**Lab 7 Report: pfSense Firewall Dashboard Creation in Kibana**

**Overview**

This lab focused on creating a centralized visualization dashboard for pfSense firewall logs using Kibana in the Security Onion environment. The task involved filtering log data, building various visual panels, and assembling them into an interactive dashboard for real-time analysis.

**Tasks Completed**

#### 1. Launching Kibana and Creating a Search Filter

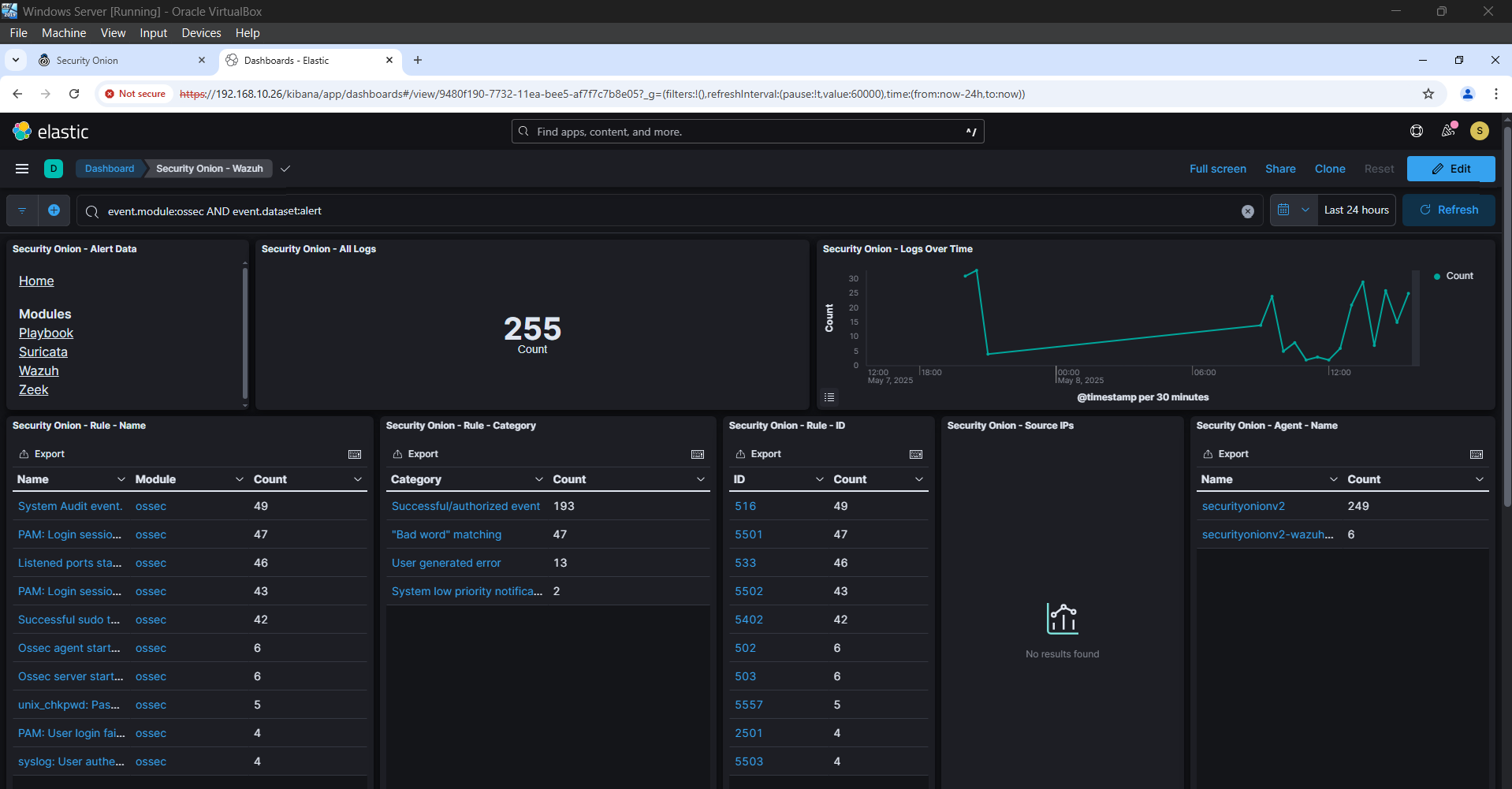
Logged into Security Onion.

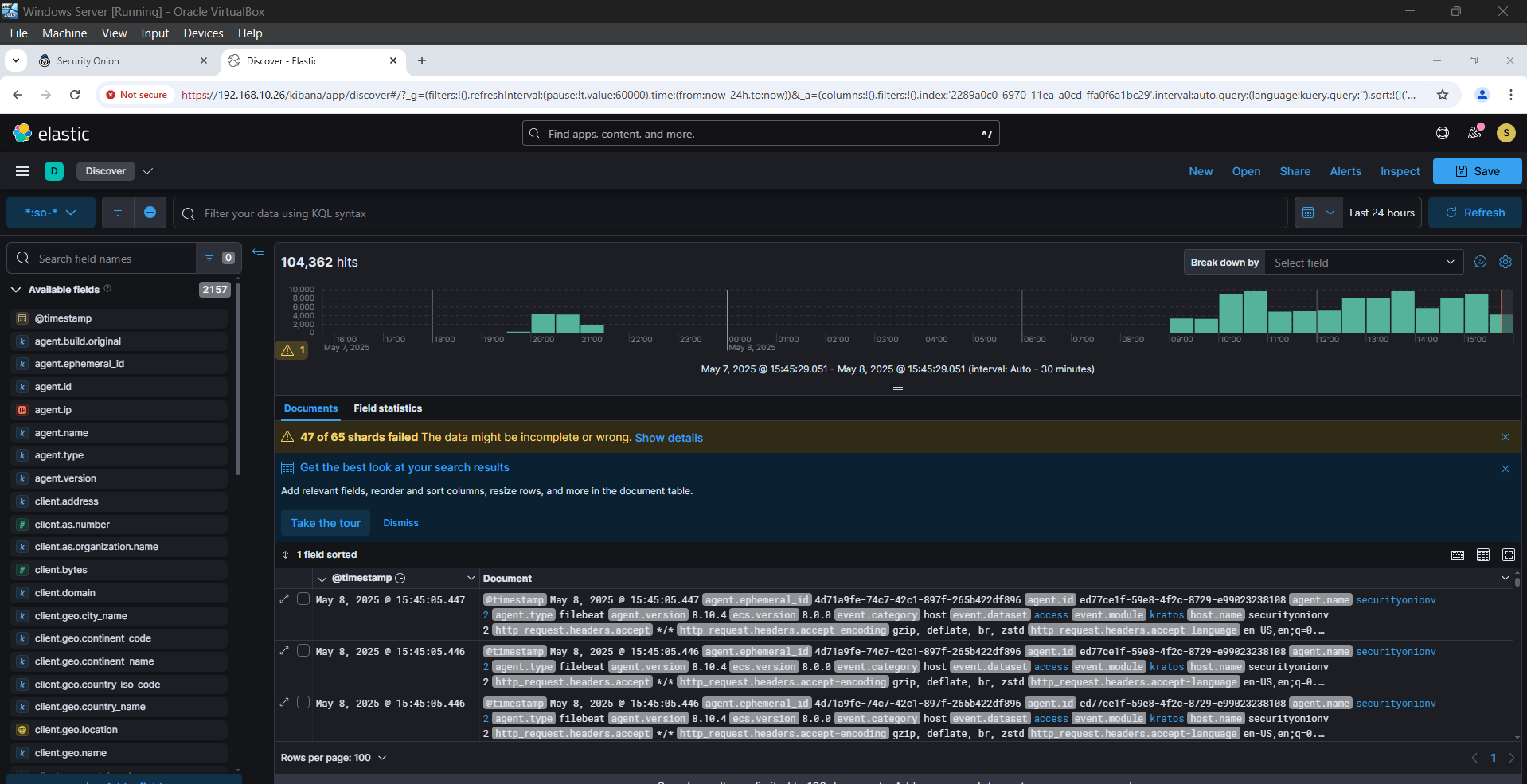
Accessed Kibana using the left-hand navigation panel.

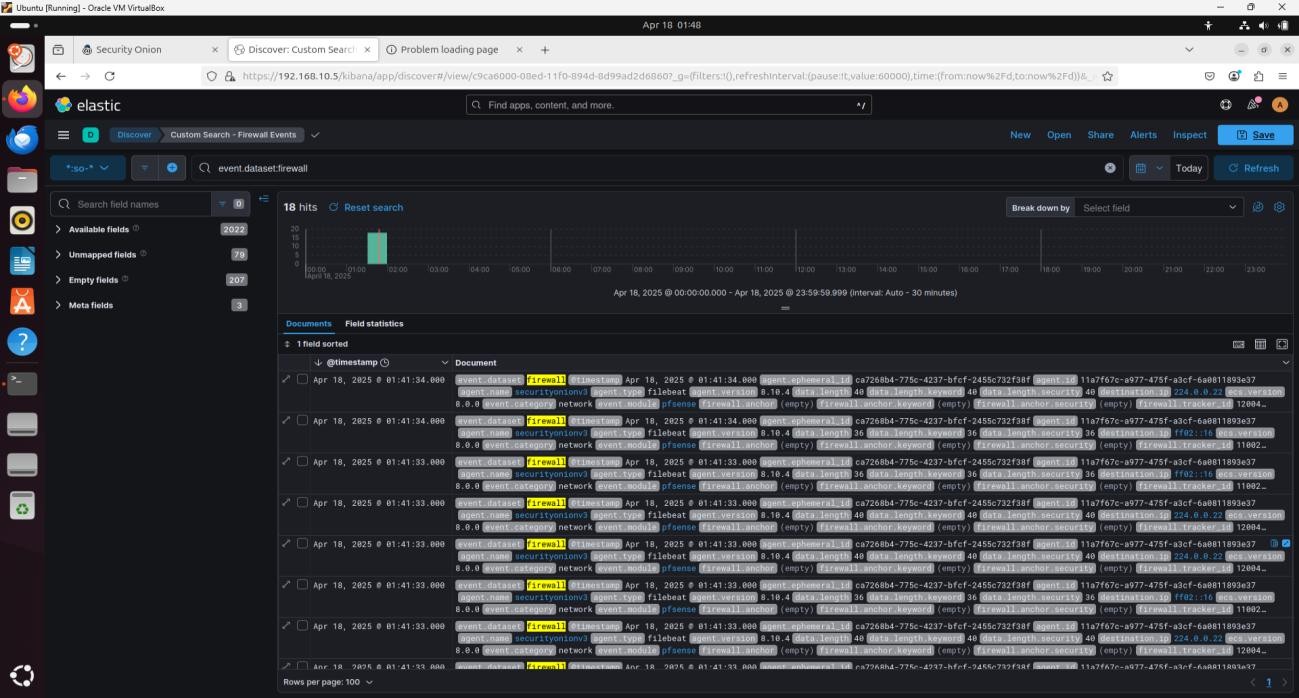
Opened **Discover** via the Kibana menu.

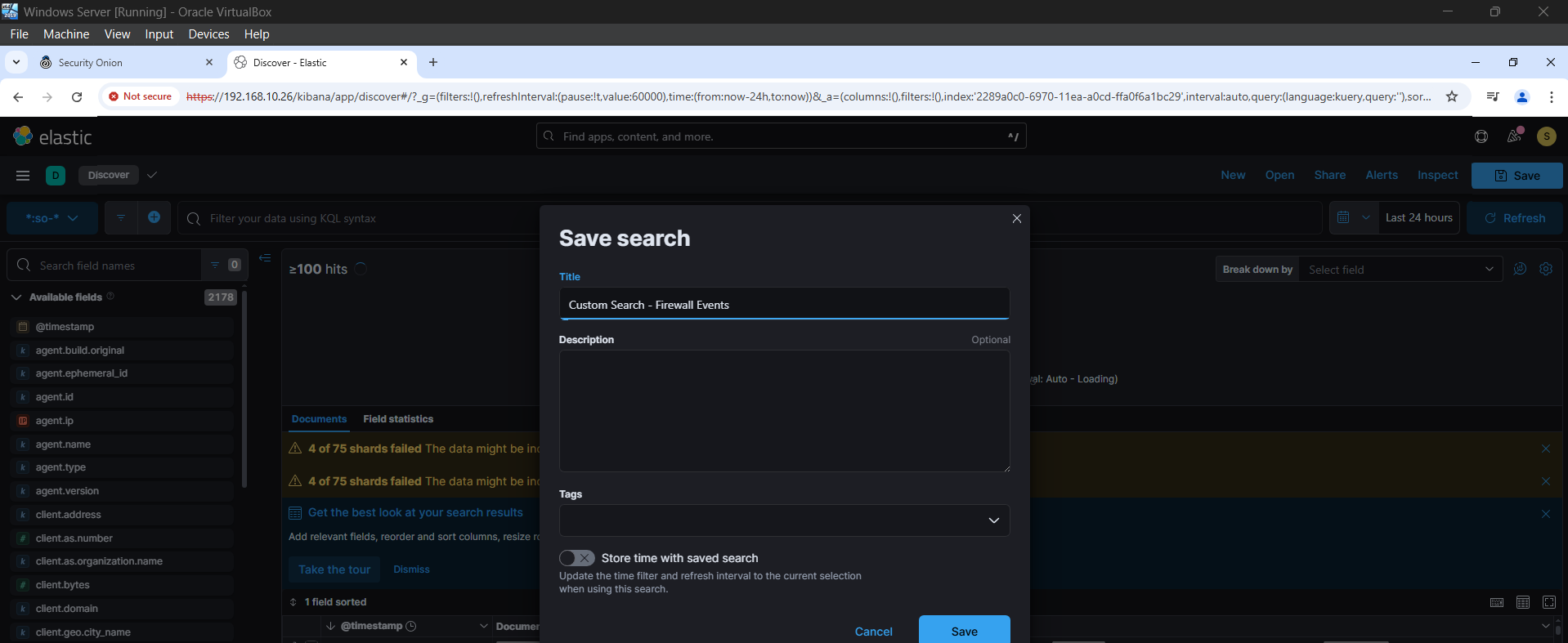
Executed the query event.dataset:firewall to isolate firewall logs.

Saved the query as **Custom Search – Firewall Events**.





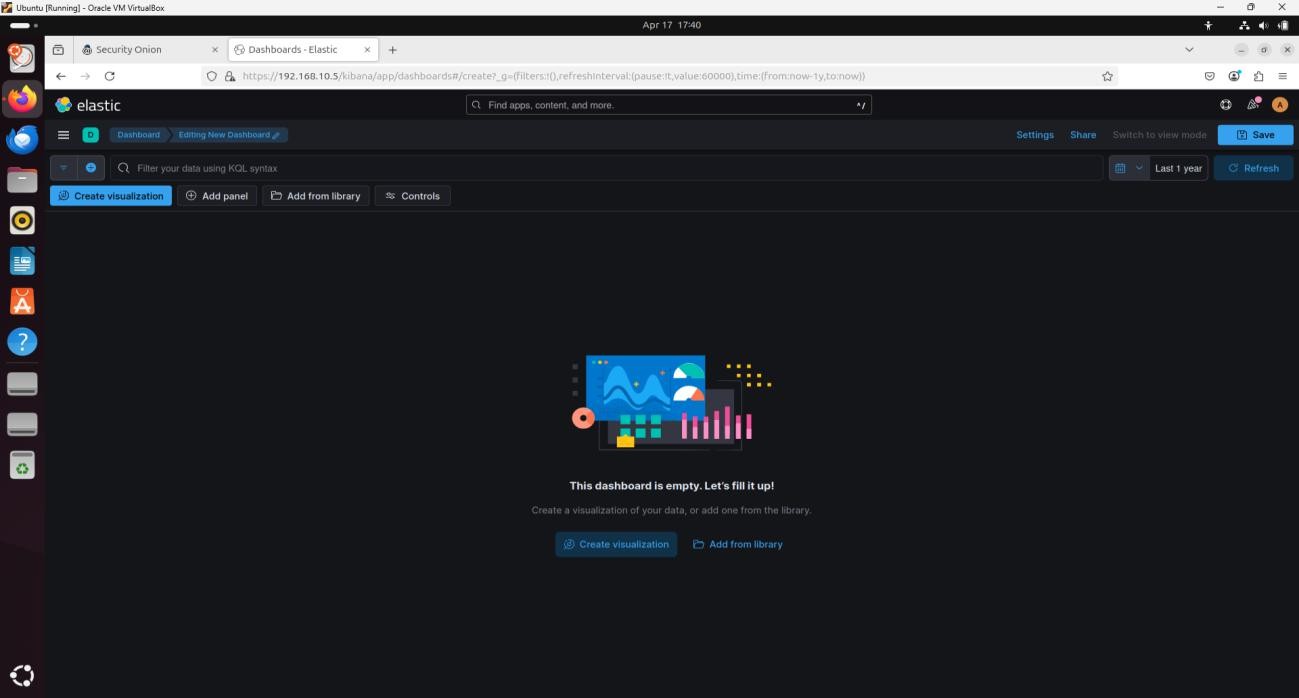




#### 2. Creating a Dashboard

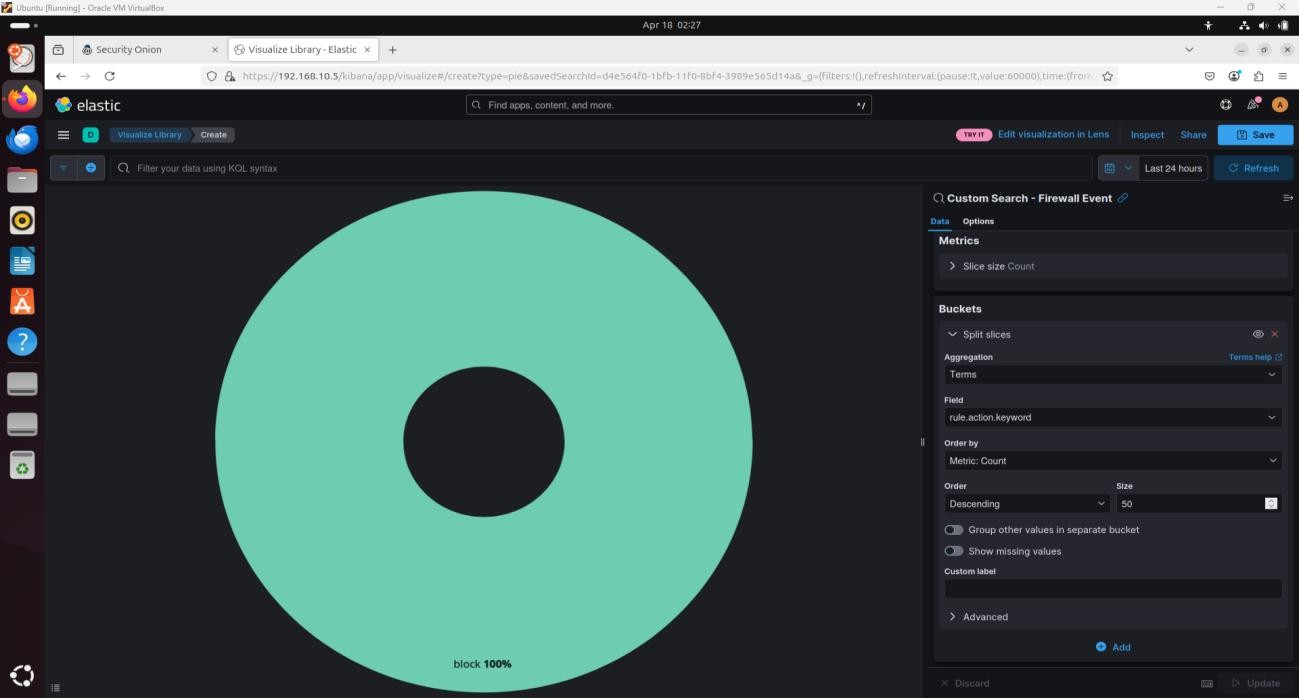
