Network switch data

Switches are network intersections, places where packets move from one network segment to another. In their purest form, switches work within a particular IP subnet and can’t route Layer 3 packets to another network. Modern data center designs typically use a two-tier switch hierarchy: top-of-rack (ToR) switches connecting servers and storage arrays at the edge, and aggregation or spine switches connecting to the network core. Although ethernet switches are far more widespread, some organizations also use fiber channel or infiniband for storage area networks or HPC interconnects, each of which has its own type of switch.

Operations teams use switch logs to see the state of traffic flow, such as source and destination, class of service, and causes of congestion. Logs can show traffic statistics in the aggregate, by port and by client, and whether particular ports are congested, failing or down. Switch data, often captured as NetFlow records, is a critical data source for flagging advanced persistent threats, analyzing traffic flows for unusual activity and identifying potential data exfiltration.

Application

When your Splunk deployment is ingesting network switch data, you can use it to accomplish security and compliance and IT Ops use cases.

- Managing Cisco IOS devices
- Finding large web uploads

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with network switch data.

- Arista Networks Telemetry For Splunk
- Splunk Add-on for Forcepoint Web Security
- Splunk Add-on for McAfee Web Gateway
- Splunk Add-on for Cisco WSA
- Cisco Networks Add-on for Splunk Enterprise
- Splunk Add-on for Websense DLP