools out-of-band for updates, installing patches, maintenance or troubleshooting to optimize and validate before pushing back inline, offering:

- Administrative isolation - No maintenance windows
- Deployment efficiency - Extend the reach of the same tools into multiple network segments, when used in conjunction with a network packet broker.
- Tool Sandbox - Pilot or deploy new tools

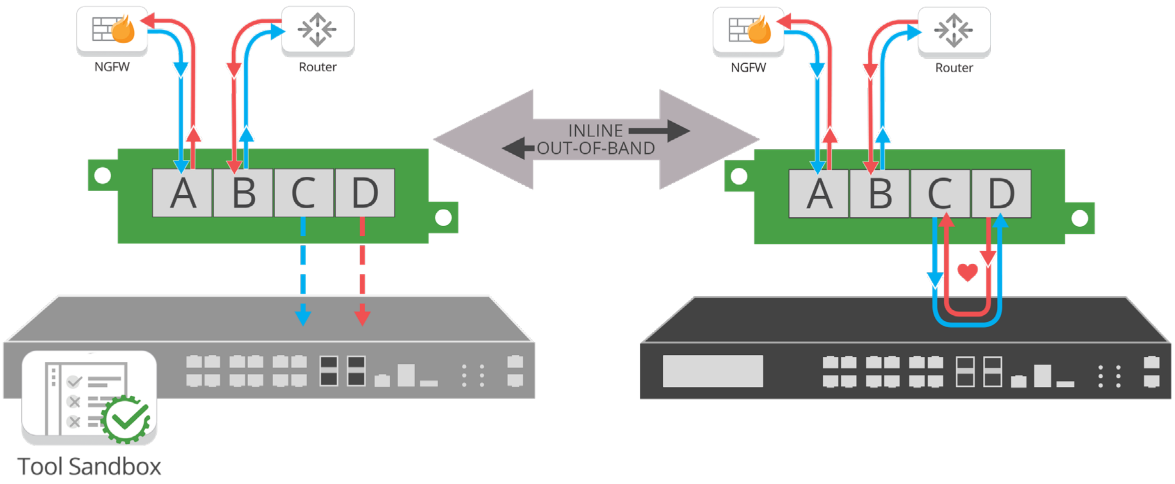


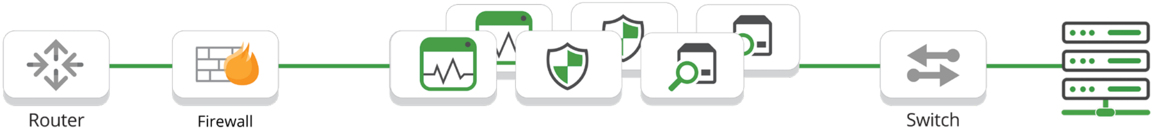
Diagram: Sandbox deployment - left show the out-of-band traffic flow and the right inline flow

In the tense moments of unplanned downtime, a bypass TAP provides expedited MTTR, or problem resolution in the event of a tool failure. By not impacting the overall availability of the connected network, administrators can focus on fixing the tool rather than having to manage the related symptom. A bypass TAP offers flexibility to bypass the tool and keep the network up, failover to a redundant link, or leverage an HA solution, including:

- Operational isolation - Expedited problem resolution of unplanned downtime without impacting general network connectivity
- Network resilience - Flexibility to bypass the tool and keep the network up, or to failover to a High Availability [HA] solution

3. Managing Mulitple Inline Tools

SecOps teams are now tasked with deploying and managing a growing list of security tools, including SIEM, logging, IPS, DDOS, encryption, firewalls, web application firewall and threat detection. How do these teams deploy and manage multiple inline tools all without creating multiple points of failure?



Solution: Inline Tool Chaining

Teams managing mulitple security solutions need an easy way to connect all of their inline and out-of-band tools, so they can effectively keep the network up and running but secure at the same time.