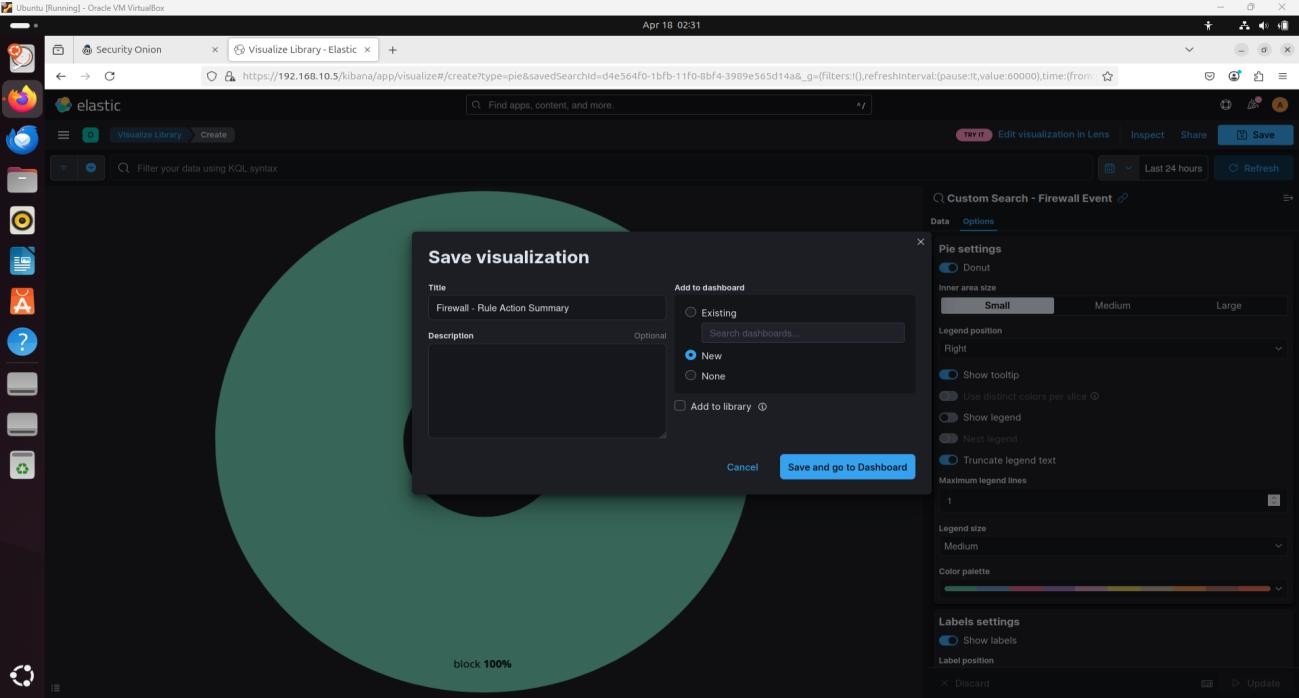
Opened the Dashboards section.

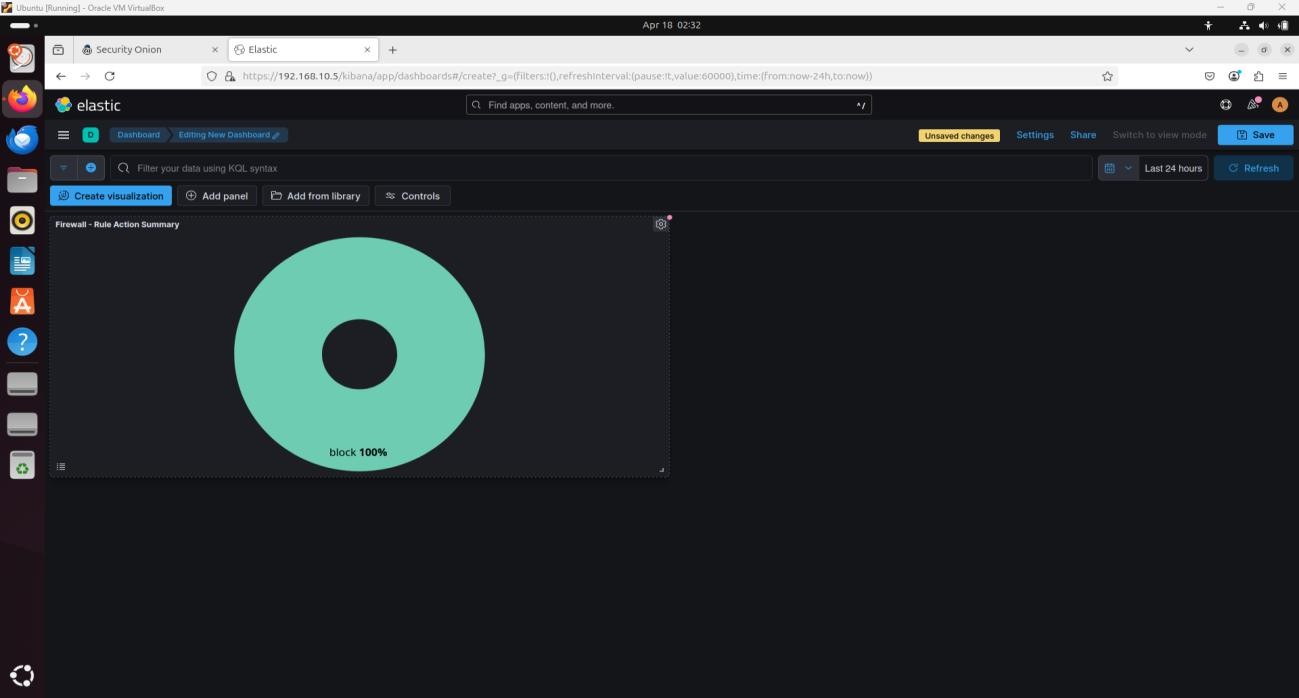
Selected **Create Dashboard** to begin with a blank canvas.

