FR

Guide Pratique

NetFlow + ntopng OPNsense

Analyse de trafic, top talkers, alertes

Mars 2026

Sommaire

Comprendre NetFlow et IPFIX

NetFlow est un protocole developpe par Cisco permettant de collecter des metadonnees sur les flux IP traversant un equipement reseau. Contrairement a une capture de paquets complète (pcap), NetFlow enregistre uniquement les en-tetes : IP source/destination, port, protocole, bytes, paquets et duree.

IPFIX (IP Flow Information Export) est la standardisation IETF de NetFlow v9. OPNsense supporte les deux formats via le plugin softflowd.

Ce que NetFlow/IPFIX vous donne :

* Top talkers : quels hotes consomment le plus de bande passante

* Distribution protocolaire : TCP/UDP/ICMP, HTTP/HTTPS/DNS/SMTP

* Analyse geographique : flux vers pays suspects ou non autorises

* Detection d'anomalies : port scans, exfiltration de donnees, botnets C2

* Audit de conformite : prouver que le trafic est conforme aux politiques

i NetFlow = metadonnees seulement. Aucune donnee de payload capturee. Respect de la vie privee preserve, performance impactee de maniere minimale (< 2% CPU sur OPNsense).

Activer le plugin NetFlow sur OPNsense

OPNsense utilise softflowd pour exporter les flux NetFlow/IPFIX. Installation en un clic depuis l'interface.

Installation

```
# Interface OPNsense : System -> Firmware -> Plugins
# Chercher : os-softflowd -> Install
# Ou via SSH :
pkg install os-softflowd
```

Configuration softflowd

Apres installation : Services -> NetFlow -> Settings

* Interface(s) : WAN, LAN, et tous VLANs a monitorer

* Collector IP : adresse IP de votre serveur ntopng

* Collector Port : 2055 (port standard NetFlow/IPFIX)

* Version : IPFIX (recommande) ou NetFlow v9

* Timeout idle : 60 secondes pour flux idle

* Timeout expiry : 3600 secondes pour flux actifs

```
# Verifier que softflowd tourne
ps aux | grep softflowd
# Verifier les exports (tcpdump sur le serveur ntopng)
tcpdump -i eth0 udp port 2055 -c 10
```

i Activez la collecte sur TOUTES les interfaces pour une visibilite complete. Le volume de donnees NetFlow est negligeable (< 1% du trafic reseau reel).

Installer ntopng sur un serveur dedie

ntopng Community Edition est gratuit et largement suffisant pour une infrastructure SMB. Installez-le sur un LXC Proxmox dedie (2 vCPU, 4 GB RAM, 50 GB SSD recommandes).

Installation Ubuntu/Debian

```
# Ajouter le depot ntopng
apt install -y wget gnupg2
wget https://packages.ntop.org/apt/ntop.key
apt-key add ntop.key
echo "deb http://packages.ntop.org/apt/22.04/ amd64/" > /etc/apt/sources.list.d/ntop.list

apt update && apt install -y ntopng nprobe redis-server

# Activer redis (requis par ntopng)
systemctl enable --now redis-server
systemctl enable --now ntopng
```

Configuration ntopng

```
# /etc/ntopng/ntopng.conf
--community                    # edition gratuite
--interface=eth0               # interface reseau locale
--http-port=8080               # port web UI (generique)
--data-dir=/var/lib/ntopng    # stockage donnees
--disable-autologout           # pas de deconnexion auto
--no-promisc                   # pas de mode promiscuous (on veut juste NetFlow)
--zmq tcp://127.0.0.1:5556    # ZMQ pour collecte interne

# Redemarrer apres modification
systemctl restart ntopng
```

Configurer le collecteur ZMQ/NetFlow

```
# Methode recommandee : via nprobe comme proxy NetFlow -> ZMQ
# /etc/nprobe/nprobe.conf
--interface=none
--collector-port 2055          # receptionne les exports OPNsense
--zmq tcp://127.0.0.1:5556     # transmet a ntopng
--ntopng tcp://127.0.0.1:5556  # integration native ntopng

systemctl enable --now nprobe
```

i Alternativement, ntopng Community peut ecouter directement sur UDP 2055 via l'interface virtuelle netflow. Verifiez votre version avec ntopng --version.

Configurer ntopng comme collecteur NetFlow

Via l'interface web ntopng

1. Acceder a http://[IP-ntopng]:8080 (admin/admin par defaut, changer immediatement)

2. Settings -> Preferences -> Interfaces

3. Ajouter une interface de type "ZMQ" pointant vers tcp://127.0.0.1:5556

4. Ou utiliser le type "NetFlow/IPFIX" avec port UDP 2055 directement

5. Sauvegarder et verifier que l'interface apparait comme "Active"

Test de connectivite OPNsense -> ntopng

```
# Sur le serveur ntopng :
netstat -ulnp | grep 2055          # verifier que nprobe ecoute
tcpdump -i any udp port 2055 -c 5  # capturer les flux entrants

# Sur OPNsense (SSH) :
# verifier que softflowd exporte vers la bonne IP
ps aux | grep softflowd
# Ex: softflowd -i em0 -n 192.168.x.x:2055 -v 10 -t maxlife=3600

# Depuis ntopng -> Status -> Interfaces
# -> Le compteur de flux devrait incrementer
```

Tableau de bord ntopng

Une fois les flux NetFlow recus, ntopng affiche une mine d'informations en temps reel et en historique.

Vues principales

* Dashboard : bande passante totale, top applications, top hotes

* Hosts : liste tous les hotes actifs avec volumes, pays, OS detecte

* Flows : flux actifs en temps reel (IP src/dst, port, protocole, bytes)

* Alerts : anomalies detectees automatiquement

* Traffic Analysis : repartition par protocole, L7 (DPI), ASN

* Historical Flows : recherche dans l'historique (ntopng Pro)

Personnaliser les seuils d'alerte

```
# ntopng Settings -> Alerts -> Threshold-based Alerts
# Exemples de seuils utiles :
# - Hote > 100 Mbps pendant 60s  -> alerte critique
# - Flux DNS > 1000 req/min -> possible tunneling DNS
# - Connexion vers pays blackliste -> alerte immediate
# - Scan de ports detecte (> 50 ports/min depuis meme IP)

# Configuration via API ntopng :
curl -u admin:motdepasse \
  'http://127.0.0.1:8080/lua/rest/v2/add/host/alert/config.lua' \
  -d 'host=192.168.1.0/24&metric=traffic&operator=gt&value=104857600'
```

Alertes comportementales et detection d'anomalies

ntopng Community inclut un moteur de detection comportementale base sur des heuristiques et des listes noires. ntopng Enterprise ajoute le machine learning.

Categories d'alertes

* Flow Alerts : flux vers IPs malveillantes (listes noires ntopng)

* Host Alerts : comportements suspects (scan ports, exfiltration)

* Network Alerts : depassement de seuils de bande passante

* System Alerts : problemes de performance du collecteur

Integration avec Wazuh/SIEM

```
# ntopng peut exporter vers syslog -> Wazuh
# /etc/ntopng/ntopng.conf
--syslog                         # activer export syslog
--syslog-facility=LOG_LOCAL1   # facility syslog

# Sur Wazuh, regles custom pour alertes ntopng :
# /var/ossec/etc/rules/ntopng_rules.xml
<rule id="100200" level="7">
  <decoded_as>syslog</decoded_as>
  <match>ntopng</match>
  <description>ntopng: Alerte flux reseau</description>
</rule>
```

Webhook vers Telegram/Slack

```
# ntopng Settings -> Alerts -> Alert Endpoints -> Webhook
# URL : https://api.telegram.org/botTOKEN/sendMessage
# Payload JSON :
{
  "chat_id": "-100XXXXXXXXX",
  "text": "ALERT: {alert_type} from {ip} - {description}"
}
```

Retention des donnees et performance

Dimensionnement storage

* 1000 hotes actifs, 100 Mbps : ~2 GB/jour de donnees ntopng

* Retention recommandee : 30 jours -> ~60 GB SSD

* ntopng utilise Redis + fichiers RRD pour l'historique

* Purge automatique : ntopng gere la rotation automatiquement

```
# Optimiser Redis pour ntopng
# /etc/redis/redis.conf
maxmemory 1gb
maxmemory-policy allkeys-lru
save 900 1
save 300 10

# Verifier l'usage memoire ntopng
curl -u admin:pass 'http://127.0.0.1:8080/lua/rest/v2/get/ntopng/info.lua'
```

Tuning softflowd pour reduire le volume

```
# Sampler 1 paquet sur 10 (environnements haut debit)
# /etc/softflowd/softflowd.conf
-s 10   # sampling rate 1:10

# Exporter uniquement WAN (et non LAN inter-VLAN)
# Si votre routeur est en hairpin, filterez via BPF :
-f 'not src net 192.168.0.0/16 and not dst net 192.168.0.0/16'
```

Cas d'usage : forensic et troubleshooting

Identifier la source d'une saturation bande passante

```
# ntopng Dashboard -> Top Hosts -> trier par Total Traffic
# Identifier les 3 premiers hotes
# Cliquer sur un hote -> Details -> Flows (historique)
# Filtrer par port : 443, 80, 8080...
# Ex: decouverte d'un backup cloud non prevu saturant le lien WAN
```

Detecter un mouvement lateral suspect

```
# ntopng Hosts -> Filtrer par hote interne suspect
# Onglet "Flows" -> trier par nombre de destinations
# Signe d'infection : un poste interne tente de contacter
# 50+ IPs internes sur port 445 (SMB) en < 5 minutes
# -> Isolation immediate du poste via OPNsense :
curl -k -u 'apikey:secret' \
  -X POST 'https://192.168.1.1/api/firewall/alias/addHost' \
  -d 'alias=blocked_hosts&address=192.168.x.x'
```

Audit de conformite : trafic vers pays non autorises

```
# ntopng Analytics -> Geo Map
# Filtrer par continent ou pays
# Exporter CSV des flux vers pays blacklistes
# Rapport mensuel : verifier que seuls FR/CA/US sont present
# Si trafic vers RU/CN/KP detecte -> investigation immediate

# Generer un rapport PDF depuis ntopng :
# Reports -> Traffic Summary -> Export PDF
```

Conclusion : visibilite totale sur votre reseau

NetFlow + ntopng transforme OPNsense en une sonde de visibilite complete. Vous savez exactement qui fait quoi sur votre reseau, en temps reel et en historique.

L'investissement est minimal : plugin softflowd gratuit sur OPNsense, ntopng Community Edition gratuit, un LXC de 4 GB RAM. Le retour : des heures de troubleshooting economisees et des incidents de securite detectes avant qu'ils ne deviennent des crises.

Serie Stack OPNsense Enterprise — Navigation

* Billet 1 : Installer OPNsense dans Proxmox
* Billet 2 : VLANs & Zero Trust
* Billet 3 : WireGuard VPN & failover LTE
* Billet 4 : WiFi & APs par VLAN
* Billet 5 : CrowdSec + fail2ban IDS/IPS
* Billet 6 : NAC avec FreeRADIUS & 802.1X
* Billet 7 : Suricata IDS/IPS
* Billet 8 : AdGuard Home + DNS over HTTPS
* Billet 9 : Monitoring Grafana + InfluxDB
* Billet 10 : CARP & Haute disponibilite
* Billet 11 : SIEM Wazuh
* Billet 12 : Ansible as Code
* Billet 13 : Backup automatise OPNsense
* Billet 14 : PKI interne & gestion certificats
* Billet 15 (ce billet) : NetFlow + ntopng

i Hub complet : blog.botum.ca/opnsense-stack-securite-enterprise-proxmox/

Article FR : blog.botum.ca/opnsense-netflow-ntopng-analyse-trafic

Telecharger ce guide PDF : www.botum.ca/guides/guide-opnsense-netflow-ntopng.pdf

Site web : www.botum.ca |

-- Canada