Lab 7 : Creating a pfSense Firewall event dashboard in Kibana

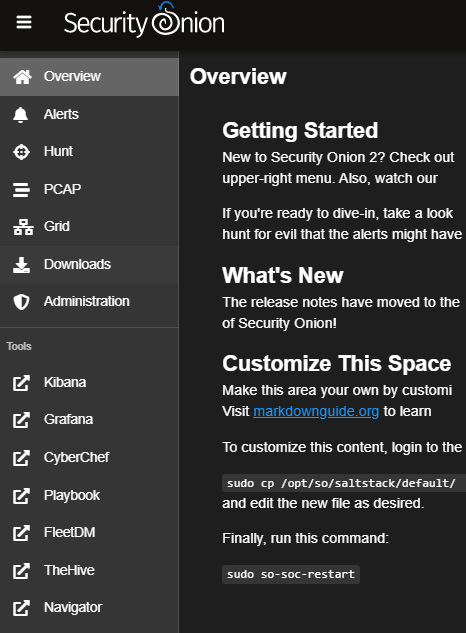
Introduction

To be able to visualize the pfSense logs in Security Onion's **Kibana** tool, we will add a dashboard with relevant data.

**Submission:** You need to submit a detailed lab report, with screenshots, to describe what you have done and observed. Questions will be defined as you progress through the lab. The lab report will be compiled as a Word document and submitted on Brightspace by **MONTH DAY at TIME AM/PM.**

The first thing we need to do to get pfSense alerts displayed on a Kibana dashboard is to define an event search filter. This will make working with firewall events easier and faster. The following instruction will have us create the firewall event search filter:

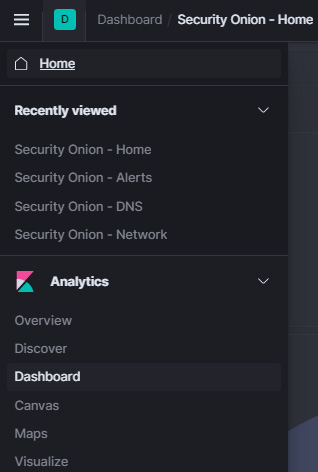
1. Log in to Security Onion and open the **Kibana** tool from the left-side selection panel:



*Figure 9.30 – Exercise 5 – Kibana tool selector*

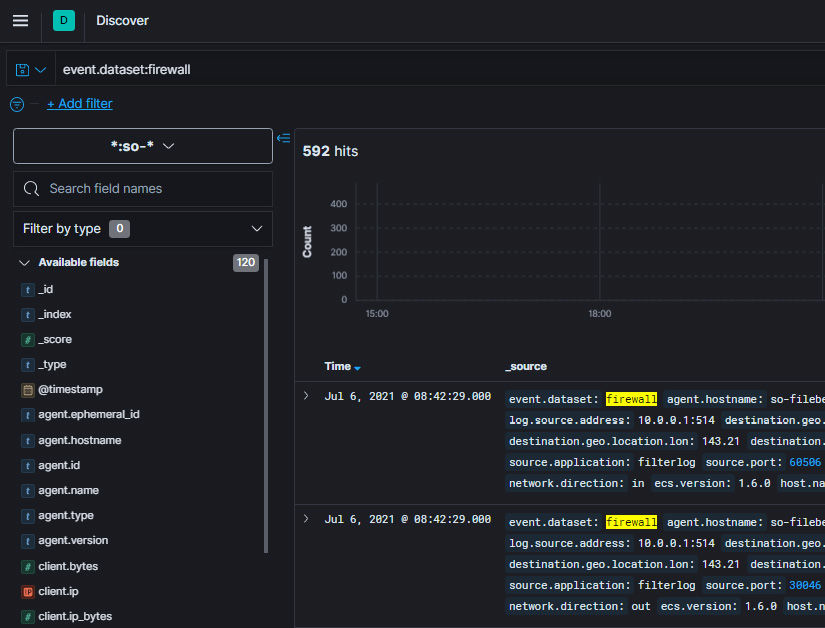
1. This opens a new tab for the Kibana **Home** page. From here, we select the **Discover**

page via the Kibana menu (the button with three horizontal lines at the top left):

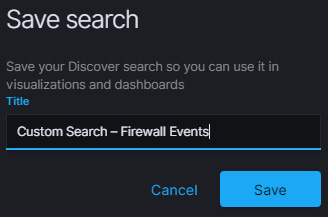


*Figure 9.31 – Exercise 5 – Kibana menu*

1. We now land on the Kibana **Discover** page, where we can perform searches for events and create and save custom search queries.
2. Enter the search string **event.dataset:firewall** to filter for events that are categorized by Zeek as firewall events