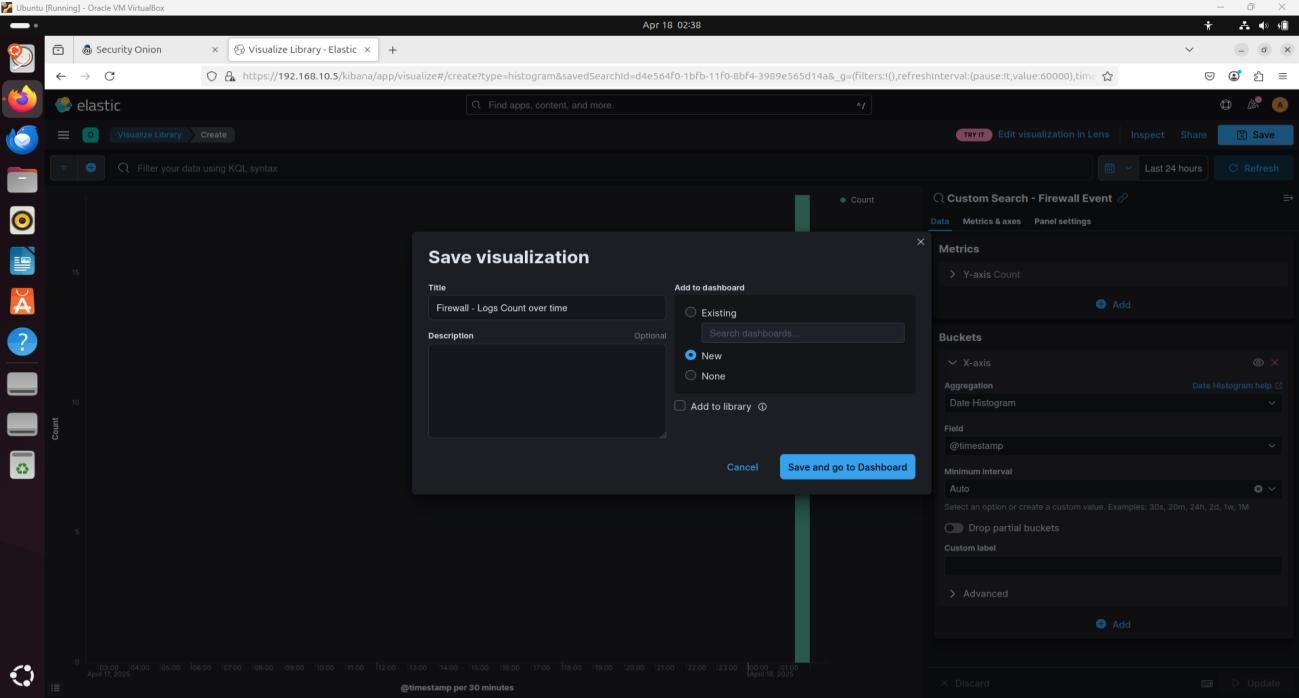


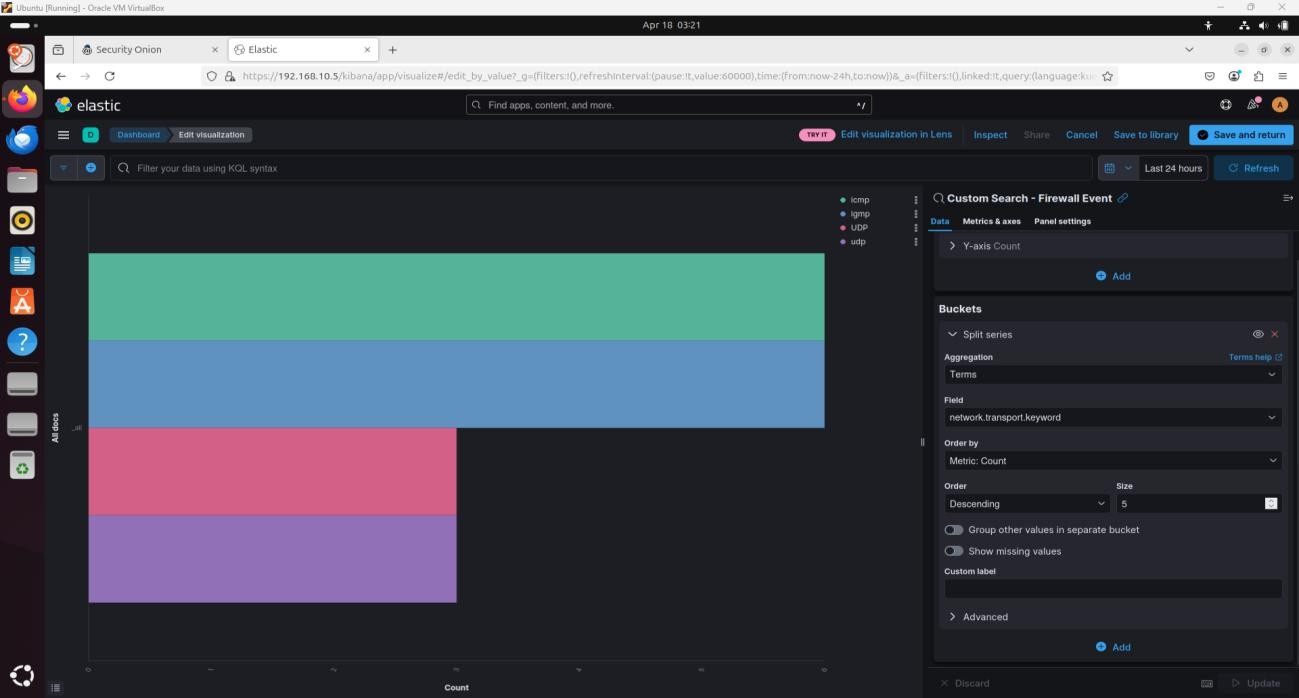
#### 3. Visualization Widgets Added

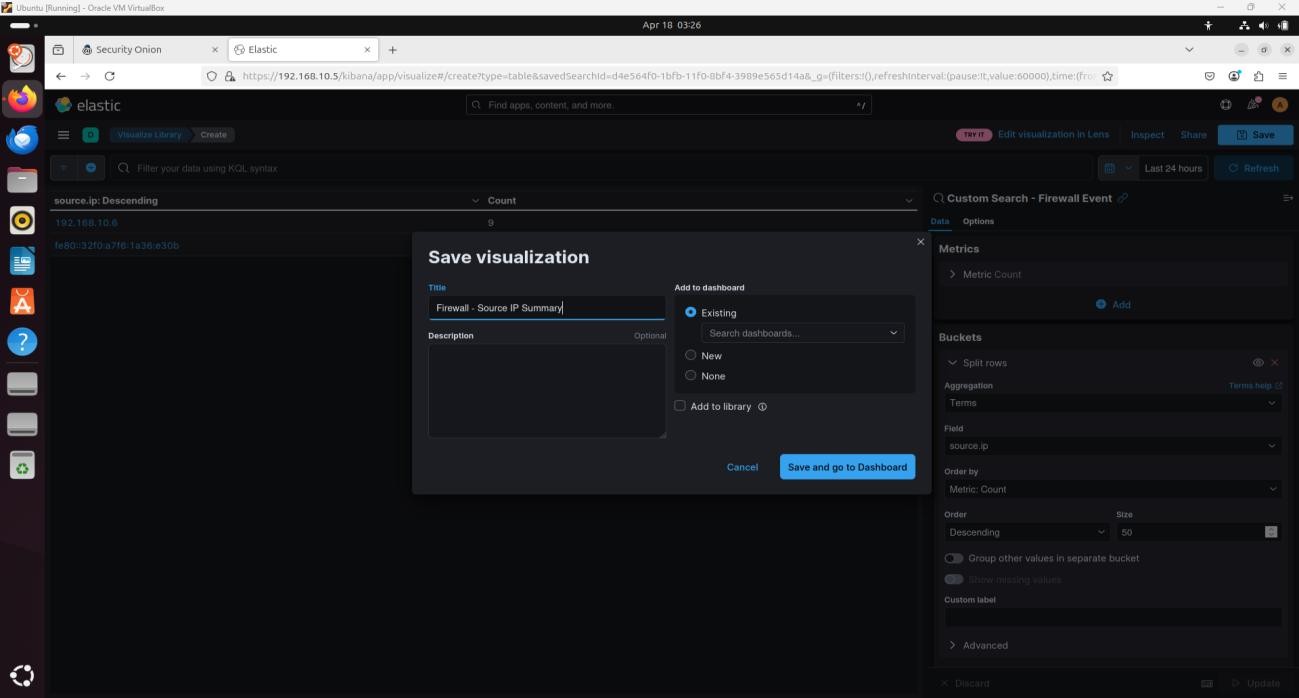
| **Visualization Type** | **Data Source** | **Aggregation Field** | **Widget Title** |
| --- | --- | --- | --- |
| Pie Chart | Custom Search – Firewall Events | rule.action.keyword | Firewall – Rule Action Summary |
| Vertical Bar Chart | Custom Search – Firewall Events | @timestamp (Data Histogram) | Firewall – Logs Count over time |
| Horizontal Bar Chart | Custom Search – Firewall Events | network.transport.keyword | Firewall – Network Protocol Summary |
