Security Use Case

Government Agency

Providing Enhanced Network Visibility for Government Security Analysts

Network Forensics for the 10Gig World

OVERVIEW

Key Requirements

- Provides a cost-effective capture solution for distributed network traffic recording
- Integrates with existing security tools to allow quick pivoting to network incident traffic
- Provides data and full packet capture on all network traffic

Solution

- Aggregates multiple links into a single capture appliance for extensive monitoring and visibility
- Integrates seamlessly with existing security dashboards and SIEM tools through RESTful API
- Provides available NetFlow index in exportable NetFlow v9 format

Results

- Provides in-place capture solutions at all key network entry/exit points, data centers, and remote office locations
- Automated Pivot2Pcap apps offer quick, real-time access to packets for security analysis
- NetFlow index is available for long-term analysis and integration with third-party tools

REQUIREMENTS

A large government agency relies on its network to transfer large amounts of secure data. The network must be protected against well-funded, highly organized, and constant threats from both nation state and criminal elements. Solutions must be scalable to full duplex 10Gbps rates and be cost-effective for network-wide deployment in multiple locations.

Their outdated solutions left them unable to determine if threats were legitimate, drained precious manpower and left them uncertain about whether new security measurements could truly mitigate future attacks. A new solution needed to add visibility, detect and analyze network traffic … *and* integrate with their current automated workflow.

SOLUTION

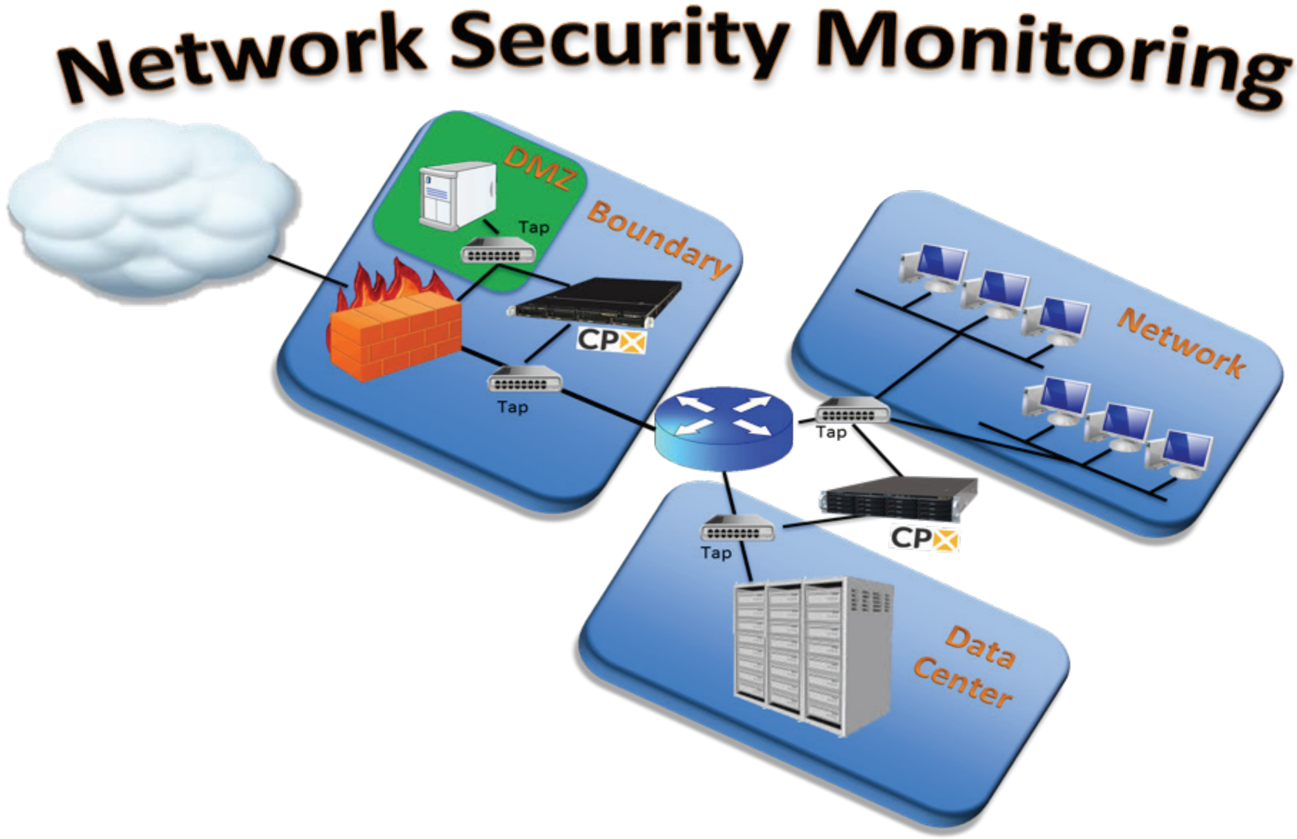
They began to research packet capture solutions that would allow them to capture and quickly search traffic. Solutions needed to:

- Provide NetFlow data for long-term flow analysis;
- Provide industry-standard pcap-formatted files;
- Provide NetFlow v5, v9, or IPFIX records for flexibility;
- Provide quick access to packet data from network events; and
- Verify new mitigation strategies against real network data.

The security team needed a high performance solution that could aggregate traffic from multiple 1Gbps links or full duplex 10Gbps links into a single 20Gbps appliance.

They turned to a Big Data analytics performance leader: nPulse Technologies.

The nPulse Capture Probe eXtreme (CPX) appliance was built to capture network traffic at ultrafast data rates. The CPX provides high-speed access to historical network traffic stored in standard pcap format. Indexed by time and flow information, the nPulse CPX can be used with their existing flow collection solutions for added visibility. Accessible via an easy-to-use web UI or integrated RESTful API, the CPX enabled the customer to leverage existing custom scripts and utilities. The CPX's easy integration into their current workflow and network SIEM tools provided quick access to data.



RESULTS After a seamless implementation and integration with the customer's existing tools and infrastructure, the security team used the ArcSight app to view alerts and pivot directly to the packet data from network security and log events. As a result, they recently **discovered a successful brute force login attempt and were able to go back in time and view the attacker's actions and the data ex-filtrated from the device** — something they could not do before using the CPX solution.

THE BOTTOM LINE: The analysts have significantly reduced their time researching network events. And the CPX has provided valuable insight into, and quick analysis of, network attacks, securing the customer's network while keeping it – and business – operational.

CONTACT US

Find out how nPulse Technologies can help provide enhanced APT analysis for your business. Visit www.npulsetech.com

About nPulse Technologies, Inc.

nPulse Technologies is the performance leader in network forensics. Leading financial institutions, government agencies, telecommunications carriers and other organizations rely on nPulse solutions to enhance security monitoring, shorten incident response times, and increase returns on existing security investments.

For network forensic analysts looking to significantly reduce incidence response time, nPulse solutions enable expeditious reconstruction of the kill chain. Unlike competitive solutions that are unable to operate at 10Gbps sustained and take hours to analyze network traffic, our solutions are designed to perform at 10Gbps full duplex, capturing, inspecting, and exposing indications of compromise within minutes, all at a fraction of the cost.

For more information, visit www.npulsetech.com.