Chaining allows you to pass traffic through multiple inline tools, while being able to independently monitor the health of each inline tool with bypass heartbeats. In the case of failed heartbeats, you can manually or automatically move your inline device out-of-band to manage, update or optimize.

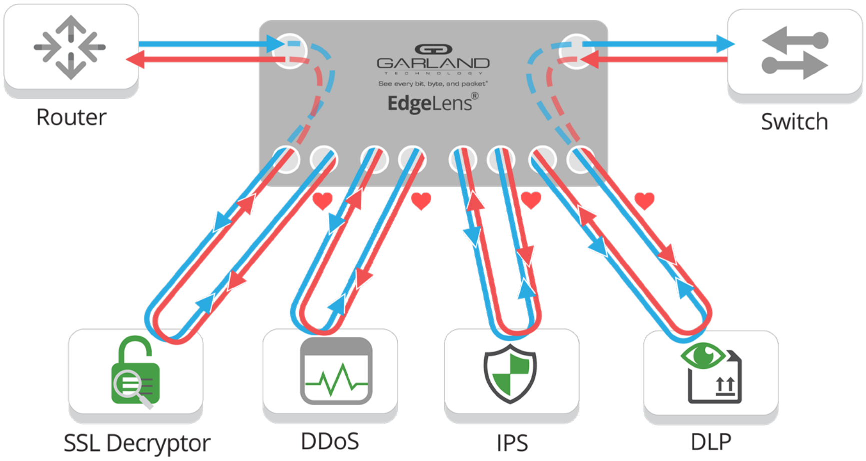
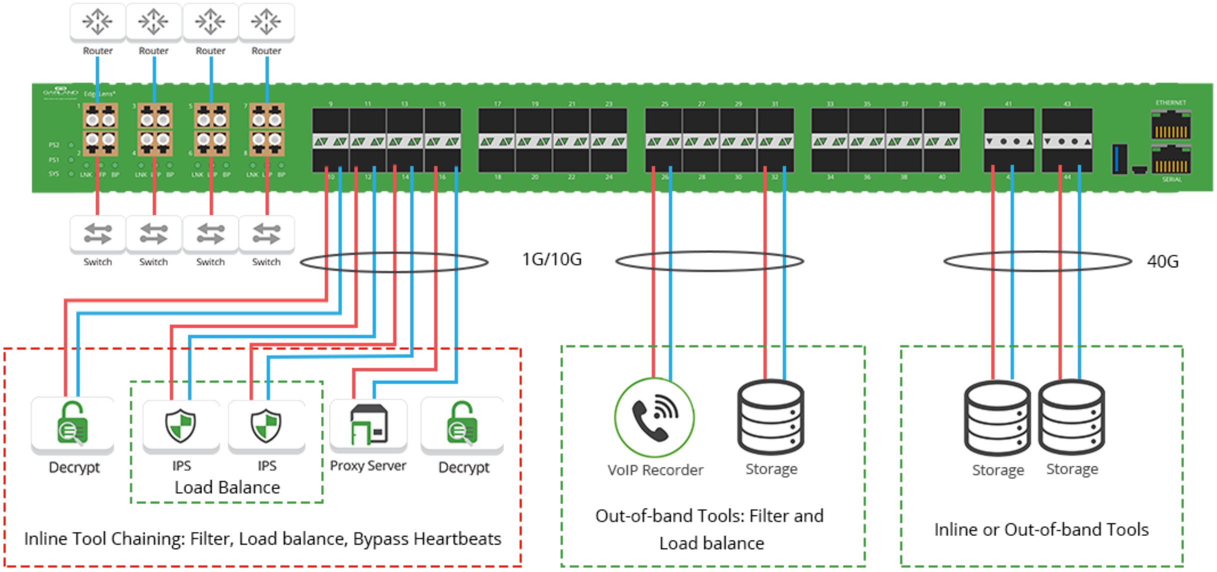


Diagram: Tool chaining concept

Garland's EdgeLens® line of bypass TAP packet broker hybrids, provides an easy, hardware base chaining solution, that allows you to plug and play multiple inline and out-of-band tools between multiple network segments. If one of the tools in the chain can't keep up, load balance to the other tools 1:1 or 1:N tools.