| Data Table | Custom Search – Firewall Events | source.ip | Firewall – Source IP Summary |
| Data Table | Custom Search – Firewall Events | source.port | Firewall – Source Port Summary |
| Data Table | Custom Search – Firewall Events | destination.ip | Firewall – Destination IP Summary |
| Data Table | Custom Search – Firewall Events | destination.port | Firewall – Destination Port Summary |

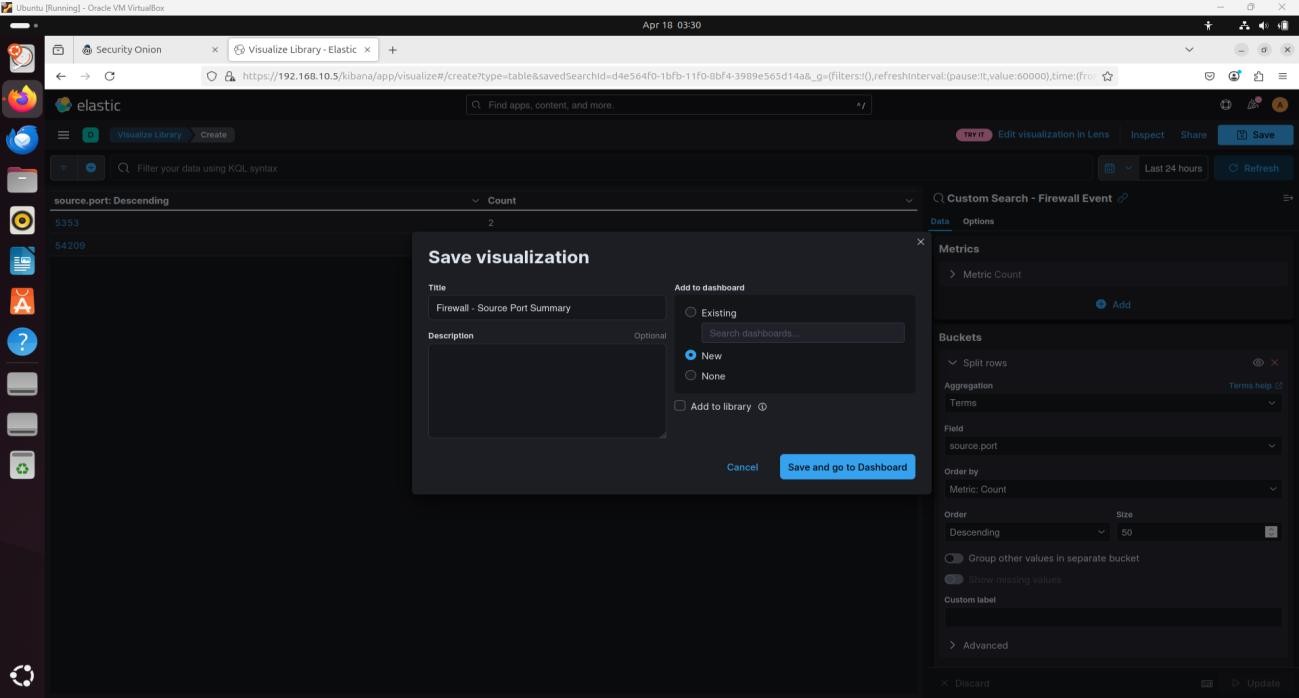
Each visualization was configured with a size limit of 50 terms (where applicable) and styled as appropriate (e.g., Pie instead of Donut).

