TECHNOLOGY BRIEF

APCON Solutions for Networks | A10

PROTECT AGAINST ZERO-DAY ATTACKS AND ONGOING CYBERSECURITY THREATS

Network Visibility with Data Decryption & Encryption

Protect the most important data whether it is in the cloud, a virtual environment, on-premise, or in a hybrid network architecture.

APCON and A10 have solutions that can assist you in gaining visibility to your data environment that optimize the traffic centrally, decrypt and store keys safely, stream high volumes of packets, and successfully store them so you can perform forensics.

THE CHALLENGE

TRAFFIC CAPTURE AND DECRYPTION

In today's business environment, zero-day attacks have become so common that how you implement a security posture must change. Protecting the most important asset, data, is a full-time job no matter if it is in the cloud, a virtual environment, on-premise, or in a hybrid architecture.

How do you ensure an attacker is unsuccessful in exfiltrating data from your environment or encrypting your data for ransom? The easy answer is total visibility into your whole environment. This ideally covers potential lateral movement, or unwanted access, to files in storage by implementing a solution with multiple security products that do different things in a distributed model. This option is extremely costly due to equipment, full-time employees that manage and maintain it, and an expanded footprint of assets to audit. Protection at the perimeter is no longer the model to follow; instead, we must address the fact that an attacker can exploit a vulnerability in your devices and then move laterally to your data without detection. Security requires full visibility of the network environment and traffic.

Another concern is the encryption of data. Data must be decrypted before it can be examined. TLS (Transport Layer Security) 1.3 is a common protocol example, implemented with strong ciphers that need to be decrypted without stepping down the ciphers and ensuring that data does not leak out. The tools you use need to view that data un-encrypted, but you also need to view that data to identify if exfiltration is occurring.

Finally, what happens if you identify and isolate an anomaly that indicates potential lateral movement or exfiltration? You need to have the ability to collect the packets, store them, and analyze the data forensically to determine the danger and mitigate it quickly.

APCON AND A10 NETWORKS OFFER THE SOLUTION

PROCESS & DECRYPT PACKETS AT HIGH SPEEDS

There are two solutions that provide visibility to your overall cloud, virtual, and physical environment that optimize the traffic centrally, decrypt and store keys safely, stream high volumes of packets, and store it successfully so you can perform forensics.

Solution 1

APCON is a network packet broker that also generates NetFlow records that can acquire the packets, optimize them, and distribute the data to your tools out of band.

Solution 2

A10 Thunder SSLi decrypts virtual and physical traffic on the fly so it can be installed inline.

As we dive into each solution, we first must collect the network traffic. APCON provides customers a cost-effective ROI path to getting that data and optimizing it so that you only deliver what is needed to the tools. When it comes to protecting you from a single point of failure, APCON takes all your inline tools off the network and provides a Bypass Inline TAP that can either bypass the tool and continue to send the traffic or bring the link down, a decision for the customer.

In addition, APCON can collect traffic from your virtual environment and send it to the tools. If you have data in the cloud as well as cloud security tools, APCON can collect the traffic from your EC2 static and elastic instances and tunnel that traffic either in the cloud to the tool or back to the data center. APCON provides flexible ways you can collect and deliver the traffic to your tools, but we will focus on the illustrations on the next page using a Bypass Inline TAP and an aggregation blade.

EXAMPLES

TRAFFIC COLLECTION AND DELIVERY

Decrypting Data

Figure 1 shows a simple diagram depicting your network connections for the Internet and firewall entering the APCON Bypass Inline TAP. The green line represents encrypted data, and the red line indicates decrypted data.

The traffic will pass through to the A10 Thunder SSLi where decryption is conducted, then data is forwarded to the various security, application, and network analysis solutions out of band.

