Firewall data

Firewalls demarcate zones of different security policy. By controlling the flow of network traffic, firewalls act as gatekeepers collecting valuable data that might not be captured in other locations due to the firewall’s unique position as the gatekeeper to network traffic. Firewalls also execute security policy and thus may break applications using unusual or unauthorized network protocols. Basic firewalls operate on layers 3 and 4 of the OSI model. Many modern firewalls can combine with other device functions and produce additional data, such as proxy and network intrusion detection data.

Firewall data can provide visibility into which traffic is blocked and which traffic has passed through. Logs provide a detailed record of traffic between network segments, including source and destination IP addresses, ports and protocols, all of which are critical when investigating security incidents.

Application

Security

- Reconstructing a website defacement
- Monitoring for network traffic volume outliers
- Managing firewall rules
- Detecting the use of randomization in cyber attacks
- Detecting network and port scanning
- Detecting TOR traffic
- Monitoring employee network traffic

Compliance

- Complying with General Data Protection Regulation
- Monitoring NIST SP 800-53 rev5 control families

Sources

Guidance for onboarding data can be found in the Spunk 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 firewall data.

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

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 Add-on for Cisco FireSIGHT
• Splunk Add-on for Cisco ASA
• Splunk Add-on for Fortigate
• Splunk Add-on for Imperva SecureSphere WAF
• Splunk Add-on for Juniper