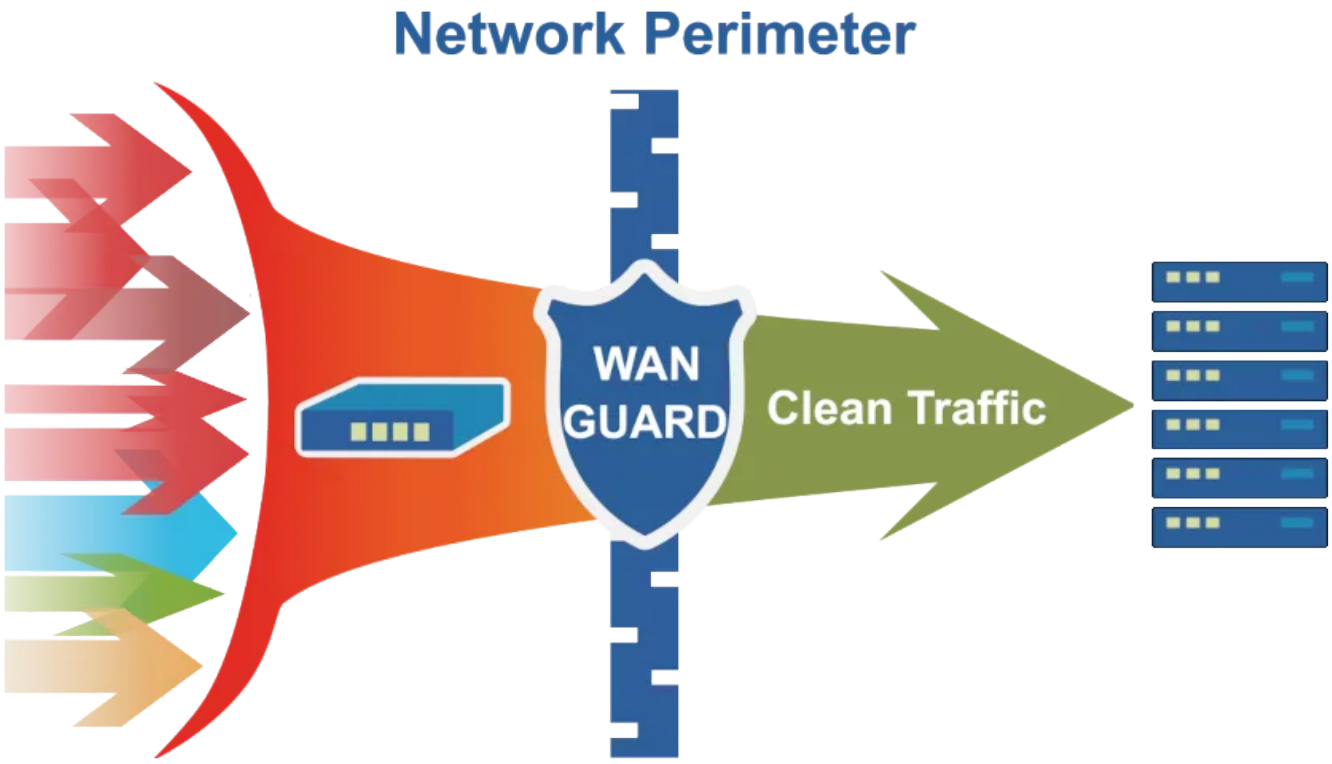
AntiDDoS

- □□ Implementasi DDoS Mitigation dengan Wanguard Flowspec + Filter (Tanpa RTBH)

□□ Implementasi DDoS Mitigation dengan Wanguard Flowspec + Filter (Tanpa RTBH)



Latar Belakang

DDoS bisa menyerang langsung IP publik tenant. Solusi klasik seperti **RTBH (Remote Triggered Black Hole)** sering digunakan, tapi punya kekurangan utama: **memutus total akses ke IP korban**.

Solusi yang lebih presisi dan modern adalah menggabungkan:

- **Wanguard Sensor** untuk deteksi serangan
- **Wanguard Filter** sebagai scrubber
- **BGP Flowspec** untuk filtering trafik jahat
- □□ Tanpa perlu RTBH (**No blackhole**)

Tujuan Arsitektur

- Melindungi tenant dari DDoS tanpa mematikan IP korban
- Menyaring trafik jahat di edge (Nokia router) sebelum masuk ke internal jaringan
- Membersihkan trafik yang lebih kompleks melalui Wanguard Filter

---

Komponen yang Digunakan

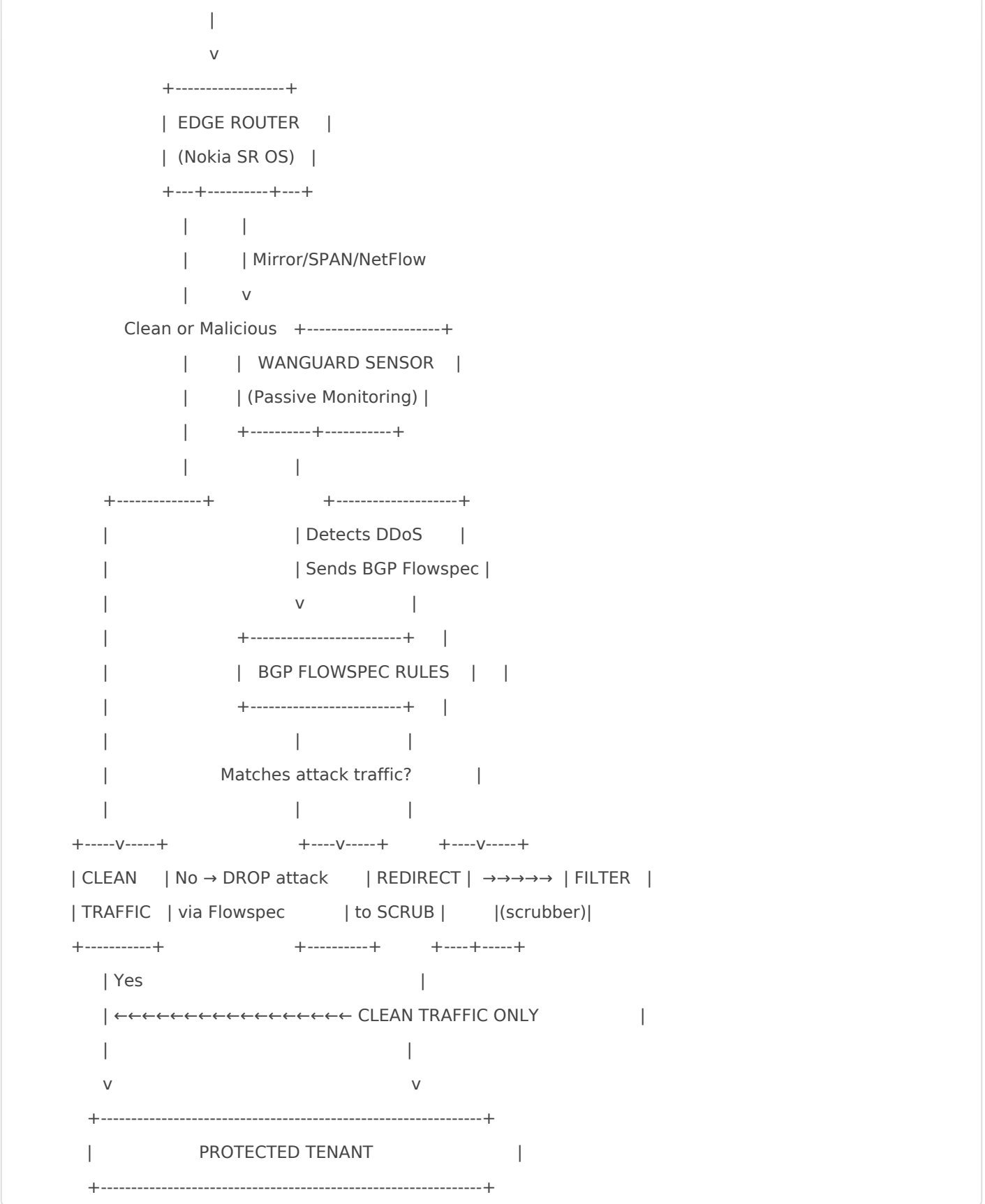
Komponen	Peran
Wanguard Sensor	Mendeteksi pola DDoS (NetFlow/sFlow/port mirror)
Wanguard Filter	Menyaring trafik berdasarkan signature (packet/flow-based)
Router Nokia SR OS	Menjadi edge router, menerima rule Flowspec
BGP Session Flowspec	Kanal komunikasi antara Wanguard dan router
Redirect to Scrubber (opsional)	Untuk serangan layer 7 atau spoofed traffic

---

Arsitektur dan Flow

image.png

https://www.andrisoft.com/software/wanguard/ddos-mitigation-protection



Penjelasan Jalur

- **Normal/Clean Traffic:**
  - Masuk dari Internet ke Edge Router
  - Tidak terdeteksi sebagai DDoS

    - Tidak cocok dengan rule Flowspec → langsung diteruskan ke tenant
- **DDoS Volume Attack (Sederhana):**
    - Terdeteksi oleh Sensor (via mirror)
    - Sensor mengirim Flowspec ke router
    - Router drop traffic yang cocok (berdasarkan dst IP, port, proto, dst prefix, dsb)
- **DDoS Kompleks (Spoofed/Layer 7)**:
    - Sensor tidak cukup untuk handle via Flowspec
    - Sensor trigger **redirect to scrubber** (Wanguard Filter)
    - Filter menyaring secara granular, hanya teruskan **clean traffic**
    - Tenant tetap dapat akses normal

Tahapan Implementasi

1. Persiapkan Infrastruktur Dasar

Komponen	Deskripsi
Router (Nokia SR OS)	Pastikan support NetFlow/sFlow/SPAN + BGP Flowspec
Server Wanguard Sensor	Pasang di lokasi yang menerima mirror flow
Server Wanguard Filter	Opsional, dipasang jika diperlukan scrubber
BGP Session Internal	Untuk koneksi Sensor → Router via Flowspec

---

2. Konfigurasi Source Traffic (NetFlow atau Mirror)

1. Masuk ke menu: **Sensors > Sources**
2. Klik **“Add New Source”**
3. Pilih **NetFlow v5/v9/sFlow** atau **Interface (mirror)**
4. Contoh NetFlow:
    - Name: `Router1`
    - Type: `NetFlow v9`
    - Port: `2055`
    - Interface IP: `0.0.0.0` *(bind ke semua interface)*
5. Klik **Save**

3. Aktifkan Sensor

1. Masuk ke: **Sensors > Sensors**
2. Klik **“Add New Sensor”**
3. Isi:

- Name: `EdgeSensor`
- Source: pilih `Router1` (yang tadi kamu buat)
- Role: `Detection only`
- Threshold (example):
  - PPS threshold: `50000`
  - BPS threshold: `200000000` (200 Mbps)

4. Klik **Save**

> Sensor ini akan mulai analisis flow/mirror secara pasif.

4. Set BGP Flowspec Connection

1. Masuk ke: **Settings > BGP Configuration**
2. Klik **“Add New Peer”**
3. Isi:
   - Type: `Flowspec`
   - Local IP: `10.0.0.10` (IP dari server sensor)
   - Remote IP: `10.0.0.1` (edge router)
   - AS Number: sesuai BGP internal (misal: 65001)
   - Enable:
4. Klik **Save**

> Pastikan koneksi BGP Flowspec ini established (lihat status).

5. Buat Response Rule (Flowspec Injection)

1. Masuk ke: **Sensors > Responses**
2. Klik **“Add New Response”**
3. Isi:
   - Name: `Flowspec-Drop`
   - Action: `Inject BGP Flowspec`
   - Match:
     - TCP SYN flood → dst port = 2211 (contoh)
     - UDP flood → dst port = 53 (contoh)
     - Bisa match berdasarkan pps/bps
   - Behavior: `discard`
4. Klik **Save**

> Wanguard akan otomatis mengirim Flowspec rule saat traffic match attack pattern.