Bypass TAP "inline lifecycle management" allows you to easily take tools out-of-band for updates, installing patches, maintenance or troubleshooting to optimize and validate before pushing back inline.



Diagrams: An example of tool chaining with the EdgeLens

4. Optimize Inline Tool Performance

After a data breach, it is vital for a security team to be able to review what happen and reduce overall MTTR after such incidents.

Mean time to repair / resolution (MTTR) is a measure of troubleshooting as the average time required to repair a failed component or device. Higher MTTRs means that more time and resources are taken for the network to recover from a problem, while a lower MTTR reflects the better off a business network may be.

IT Teams may have IPS and firewalls deployed and think they are blocking any potential threats. Inevitably the network is still attacked and breached. Was it the security tool? Could it have responded better? Many teams are lacking the ability to trouble-shoot if their IPS or firewall was configured properly and to address how it missed the breach.

Solution: Before and After Optimization & Validation

Adding packet capture and storage capabilities to your inline deployment, provides the next evolution of active blocking. If you experience a breach, now you have data for historical look-back built-in, for look back forensics or before and after optimization.

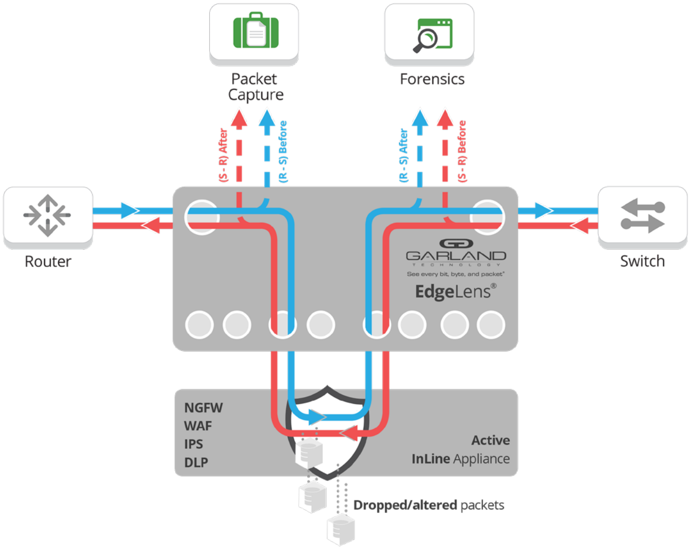
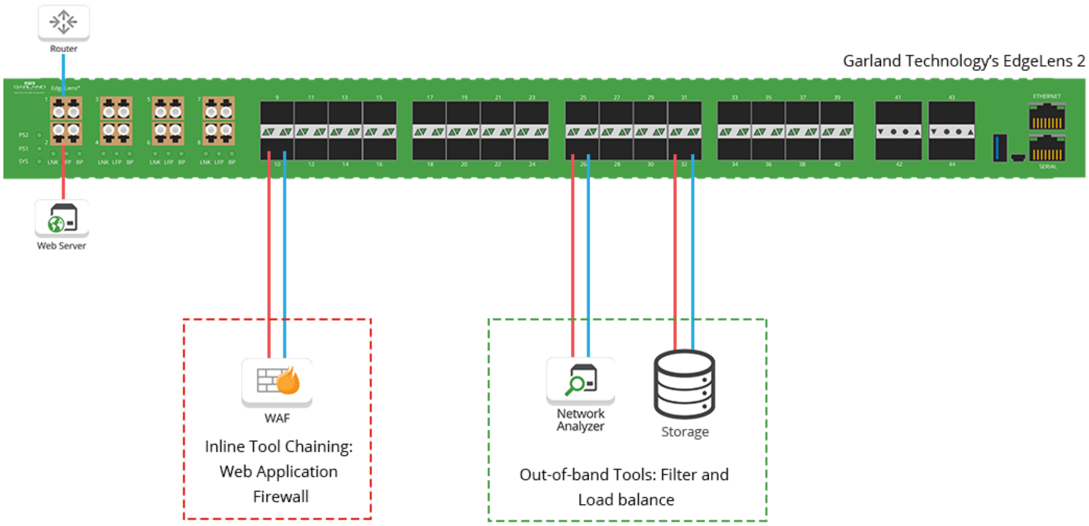


Diagram: Collecting traffic before and after the inline tool for optimization and analysis

Analyze packet data before and after your inline device to ensure optimal tool performance to validate any updates or troubleshoot why threats weren't blocked.


