zurück

IDS & IPS – Grundlagen

Ein IDS (**I**ntrusion **D**etection **S**ystem) und ein IPS (**I**ntrusion **P**revention **S**ystem) überwachen den Netzwerkverkehr und erkennen Angriffe, Malware-Kommunikation, verdächtige Aktivitäten und Regelverstöße.

Warum IDS/IPS?

Moderne Netzwerke müssen gegen:

- Malware
- Botnet-Kommunikation
- Exploits
- Portscans
- Brute-Force
- C2-Verbindungen
- verdächtiges HTTP-Verhalten

geschützt und beobachtet werden.

IDS/IPS sind zentrale Bausteine von Defense-in-Depth und Zero Trust.

IDS vs IPS

System	Bedeutung	Wirkung
IDS	Intrusion Detection System	erkennt Angriffe, protokolliert
IPS	Intrusion Prevention System	erkennt & blockiert aktiv

```
IDS: Traffic → Analyse → Meldung
```

```
IPS: Traffic → Analyse → Blockierung
```

Prominente Lösungen

- **Suricata** (modern, multi-thread, sehr verbreitet)
- **Snort** (klassiker, Snort3 modernisiert)
- Zeek (Netzwerk-Protokoll-Analyse)
- Wazuh (Host-IDS)
- CrowdSec (regelbasierte Verhaltensanalyse)

In meinem Heimlabor nutze ich **Suricata + CrowdSec + EveBox** → perfekte Kombi (meine Meinung).

Wie erkennt ein IDS Angriffe?

Zwei Haupttypen:

1. Signaturbasiert (klassisch)

Vergleich mit einer Datenbank bekannter Angriffe:

- Exploit-Muster
- Malware-Domains
- C2-Server
- Portscan-Signaturen
- Buffer Overflow Erkennung

Beispiel (Snort-Regel):

```
alert tcp any any -> any 80 (msg:"Bad HTTP"; content:"evil"; sid:10001;)
```

2. Anomaliebasiert (modern)

Erkennt ungewöhnliches Verhalten:

- plötzliche Traffic-Spitzen
- ungewöhnliche Ports
- DNS-Anomalien
- abweichende Protokolle

Suricata kombiniert beide Ansätze.

Platzierung im Netzwerk

Es gibt zwei grundlegende Einsatzmodi:

IDS im Monitoring-Modus (passiv)

Kopiert Traffic über:

- Spiegelport (SPAN)
- TAP

`Traffic → Switch → (Kopie) → IDS`

IPS inline (aktiv)

Der Traffic muss **durch** das IPS hindurch.

`Traffic → IPS → Ziel`

Ports & Protokolle

IDS/IPS arbeiten typischerweise auf Layer 3/4/7:

- TCP, UDP, ICMP
- HTTP, DNS, TLS, FTP, SMB usw.

Suricata – moderne, multithreaded Engine

Merkmale:

- sehr hohe Performance
  * Multi-Core-fähig
  * versteht viele Protokolle tiefgehend
  * Output als `eve.json`
  * Unterstützt IDS & IPS

Typische Dateien:

```
/etc/suricata/suricata.yaml
/var/log/suricata/eve.json
```

Snort – der Klassiker

Snort ist eines der ältesten IDS-Systeme.

Snort3 = moderne, modulare Neuauflage.

Eve.json Beispiel (Suricata)

```
{
  "timestamp": "2025-07-10T14:23:11",
  "event_type": "alert",
  "alert": {
    "signature": "ET TROJAN Agent Tesla",
    "severity": 1
```

```
  },
  "src_ip": "192.168.178.96",
  "dest_ip": "79.254.205.77"
}
```

Erlaubt direkte Analyse in:

- Grafana
- EveBox
- Kibana
- Loki/Promtail
- CrowdSec

Regeln & Regelquellen

Gängige Rule-Sets:

- Emerging Threats (ET Open & ET Pro)
  * Snort Community Rules
  * Abuse.ch Feeds
  * ThreatFox
  * Spamhaus
  * Suricata TLS Fingerprints

Eintrag in Suricata:

```
rule-files:
  - emerging-threats.rules
  - local.rules
```

Performance & Hardware

IDS/IPS hängen stark ab von:

- CPU-Kernen
    - Netzwerkkarten (Offloading deaktivieren!)
      * RAM (Signaturdatenbank)
      * Traffic-Volumen
      * Regelmenge

Statistiken & Monitoring

Typische Metriken:

- Alerts pro Minute

    - Top Source IPs
      * Top Destinations
      * Protokollverteilung
      * TLS-Client-Fingerprints
      * DNS-Anomalien

  Viele Hersteller nutzen Dashboards (Grafana, Kibana, EveBox).

Einsatzgebiete von IDS/IPS

- Unternehmensnetzwerke
    - Firewalls (OPNsense: Suricata integriert)
      * Heimnetzwerke (pfSense/OPNsense)
      * SOC/ Blue Team
      * Zero Trust Architekturen
      * Netzwerkforensik

Vorteile von IDS

- erkennt Angriffe
    - erkennt C2-Kommunikation
      * erkennt Probing/Scanning
      * liefert forensische Beweise
      * keine Netzwerkunterbrechung

Vorteile von IPS

- blockiert Angriffe aktiv
    - schützt Systeme automatisch
      * im Inline-Modus sehr wirksam

Nachteile

IDS:

- erkennt nur → blockiert nicht
  * sehr viele Logdaten

IPS:

- kann legitimen Traffic blockieren
  * Konfiguration muss sehr sauber sein

Zusammenfassung

- IDS → erkennt Angriffe

- IPS → blockiert Angriffe
  * Suricata & Snort sind die wichtigsten Tools
  * Signatur- und Anomalieerkennung
  * zentral in Security-Strategien
  * integriert in Firewalls wie OPNsense
  * liefert Alerts via eve.json, Logs, Dashboards