Copper River
Information Technology

CASE STUDY: UNIVERSITY OF MARYLAND EASTERN SHORE (UMES) – NEXT-GENERATION NETWORK SECURITY & INFRASTRUCTURE MODERNIZATION

CHALLENGE

UMES's legacy firewall and security infrastructure had reached end-of-life and could no longer provide the performance or visibility required to protect the university's growing data environment.

Key challenges included:

- Limited visibility into network traffic and user behavior.
- Outdated firewall hardware unable to handle modern encrypted traffic loads.
- Fragmented management of multiple security devices across departments.
- Increased cyber threats targeting higher education institutions, including ransomware and phishing attacks.
- Lack of centralized policy management and incident response visibility.

UMES needed a scalable, next-generation solution to strengthen its cybersecurity posture while simplifying management and providing real-time analytics.

SOLUTION

Copper River IT partnered with UMES to design and deploy a comprehensive network security modernization built on Palo Alto Networks technologies.

The solution included:

Next-Generation Firewalls (NGFW): Deployment of Palo Alto Networks PA-3430 firewalls at the campus core and internet edge, providing advanced threat prevention, URL filtering, intrusion detection and prevention (IDP/IPS), and deep packet inspection.

Centralized Management: Implementation of Palo Alto Networks Panorama, enabling unified policy management, log collection, and visibility across all campus firewalls from a single console.

Security Storage and Logging Infrastructure: Integration of a high-performance security storage system for long-term log retention and compliance, ensuring continuous analytics and forensics capability.

High Availability and Redundancy: Configured active/active HA pairs for seamless failover and zero downtime during updates or failures.

Integration with Existing Infrastructure: The new NGFW environment was fully integrated with UMES's existing authentication, identity, and campus network systems, minimizing disruption during the transition.

Copper River
Information Technology

IMPLEMENTATION APPROACH

Copper River IT followed a structured, collaborative deployment process:

Assessment & Design: Conducted a full network security audit and capacity analysis to determine optimal firewall sizing and placement.

Proof of Concept: Validated performance of the PA-3430 in UMES's real traffic environment.

Deployment: Implemented the new firewalls in a phased rollout, ensuring uninterrupted network operations.

Panorama Setup & Policy Migration: Transferred existing firewall rules, optimized configurations, and established global policy templates for streamlined management.

Training & Knowledge Transfer: Delivered hands-on workshops for UMES IT staff to operate, monitor, and maintain the new systems confidently.

RESULTS

- **Enhanced Security Posture:** The new NGFWs provide application-layer visibility, threat prevention, and zero-day protection across the UMES network.
- **Centralized Management:** Panorama simplifies administration and provides a unified view of security events and compliance data.
- **Improved Network Performance:** The PA-3430 appliances deliver up to 15 Gbps throughput, accommodating the university's bandwidth growth and future expansion.
- **Operational Efficiency:** Reduced time spent on manual policy updates and troubleshooting through automation and centralized logging.
- **Future-Ready Infrastructure:** The new environment positions UMES for secure adoption of cloud services, IoT devices, and next-gen campus technologies.

TECHNOLOGIES USED

- **Palo Alto Networks PA-3430 Next-Generation Firewalls**
- **Palo Alto Networks Panorama**
- **Copper River IT Professional Services (Design, Implementation, and Support)**
- **Security Storage Infrastructure for Centralized Logging and Analytics**