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

Diagrams: An example of historical look-back with the EdgeLens

Garland's EdgeLens® line of bypass TAP packet broker hybrids, provides visibility to out-of-band packet capture, storage and analysis tools the traffic from your inline IPS, Firewalls and WAFs. Capturing traffic before it goes into the inline tool and after, allows you to send both copies of data to out-of-band packet capture, storage and analysis tools. This solution allows you to analyze your inline device to see if it is configured properly or if it may be missing the threat.

- Provide easy to correlate events generated by IPS/NGFW PCAP data
- Enable real-time security proof-of-concept evaluations without impacting the network
- Validate changes or updates that your tool is configured properly
- Increase efficiency of inline and out-of-band tools
- Reduce network downtime, with inline lifecycle management

5. Redundant Security Solutions

IT Teams may follow all the standard industy best pacties, incorporating inline bypass and failsafe technology, but for some industries it isn't enough. The finacial and banking industries have to ensure sensitive user data isn't compromised while providing a flawless user experience. So network downtime is not an option.

Network redundancy is a strategy where additional or alternate network devices are installed within network infrastructure, ensuring network availability in the case of a network device or path failure or unavailability.

Enterprise IT teams are often tasked with architecting redundant designs for their critical network links to combat this issue, while looking for the best way to effectively deploy and update these tools effectively, without creating a single point of failure for each device.

Solution: High Availability (HA) Deployments

High availability (HA) inline bypass TAP deployments add additional layers of resiliency and reliability. In an HA scenario, when the primary link goes down, traffic can automatically be triggered to a secondary tool or redundant link.

Garland offers two options for incorporating High Availability (HA) solutions into your network, Active/Standby and Active/Active. Active Standby (Or Active/Passive) deploys to a secondary tool, providing failover from primary device to backup appliance. The Active/Active Crossfire design incorporates a secondary bypass TAP, tool and redundant link, providing the ultimate failover if either active device fails.

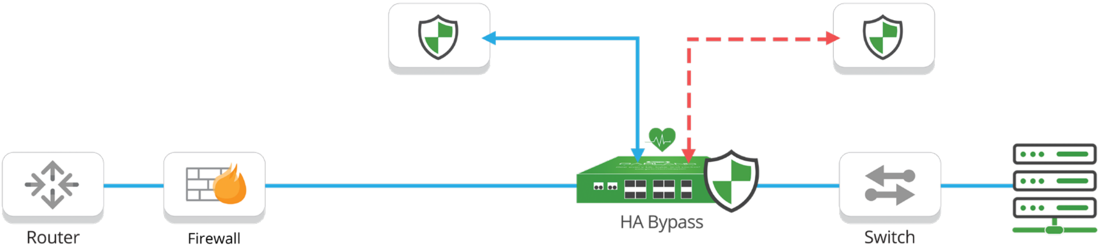


Diagram: Active/Passive HA solution provides failover from primary tool to backup tool

