EN

Quick Reference Guide

NetFlow + ntopng on OPNsense

Traffic analysis, top talkers, anomaly alerts

Mars 2026

Table of Contents

Understanding NetFlow and IPFIX

NetFlow is a protocol developed by Cisco for collecting metadata about IP flows traversing a network device. Unlike full packet capture (pcap), NetFlow records only headers: source/destination IP, port, protocol, bytes, packets, and duration.

IPFIX (IP Flow Information Export) is the IETF standardization of NetFlow v9. OPNsense supports both formats via the softflowd plugin.

What NetFlow/IPFIX gives you:

* Top talkers: which hosts consume the most bandwidth

* Protocol distribution: TCP/UDP/ICMP, HTTP/HTTPS/DNS/SMTP

* Geographic analysis: traffic to suspect or unauthorized countries

* Anomaly detection: port scans, data exfiltration, botnet C2 traffic

* Compliance audit: prove traffic matches security policies

i NetFlow = metadata only. No payload data captured. Privacy preserved, performance impact minimal (< 2% CPU on OPNsense).

Enabling the NetFlow Plugin on OPNsense

OPNsense uses softflowd to export NetFlow/IPFIX flows. One-click installation from the interface.

Installation

```
# OPNsense interface: System -> Firmware -> Plugins
# Search: os-softflowd -> Install
# Or via SSH:
pkg install os-softflowd
```

Softflowd Configuration

After installation: Services -> NetFlow -> Settings

* Interface(s): WAN, LAN, and all VLANs to monitor

* Collector IP: IP address of your ntopng server

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

* Version: IPFIX (recommended) or NetFlow v9

* Idle timeout: 60 seconds for idle flows

* Expiry timeout: 3600 seconds for active flows

```
# Verify softflowd is running
ps aux | grep softflowd
# Check exports (tcpdump on ntopng server)
tcpdump -i eth0 udp port 2055 -c 10
```

i Enable collection on ALL interfaces for complete visibility. NetFlow data volume is negligible (< 1% of actual network traffic).

Installing ntopng on a Dedicated Server

ntopng Community Edition is free and fully sufficient for SMB infrastructure. Install it on a dedicated Proxmox LXC (2 vCPU, 4 GB RAM, 50 GB SSD recommended).

Installation on Ubuntu/Debian

```
# Add the ntopng repository
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

# Enable redis (required by ntopng)
systemctl enable --now redis-server
systemctl enable --now ntopng
```

ntopng Configuration

```
# /etc/ntopng/ntopng.conf
--community                    # free edition
--interface=eth0               # local network interface
--http-port=8080               # web UI port (generic)
--data-dir=/var/lib/ntopng    # data storage
--disable-autologout           # no auto-logout
--no-promisc                   # no promiscuous mode (NetFlow only)
--zmq tcp://127.0.0.1:5556    # ZMQ for internal collection

# Restart after changes
systemctl restart ntopng
```

Configure the ZMQ/NetFlow Collector

```
# Recommended: use nprobe as NetFlow -> ZMQ proxy
# /etc/nprobe/nprobe.conf
--interface=none
--collector-port 2055           # receive OPNsense exports
--zmq tcp://127.0.0.1:5556      # forward to ntopng
--ntopng tcp://127.0.0.1:5556   # native ntopng integration

systemctl enable --now nprobe
```

i Alternatively, ntopng Community can listen directly on UDP 2055 via the netflow virtual interface. Check your version with ntopng --version.

Configuring ntopng as a NetFlow Collector

Via the ntopng Web Interface

1. Access http://[ntopng-IP]:8080 (admin/admin by default -- change immediately)

2. Settings -> Preferences -> Interfaces

3. Add a "ZMQ" type interface pointing to tcp://127.0.0.1:5556

4. Or use "NetFlow/IPFIX" type with UDP port 2055 directly

5. Save and verify the interface shows as "Active"

Connectivity Test OPNsense -> ntopng

```
# On the ntopng server:
netstat -ulnp | grep 2055          # verify nprobe is listening
tcpdump -i any udp port 2055 -c 5  # capture incoming flows

# On OPNsense (SSH):
# Verify softflowd exports to correct IP
ps aux | grep softflowd
# Ex: softflowd -i em0 -n 192.168.x.x:2055 -v 10 -t maxlife=3600

# In ntopng -> Status -> Interfaces
# -> Flow counter should be incrementing
```

ntopng Dashboard: Top Talkers, Protocols, Geolocation

Once NetFlow flows are received, ntopng displays a wealth of information in real time and historically.

Main Views

* Dashboard: total bandwidth, top applications, top hosts

* Hosts: lists all active hosts with volumes, country, detected OS

* Flows: real-time active flows (IP src/dst, port, protocol, bytes)

* Alerts: automatically detected anomalies

* Traffic Analysis: protocol breakdown, L7 (DPI), ASN

* Historical Flows: search history (ntopng Pro)

Customizing Alert Thresholds

```
# ntopng Settings -> Alerts -> Threshold-based Alerts
# Useful threshold examples:
# - Host > 100 Mbps for 60s  -> critical alert
# - DNS flows > 1000 req/min -> possible DNS tunneling
# - Connection to blacklisted country -> immediate alert
# - Port scan detected (> 50 ports/min from same IP)

# Configuration via ntopng API:
curl -u admin:password \
  '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'
```

Behavioral Alerts and Anomaly Detection

ntopng Community includes a behavioral detection engine based on heuristics and blacklists. ntopng Enterprise adds machine learning.

Alert Categories

* Flow Alerts: flows to malicious IPs (ntopng blacklists)

* Host Alerts: suspicious behaviors (port scans, exfiltration)

* Network Alerts: bandwidth threshold exceeded

* System Alerts: collector performance issues

Integration with Wazuh/SIEM

```
# ntopng can export to syslog -> Wazuh
# /etc/ntopng/ntopng.conf
--syslog                         # enable syslog export
--syslog-facility=LOG_LOCAL1   # syslog facility

# On Wazuh, custom rules for ntopng alerts:
# /var/ossec/etc/rules/ntopng_rules.xml
<rule id="100200" level="7">
  <decoded_as>syslog</decoded_as>
  <match>ntopng</match>
  <description>ntopng: Network flow alert</description>
</rule>
```

Webhook to Telegram/Slack

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

Data Retention and Performance Tuning

Storage Sizing

* 1000 active hosts, 100 Mbps: ~2 GB/day of ntopng data

* Recommended retention: 30 days -> ~60 GB SSD

* ntopng uses Redis + RRD files for history

* Auto-purge: ntopng manages rotation automatically

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

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

Softflowd Tuning for High-Bandwidth Environments

```
# Sample 1 packet in 10 (high-throughput environments)
# /etc/softflowd/softflowd.conf
-s 10   # sampling rate 1:10

# Export WAN only (not LAN inter-VLAN)
# If your router uses hairpinning, filter via BPF:
-f 'not src net 192.168.0.0/16 and not dst net 192.168.0.0/16'
```

Use Cases: Network Forensics and Troubleshooting

Identifying the Source of Bandwidth Saturation

```
# ntopng Dashboard -> Top Hosts -> sort by Total Traffic
# Identify the top 3 hosts
# Click on a host -> Details -> Flows (history)
# Filter by port: 443, 80, 8080...
# Example: discovering an unplanned cloud backup saturating the WAN link
```

Detecting Suspicious Lateral Movement

```
# ntopng Hosts -> Filter by suspect internal host
# Tab "Flows" -> sort by number of destinations
# Sign of infection: internal workstation attempts to contact
# 50+ internal IPs on port 445 (SMB) in < 5 minutes
# -> Immediate isolation 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'
```

Compliance Audit: Traffic to Unauthorized Countries

```
# ntopng Analytics -> Geo Map
# Filter by continent or country
# Export CSV of flows to blacklisted countries
# Monthly report: verify only FR/CA/US are present
# If traffic to RU/CN/KP detected -> immediate investigation

# Generate PDF report from ntopng:
# Reports -> Traffic Summary -> Export PDF
```

Conclusion: Complete Visibility on Your Network

NetFlow + ntopng transforms OPNsense into a complete visibility probe. You know exactly who is doing what on your network, in real time and historically.

The investment is minimal: free softflowd plugin on OPNsense, free ntopng Community Edition, a 4 GB RAM LXC. The return: hours saved in troubleshooting and security incidents detected before they become crises.

OPNsense Enterprise Stack -- Navigation

* Article 1: Install OPNsense in Proxmox
* Article 2: VLANs & Zero Trust
* Article 3: WireGuard VPN & LTE failover
* Article 4: WiFi & APs per VLAN
* Article 5: CrowdSec + fail2ban IDS/IPS
* Article 6: NAC with FreeRADIUS & 802.1X
* Article 7: Suricata IDS/IPS
* Article 8: AdGuard Home + DNS over HTTPS
* Article 9: Monitoring Grafana + InfluxDB
* Article 10: CARP & High Availability
* Article 11: Lightweight SIEM with Wazuh
* Article 12: Ansible as Code
* Article 13: Automated OPNsense Backup
* Article 14: Internal PKI & Certificate Management
* Article 15 (this article): NetFlow + ntopng

i Hub: blog.botum.ca/opnsense-enterprise-network-stack-overview/

Full article (EN): blog.botum.ca/opnsense-netflow-ntopng-traffic-analysis

Download this PDF guide: www.botum.ca/guides/guide-opnsense-netflow-ntopng-en.pdf

Website: www.botum.ca |

-- Canada