Informations:

ElasticSearch IPv4 address: 207.#.10.35 Netflow Port: 9995

Timout Values:

General:	60
Maximum Lifetime:	60
Expire Interval:	0
TCP, TCP RST, TCP FIN, UDP:	60

Interface: WAN, DMZ, Development, Worker

Flow Tracking Level: Full

Netflow version: 9

1. Logging into the pfSense Interface
    - Open your browser and log into the pfSense administrative interface.

2. Configuring Softflowd

- Go to the **Services** menu and select **softflowd**. Main settings:
    - **Interface**: Select the interface [INTERFACE] through which you want to monitor the network traffic. This will be the interface through which the NetFlow data is collected.
    - **Host**: Enter the IP address and port of the NetFlow collector here. For example: 207.#.10.35:2055, where [Elastic_IPv4] is the IP address of the NetFlow server, and [PORT] is the NetFlow port.
    - **NetFlow Protocol Version**: Select the NetFlow protocol version. The most common versions are:
        - **v5**: Provides basic NetFlow statistics.
        - **v9**: Provides more advanced features and flexibility, such as support for user-defined templates.
    - **Timeouts**: Here, you can fine-tune the timing settings, such as the inactive and active connection timeouts. The default settings should be sufficient in most cases, but you can adjust them if necessary.

3. Starting Softflowd

- After saving the settings, click the **Save** button.
- Then, you need to enable the **softflowd** service. Once the **Save** button is clicked, NetFlow data collection will begin within 10 minutes.

4. Creating an Elasticsearch Index

In the **Analytics** section, click on the **Discover** tab and create a new data view. For NetFlow data, the name format follows the **netflow-[date]** pattern with the exact date.
The name is freely selectable, but for the **Index Pattern**, set the following value: **netflow-***. Once done, click the **Save** button.