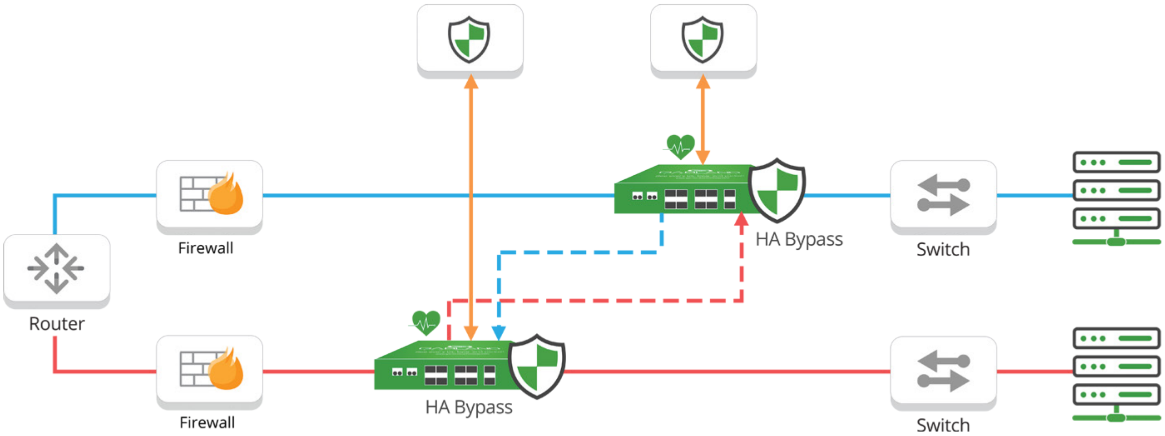
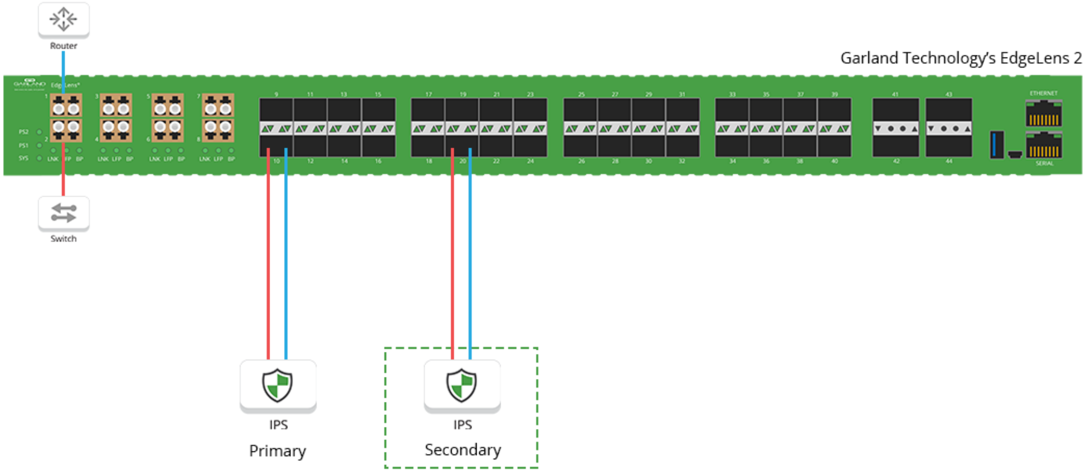


Diagram: Active/Active Crossfire HA provides failover if either active tool fails.



Diagrams: An example of active/passive HA deployment with the EdgeLens

Instead of relying on a single bypass TAP for each device, Garland has specifically designed HA Bypass TAPs and Inline Security Packet Brokers that not only provide the same reliability and management controls of a standard bypass, but also provide the ability to manage multiple inline and out-of-band tools from the same device with packet broker functionality.

Simplify Your Entire Security Stack

Today's security strategies incorporate both inline and out-of-band solutions, with a suite of active blocking and passive monitoring tools. Many security teams are looking for ways to future proof their network ahead of the Edge explosion by architecting remote locations and data centers with purpose-built inline bypass, packet broker and cloud visibility solutions, which provide the resiliency and performance your tools need to ensure these segments are secure and scalable.

Garland Technology's full line of inline bypass TAPs and packet brokers are designed to simplify modern security stacks, with the first integrated bypass family to handle your entire security strategy - from remote sites, data center and enterprise.

Setting Yourself Up for IT Security Success

Looking to add inline or out-of-band security monitoring solutions, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do.

[1] -https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses