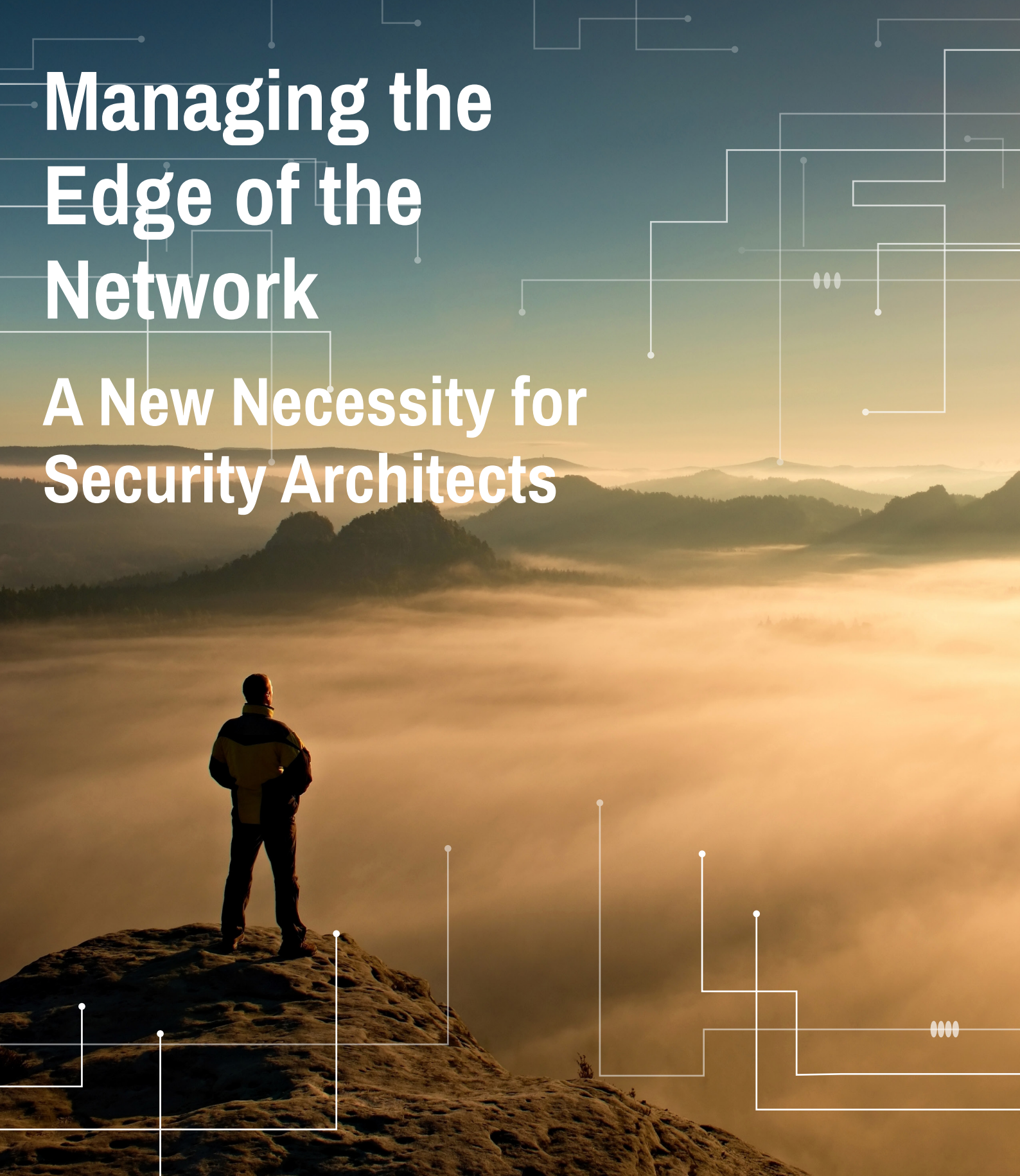


Managing the Edge of the Network

A New Necessity for Security Architects




GARLAND
T E C H N O L O G Y
See every bit, byte, and packet®

Introduction

The Evolution of Enterprise Network Security

For networking professionals who have been around since the early 1990s when firewalls first came into play, there's an understanding that there were certainly simpler days of cyber security. In fact, back then there were very few network security engineers, let alone the security architects that exist today.

For network security engineers in the 1990s, threats were weak enough and traffic demands were low enough that they could simply pull the plug on the network, taking it down entirely to troubleshoot. At that time, networking professionals were focused on building up the network core to improve packet forwarding—managing the edge of the network wasn't even a thought.

The new networking reality is a hybrid network supporting internal business apps and cloud-based solutions—all of which function at the network's edge.

With cyber attackers becoming increasingly sophisticated, security architects are tasked with bolstering network edge defenses with in-line appliances.

Early iterations of firewalls were simply placed on the live wire to capture traffic data; but networks no longer consist of just a primary link with a secondary link positioned for any necessary support. Instead, security architects must contend with multiple links and load balance accordingly. Having so many links connected at the edge of the network has caused the cyber security challenges that exist today and has left security architects with multiple pressing questions:



- How do I connect more than one tool at the edge?
- How do I access data at the edge?
- How do I distinguish between in-line and out-of-band connectivity?
- How do I manage my day-to-day traffic?
- How do I install multiple devices and manage them individually?

In addition to these barriers to modern network security, security architects must ensure protection without sacrificing any uptime. According to [recent research from Ponemon Institute](#), the average cost of an unplanned data center outage is almost \$9,000 per minute. The demand of 100% network uptime, security architects are turning to bypass network TAPs to manage their inline device(s) which allows for simple, flip of a switch ability to take an active inline device and make it out-of-band for maintenance and trouble-shooting, while still providing 100% network uptime.

This is a successful strategy when tapping 1 or 2 links, but there are multiple tapping scenarios that security architects must understand to properly meet the demands of their environments.

Challenges When Deploying Many In-Line Security Appliances

Network security has evolved to a point that companies have a somewhat standard set of in-line security appliances that go beyond basic firewalls. These appliances include: next-gen firewalls, denial of service protection, data leakage prevention, intrusion prevention systems, compliance systems, web application firewalls, SSL encryption, network monitoring forensics and more.

While these in-line security appliances have become all but necessities for protection, there is still reluctance on the part of security architects to deploy the full stack. Some of the more debilitating challenges that keep security architects from deploying so many in-line appliances include:

1

The Silo Issue: Today's network trends are all about breaking down silos for greater efficiency, but as in-line security appliances are deployed they can become silos themselves. As links are routed to specific appliances, improper deployment can lead to segmentation that leads to a disconnected security stack.

2

The Possibility of Network Outages: Security architects face challenges from two perspectives. On the one hand, not deploying the necessary set of in-line security appliances can result in network outages due to data breaches. However, without proper deployment, in-line security appliances can quickly become points of failure in the network. With such focus placed on network uptime, network outage concerns can often seem insurmountable.

3

Deployment Complexity: When security architects must deploy in-line security appliances into an enterprise network that was designed years ago, it can be difficult to determine proper and efficient placement.

4

In-Line Security Appliances Require Many Ports: Many security architects turn to SPAN ports to connect in-line security appliances. However, there are only so many SPAN ports for connectivity and they can easily be overwhelmed by traffic demands. Without a support system of network TAPs, it's nearly impossible to meet the port needs of all in-line security appliances.

All of these challenges exist within the controlled environment of a single enterprise network. However, the new reality for many large enterprises is an increasing number of branch offices and remote sites.

With the number of cyber attacks increasing exponentially each year, security architects must find an effective way to deploy these in-line security appliances and manage the edge of the network—both locally and remotely.

Chaining the Edge—What Today's Network Visibility Should Look Like


Previous white papers and articles have discussed the inefficiencies of [SPAN](#) ports for network visibility and security appliance connectivity; but security architects need a more concrete answer to network edge management questions.


To overcome the glaring in-line security appliance and network edge management challenges, security architects must turn to chaining for proper deployment. Chaining (aka daisy-chaining) is a simple concept—a wiring scheme in which multiple devices are wired together in a sequence or ring. In the active, in-line security device world, it is also the process of chaining all security appliances into a single unified layer of visibility created by a network packet broker (NPB).


NPB's are equipped with various specifications, including network speed, number of monitoring/security ports, and media management options. What defines a NPB is the ability to connect multiple in-line or out-of-band devices with the functionality to aggregate, filter, regenerate and load balancing to the appliances it serves. When we talk about managing the edge, the NPB's have an additional requirement of monitoring the health of the active, in-line devices with a failsafe feature.





With this layer mediating between the actual in-line appliances and the flow of network traffic, security architects can achieve the necessary level of edge protection and management without worrying about single points of failure or port mismanagement. In a modern, hybrid network supporting internal business apps and cloud solutions, this is how network visibility with chaining the edge should work:

- 

Traffic flows from internet to the internal network where it is copied by the NPB
- 

The NPB then routes packets through the chain of in-line security appliances. The security devices can see all the data—every bit, byte, and packet[®]—or rule-based filters can be applied for specific tools.
- 

Visibility both before the in-line appliances and after them allows security architects to compare packets at both ends to spot any deviations from baseline expectations.
- 

Copies of the network traffic are sent to connected out-of-band monitoring solutions for forensics.
- 

When all security and monitoring tools have played their parts, traffic flows back to the NPB and is sent to its final destination in the network core.

Having a layer of visibility separating in-line security appliances from the live wire means security architects can spot any performance issues and troubleshoot without disrupting the flow of traffic. Because uptime is so important for modern enterprises, the chaining approach to security architecture is essential to efficiency and appliance effectiveness.

Security architects in companies of all sizes face the same in-line security appliance challenges; but that doesn't mean there is a one-size-fits-all solution for implementing the NPBs that are necessary for visibility. Depending on individual network specifications, there are different solutions for managing the edge of the network.

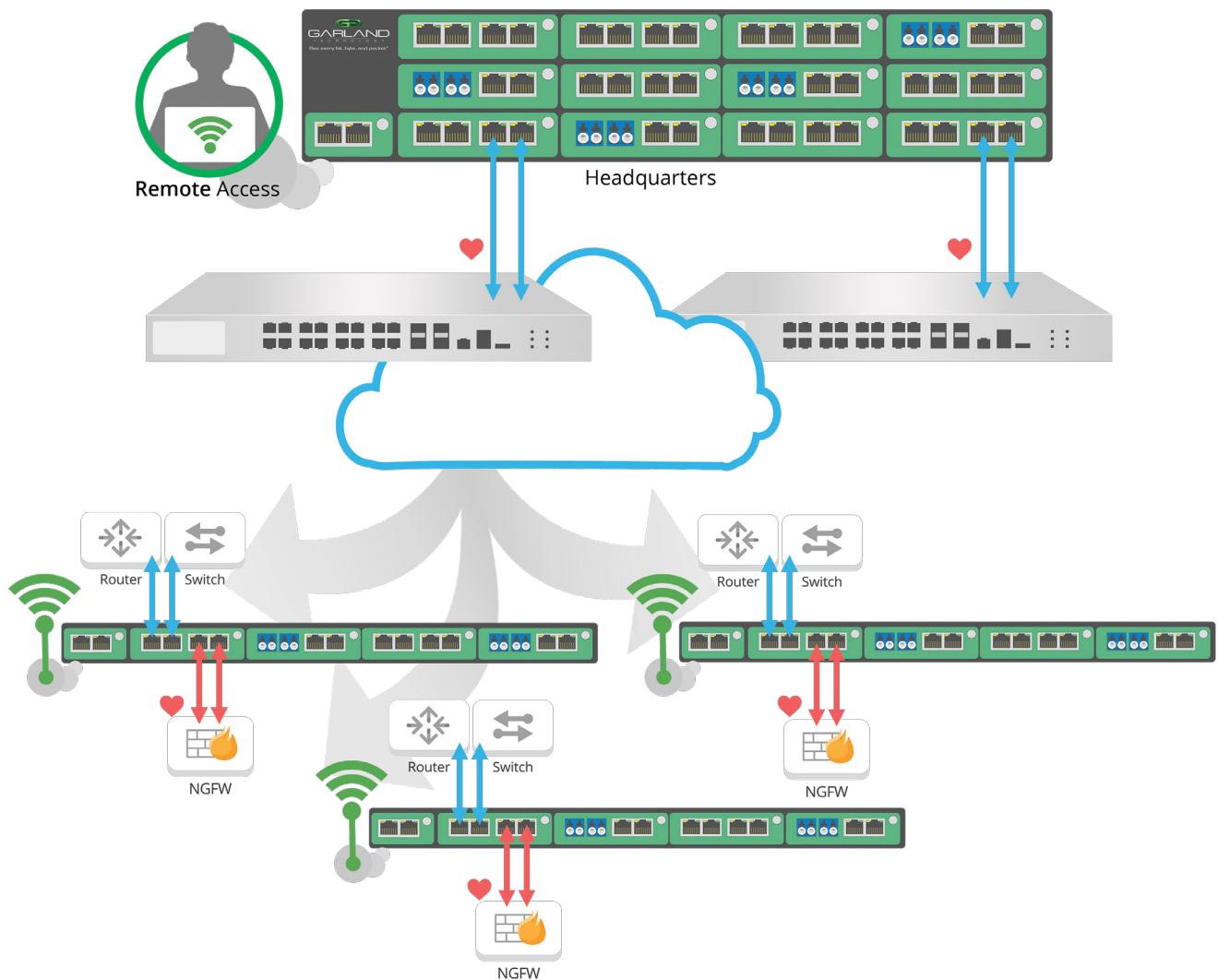
Four Common In-Line Security Appliance Tapping Scenarios

There are NPB solutions available for a wide range of in-line security appliance connectivity needs. Whether the environment is a small business with one or two in-line appliances or a massive enterprise operating at advanced network speeds, security architects must choose an approach appropriate for their network needs today and tomorrow.

Four common scenarios include:

- The 1G Data Center Solution with Remote Site Management
- A High Availability (HA) solution
- A 10G Chaining the Edge with Media Conversion
- The EdgeLens - Advanced Edge Management

1G Data Center with Remote Site Management Solution

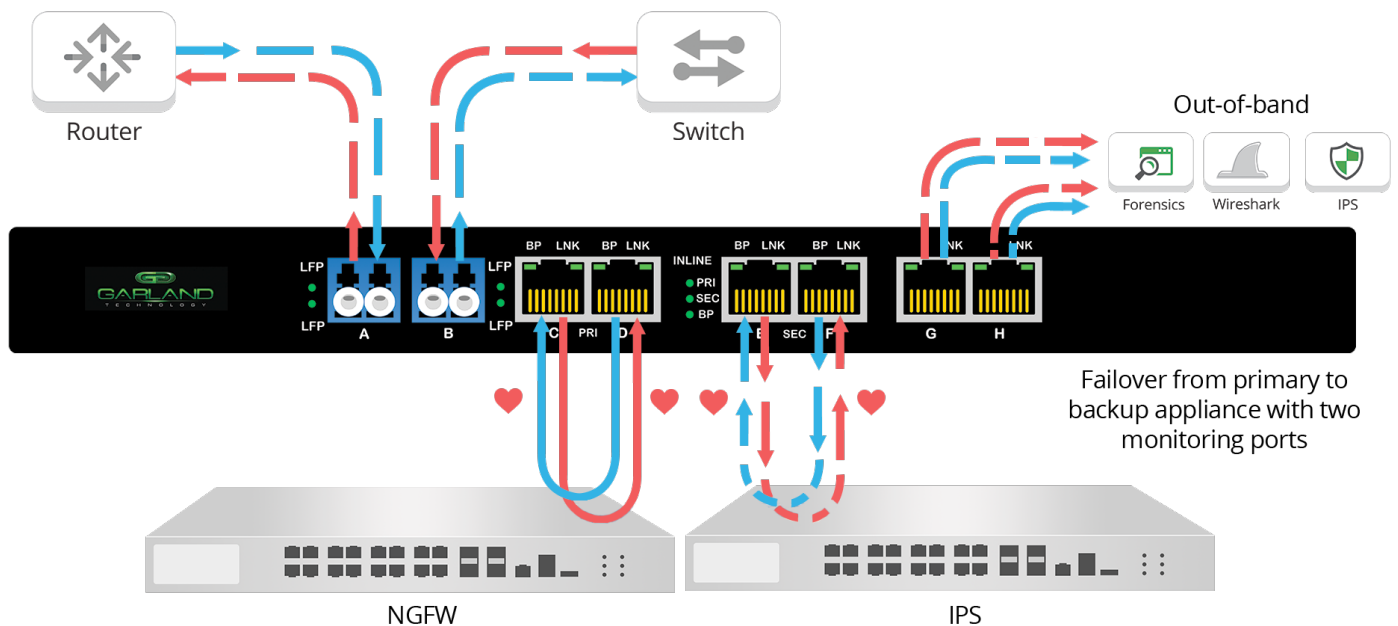


This is a common solution for data center deployments with remote site management (retail, banking, etc.). The data center houses two in-line, active security appliances. The remote sites, connected via the cloud, require their own two in-line, active security appliances.

Benefits of this solution include:

- Scalability: Add modular TAPs when required
- 1G Media Conversion—copper to fiber
- Remote management via GUI or CLI

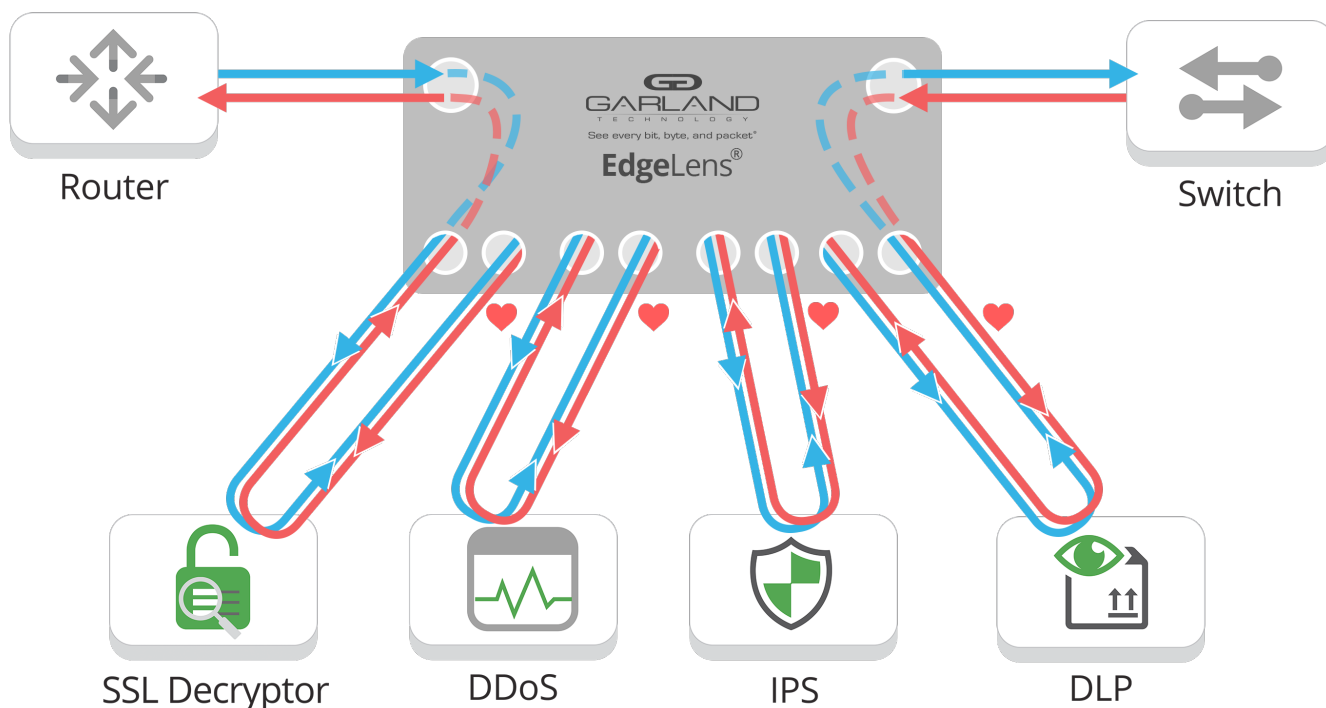
High Availability Solution



This solution again offers a single bypass TAP that can support two in-line security appliances; however, it is specifically designed for high availability environments.

With failover functionality from a primary device to a backup appliance and two monitoring ports, the High Availability Solution offers failsafe protection for firewalls, IPSs, DLP, web content filters and more.

10G Chaining the Edge: Support Up to 4 Active, In-Line Devices

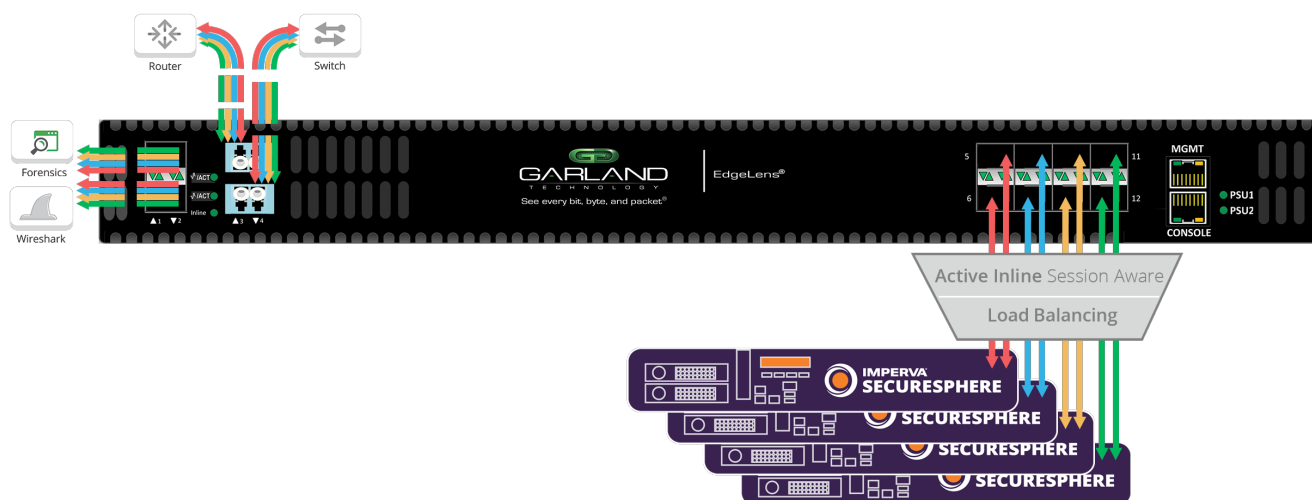


This solution is geared more toward security architects that must support high-traffic organizations (for example, retail or financial services companies). The solution monitors four in-line security appliances and maintains the failover assurance that large enterprises require.

With a flexible 1U design, security architects can mix and match fiber and deploy up to four bypass TAPs.

While these solutions offer the functionality and flexibility that security architects require, there is still demand for a more efficient way to direct traffic from an ever-growing chain of in-line security appliances. This is where the EdgeLens®, a hybrid bypass TAP with packet broker capabilities, comes into play for enterprise security architects.

EdgeLens—How Security Architects Can Meet Advanced Edge Management Needs



The EdgeLens is the solution for security architects tasked with managing multiple in-line security appliances and load balancing to support increasing bandwidth demands. As a hybrid bypass TAP and packet broker in one, EdgeLens offers one 10G TAP and eight monitoring ports. This enables security architects to filter, aggregate and load balance the in-line data stream of security appliances and monitoring solutions in up to 12 ports.

With EdgeLens, security architects are free to tap a 10G circuit and filter it for separate 1G appliances. This is a cost effective way to attach multiple devices through a single network TAP—all within a 1U chassis for data center efficiency.

In this example, we highlight our technology partner Imperva with load balancing four in-line WAF's at the network's edge. The EdgeLens has one or four 1G/10G TAPs that can filter, aggregate and load balance up to four 1G/10G inline security devices.

Consider the following benefits of chaining the edge with the EdgeLens:



Gain intelligent and optimized packet visibility and access to both in-line and out-of-band security/monitoring tools.



Enable real-time security proof-of-concept evaluations without impacting the network



Shield monitoring devices from cyber attackers



Increase efficiency of in-line and out-of-band tools by ensuring 100% traffic visibility

Security architects are under tremendous pressure to manage the edge of the network, defending the valuable core from increased cyber threats. The more typical tapping scenarios offer flexibility, but the EdgeLens is the all-in-one solution for security architects looking to achieve an effective chaining approach.

If you want to learn more about how you can manage the edge of the network with the EdgeLens, contact Garland Technology today for a Design-IT consultation to discuss a security design tailored specifically to your needs.

Garland Technology is all about connections – connecting your network to your appliance, connecting your data to your IT team, and reconnecting you to your core business. It's all about better network design. Choose from full line of access products: a network TAPs that supports aggregation, filtering, regeneration, bypass and breakout modes; packet brokering products; and cables and pluggables. We want to help you avoid introducing additional software, points of failure and bulk into your network. Garland's hardware solutions let you **see every bit, byte, and packet®** in your network.

Contact

Sales, quotations, product inquiries:
sales@garlandtechnology.com

Garland Technology, LLC.
New York | Texas | Germany

Copyright © 2016 Garland Technology. All rights reserved.