Total bytes out from source IP addresses

You might want to compare the total bytes going out from a source IP address to those going to each destination IP address 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 want to create an accurate picture of outbound traffic on your network from each source IP address so that you can monitor for anomalous behavior.

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> NOT (dest=<Internal IP address> OR dest=<DNS>) bytes_out>0 | eventstats sum(bytes_out) AS total_bytes_out BY src | table src dest bytes_out total_bytes_out | sort src – 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.

<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>
</tbody>
</table>
**Splunk Search**

<table>
<thead>
<tr>
<th>src=&lt;IP address sending the request&gt;</th>
</tr>
</thead>
</table>

**Explanation**

Search data coming from this IP address.

If you want to search all IP addresses in a netblock, use a wildcard search. For example, src=192.168.255.*

<table>
<thead>
<tr>
<th>NOT (dest=&lt;Internal IP address&gt; OR dest=&lt;DNS&gt;)</th>
</tr>
</thead>
</table>

**Explanation**

Exclude internal and DNS destination IP addresses.

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.

**Example:**

(dest="192.0.2.0" OR dest_ip="192.0.2.0")

**Example:**

(dest="192.0.2.0" OR dest="example.com")

<table>
<thead>
<tr>
<th>bytes_out&gt;0</th>
</tr>
</thead>
</table>

**Explanation**

Exclude results that do not have any outgoing traffic.

<table>
<thead>
<tr>
<th>eventstats sum(bytes_out) AS total_bytes_out BY src</th>
</tr>
</thead>
</table>

**Explanation**

Calculate the total volume of bytes_out to any destination for each source and display in a total_bytes_out column.

<table>
<thead>
<tr>
<th>table src dest bytes_out total_bytes_out</th>
</tr>
</thead>
</table>

**Explanation**

Display the results in a table with columns in the order shown.

<table>
<thead>
<tr>
<th>sort src – bytes_out</th>
</tr>
</thead>
</table>

**Explanation**

Sort the results by source with the lowest IP address first, and then by bytes_out with the largest volume of bytes_out for each source first.
Result

Use the results to establish baselines for each source IP address. You may want to investigate any destination that receives an unusually high amount of traffic from the overall bytes_out of a source. Adding on to your search to show percentages can help you determine more quickly whether there are IP addresses you want to investigate.