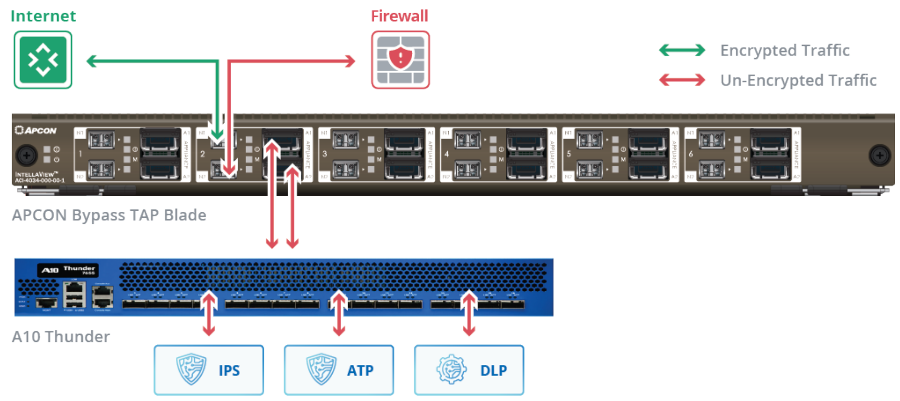

FIGURE 1

Meet Network Needs

In Figure 2, the same functionality is provided, but there may not be enough ports on the A10 Thunder SSLi product. APCON provides customers the ability to send traffic to our various aggregation blades via port mirror function or inline from an optical TAP. This diagram is the same as in Figure 1 except APCON can mirror the traffic over to the aggregation blade and send the traffic to packet capture probes for forensics analysis.

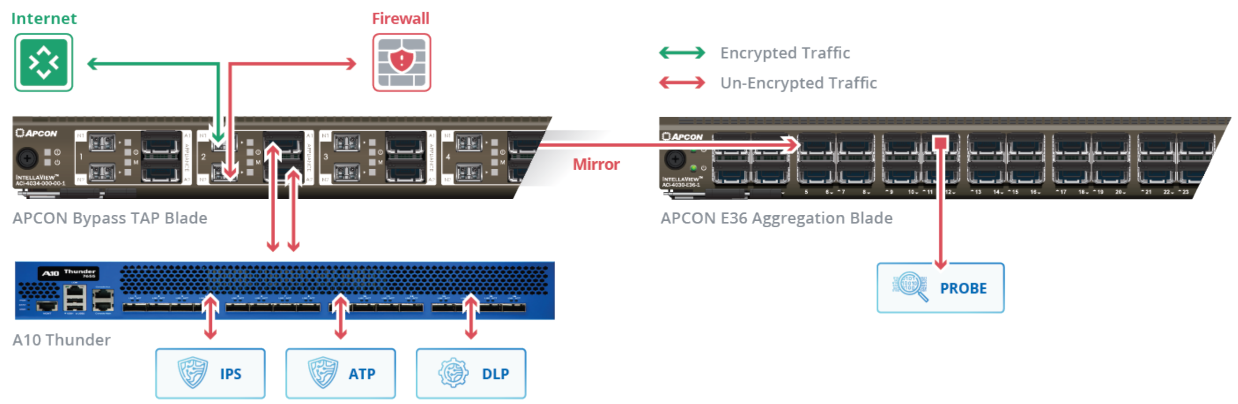

FIGURE 2

Tracking The Attack

Figure 3 has the same layout as Figure 2, but we need to bring traffic into the A10 Thunder SSLi to decrypt the traffic and send it to the various security tools, to network packet probes for packet storage, or to the production network. APCON has a unique feature where we can preserve the ERSPAN VLANID often used in Cisco ACI fabric and on-prem Virtualization. APCON will receive the traffic from the virtual or the ACI environment, pull out the ERSPAN VLANID and discard the GRE and ERSPAN headers before sending it to the tools like Endace. We do this so the forensic analyst can identify where in the network the attack is occurring.

