Solution Brief

Gain Visibility into Encrypted Network Traffic with A10

Visibility into SSL/TLS Encrypted Traffic is Necessary for a Strong Cybersecurity Posture

Business Benefits

- Business Continuity
  Eliminate exposure and risk of cyberattacks penetrating the IT infrastructure cloaked by encryption
- Maximize Security ROI
  Provide the right data, in the right decrypted format, at the right data rate to your existing cybersecurity tools extends their usefulness and life
- Regulatory Compliance
  Use policies to isolate and segment unencrypted data to comply with data privacy regulatory mandates, and leverage captured data for regulatory record-keeping and reporting

Technology Benefits

- Prevent Covert Cyberattacks
  Eliminate blind spots with single points of decryption and re-encryption that maximizes the effectiveness of existing cybersecurity tools for Network Detection and Response
- Ease of Deployment
  Organizations can add visibility and inspection into their existing networks and security architectures without any service disruption
- Network Performance KPIs
  The visibility fabric also provides metrics that help the IT teams optimize network and application performance and end-user experiences

Challenge

Cybercriminals are clever, well-funded, and use many methods of attacking IT infrastructure, including being stealthy. Technologies used for good purposes, including encryption, are weaponized by cybercriminals. They use encryption to hide malware in payloads in hopes that it bypasses cybersecurity defenses by exploiting the blindness of cybersecurity tools to encrypted traffic.

As with all cyberattacks, malware and malicious activity hidden by encryption must be detected to be prevented. Therefore, all traffic, including encrypted traffic, must be visible to cybersecurity tools for inspection, detection, and prevention.

The following interrelated requirements must be met to address this challenge to ensure a strong cybersecurity posture:

- Visibility of all network traffic
- Decryption of network traffic (including traffic encrypted with SSL/TLS)
- Detection of malicious and suspicious activity within all network traffic
- Timely and appropriate manual and/or automated responses

Solution

The validated joint solution combines cPacket Networks' cVu® series Network Packet Broker+ products with A10 Networks' SSL Insight (Thunder SSLi) – a natural fit for robust Network Detection and Response. With this solution organizations can comply with privacy mandates while confidently delivering secure and scalable application services from on-premises, cloud, edge-cloud, and hybrid environments.

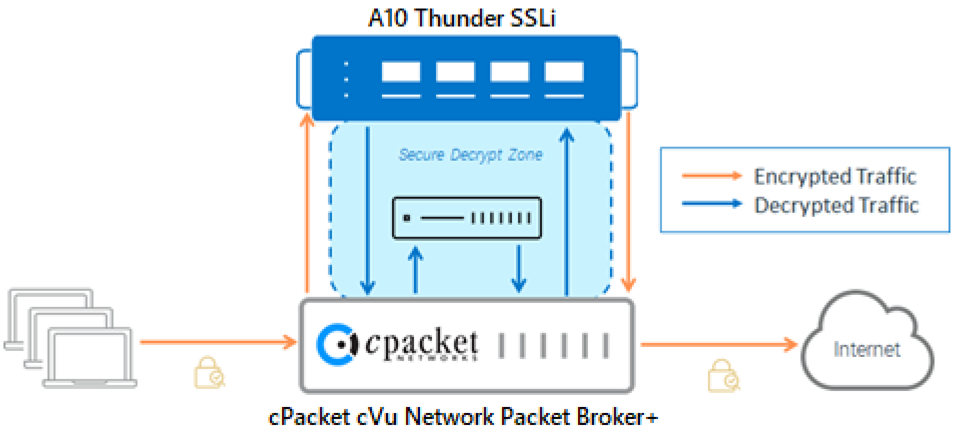

Figure 1: Logical Diagram, Basic Implementation (inline implementation requires a bypass switch)

As shown in Figure 1 network traffic data is losslessly acquired by a Network Packet Broker (NPB). The packets are timestamped, counted, and optionally filtered to meet the ingestion requirements of the A10 Thunder SSLi. Encrypted TLS traffic over port 443 or any other TCP port received by the A10 Thunder SSLi is decrypted and returned to the NPB to perform additional processing prior to routing the traffic to its destination. Examples of on-the-fly processing are removing duplicates and adjusting the data rate to match the ingestion requirements of cybersecurity tools that will inspect the decrypted data to detect threats and initiate a response.

The NPB can be configured to balance loads across multiple tools and/or replicate the traffic for simultaneous delivery to multiple tools. This traffic-efficient implementation creates a single point of decryption and re-encryption, so the overall solution can facilitate multiple inspections by only decrypting and re-encrypting once.

The advanced processing done at wire speed by the NPB ensures that all tools throughout the security delivery chain operate at optimal efficiency because they receive only the data needed, in the right decrypted format, and at the right data rate. The NPB can also ensure that sensitive decrypted traffic is isolated and only delivered to specific cybersecurity tools to perform real-time inspection of layer-2 through layer-7 network traffic.

Summary

The combined cPacket and A10 solution extends network traffic visibility to include encrypted traffic, hence providing full visibility into all network traffic that drives a strong cybersecurity posture by:

- Decrypting traffic across all TCP ports and protocols such as SSL/TLS, STARTTLS, SSH, XMPP, SMTP, and POP3
- Selectively decrypting traffic for privacy and regulatory compliance
- Using high-performance decryption with multiple cipher suites including elliptical curve cryptography (ECC) for perfect forward secrecy (PFS) support
- Providing network traffic data to all cybersecurity solutions, including inline, out-of-band, and ICAP-enabled devices

Additional benefits of incorporating visibility from cPacket Networks includes making the following network intelligence available to IT personnel and the network performance management tools they use:

- Detailed network traffic statistics
- Troubleshooting alerts
- Flow data
- Stored network data for post-event forensic analysis and for regulatory record-keeping and reporting

About cPacket Networks

cPacket Networks enables IT through network-aware application performance and security assurance across the distributed hybrid environment. Our AIOps-ready single-pane-of-glass analytics provide the deep network visibility required for today's complex IT environments. With cPacket, you can efficiently manage, secure, and future-proof your network – enabling digital transformation. cPacket solutions are fully reliable, tightly integrated, and consistently simple. cPacket enables organizations around the world to keep their business running. Our cutting-edge technology enables network, application, and security teams to proactively identify issues before negatively impacting the business. The result: increased security, reduced complexity, and increased operational efficiency. Learn more at www.cpacket.com.

About A10

A10 Networks provides Reliable Security Always™, with a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.
For more information, visit: www.a10networks.com and @A10Networks.