The Center for Cyber Defenders
Expanding computer security knowledge

Secure Software-Defined Networking

Policy Enforcement in Hybridized Networks

Students: Luke Rindels, Jacob Valencia, Samuel Short, Harrison Hill, Ethan Brown
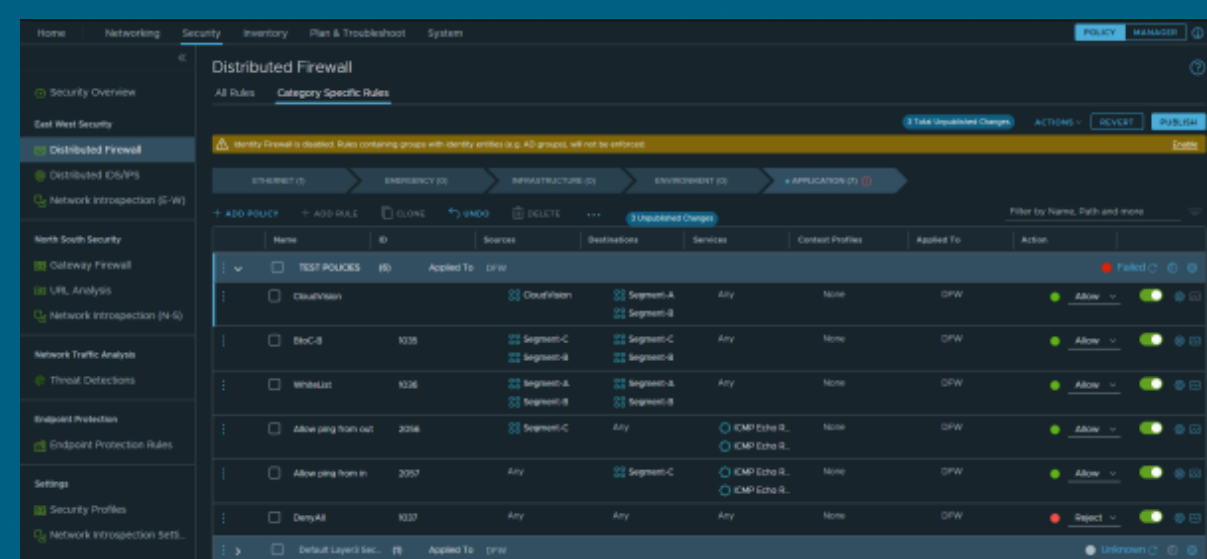
Project Mentors: Joseph Maurer, Elijah Orozco

Problem Statement:

- Networks are transitioning to software-defined paradigms

- Network configuration is represented as Infrastructure as Code (IaC)

- Network implementations are highly dynamic and intent-based

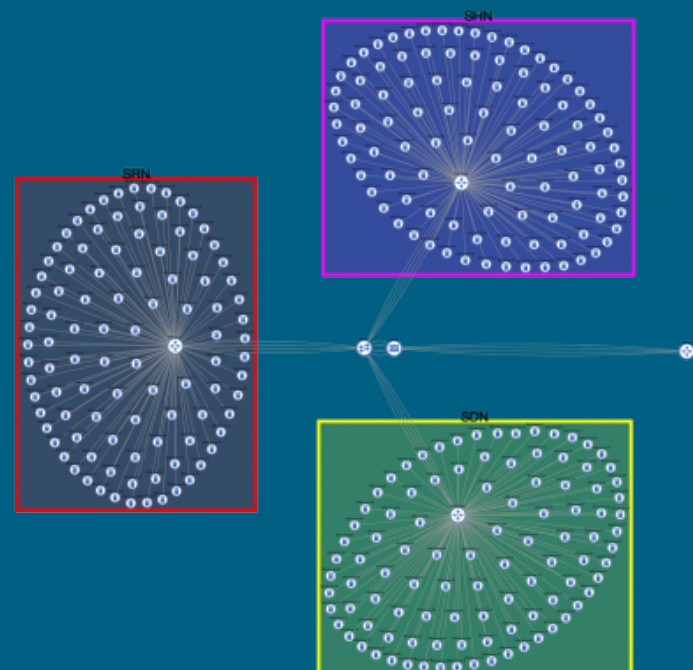- Networked services use virtual machines, containers and bare-metal servers

Objectives and Approach:

- Consistent application of policy enforcement in transitive states, such as when moving from physical to virtual

- Visualizing policy enforcement over time

Results

- Network Visualization:
    - Plotly based network graphing tool
    - Survey of visualization tools
    - Survey of network layouts

- Device Registration:
    - Custom Ansible module
    - Create, Modify, Update, Delete (CRUD)

Containerized Services:

- E-AKS Kubernetes
- Nginx, containerized switching, and web app hosting

Physical Device Management:

- CloudVision
- cEOS

Distributed Policy:

- NSX and CloudVision Exchange

Impact and Benefits:

- Network Visualization:
    - Demonstrates physical and logical connections in the network for use by CCD

- Device Registration:
    - Eliminates manual processes
    - Eliminates sync between what exists and what is registered

- Containerized Services:
    - Scalable solution for deploying networking and security services
    - Rapid Prototyping
    - CI/CD

- Physical Device Management
    - Abstracts and centralizes management of physical and virtual devices

- Distributed Policy:
    - Steps toward zero-trust architecture with dynamic policy enforcement

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration