AI Security Report

AI Security Findings

Traffic Graph

This graph visualizes the network connections, potential issues, and recommendations.

AI Advisor Output

This section provides AI-generated security and microsegmentation recommendations based on the analyzed data.

Certainly! Below is a markdown-formatted response with an analysis based on the provided network data.

- --

Security and Microsegmentation Recommendations

1. Potential Security Risks

Unsecured Open Ports

- **Port 22 (SSH):** Widely used for remote administration. High count (152); ensure it's secured with strong authentication methods like key-based authentication.
- **Port 111 (RPC):** Both TCP and UDP versions are open. This port is often targeted for exploits due to its history of vulnerabilities.
- **Port 3389 (RDP):** Open RDP ports can lead to unauthorized remote access if not secured properly.
- **Port 21 (FTP):** Known for transmitting data in plaintext, making it susceptible to interception.

Operating System Diversity

- **Legacy Systems:** The presence of older systems like `centos-x86_64-7.0` and `ubuntu-x86_64-xenial` increases the risk of unpatched vulnerabilities.
- **Mixed Platforms:** A diverse set of operating systems can complicate security patch management.

2. Microsegmentation Recommendations

Grouping by Functionality

- **Segment by OS:** Create segments for each operating system type to simplify policy enforcement and monitoring. This helps in isolating vulnerabilities specific to certain OS versions.

- **Application-Based Segmentation:** Differentiate between server and client workloads (e.g., `win-x86_64-server` and `win-x86_64-client`) to apply specific security policies.

Restricting Access

- **Limit SSH Access:** Only allow SSH from trusted IP addresses or segments.
- **RPC and RDP Restrictions:** Ensure RPC and RDP access is restricted to necessary segments only, potentially using VPNs for secure access.

3. Best Practices for Improving Overall Network Security

Patch Management

- **Regular Updates:** Ensure all systems, especially legacy ones, receive timely security patches.
- **Deprecation Plan:** Plan to upgrade or replace older systems like `centos-x86_64-7.0`.

Authentication and Access Controls

- **Multi-Factor Authentication (MFA):** Implement MFA for administrative access, especially for SSH and RDP.
- **Least Privilege Principle:** Apply the principle of least privilege to all user accounts and services.

Network Monitoring

- **Intrusion Detection Systems (IDS):** Deploy IDS to monitor and alert on suspicious activities.
- **Regular Audits:** Conduct regular security audits and penetration testing to identify vulnerabilities.

4. Recommendations for Optimizing Enforcement Modes

Transition to Full Enforcement

- **Increase Full Enforcement:** Currently, only 19 are in full enforcement mode. Gradually move more workloads to full enforcement by testing policies in `selective` mode first.
- **Visibility to Selective to Full:** Transition workloads from `visibility_only` to `selective` mode to test policies without enforcement, then move to full enforcement once verified.

5. Recommendations for Traffic Analysis and Security

Detailed Traffic Monitoring

- **Log Analysis:** Implement centralized logging for all network activities to facilitate analysis and forensic investigation.
- **Anomaly Detection:** Use machine learning or behavior analytics to detect anomalies and potential threats in network traffic.

Port Usage Review

- **Restrict High-Risk Ports:** Regularly review the necessity of open ports, especially those with higher counts and known vulnerabilities.
- **Port Closure:** Consider closing ports that are not actively used or required for business operations.
- --

By addressing these areas, organizations can significantly enhance their network security posture and reduce the risk of potential breaches.