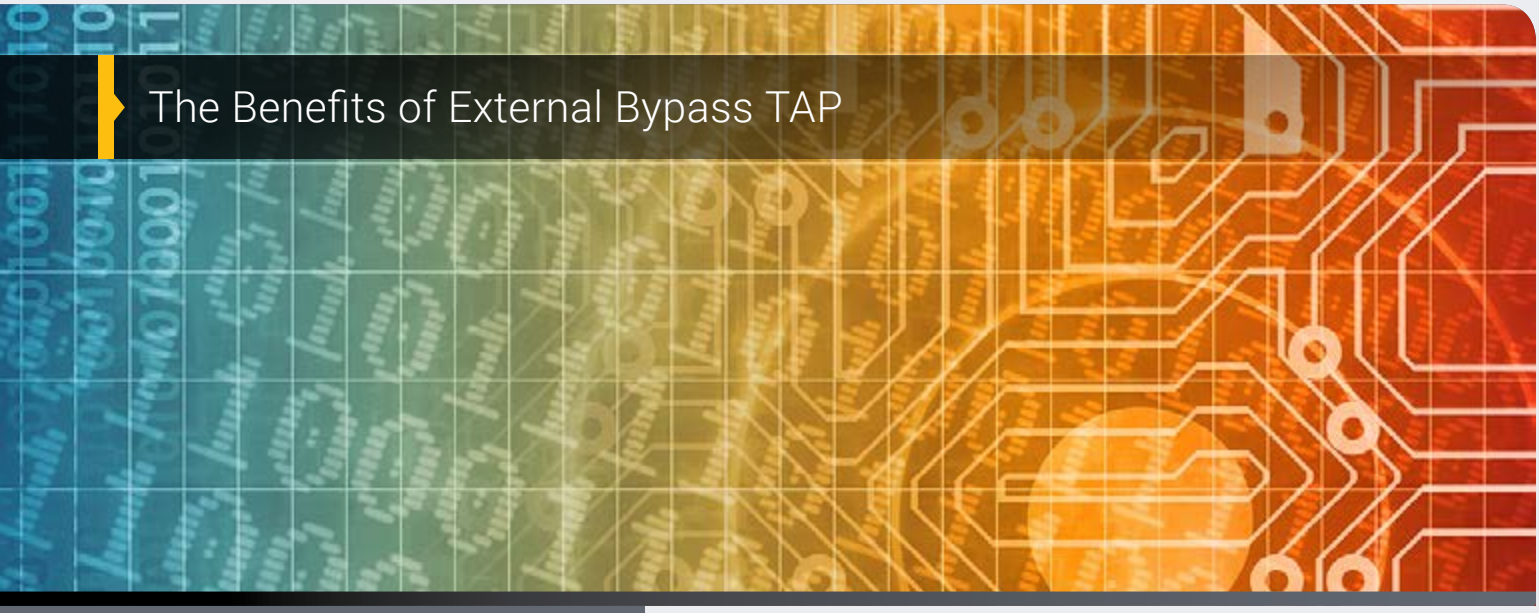
Layer Network Security with High Availability



Summary

Industry: Large Enterprise

Challenge:
- Deploying multiple security systems
- Ensure high network availability
- Simplify maintenance

APCON Monitoring Solution:
- IntellaFlex Bypass TAPs, optical and copper options
- TitanXR and Mobile App (optional)

Benefits:
- Keeps the network operational
- Security system heartbeat with failover
- Simplify offline maintenance
- Load balancing and redundancy
- Network visibility for offline tools
- Modular migration and services
- Central management and alerts

A bypass TAP or switch monitors inline security systems to keep the network alive at all times.

To combat the many types of network threats, enterprises have added layers of security protection utilizing multiple defenses including firewalls, intrusion protection (IPS), data loss prevention (DLP), flow analytics, advanced threat protection, flow analytics, application control, and filtering.

While the idea of a single system that provides every type of border protection may seem attractive, most often utopia systems don't provide all the types of protection or may not be best of breed in some areas. The reality is enterprises often deploy multiple layers of security protection including best of breed devices.

Enterprise network availability is critical, and outages can have profound business impact. Adding layers of advanced complex security systems clearly adds risk to network performance and increases potential of network outages and maintenance requirements.

How can enterprises maintain high network availability while deploying layers of security? Answer: use a Bypass TAP.

Security System Heartbeat with Failover

Critical networks must continue operation even if a security layer goes offline. A bypass TAP monitors a security system's health using heartbeat packets that confirm the security device is passing traffic normally, and will automatically bypass security systems that go offline or are performing poorly. This prevents a network outage and continues normal operation. Network engineers are alerted of a system bypass, enabling them to resolve the issue offline, and re-insert the security system when ready.

Security systems can be complex, constantly monitoring traffic for threats, and may themselves be under attack. They often have more software updates than most network equipment, and may be more actively changed with policy updates or application control. With this level of complexity, software updates and configuration changes – it's not a matter if network outages or performance issues will occur, but when. A bypass TAP protects network operations by bypassing non-performing systems.

