

# Cisco: Intrusion Prevention System (IPS / IDS)

## Wprowadzenie

Intrusion Prevention System (IPS) oraz Intrusion Detection System (IDS) są mechanizmami bezpieczeństwa służącymi do monitorowania ruchu sieciowego i wykrywania potencjalnych ataków. Na routerach Cisco można wdrożyć podstawową wersję IPS/IDS bez potrzeby zewnętrznych urządzeń.

- **IDS** – system wykrywający zagrożenia (informuje, nie blokuje).
- **IPS** – system wykrywający i blokujący zagrożenia.

Cisco umożliwia realizację IPS/IDS bezpośrednio w systemie IOS przy użyciu wbudowanych sygnatur oraz odpowiednich polityk.

## Wymagania

- Cisco IOS z obsługą funkcji IPS
- Dostęp do sygnatur IPS (plik `.pkg`)
- Pamięć flash z odpowiednim miejscem
- Włączenie usługi i konfiguracja odpowiednich polityk

## Konfiguracja IPS w trybie inline

### 1. Włączenie inspekcji

```
conf t
ip ips name moj_ips
```

### 2. Załaduj sygnatury IPS

Sygnatury muszą zostać pobrane i załadowane do routera (z TFTP lub lokalnie). Przykład:

```
ip ips signature-definition
load tftp://192.168.1.100/IOS-Sxxx.pkg
```

### 3. Włączenie IPS na interfejsach

Na interfejsach należy przypisać politykę IPS:

```
interface FastEthernet0/0
ip ips moj_ips in
```

```
exit

interface Serial0/0
 ip ips moj_ips out
exit
```

## 4. Konfiguracja alertów i logowania

```
ip ips notify log
ip ips notify sdee
```

Dodatkowo, jeśli router ma możliwość zapisu logów:

```
logging buffered 51200 debugging
```

### Tryby działania

- **inline (IPS)** – pakiety są analizowane i mogą być blokowane przed dotarciem do celu.
- **promiscuous (IDS)** – pakiety są tylko analizowane i raportowane (wymaga SPAN/mirroring).

### Integracja z Snort (IDS Open Source)

Snort to popularny, darmowy system IDS/IPS, który może być skonfigurowany do analizy ruchu przepływającego przez router.

## A. Instalacja Snort

Na systemie Linux (np. Ubuntu/Debian):

```
sudo apt update
sudo apt install snort
```

## B. Konfiguracja Snort do analizy ruchu

### 1. Tryb sniffera (monitorowania):

```
sudo snort -i eth0 -A console -c /etc/snort/snort.conf
```

2. **Ustaw interfejs routera w tryb SPAN/monitor** (jeśli korzystasz z GNS3, zrób „port mirroring” na interfejsie):

```
monitor session 1 source interface FastEthernet0/0
monitor session 1 destination interface FastEthernet0/1
```

3. **Podłącz Snorta** do portu docelowego SPAN (np. `FastEthernet0/1`).

## C. Tworzenie własnych sygnatur

Sygnatury Snort są przechowywane w plikach `.rules`. Przykład reguły:

```
alert tcp any any -> any 80 (msg:"HTTP access detected"; sid:1000001; rev:1;)
```

Umieść własne reguły w katalogu `/etc/snort/rules/local.rules` i włącz je w pliku konfiguracyjnym.

### Automatyczne pobieranie sygnatur dla Snort

Najwygodniejszym sposobem aktualizacji reguł Snorta jest użycie narzędzia **PulledPork**.

#### A. Instalacja PulledPork

Na systemie Linux:

```
sudo apt install pulledpork
```

Lub pobierz z repozytorium:

```
git clone https://github.com/shirkdog/pulledpork.git
```

#### B. Konfiguracja PulledPork

Edytuj plik konfiguracyjny `pulledpork.conf`:

```
rule_url=https://www.snort.org/reg-rules/snortrules-snapshot-29120.tar.gz|sn  
ortrules-snapshot.tar.gz|oinkcode  
oinkcode=TWÓJ_KOD_OINK  
snort_path=/usr/sbin/snort  
config_path=/etc/snort/snort.conf  
rule_path=/etc/snort/rules/snort.rules  
local_rules=/etc/snort/rules/local.rules  
sid_msg=/etc/snort/sid-msg.map
```

Aby uzyskać `oinkcode`, zarejestruj się na <https://www.snort.org/>

#### C. Uruchamianie aktualizacji

```
sudo ./pulledpork.pl -c /etc/pulledpork/pulledpork.conf -l
```

Można dodać do `cron` aby aktualizować codziennie.

## D. Sprawdzenie załadowanych reguł

```
sudo snort -T -c /etc/snort/snort.conf
```

### Zastosowania

- Ochrona brzegowa w małych sieciach.
- Monitorowanie i kontrola dostępu w sieciach kampusowych.
- Integracja z politykami bezpieczeństwa (ACL, CBAC, ZBF).
- Wykrywanie znanych exploitów i ataków (Snort).

### Podsumowanie

IPS/IDS na routerze Cisco to skuteczne, choć ograniczone rozwiązanie wykrywania i zapobiegania atakom. W połączeniu z narzędziem takim jak **Snort** i **PulledPork**, administrator zyskuje możliwość wdrażania aktualnych reguł wykrywających najnowsze zagrożenia.