*Figure 9.32 – Exercise 5 – Firewall events dataset*

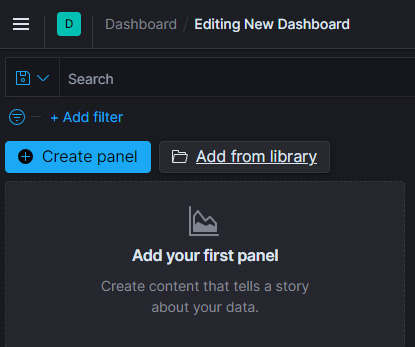
1. That is all we need for now. Click on **Save** (in the top-right corner of the screen) and save as **Custom Search – Firewall Events**:



*Figure 9.33 – Exercise 5 – Save custom search*

With the custom search defined, next, we will add a dashboard to Kibana to display the widgets on. Follow these instructions to get the dashboard created:

1. To get an initial (blank) dashboard started, log in to the Security Onion web portal, open the Kibana tool, and then navigate to [**https://172.25.100.250/kibana/app/dashboards**](https://172.25.100.250/kibana/app/dashboards). From the **Dashboards list** page, click on **Create dashboard**, which will open a blank **Editing New Dashboard** page, as illustrated in the following screenshot:

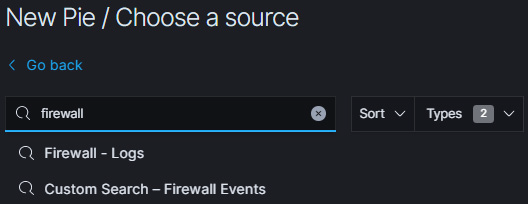


*Figure 9.34 – Exercise 5 – Creating a new dashboard*

2. Now we will add some visualization widgets (panels) to our blank canvas. To do so, click

on Create panel, find and select the pie chart visualization, and search for and select the

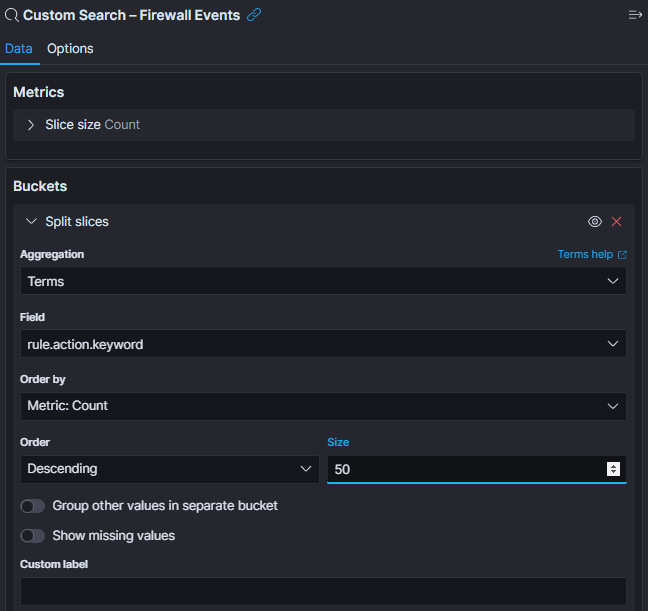
Custom Search – Firewall Events source:



*Figure 9.35 – Exercise 5 – Adding a pie chart widget*

1. Now we will add some visualization widgets (panels) to our blank canvas. To do so, click on **Create panel**, find and select the pie chart visualization, and search for and select the **Custom Search – Firewall Events** source:

For **Field**, select **rule.action.keyword**:

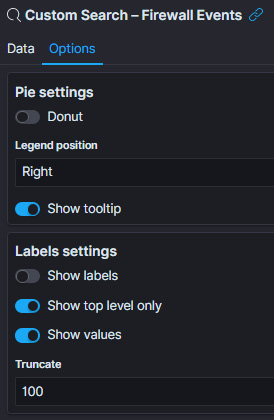
*Figure 9.36 – Exercise 5 – Adding an event data bucket to the pie chart widget*

4. Finally, set Size to 50 and click Update at the bottom of the Buckets configuration

section to save the changes.

5. Our widget is now ready. You could change some of the visual style settings via the

Options menu, such as changing the style from Donut to Pie:



*Figure 9.37 – Exercise 5 – Pie widget options*

1. Once you're done styling the widget, save it via the **Save** button (in the top-right corner of the screen) and name it **Firewall – Rule Action Summary**. This takes us back to the **Dashboard Editing** screen. Here, we can resize the newly created pie chart widget.

