**SOPHOS Web Application Firewall: -**

**Prepared by: Chetan Sai C**

Purpose: To ensure secure web access by filtering malicious, inappropriate, and unauthorized web content using Sophos Web Protection. This SOP outlines the steps to monitor, manage, and maintain Web Protection policies.

**Scope:**

* Applies to 3 servers -IDP, DRUPAL and test ERP server, all users and systems using the organization's internet through the Sophos firewall or endpoint agents with web protection enabled.

**URL’s: -**

* idp.alliance.edu.in
* aulibrary.alliance.edu.in
* Waf.alliance.edu.in

**Key Features of Sophos Web Protection:**

* URL Filtering: Categorizes and blocks access to risky or non-compliant websites (e.g., gambling, adult, proxies). Uses reputation-based analysis and custom URL groups.
* Download Scanning (Web Threat Protection): Scans files and websites in real-time before download. Blocks or warns users if files contain malware, exploits, or are hosted on compromised domains.
* HTTPS Scanning (SSL Inspection): Decrypts and inspects HTTPS traffic to detect hidden threats. Ensures secure applications are also filtered for content threats. Policy Enforcement: Applies user/group-based web filtering policies.
* Integration with Active Directory or LDAP for role-based control. Time-Based Browsing Control: Limits internet usage for specific categories during work hours (e.g., block social media 9 AM–6 PM).
* Reporting and Logging: Provides detailed logs of web usage and threat detection. Alerts for policy violations and access attempts to blocked websites.

A screenshot of a computer

AI-generated content may be incorrect.



* To view WAF logs in Sophos Firewall, log in to the firewall dashboard, navigate to the 'Log Viewer' section, and from the dropdown menu, select 'Web Server Protection'—you will then see all relevant WAF events and logs.

A screenshot of a computer

AI-generated content may be incorrect.

| * **Field Name** | * **Description** | * **Use/What to Look For** |
| --- | --- | --- |
| * **Time** | * Timestamp of the event | * Helps correlate events with user activity or attacks |
| * **Server** | * Destination web server IP or name (reverse proxy target) | * Identifies which internal server was accessed or attacked |
| * **Source IP/Name** | * IP address or hostname of the request initiator | * Key for identifying attackers or clients |
| * **URL** | * Requested URL | * Analyse for suspicious paths, injection attempts, or unauthorized access |
| * **Reason** | * Why the request was blocked or logged (e.g., SQLi, XSS, Invalid Header) | * Indicates type of threat or rule triggered |
| * **Message** | * Detailed description of the event | * Gives context to the reason field |
| * **Status Code** | * HTTP status returned (e.g., 200, 403, 500) | * Useful for diagnosing failed requests or blocked responses |
| * **Bytes Received** | * Data received by the server from client | * Helps understand size of upload or request |
| * **Bytes Transmitted** | * Data sent by server to the client | * Indicates size of response or file download |
| * **Message ID** | * Unique ID for the log entry | * Used for tracking and referencing specific logs |
| * **Policy ID** | * The WAF policy or rule ID triggered | * Useful for tuning or identifying misconfigured rules |
| * **Live PCAP** | * Option to download/view packet capture for the event | * Used for deep packet inspection and forensic analysis |

* In Sophos WAF logs, events are color-coded—red indicates a bad reputation or malicious attempt, while green represents legitimate or successful access requests.

A computer screen shot of a computer screen

AI-generated content may be incorrect.