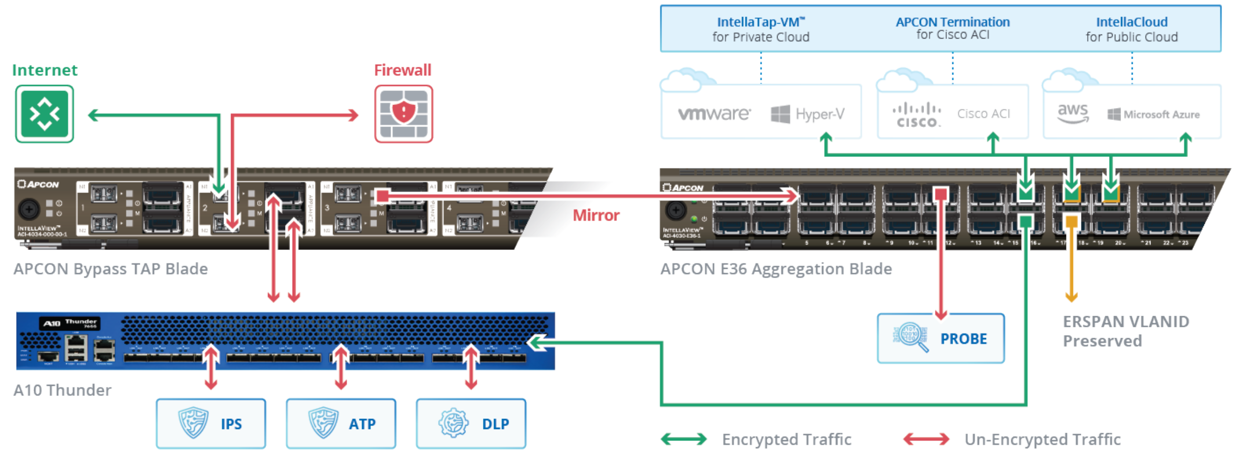

FIGURE 3

More Use Cases

There are numerous scenarios for which the APCON Bypass Inline TAP and aggregation blades are used to ensure data gets to the tools. The key is also having the ability to filter traffic and send only what the tool needs to avoid oversubscription. APCON can also strip headers, slice payloads, and mask credit card numbers, social security numbers, or other data in the packets.

Now that APCON has collected the packets, shaped, filtered, sliced, and masked the decrypted traffic, we can now focus on what A10 and Endace do best.

Thunder SSLi eliminates the blind spot introduced by SSL encryption by offloading CPU-intensive SSL decryption and encryption functions from third-party security devices while ensuring compliance with privacy standards.

While dedicated security devices provide in-depth inspection and analysis of network traffic, they are not designed to decrypt and encrypt traffic at high speeds. In fact, many security products cannot decrypt traffic at all.

Thunder SSLi boosts the performance of the security infrastructure by decrypting traffic and forwarding it to one or more third-party security devices, such as a firewall, for deep packet inspection (DPI). Thunder SSLi re-encrypts traffic and forwards it to the intended destination. Response traffic is also inspected in the same way.

The capabilities of the A10 Thunder SSLi allow users to:

- Gain full visibility to encrypted traffic at high speeds.
- Decrypt traffic for all security devices.
- Secure and store keys.
- Validate certificate status.
- Ensure compliance and privacy.
- Reduce operational costs by centralizing the decryption services using APCON's solution to collect traffic from all points of the network.
- Provide throughput performance rates for decryption and encryption up to 72G.
- Support concurrent sessions up to 4 million.
- Handle bulk SSL\TLS throughput of up to 145G.
- Supports port speeds up to 100G.

THE SUMMARY

VERSATILE DECRYPTION & PACKET DELIVERY

Companies can save money protecting against zero-day attacks and everyday cybersecurity threats by integrating a versatile decryption solution with a powerful packet broker that empowers you to acquire a high volume of packets, optimize them, and distribute them to other tools in your environment.

APCON can optimize the delivery of data packets by shaping and filtering traffic from Layer 1 up to Layer 7 of the OSI model as well as mask sensitive information that should not be exposed on the wire in transit, thus keeping companies in regulatory compliance.

The APCON Difference

APCON solutions provide the flexibility and means to gain visibility to data more efficiently, resulting in savings across the board, including time, resources, and maintenance.

APCON leverages its proprietary IP and deep expertise to provide flexible, focused solutions across:

- Government
- Healthcare
- Higher Education
- Financial Services
- Manufacturing
- Telecommunications

About APCON

Since 1993, APCON has consistently delivered technology designed with unparalleled innovation, stability, and scalability to mid-sized and Fortune 1000 customers in over 40 countries.

Our products instill network and security professionals with the confidence that data is monitored, secured, and protected in both physical and virtual environments. APCON helps companies sustain maximum performance by empowering total network visibility.

APCON
Solutions for Networks

APCON, Inc. ▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070
+1 503–682–4050 ▪ 1–800–624–6808 ▪ @APCON ▪ company/APCON ▪ **apcon.com**