Following the same principle, add the following widgets to the dashboard:

* Vertical bar visualization:
  1. **Custom Search – Firewall Events** source
  2. **Data Histogram** data bucket, **Aggregation** set to **@timestamp**
  3. Save as **Firewall – Logs Count over time**:

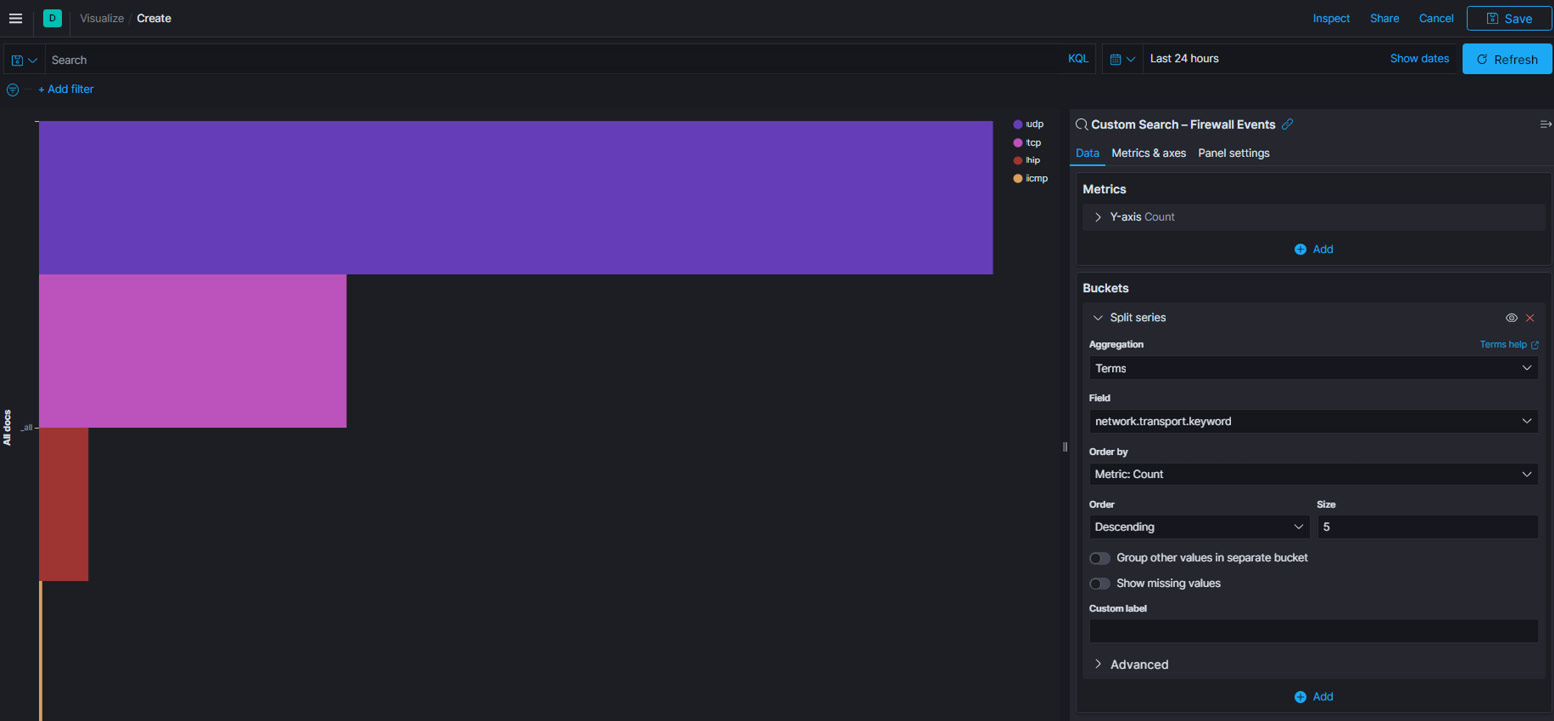
*Figure 9.38 – Exercise 5 – Log Count over time widget*

* Horizontal bar visualization:

1. **Custom Search – Firewall Events** source
2. **Split series** data bucket, **Aggregation** set to **Terms**, and **Field** set to