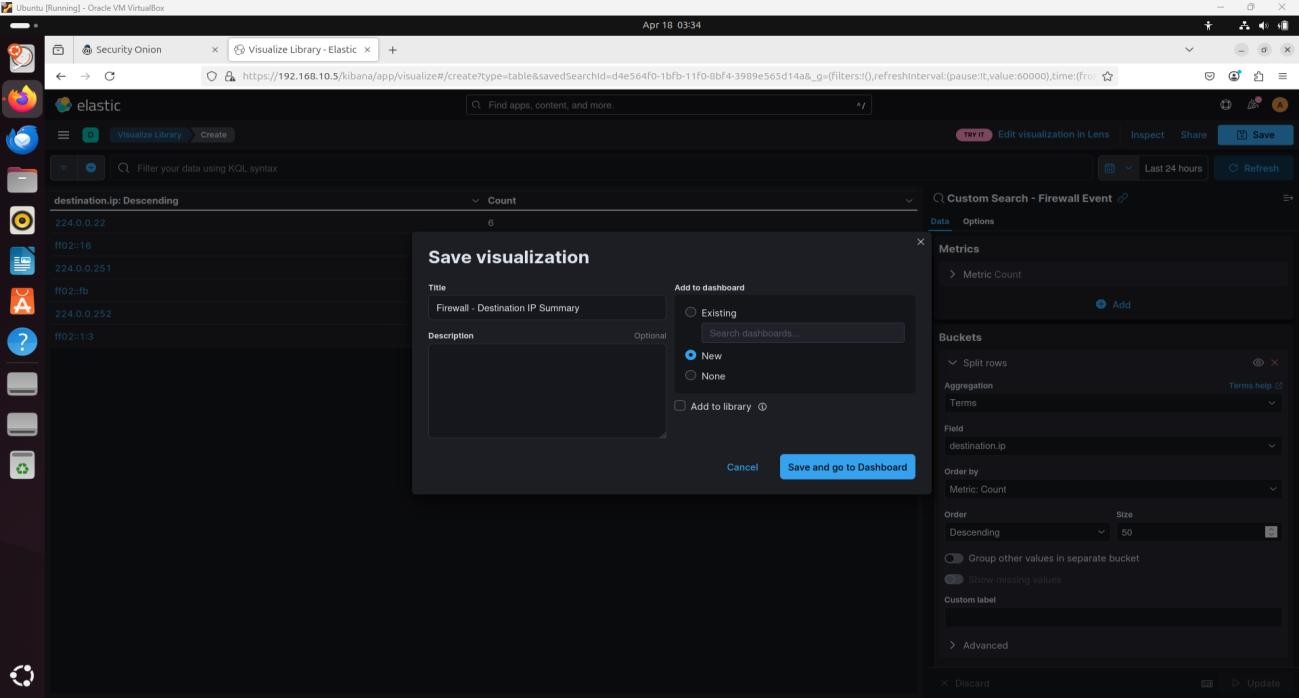


****





****

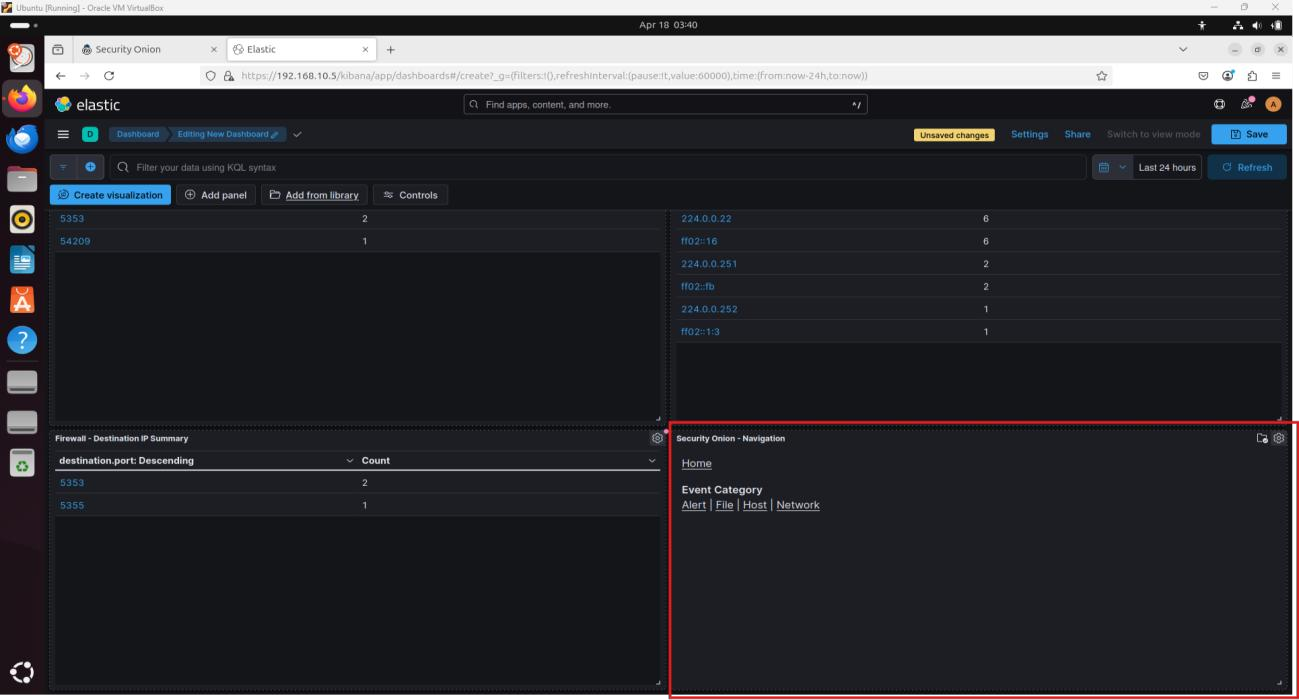


# 

#### 4. Added Library Panels

Used **Add from library** to include:

**Security Onion Navigation** panel

**Custom Search – Firewall Events** detail panel

#### 5. Final Dashboard Assembly

All visualizations were resized, positioned, and arranged for optimal readability.

