**Guide to Installing and Configuring Suricata on pfSense (On LAN)**

This guide provides a step-by-step approach to installing and configuring Suricata on pfSense while using **Legacy Block Mode**.

**Step 1: Install Suricata on pfSense**

1. Log in to your **pfSense WebGUI**.
2. Navigate to **System > Package Manager**.
3. Click on the **Available Packages** tab.
4. Scroll down or use the search bar to find **Suricata**.
5. Click **Install** and confirm.
6. Wait for the installation to complete, then navigate to **Services > Suricata**.

**Step 2: Configure Global Settings**

1. Navigate to **Services > Suricata > Global Settings**.
2. **Install ETOpen Emerging Threats rules** by selecting the checkbox.
3. Under the **Rules Download** section, uncheck all other rule sources such as:
   * Emerging Threats Pro
   * Snort VRT rules
   * SSL Blacklist
   * Any other third-party rule sets.
4. In the **Rules Update Settings**:
   * Set the **Update Interval** to 12 HOURS.
   * Set **Update Start Time** to 00:00.
   * Ensure **Live Rule Swap on Update** is enabled.
5. **Remove Blocked Hosts Interval** should be set to NEVER.
6. Enable **Log to System Log** to keep track of Suricata messages.
7. Ensure **Keep Suricata Settings After Deinstallation** is enabled.
8. Click **Save**.

**Step 3: Configure Suricata on the LAN Interface**

1. Go to **Services > Suricata**.
2. Click the **Interfaces** tab.
3. Click **Add** to configure Suricata for the **LAN** interface.
4. Under the **LAN Settings** tab:
   * **Enable** the interface by checking the box.
   * Set **Interface** to LAN (v4).
   * Set **IPS Mode** to Legacy Mode.
   * Ensure **Block Offenders** is checked.
   * Set **Which IP to Block** to BOTH.
5. In **Logging Settings**:
   * Enable **Stats Collection**.
   * Enable **TLS Log**.
   * Ensure **HTTP Log**, **Extended HTTP Log**, **File-Store**, **Packet Log**, and **Verbose Logging** are disabled.
6. In **Alert and Block Settings**:
   * **Kill States** should be enabled.
   * **Block on DROP only** should be disabled.
7. Under **Performance and Detection Engine Settings**:
   * Set **Run Mode** to Workers.
   * Set **Max Pending Packets** to 2048.
   * Set **Detect-Engine Profile** to High.
   * Enable **Promiscuous Mode**.
8. Click **Save**.

**Step 4: Disable All Default Rules and Enable TLS Event Rule**

1. Navigate to **Services > Suricata > Interfaces**.
2. Select the **LAN** interface where Suricata is enabled.
3. Click on the **LAN Rules** tab.
4. Click **Active Rules** and select **Disable All**.
5. In the category dropdown, scroll down and select lts-events.rules to filter the rule list.
6. Click Enable all button to Enable all rules under **TLS Event Rule**.
7. Click **Save**.

**Step 5: Add Custom Rules (Including Google Services Whitelist)**

1. Navigate to **Services > Suricata > Interfaces**.
2. Select your configured **LAN** interface.
3. Click on the **LAN Rules > Custom Rules**.
4. Enter the rule in the custom rule editor.
5. Ensure your custom rules includes whitelist for Google services, to allow traffic to Google while still blocking YouTube.
6. Click **Save**.

**Step 6: Restart Suricata**

1. Navigate to **Services > Suricata**.
2. Click on the **Interfaces** tab.
3. Select the **LAN** interface where Suricata is enabled.
4. Click the **Restart** button.

**Step 7: NOTE! Suricata now requires that Hardware Checksum Offloading, Hardware TCP Segmentation Offloading and Hardware Large Receive Offloading all be disabled for proper operation.**

1. Navigate to **System > Advanced > Networking** tab and ensure all **three** of these Offloading settings are **disabled.**
2. After saving this changes you will be prompted to **restart,** so go ahead and **restart your Pfsense device**

**Step 8: Verify Functionality**

1. Clear your browser history and try to access a blocked site.
2. If needed, adjust the rules and restart Suricata again.

**NOTE AFTER EVERY CHANGIES YOU NEED TO RESTART SURICATA, AND SOMETIMES YOU NEED TO WAIT FOR SOME TIME FOR THE RULES TO TAKE EFFECT.**