6. Konfigurasi Wanguard Filter (Scrubber)

Kalau kamu pakai Wanguard Filter juga, maka:

1. Masuk ke **Filters > Filters**
2. Klik **“Add New Filter”**
3. Isi:
   - Mode: `Bridge` atau `Redirect`
   - Input Interface: `eth0`
   - Output Interface: `eth1`

Mode	Kapan digunakan	Penjelasan
Bridge	Jika Wanguard Filter berada **inline** (di tengah jalur)	Traffic melewati eth0 → difilter → keluar lewat eth1
Redirect	Jika router **mengarahkan** (Flowspec redirect) ke IP filter	Traffic masuk ke IP filter lalu dikembalikan setelah dibersihkan

Pilih yang mana?

- Kalau kamu **taruh Filter langsung di jalur trafik** (di antara router dan infra/tenant): pakai **Bridge**
- Kalau kamu **gunakan Flowspec redirect**, router akan kirim traffic ke IP filter: pakai **Redirect**

Interface	Fungsi	Tersambung ke
`eth0`	Input: menerima trafik mentah	Dari router / port mirror
`eth1`	Output: kirim trafik bersih	Ke tenant / LAN clean zone

4. Atur rule filtering:
   - TCP SYN threshold
   - Drop spoofed IP
   - Allow specific ports/IPs

TCP SYN Threshold

Digunakan untuk mendeteksi TCP SYN flood

- Contoh: `1000 pps`

> “Artinya, kalau ke satu IP/port ada >1000 TCP SYN per detik, dianggap attack

Rekomendasi:

- Di bawah 500 → false positive
- Di atas 2000 → bisa telat mendeteksi

Saran: **1000–3000 pps** tergantung kebutuhan

Drop Spoofed IP

Fungsi: otomatis drop traffic dari IP **tidak valid** atau **spoofed**
Yang dideteksi dan di-drop:

- Private IP dari Internet (misal `192.168.x.x`)
- IP loopback, multicast, reserved
- TTL aneh (TTL <10)
- IP yang tidak sesuai routing table

> Aktifkan opsi ini untuk mengurangi noise attack yang tidak valid

---

Allow Specific Ports/IPs

Fungsi: memperbolehkan traffic tertentu tetap lewat meskipun sedang ada mitigasi
Contoh use case:

- Kamu ingin tetap allow port 443 (HTTPS) meskipun sedang diserang SYN port 2211
- Atau ingin tetap allow IP internal tertentu (misal IP CDN)

Setting	Value yang disarankan
Mode	`Redirect` *(jika pakai Flowspec)* atau `Bridge` jika inline
Input Interface	`eth0` (dari router/SPAN/Flowspec)
Output Interface	`eth1` (ke tenant atau clean segment)
TCP SYN threshold	`1000–3000 pps`
Drop Spoofed	☑ Aktifkan
Allow ports/IP	Tambahkan sesuai kebutuhan (port 443, IP tertentu)

5. Klik **Save & Start Filter**

> Kamu bisa sambungkan sensor ke filter melalui Response type: **Redirect via BGP next-hop** jika router support redirect via Flowspec.

---

7. Uji Coba dan Simulasi

- Simulasikan SYN flood atau DNS flood
- Lihat apakah:
  - Sensor mendeteksi trafik
  - Flowspec muncul di router
  - Traffic jahat di-drop
  - Clean traffic tetap jalan

---

8. Monitoring & Logs

- **Dashboard** → untuk serangan aktif
- **Logs > Flowspec** → lihat rule yang di-inject
- **Sensors > Attacks** → histori serangan
- **Filters > Cleaned Packets** → statistik scrubber

Hasil Akhir yang Diharapkan

Komponen	Fungsi
Sensor	Monitor trafik tanpa mengganggu jalur
Router	Menerapkan Flowspec rules (drop/redirect)
Filter	(Jika dipakai) Membersihkan trafik lalu meneruskan ke tenant
Tenant	Tetap online, trafik jahat disaring sedini mungkin