Saved the dashboard with the name: **Custom Dashboards – Firewall**

**Outcome**

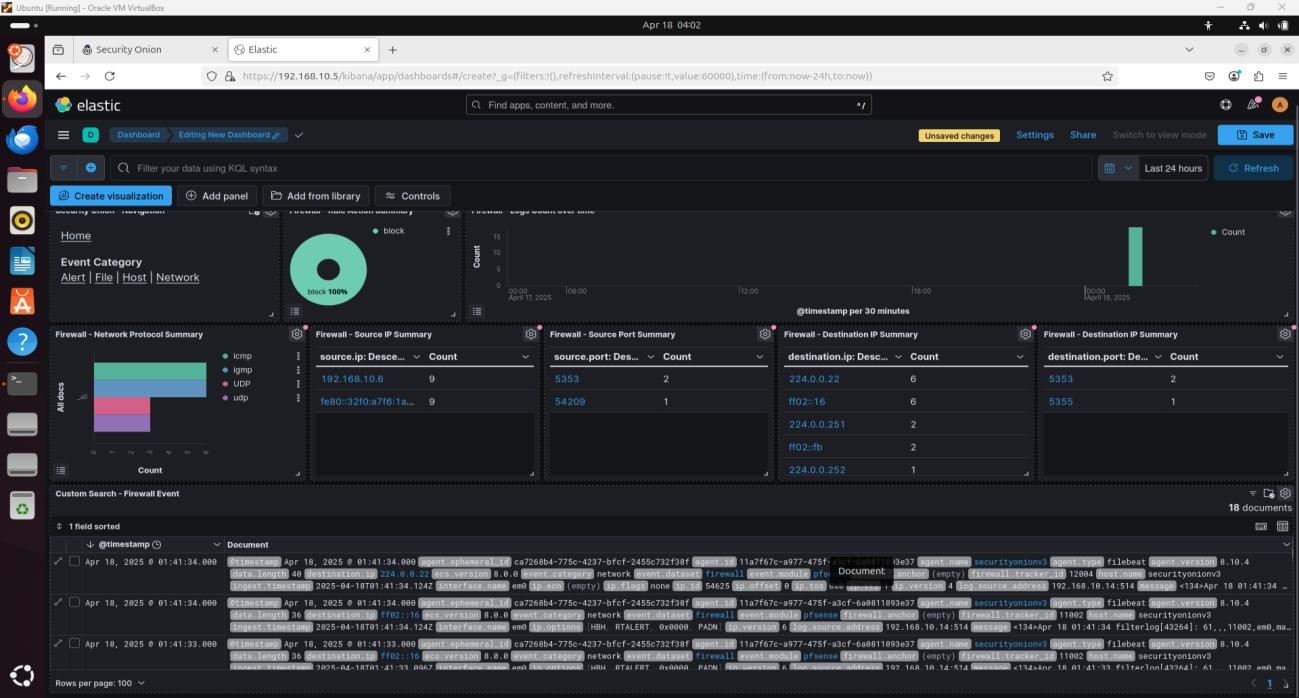
The final result was a unified dashboard providing insights into:

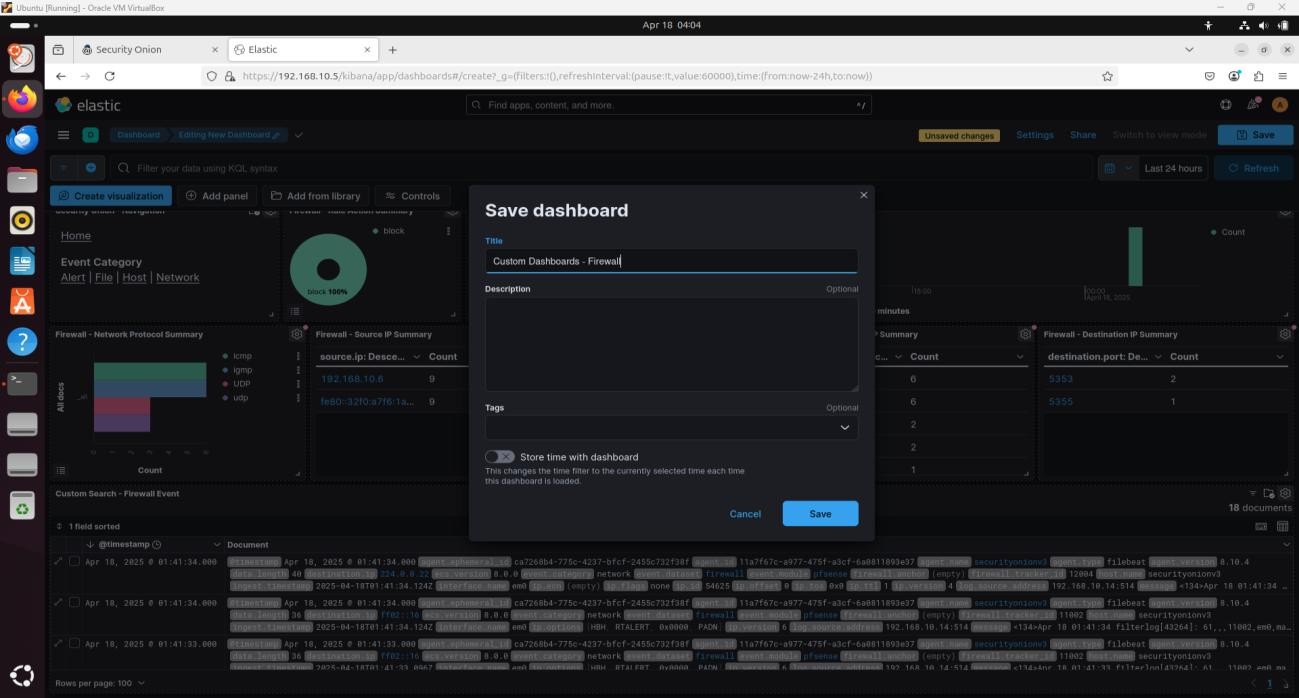
Actions performed by firewall rules

Frequency and time distribution of log entries

Usage of various transport protocols

Frequent source/destination IPs and ports





This dashboard significantly enhances the ability to analyze pfSense firewall data within the Security Onion SIEM platform.

**Reflection**

By completing this lab, I gained practical experience in customizing Kibana dashboards for firewall event analysis. The hands-on process improved my understanding of SIEM visualization workflows and log correlation for network security monitoring.