USE CASE - Network Security

APS Networks

Using P4 (Programming Protocol-independent Packet Processors) Ethernet switches for network security offers several advantages due to the highly programmable and flexible nature of P4-based devices.

Here are some key reasons why P4 Ethernet switches are beneficial for network security:

Real-Time Threat Detection and Mitigation

P4 switches can be programmed to inspect and modify packets in real-time, enabling immediate detection and response to security threats. This capability helps in mitigating attacks as they happen, reducing the potential damage.

Dynamic Policy Updates

Security policies can be updated dynamically on P4 switches without needing hardware changes. This adaptability ensures that network security measures can evolve quickly in response to emerging threats and vulnerabilities.

Network Visibility and Analytics

P4 switches can provide detailed visibility into network traffic, which is crucial for monitoring and analyzing security events. Custom telemetry and logging functions can be implemented to capture specific data points, aiding in forensic analysis and compliance reporting.

Segmentation and Isolation

P4 allows for the creation of complex network segmentation and isolation policies. By defining how traffic is routed and processed, network administrators can isolate sensitive parts of the network, reducing the attack surface and containing potential breaches.

Enhanced DDoS Protection

P4 switches can be programmed to detect and mitigate Distributed Denial of Service (DDoS) attacks at the network edge. By identifying abnormal traffic patterns, the switch can take actions such as rate limiting or dropping malicious packets before they impact critical systems.

Custom Packet Filtering and Inspection

With P4, specific packet fields can be inspected and filtered based on custom criteria. This capability allows for the implementation of precise and granular security rules, which are essential for protecting against sophisticated attacks.

Cost Efficiency

By offloading security functions to P4 switches, organizations can reduce the need for additional dedicated security appliances. This consolidation can lead to cost savings in both hardware and operational expenses.

Future-proofing your network

The programmability of P4 ensures that the network infrastructure can adapt to new security protocols and standards as they emerge. This future-proofing is critical in a landscape where security threats and technologies are constantly evolving.

Specific Use Cases

Network Packet Brokers

P4 Enhancing Network Security

Inband Network Telemetry

Your Benefits

- Customizable Security Policies
- Enhanced DDoS Protection
- Cost Efficiency
- Future-proofing your network

The APS Networks P4 enabled Ethernet switches provide a powerful platform for enhancing network security through programmability and flexibility. By leveraging the capabilities of P4, network operators can implement advanced and customized security measures, ensuring robust protection against a wide range of threats while maintaining high performance and scalability.

Why APS Networks?

Security by Design

Our switches are designed based on the security by design principles. We have full control of our hardware supply chains and have Software Bill of Materials (SBoMs) in place for all software used. Further security features all for use of our products in Critical National Infrastructure (CNI).

Programmability with P4

The innovative technology of the Intel Tofino chipset offers unlimited open networking possibilities by the use of P4 programming language, featuring in-band telemetry and mega scale data center switching. P4 is easy to access, it enables hardware offloading of protocols, arbitrary tagging of packets, and controlling behavior based on individual data pattern matches. The switch has a non-blocking switching capacity of 2.0 Tb/s and is capable of complex protocol processing at wire speed.

Innovative Designs

Our technologies provide the ultimate, stable and supported platform for open network innovation. And our dedicated hardware solutions are built around enabling the latest open technologies to serve vertical industry needs. Open technology enables hardware and software diversity: reducing risk and lock-in to tardy vendor roadmaps.

Made in Europe

Our switches are produced in Europe, as the final manufacturing will be done in Belgium, and most of the components are provided by European suppliers. The printed circuit boards (PCBs) come from Austria and most of the design is done in The Netherlands.

We Deliver!

Modularity

All our new models can be upgraded with a daughter board, supporting a full range of Precision Timing Protocol (PTP) profiles. For the CPU you have the choice of AC or DC power supplies with front to back (port to power) and back to frond (power to port) airflow. The PSUs are of Titanium-grade, to provide the highest possible power efficiency levels.

PTP Timing & Synchronization

Our advanced programmable switches are the first to deploy the Tofino chipset with a time synchronization function, which is an essential capacity in the field of telecommunications as well as in media and entertainment. This feature enables

Efficient Power Consumption

The switches are equipped with low-consump-tion CPUs and energy-efficient PSUs and Fans. The intelligent automatic control system recognizes and manages the operating mode to reduce the power consumption to an optimized minimum, in particular when not in use.

Certification/Traceability

APS Networks and its design partners have invested in simulation tools to augment our capabilities and our engineers have a high level of expertise in designing products that not only meet but exceed requirements in these areas and most importantly we have a track record of largely passing the first time. That saves time, avoids rework and ultimately cuts costs.

Contact our Design Experts to help you choose your switch: +31 35 689 1689