Információk:

ElasticSearch IPv4 cím: 207.12.10.35 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. Bejelentkezés a pfSense felületére

* Nyisd meg a böngészőt, és jelentkezz be a pfSense adminisztrációs felületére.

## 2. A Softflowd Konfigurálása

* Lépj a **Services** menüpontra, és válaszd ki a **softflowd** lehetőséget.

**Főbb beállítások:**

* + **Interface**: Válaszd ki azt az interfészt [INTERFACE], amelyen monitorozni szeretnéd a hálózati forgalmat. Ez az interfész lesz az, amelyen keresztül a NetFlow adatokat gyűjtik.
  + **Host**: Itt add meg a NetFlow gyűjtő IP-címét és portját. Például: 192.168.1.100:2055, ahol [Elastic\_IPv4] a NetFlow szerver IP-címe, és [PORT] a NetFlow port.
  + **NetFlow Protocol Version**: Válaszd ki a NetFlow protokoll verzióját. A legelterjedtebb verziók:
    - **v5**: Alapvető NetFlow statisztikákat biztosít.
    - **v9**: Haladóbb funkciókat és rugalmasságot biztosít, például támogatja a felhasználói sablonokat.
  + **Timeouts**: Itt finomhangolhatod az időzítési beállításokat, mint az inaktív és aktív kapcsolat időtúllépését. Az alapértelmezett beállítások a legtöbb esetben megfelelőek, de ha finomhangolást szeretnél.

## 3. A softflowd indítása

* A beállítások mentése után kattints a **Save** gombra.
* Ezután a softflowd szolgáltatást el kell Enabled állapotra kell tenni. A **Save** gomb megnyomása után elindul a Netflow adatgyűjtés 10 percen belül.

4. Elasticsearch Index létrehozása

Az Analytics szekcióban, a Discover fülre kattintva hozz létre egy új adatokra vonatkozó nézetet. NetFlow adatok esetén a név formátuma napra pontosan követi a netflow-[dátum] mintát.

A név szabadon választható, de az Index Pattern-nél állítsd be a következő értéket: netflow-\*. Miután ezzel végeztél, kattints a Mentés gombra.