Large Financial Services Company

Providing Enhanced Network Visibility for 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

Solution

- Allows aggregation of multiple links into a single, ultra high-performance capture appliance for cost-effective monitoring and visibility across the network
- Enables seamless integration with existing security dashboards and SIEM tools through RESTful API

Results

- Provides in-place capture solutions at all key network entry/exit points, data centers, and remote office locations
- Linux container capability allows cost-saving consolidation of security tools into the CPX
- Allows quick, real-time access to session packets through automated applications with industry partners like Splunk, SourceFire and ArcSight
- Enables quicker analysis of security events and suspicious behavior

REQUIREMENTS

A leader in the financial market data services industry counts on its network to deliver real-time news and financial market analysis to customers. This makes their network a critical part of day-to-day business and means the IT security team must protect against the constant threat of intruders and malicious traffic. But with 15,000+ employees in nearly 150 locations worldwide, the company needs options that are both cost-effective and scalable.

The security team needed a next-gen solution that provided added visibility, detection, and analysis of network traffic. The key? Integrating all of these solutions for quick analysis of real-time events while keeping the network operational.

SOLUTION

The analysts needed to access packet data and pivot back to the actual network traffic that created the event. The successful solution needed to:

- Capture traffic and index it for quick retrieval;
- Provide industry-standard pcap-formatted files;
- Aggregate traffic from multiple links into a single appliance;
- Enable a way to replay traffic; and
- Verify new mitigation strategies against real network data.

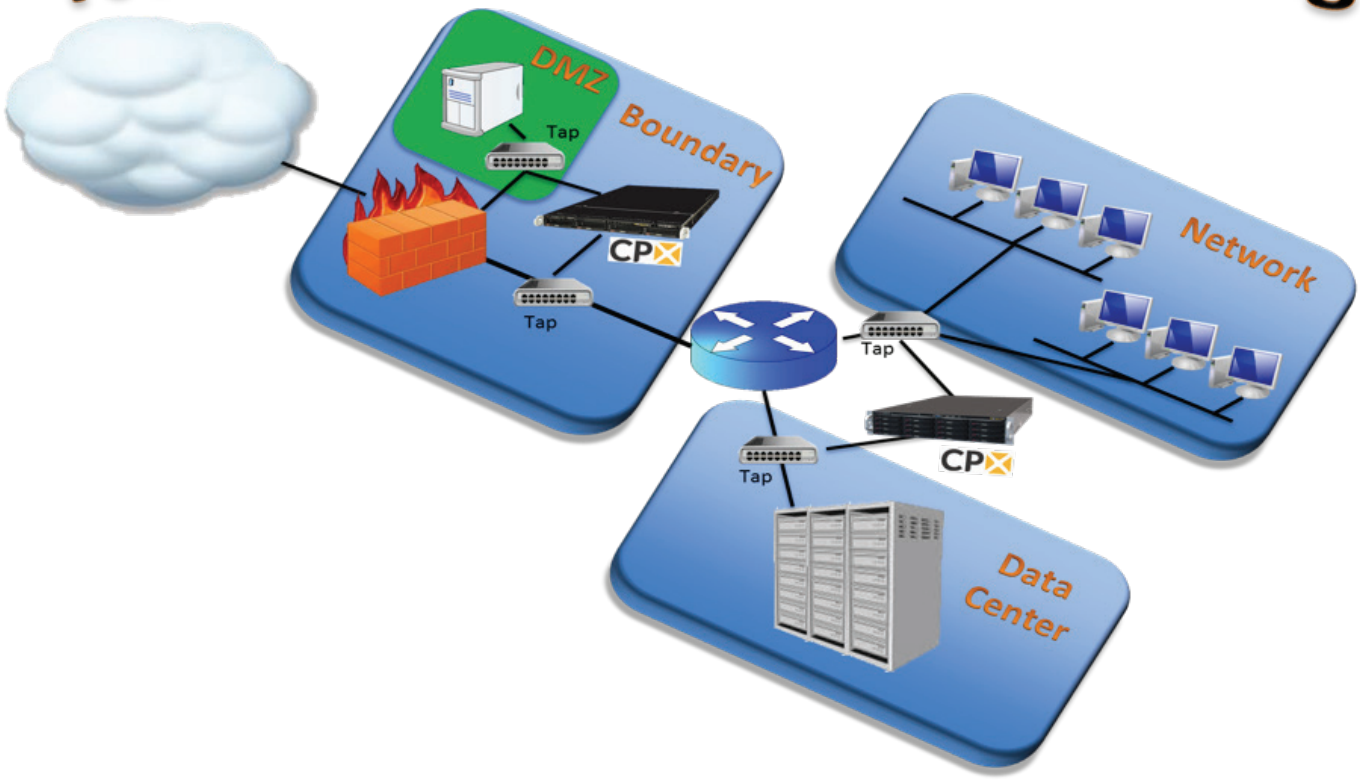
The team turned to a Big Data analytics performance leader: nPulse Technologies.

The nPulse Capture Probe eXtreme (CPX) appliance was built to capture network traffic at ultrafast data rates. The CPX provided the customer high-speed access to historical network traffic stored in standard pcap files.

CPX's capture capabilities allowed aggregation of multiple 1Gig and 10Gig links into the 20Gbps capture appliances. This provided traffic monitoring into and out of firewalls and internal data center links to enable total visibility into any malicious events anywhere on the network.

Increased capture data, additional NetFlow records, and more link monitoring by the ultrafast CPX ensured that packet and flow data was always available on external, gateway, and internal data center traffic. The customer now uses pcap data from verified malicious events to test new workflow mitigation rules and signatures.

Network Security Monitoring



RESULTS The CPX implementation was straightforward with a seamless integration with customer's existing tools and infrastructure. The security team's ability to view alerts and pivot directly to the packet data from network security and log events saved valuable time and eliminated manually finding and sifting through large pcap files.

THE BOTTOM LINE: The analysts have significantly reduced their time researching network events. In fact, the CPX is now part of the customer's standard network equipment at each of its nearly 150 remote sites. And the integration of the Suricata IDS engine on their CPX probes allowed them to do real-time alerting on the same appliance - saving rack space, complexity, and substantial cost.

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.