Standard Operating Procedure (SOP) - Information Security Management

Document ID: ISM-SOP-001
Effective Date: 18th Jan 2024
Version: 1.0
Prepared By: Information Technology Team
Approved By: Senior IT Manager – Sagar Pardeshi

---

1. Purpose

This SOP provides a structured approach for managing network security using Sophos Firewall to protect organizational data, monitor traffic, detect threats, and enforce security policies.

---

2. Scope

Applies to all systems, users, and third-party vendors connected to the organization's internal network and managed through Sophos Firewall.

---

3. Objectives

- Control and secure internet access.
- Implement and enforce firewall policies.
- Monitor and report network activity.
- Prevent data leakage, malware, and unauthorized access.

---

4. Responsibilities

Role	Responsibilities
Senior IT Manager	Approve and review security rules and configurations.
IT Manager	Manage, update, and monitor Sophos Firewall.

Role	Responsibilities
IT Manager	Execute configurations and respond to alerts.
All Employees	Comply with security policies and report any suspicious activity.

---

5. Firewall Management Procedures

5.1 Configuration & Deployment

- Configure and maintain the Sophos Firewall to ensure continuous network protection.
- Establish and label distinct network zones such as:

  LAN (Local Area Network): Internal, trusted network where users, servers, and workstations reside.
- WAN (Wide Area Network): External network, typically the internet and the connectivity between branch offices.
- DMZ (Demilitarized Zone): DMZ isolates external access and enforcing firewall rules to prevent attackers from reaching sensitive internal systems, thereby enhancing overall security of web servers and data storage devices.
- VPN (Virtual Private Network): A secure zone for encrypted remote access, allowing users to connect to the internal network over the internet.

5.2 Access Control

- Apply User-Based Access Policies using Active Directory integration.
- Integrating firewall with Active Directory (AD) enables centralized authentication and policy enforcement and employees gets access to resources based on their group, department.
- Define application control rules (block social media, entertainment, etc., as per policy).
- Web filters categorize websites and allow/block them based on company policy (e.g., block gambling, adult content, unauthorized cloud storage).

5.3 Firewall Rules & NAT

- Firewall rules control which services are permitted to communicate across network zones (LAN, DMZ, WAN, etc.). This protects systems from unauthorized access and unnecessary exposure.

- Set up firewall rules for allowed services (e.g., DNS, HTTP/S, mail).
- Use Least Privilege Principle – deny all by default, allow by exception. Only explicitly approved traffic/services are allowed through firewall rules. (e.g., Instead of allowing all outbound ports, only open the required ones like 443 (HTTPS) for internet browsing).
- **NAT (Network Address Translation)** hides internal (private) IPs by mapping them to a public IP when accessing external networks (like the Internet). This ensures security and privacy by masking internal network topology.

5.4 Threat Protection Modules

Enable the following Sophos modules:

- **IPS (Intrusion Prevention System)** monitors network traffic in real time to identify and block known exploits, intrusion attempts, and vulnerabilities (e.g., SQL injection, buffer overflows).
- **Web Filtering** enables to filter internet traffic based on URL categories, reputation, and custom blocklists (e.g., block adult content, gambling, malware sites). This prevents users from accessing harmful or non-business websites
- **Application Control** enables to restrict usage of unwanted applications (e.g., torrents, proxy tools, games, remote desktop apps).
- **AV Scanning** scans incoming and outgoing files and traffic for viruses, spyware, Trojans, etc., and protects against known malware threats at the gateway level.

5.5 VPN Access

- **SSL VPN** provides secure, encrypted access to internal network resources (servers, files, apps) via the internet. It uses SSL/TLS protocols (same as HTTPS) and is ideal for remote employees or field staff. Access is typically done via dedicated VPN client.
- **IPSec VPN** securely connects two fixed networks (Head office connectivity with branch office).
- Regularly review **VPN logs** for anomalies (e.g., access from unknown IPs or geographies).

---

6. Monitoring & Reporting

- **Intrusion Attempts (IPS Alerts):**
  Real-time alerts notify IT when hackers try to exploit known vulnerabilities or scan the network. IPS blocks these threats instantly to prevent compromise.

- **Malware Infections (AV Alerts):**
  Alerts are triggered when antivirus detects viruses, ransomware, or suspicious files. These allow IT to isolate affected systems before the infection spreads.
- **Bandwidth Abuse:**
  Alerts flag users or devices consuming excessive internet bandwidth, indicating misuse or compromise. Helps ensure fair usage and identify potential threats.
- **Generate monthly reports:**
    - **Top users by bandwidth:**
      Identify users consuming the most internet data to detect potential misuse or unusual activity.
    - **Blocked threats:**
      Summarize malware, intrusion attempts, and policy violations that were successfully blocked by security systems.
    - **VPN usage logs:**
      Track remote user access details, including login times, IP addresses, and session durations for audit purposes.
    - **Web category hits:**
      Report on which website categories (e.g., social media, adult, gaming) were most accessed or blocked by users.

---

7. Backup & Updates

- **Schedule configuration backup to a secure location:**
  Ensure firewall settings are backed up before any network activity.
- **Document all changes in the firewall change log:**
  Maintain a log of configuration changes for tracking, auditing, and rollback if needed.

---

8. Incident Response

- Monitor logs for anomalies using **Sophos Central / Firewall Manager**.
- For any security incident:
    - **Threat Detection & Alerts**
      Sophos Firewall identifies threats in real-time using IPS, ATP, and other security tools, and generates alerts for suspicious activities like malware, intrusions, or botnet traffic.

- **Investigation & Containment**
  Admins analyse logs, monitor live traffic, and use tools like packet capture to investigate incidents. Malicious IPs, URLs, or users are then blocked or isolated to stop the spread.
- **Recovery & Improvement**
  After resolving the threat, affected systems are restored, and detailed reports are documented. Policies and rules are updated to strengthen future defences.

---

9. Review & Audit

- **Log Review and Analysis**
  Regularly review firewall logs (traffic, security events, user activity) to detect anomalies, policy violations, or unusual behaviour that may indicate a threat.
- **Policy and Rule Audit**
  Periodically audit firewall rules, NAT policies, and user access controls to ensure they follow security best practices and are aligned with current organizational needs.
- **Report Generation and Review**
  Generate and analyse scheduled reports (e.g., top users, threat types, blocked attempts) to evaluate network health, usage trends, and effectiveness of security measures.
- **Compliance and Documentation**
  Maintain audit trails of configuration changes, incident responses, and access logs to support IT governance.

----END---