External Bypass TAP vs Internal Bypass

Some security systems offer an internal bypass option, however there are advantages to using external bypass TAPs.

Increased reliability: while an internal bypass may work for power failure or hard crash, assuming that a failing or poorly performing security system can effectively monitor it's own health while it's failing is problematic. An external bypass TAP provides independent health monitoring, including heartbeat checks, to proactively bypass under-performing systems and notify operations of issues.

Layered tools: an internal bypass is typically per device, therefore layered security would require purchase of internal bypass for every system, each working independently.

Advanced features: external bypass TAPs may offer advanced features such as load balancing, tool redundancy, expansion options, traffic filtering, network monitoring and other advanced features.

Tool changes: external bypass TAPs provide an easy option for tool changes, allowing for systems to be taken offline to replace tools without network impact.

Cost effective: An external bypass TAP is often more cost efficient and provides a consistent protection architecture compared to purchasing internal bypass over multiple security tools. And security systems can change over time which could require the repurchase of the internal bypass option.

Simplify Maintenance

The combination of complex software systems and evolving security threats results in constant updates and maintenance. The external bypass TAP enables network engineers to switch security systems offline to replace the system or to apply software or policy configuration updates. Returning to normal operations requires only the click of a mouse. This enables engineers to do security system updates during normal production hours versus off-hour maintenance windows. And it enables engineers to test new security tools, or move a security device to a hot spot in another part of the network.

Load Balancing and Redundancy

Security systems analyze traffic for security threats in real time, which can be processor-intensive. Not all security systems can keep up with line rate 10 Gbps traffic.

Premium bypass devices can distribute traffic across multiple security devices, enabling lower speed tools to secure a higher speed network. For example, three IPS systems with 4 Gbps capacity can monitor a 10 Gbps network.

Load balancing not only enables load sharing across multiple tools, it also can provide redundancy. In the example above, if one IPS fails the two remaining systems will support 8 Gbps, keeping the network running with IPS security at near-capacity speeds.

Network Visibility

In addition to inline production security protection, out-of-band monitoring for security forensics, network and application performance is an important part of a security architecture.

The WAN or Internet access network is an ideal location to see all traffic going in and out of the network. Premium bypass devices can include network visibility ports for out-of-band monitoring tools.

Network monitoring ports may include traffic aggregation, port tagging, and filtering capabilities. And modular systems may be able to add deduplication, time stamping, protocol stripping and payload removal. These features can significantly increase monitoring tool efficiency. Plus this visibility solution can be combined with the overall enterprise and data center monitoring architecture, utilizing the same diagnostic tools, staff and procedures.

RESOURCES

The IntellaFlex Bypass TAPs keep traffic moving when security systems go off line or perform poorly. With copper and optical connectivity options, APCON's Bypass TAPs provide a premium feature set as described in this paper. For more information, contact apcon.com or your local reseller.

DATASHEETS

IntellaFlex Copper Bypass TAP Appliance

IntellaFlex Optical Bypass TAP

Migration and Flexibility

Low-end bypass devices may be fixed to 1G or 10G rates, and require purchase of new hardware to change systems to higher speeds.

Premium bypass devices include 1G/10G flexibility, enabling independent migration of port speeds on routers, switches and security equipment. Two examples:

1. The incoming WAN uses 1G Ethernet today, but a new security device supports a 10G port with 3 Gbps performance. The bypass device should be able to support 1G bypass ports and 10G security devices.
2. The incoming Internet Service is 500Mbps on a 1G Router port, but to reduce latency the internal router and switch ports are 10G optical interfaces. The bypass device should allow a 10G bypass port to be used in conjunction with 1G security tools, or in a layered environment there may be a mix of 1G/10G devices.

The software selectable 1G or 10G bypass, appliance and monitoring ports enable network engineers to mix and match to meet current traffic engineering needs, and it simplifies equipment migration as network needs grow.

Modularity and Advanced Services

Modular network bypass TAPs can meet both your current layered security needs and also provide growth options for the future including ability to add more bypass ports and high capacity, high speed monitoring ports. With integration into a complete network visibility solution, additional filtering features become available such as deduplication, time stamping, and protocol stripping.

There may be a range of advanced service options. Add an all-in-one monitoring appliance with virtual environment to test new monitoring applications. Or add NetFlow/IPFIX for overall network management systems.

Versatile Management and Alerts

Security system protection and network monitoring are critical parts of the network, and should include an easy-to-use central management interface with graphical dashboards, system status and real-time notifications of network issues, traffic conditions or thresholds. Solutions should include single screen visibility to any monitoring system in the network, as well as a mobile or tablet application for network engineers to have remote visibility and take immediate action.

About APCON

APCON is headquartered near Portland, Oregon, where it has operated since 1993. APCON's in-house staff manages product design and development, manufacturing, quality assurance and final testing, customer training and long-term servicing of its solutions – whether for a system with a single switch or a global installation that spans across multiple geographical locations.