Sophos Firewall BYOD Monitoring Guide

1. Captive Portal Setup for BYOD

A Captive Portal is a web page that appears when a user connects to the office Wi-Fi, requiring login or acknowledgment before accessing the internet.

Why use it?

- Identifies who is connecting.
- Tracks internet activity by user.
- Can restrict or apply policies based on user identity.

How to set it up:

1. Navigate to: Wireless Protection > Hotspots
2. Click "Add Hotspot" and name it appropriately (e.g., BYOD Portal)
3. Choose an authentication method:
   - Voucher-based (quick and simple)
   - Username/Password (more secure and traceable)
4. Apply the captive portal to a Wi-Fi network via Wireless Networks > Edit SSID > Hotspot
5. (Optional) Enable MAC registration via Authentication > Device Registration

MAC Registration:

- MAC address is captured automatically during login.
- Manual input is not required from users.
- Useful for auto-authentication or limiting devices per user.

Important Distinction:

- The Captive Portal is not a policy itself. It is a login mechanism used to identify users or devices.
- Policies (e.g., Web Filtering, Application Control) are applied after the user is identified through the Captive Portal.

2. Choosing Between Username/Password vs Voucher Authentication

Username/Password:

- Suitable for permanent employees

- Requires manual user creation via Authentication > Users
- Enables detailed tracking and group-based access policies

Voucher-Based Access:
- Ideal for guests or short-term users
- Does not require individual user creation
- Vouchers can be generated with expiry dates and usage limits

Recommended Approach:
- Use Username/Password for employees
- Use Vouchers for guests and BYOD users

3. HTTPS Decryption and Web Filtering (Without Installing SSL Certificate)

Objective:

To monitor browser activity and apply filtering without requiring SSL certificate installation on devices.

Functionality:
- Logs and controls web traffic at the domain level
- Allows blocking or monitoring based on category or destination

How to configure:
1. Navigate to: Web > General Settings
2. Enable Web Filtering without enabling HTTPS Decryption
3. Create filtering policies in Web > Policies:
   - Block or monitor categories such as Social Media, Video Streaming, Games
4. Assign the policy via Web > Filter Assignments
5. View reports via Reports > Web > Web Activity by User/IP

Limitations without SSL Decryption:
- Visibility limited to domains only (e.g., facebook.com)
- Cannot view detailed paths or encrypted search queries

- Reduced visibility into app-specific encrypted content

4. Application Control

Purpose:

To detect, log, or block the use of specific applications, including mobile apps, regardless of browser usage.

Configuration Steps:

1. Navigate to: Protect > Application Control
2. Add a new policy and assign a relevant name
3. Search for and select applications such as Facebook, WhatsApp, YouTube
4. Choose the desired action for each application: Block, Allow, or Monitor
5. Apply the policy via Rules and Policies > Firewall Rules > Application Control

Reporting:

- Access via Reports > Applications & Web Usage
- Review application usage by user/IP, bandwidth, and access times

Note:

- Application Control works without SSL certificate installation
- Fully compatible with Captive Portal-based identification

Summary Table

Feature	SSL Certificate Required	Compatible with Captive Portal	Supports BYOD Monitoring
Captive Portal	No	Yes	Yes
Username/Password Auth	No	Yes	Yes
Voucher Auth	No	Yes	Yes
Web Filtering (No SSL)	No	Yes	Yes (domain-level only)
HTTPS Decryption (Full)	Yes	Yes	Yes (full visibility)
Application Control	No	Yes	Yes