Network traffic patterns between a source-destination pair

You might want to know the frequency and volume of network traffic between a source-destination pair in a certain period of time compared to all-time when doing the following:

- Monitoring for network traffic outliers

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Firewall data

Example

You hypothesize that a network user only accesses a certain external website sporadically. You want to see when those connections occur and how much each occurrence contributes to the overall bytes out from that source to the destination.

To optimize the search shown below, you should specify an index and a time range. In addition, this sample search uses Fortinet FortiGate data. You can replace this source with any other firewall data used in your organization.

1. Run the following search:

```
sourcetype=fgt_traffic src=<IP address sending the request> dest=<IP address receiving the request> bytes_out>0
| sort date
| streamstats sum(bytes_out) AS total_bytes_out BY src
| table date bytes_out total_bytes_out
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
### Splunk Search

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=fgt_traffic</td>
<td>Search only Fortinet FortiGate network traffic data.</td>
</tr>
<tr>
<td>src=&lt;IP address sending the request&gt;</td>
<td>Search data coming from this IP address.</td>
</tr>
<tr>
<td>dest=&lt;IP address receiving the request&gt;</td>
<td>Search data going to this IP address. Logs vary in the information they contain. Not all logs have hostnames or IP addresses. Sometimes the dest field will have a hostname in it but sometimes it will have an IP address. Parentheses and OR statements will broaden your search so you don’t miss anything.</td>
</tr>
<tr>
<td>bytes_out&gt;0</td>
<td>Exclude results that do not have any outgoing traffic.</td>
</tr>
<tr>
<td>sort date</td>
<td>Sort the results with the oldest date first.</td>
</tr>
<tr>
<td>streamstats sum(bytes_out) AS total_bytes_out BY src</td>
<td>Stream a running total volume of bytes_out for all preceding events and display in a total_bytes_out column.</td>
</tr>
<tr>
<td>table date bytes_out total_bytes_out</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

### Result

The results display the total bytes out for the destination on each day and a cumulative bytes out for the time range you specify.
selected. Selecting the Visualizations tab and displaying the results in an area chart or a line chart can give you a quicker understanding of the network communication pattern between the source and the destination. You can compare these results to those of network users who your baselines show should have similar usage patterns to start to understand if there is anything unusual happening.