Virtual private network data

Virtual private networks (VPNs) are a way of building a secure extension of a private network over an insecure, public one. VPNs can be established either between networks, routing all traffic between two sites, or between a client device and a network. Network-to-network VPNs typically are created using strong credentials such as certificates on each end of the connection. Client-to-network VPNs rely on user authentication, which can be as simple as a username and password. VPNs use network tunneling protocols such as IPSec, OpenVPN plus SSL or L2TP with cryptographically strong algorithms to scramble information in transit and ensure end-to-end data integrity.

VPN logs help analyze users coming onto the network. This information can be used in a number of ways, including situational awareness, monitoring foreign IP subnets, and compliance monitoring of browsers and applications of connected hosts. Connection logs are generated by the majority of VPN devices and services. Information included in these logs reflects activity such as login/logout, dates, times, remote IP addresses, and user login names. Usage logs provide activity data that includes online browsing history and activity that reflects a user's navigation and access of network resources during the session. In the Common Information Model, VPN data is typically mapped to the Network Sessions data model and Authentication data model.

Application

When your Splunk deployment is ingesting VPN data, you can use it to accomplish security and compliance use cases.

- Processing DMCA notices
- Securing a work-from-home organization

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 VPN data.

- Splunk Add-on for Check Point OPSEC LEA
- Palo Alto Networks Add-on for Splunk
- Splunk Add-on for Citrix NetScaler