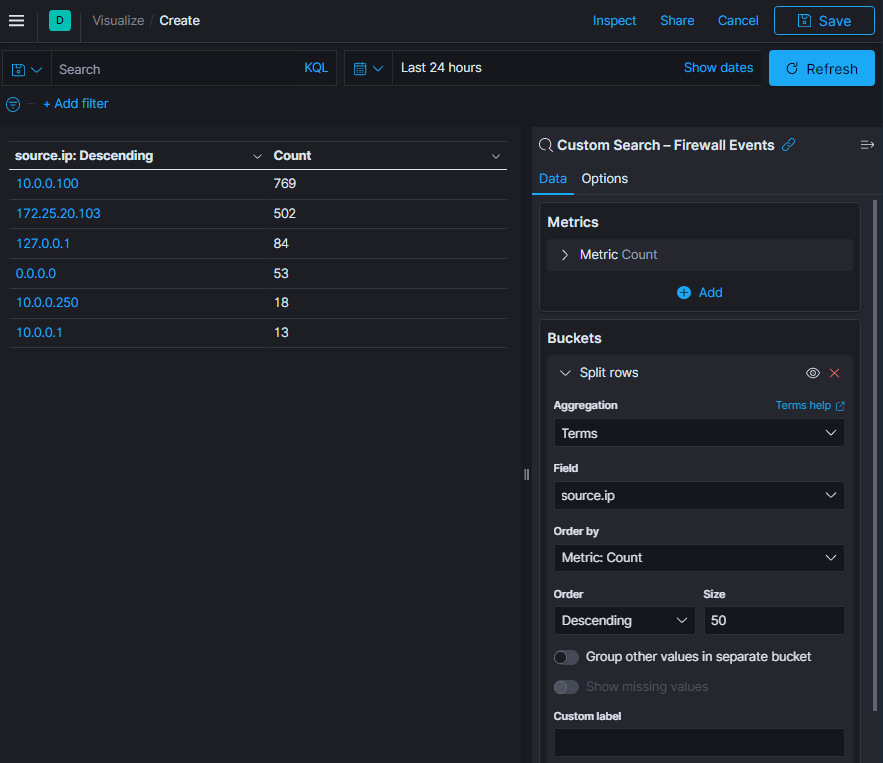
**network.transport.keyword**

1. Save as **Firewall – Network Protocol Summary**:

  *Figure 9.39 – Exercise 6 – Network Protocol Summary widget*

* Data table visualization:

1. **Custom Search – Firewall Events** source
2. **Split rows** data bucket, **Aggregation** set to **Terms**, and **Field** set to **source.ip**
3. Set **Size** to **50**
4. Save as **Firewall – Source IP Summary**:

*Figure 9.40 – Exercise 5 – Source IP Summary widget*

* Data table visualization:

1. **Custom Search – Firewall Events** source
2. **Split rows** data bucket, **Aggregation** set to **Terms**, and **Field** set to

**source.port**

1. Set **Size** to **50**
2. Save as **Firewall – Source Port Summary**

* Data table visualization:

1. **Custom Search – Firewall Events** source
2. **Split rows** data bucket, **Aggregation** set to **Terms**, and **Field** set to

**destination.ip**

1. Set **Size** to **50**
2. Save as **Firewall – Destination IP Summary**

* Data table visualization:

1. **Custom Search – Firewall Events** source
2. **Split rows** data bucket, **Aggregation** set to **Terms**, and **Field** set to

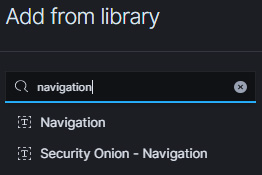
**destination.port**

1. Set **Size** to **50**
2. Save as **Firewall – Destination Port Summary**

To wrap up the firewall logs dashboard, we will add some existing panels:

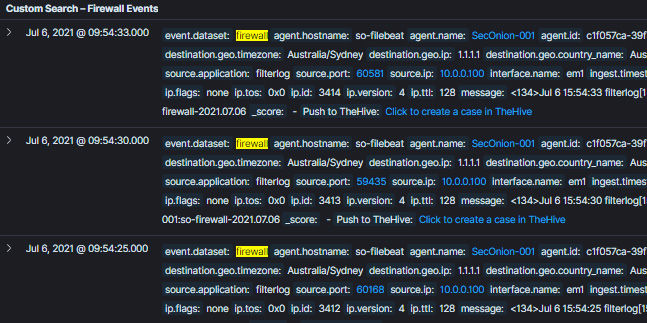
1. Click on the **Add from library** button and search for and select the Security Onion

**Navigation** panel.



*Figure 9.41 – Exercise 5 – Adding a widget from the library*

1. Next, search for and select the **Custom Search – Firewall Events** custom search panel. This adds an event detail panel to the dashboard, much like what's shown on the **Discover** page:

*Figure 9.42 – Exercise 5 – Event detail panel*

Close the **Add from library** screen.

We are done editing the new dashboard. You should reorganize, shovel, position, and resize the widgets (panels) to your liking and save the dashboard as **Custom Dashboards – Firewall** via the **Save** button once you are done. The following figure shows my firewall dashboard layout:

*Figure 9.43 – Exercise 5 – The author's firewall dashboard – for illustrative purposes only*

We now have a convenient way to view, search, correlate, and display firewall event logs.