**SOPHOS XGS7500 (SFOS 21.0.1 MR-1-Build277)**

**Prepared by: Chetan Sai C**

**1. Objective**

To define standard procedures for monitoring, managing, and responding to security events using Sophos XG 7500 firewall. This SOP applies only to the security module and functions managed by the security operations team.

**2. Scope**

Covers only security-related features such as IPS, ATP, Web Filtering, threat signatures, and incident logging.

**Daily Tasks**

| **Task** | **Description** |
| --- | --- |
| **Check Security Dashboard** | Navigate to Monitor & Analyse > Dashboard to review threat summary, dropped packets, and high-risk applications. |
| **Review ATP & IPS Alerts** | Go to Protect > Advanced Threat Protection and Protect > Intrusion Prevention for any blocked IPs, exploits, or intrusions. |
| **Log Status Check** | Check logs in Log Viewer under Security, Web Filter, and IPS tabs. |
| **Update Signatures** | Verify IPS/ATP updates under System > Backup & Firmware > Pattern Updates. Ensure definitions are updated daily. |

**Sophos Dashboard: -**

A screenshot of a computer

AI-generated content may be incorrect.

**Checking the logs:**

A screenshot of a computer

AI-generated content may be incorrect.

* First click on the top right corner log viewer button to view the logs
* After clicking on the log viewer, we will be navigated to the log viewer dashboard

A screenshot of a computer

AI-generated content may be incorrect.

* We will be having various components to search the logs from i.e. Add filters which consists of Source IP, Destination IP, PORTS, Username etc
* The below is attached screenshot of the add filters button
* A screenshot of a computer

  AI-generated content may be incorrect.
* The next components are Log Categories which consists of Firewall, IPS, Malware, Zero day, WAF

A screenshot of a computer

AI-generated content may be incorrect.

* The last components is the time filter, we can see filter by time to view the logs

A screenshot of a computer

AI-generated content may be incorrect.

**Reports: -**

In Sophos Firewall, the Reports section dashboard provides a centralized visual summary of key network and security activities

A screenshot of a computer

AI-generated content may be incorrect.

* Next section outlines the Application and Web reports

A screenshot of a computer

AI-generated content may be incorrect.

* The below screenshot showcases the High-Risk applications present in our network.

A screenshot of a computer

AI-generated content may be incorrect.

* To view detailed information about high-risk applications, click the 'View More' button.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* If we observe any external VPNs, proxies, adult content, gaming, or torrent websites in the list, we must inform the network team and block the relevant applications. Additionally, we should check the amount of data transferred, especially if it is in GB or TB.

**Network and threats**

* There is various type of attack categories present in the network and threats reports i.e. Intrusion attacks, Active threat response, wireless, security heartbeat and zero protection

**Intrusion Attacks** – Detected by the IPS engine (e.g., exploit attempts, port scans).

A screenshot of a computer

AI-generated content may be incorrect.



**Intrusion attacks**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Active threat response: -**

Real-time threat mitigation events initiated by the firewall or synchronized endpoints.

**A screenshot of a computer

AI-generated content may be incorrect.**



**Zero-Day Protection** – Threats detected using machine learning or sandboxing, including unknown or newly emerging threats.

A screenshot of a computer

AI-generated content may be incorrect.

**Intrusion prevention**

* The Intrusion Prevention section in Sophos Firewall focuses on detecting and blocking suspicious or malicious network activity that matches known attack patterns or behaviours.
* In the below attached screenshot, we need to check the time of signature update and review it regularly to make sure signatures are getting updated.

A screenshot of a computer

AI-generated content may be incorrect.