Solution Brief

Security Delivery and Incident Response

Palo Alto Networks and cPacket Networks Integrated Solution for Fast Forensics and NPM Data

Business Benefits

- **Business Continuity**
  Proactive security posture and visibility mechanisms prevent mission-critical down time
- **Operational Efficiency**
  Consolidation of network traffic delivery to security tools reduces costs and increases operational efficiency
- **Business Agility**
  Integrated threat mitigation and forensics capabilities enable faster time to resolution, incident response and minimizes losses

Technology Benefits

- **Complete Visibility**
  Security analysts achieve broader visibility on events by leveraging cPacket's Integrated Monitoring Fabric's ability to perform wide searches on Palo Alto Networks next-generation firewalls
- **Fast Forensics**
  Historical packet retrieval for forensics investigation is now possible at any segment of the network
- **Ease of Deployment**
  Palo Alto Networks next-generation firewalls access cPacket's information through a set of Restful APIs, enriching its set of tools to prevent security breaches

The Challenge

Cyber-attacks and data breaches continue to increase in frequency and sophistication, and it is not a matter of if but when an enterprise or service provider can become a target. Network is a prime target for the attackers because of the vulnerabilities of network traffic in motion from point A to point B and in between. The first challenge is the lack of visibility into the network traffic for proper remediation and threat analysis. The traffic is usually scattered and hence are the tools, leaving several blind spots across the network. Security tools such as next-generation firewalls can provide detailed information concerning the events or the devices whose traffic is directly handled or accessed by them. This information is normally only related to the traffic which is flowing through the firewall itself (inline); traces normally need to be activated on-demand and must be used with cautions not to affect the firewall performances.

Second challenge is that when facing an attack, IT SecOps is in shock because they lack the appropriate preparation, tools and processes needed to respond. One of the most critical components at that point is having the access to detailed network data for before, during, and after an incident to run forensics analysis. Without proper forensics, the sources of the attack cannot be determined and hence intercepting it and responding to it becomes extremely difficult, ineffective and delayed – while the business suffers.

The Solution

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches. Tight integrations across the platform and with cPacket Networks deliver consistent security across clouds, networks and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

cPacket adds wide forensics and Network Performance Monitoring (NPM) capabilities to Palo Alto Networks Next-Generation Firewalls (NGFW). Faster time for resolution of incidents is acquired leveraging the information that cPacket can provide, easily accessible from within Palo Alto Networks console. The user no longer needs to contact other groups to ask for network traces or to add context to events detected by Palo Alto Networks NGFW. cPacket Networks complements Palo Alto Network in three ways:

Complete Network View with Faster MTTR

To have a complete understanding of security related events and causes, SecOps need to have also quick access to information about the status and performances of the surrounding network at the time of the incident, without necessarily involve other groups in long troubleshooting sessions Integrate cPacket cClear into Palo Alto Networks NGFW and let it quickly provide NPM information (plots and tabs) directly from the firewall GUI.

