**A DOCUMENT ON LOG MONITORING**

**Overview**

Log and event management is the process of collecting, analysing, and managing log data and event information generated by various systems and applications within an organization. The purpose of log and event management is to detect and respond to security incidents, system failures, and operational issues.

Log data is generated by various systems and applications within an organization. This data includes information such as user activity, system events, and application behaviour. Event information is generated when a specific event occurs, such as a system crash or a security breach.

Log and event management solutions provide organizations with the ability to collect and analyze log data and event information in real-time. This helps organizations detect security threats and operational issues before they become serious problems.

The process of log and event management involves several steps, including:

1. Collection: Logs and events are collected from various systems and applications within an organization.

2. Normalization: The collected logs and events are normalized into a common format, making it easier to analyse the data.

3. Aggregation: The normalized logs and events are aggregated into a centralized repository for analysis.

4. Analysis: The aggregated logs and events are analysed to identify security threats, system failures, and operational issues.

5. Alerting: When a security threat or operational issue is detected, an alert is sent to the appropriate personnel.

6. Reporting: Reports are generated to provide insights into system and application behavior, security incidents, and operational issues.

7. Effective log and event management is essential for organizations to maintain the security and stability of their systems and applications. It allows organizations to detect and respond to security incidents and operational issues in a timely manner, reducing the impact on the organization.

**Product and Environment**

**Sophos Firewall - All supported versions**

****

Device provides extensive logging capabilities for traffic, system, and network protection functions. Detailed log

information and reports provide historical as well as current analysis of network activity to help identify security

issues and reduce network misuse and abuse.

Device provides following logs:

• System Logs

• Web Filter Logs

• Application Filter Logs

• Malware Logs

• Email Logs

• Firewall Logs

• IPS Logs

• Authentication Logs

• Admin Logs

• Sandstorm Logs

• Web Server Protection Logs

• Advanced Threat Protection Logs

• Security Heartbeat Logs

• Web Content Policy Logs

To view logs for all modules, go to Log Viewer page.

**Log Viewer**

Use Log Viewer to view the logs for modules like System, Web filter, Application Filter, Malware, Email, Firewall, IPS, Authentication, Admin, Sandstorm, Web Server Protection, Advanced Threat Protection, Security Heartbeat and Web Content Policy. This page gives consolidated information about all the events logged by your device.

You can also open multiple live packet capture windows with different filers from this page. To view them, you need to enable Packet Capture from Monitor & Analyze > Diagnostics > Packet Capture. It is recommended to enable Wrap Capture Buffer Once Full on Configure Capture Filter page to continue capturing packets after the buffer is full.

Click Open PCAP link under Live PCAP column to view packet capture in a new window. It will display the packet captures that are automatically filtered based on the values of the currently selected packet. Click Display Filter in the packet capture window to modify the filters.



