Number of active VPN sessions

You might need to know how many active VPN sessions there are on your network when doing the following:

- Securing a work-from-home organization

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security analyst
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: [VPN data](#), normalized to [the Network Sessions data](#) Common Information Model (CIM). For information on installing and using the CIM, see the [Common Information Model](#) documentation.

Example

Your workforce is fully remote. To ensure network security, you want to report on how many active VPN sessions there are on your network at certain times of the day.

To optimize the search shown below, you should specify a time range.

1. Run the following search:

   ```splunk
   | tstats count(All_Sessions.user) FROM datamodel=Network_Sessions WHERE `rw_vpn_indexes` nodename=All_Sessions.VPN
   ```

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></td>
<td>tstats count(All_Sessions.user) FROM datamodel=Network_Sessions WHERE <code>rw_vpn_indexes</code> nodename=All_Sessions.VPN</td>
</tr>
</tbody>
</table>

Search the All_sessions data set for users in a VPN network session event.

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.
Result

This search returns a simple count of all active VPN sessions during the time you specify. Correlate this information with the results of other searches to determine what is normal or anomalous activity on your network.