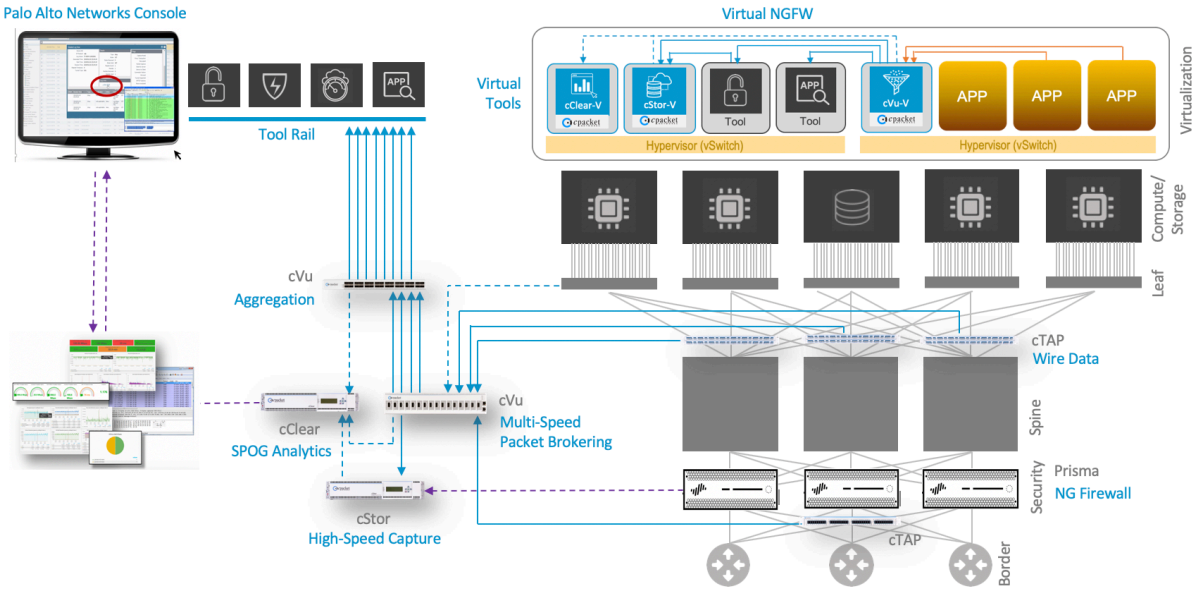
Consolidation and Delivery of the Network Data

cPacket cVu series Network Packet Broker consolidates and simplifies the overall data delivery job to Palo Alto Networks' as a lossless high-performance Security Delivery Fabric. This eliminates traffic blind spots and assures a reliable delivery of network traffic so that no crucial events are missed, increasing the operational efficiency.

cVu series is not only a best in class packet broker but offers a complete set of additional performance and monitoring features on all the ports. cVu series distributed architecture and advanced features such as smart filtering, deduplication, slicing, micro-bust analysis etc. all under single license, ensures that right data is delivered to the right tools in the right form. cPacket cVu-V provides same functionality for the virtual tools in a software-defined data center (SDDC) or cloud.

Access to Always-On Fast Forensic Data

Accessing packet traces related to security incidents or events is usually a resource intensive task for firewalls and normally it is activated on demand and is limited to the place where the firewall sits. cPacket cStor series as an integrated tool continuously capturing packets, gives the access to present and past traces related to an incident in one click is very powerful for SecOps/NetOps. Users can leverage cPacket's broad network coverage and have access to data to collect information from different locations merged into a single PCAP file to be shared with internal/external customers and to further analyze for deep troubleshooting. IT security personnel can access forensics information related to distant nodes in the network directly from the Palo Alto GUI. They can also access NPM data or perform searches across the network to understand the impact caused by the activity of the system under analysis.



cPacket's integrated visibility solution with Palo Alto Networks allows IT SecOps personnel to take advantage of a single, integrated workflow supporting CISO's digital transformation objectives.

To learn more, visit www.cpacket.com and www.paloaltonetworks.com

About cPacket Networks

cPacket Networks delivers visibility you can trust through network monitoring and packet brokering solutions to solve today's biggest network challenges. Our cutting-edge technology enables network and security teams to proactively identify issues in real-time before negatively impacting end-users. Only cPacket inspects all the packets delivering the right data to the right tools at the right time and provides detailed network analytics dashboards. Whether you need greater network visibility for security tools or performance monitoring tools, our solutions are designed to overcome scalability issues and reduce troubleshooting time. The result: increased security, reduced complexity, with lower costs, and a faster ROI.

Based in Silicon Valley, CA, cPacket enables organizations around the world to keep their business running. Leading enterprises, service providers, healthcare organizations, and governments rely on cPacket solutions for improved agility, higher performance, and greater efficiency. Learn more at www.cpacket.com, the cPacket blog, or follow us on Twitter, LinkedIn, and Facebook.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.