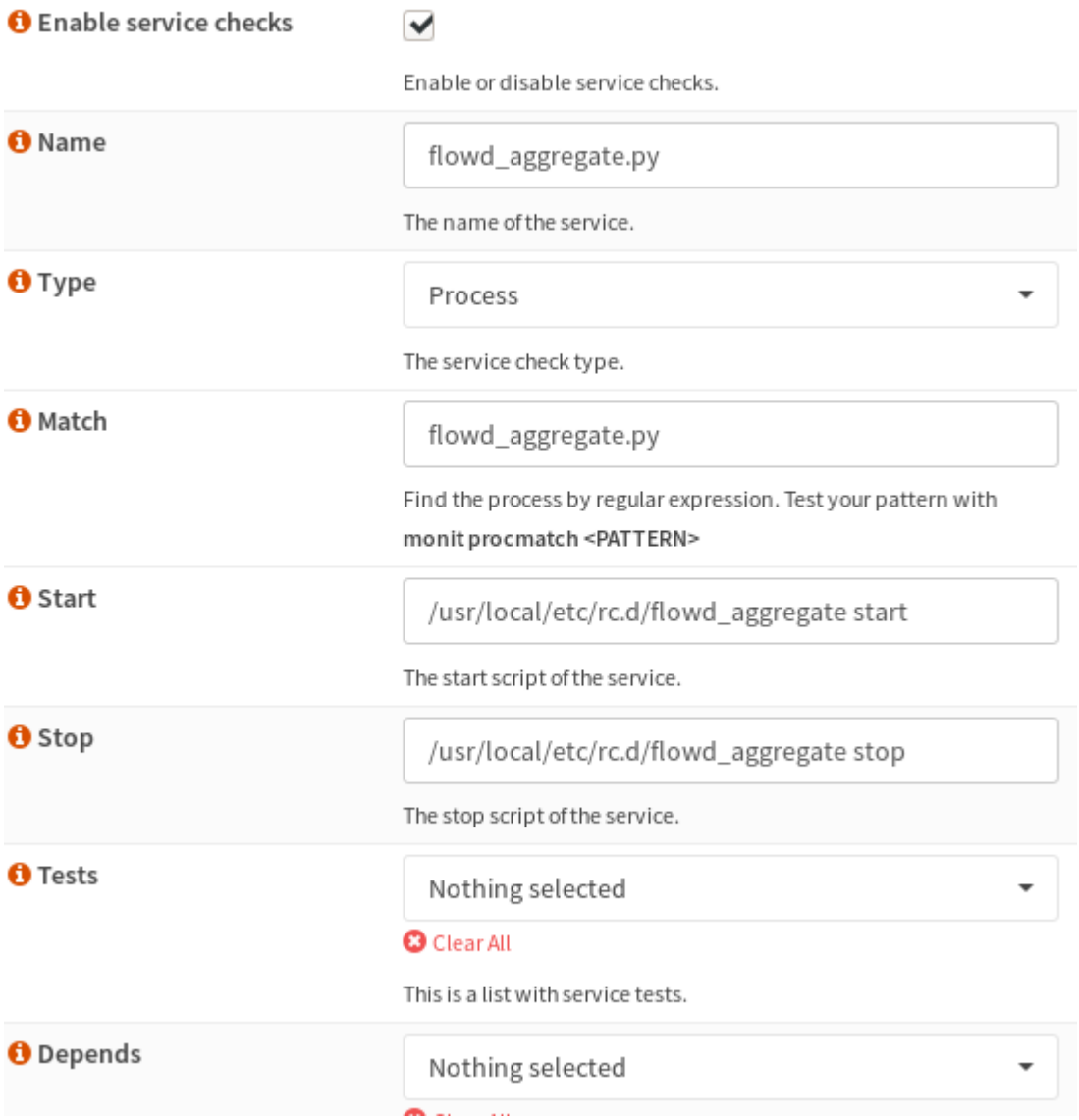
ISSUES

flowd

flowd.log is 5GB. flowd_aggregate.py died (Insight Aggregator service). Workaround is to use monit:



Multiwan

multiwan: when primary WAN fails, local connectivity stops

Primary WAN fails:

1. Local (from OPNSense host) DNS doesn't work
2. local connectivity also doesn't work ``No route to host``
3. internet for LAN users works (switched to WAN2)
4. one LAN device cannot connect to 8.8.8.8 DNS server, because this request is still forwarded to

WAN1

SOLUTION ? PROPOSALS:

1. Allow DNS server list to be overridden by DHCP/PPP on WAN = CHECKED <– uncheck this

multiwan: port reflection not working

Scenario:

- Not possible to connect to port-forwarded service using WAN IP

Problem 1

- Problem caused by Policy based routing with Multi WAN setup:
  - Firewall–>Rules–>LAN, when all LAN traffic has gateway set. LAN to LAN traffic should use default gateway.

Solution 1

- Add rule before default gateway rule: LAN net –> LAN net to use Gateway default

Problem 2

- When interface group is used as interface in **Firewall –> NAT –> Port Forward**, reply-to rules are not generated.

Solution 2

- Do not create NAT rule for **interface group**. Use duplicated rules for each WAN interface

multiwan: port forwards

Scenario:

- Interface group WAN created, to group to WAN1 and WAN2 interfaces.
- Prot forward defined from WAN to WAN:NETWORK TCP/UDP port 2196. to host 192.168.0.231:2196.

Problem:

- Connection from world to WAN1 IP port 2196 works.
- Connection from world to WAN2 IP prot 2196 doesn't work. It is correctly forwarded to LAN host, but response is sent using wrong WAN1 interface (src IP is WAN2 IP).

Solution

- Do not create NAT rule for **interface group**. Use duplicated rules for each WAN interface

multi wan: lan gw was chosen

If gateway switching is used, it is needed to set all not WAN gateways as forced down.

System –> Settings –> General –> Allow default gateway switching

```
If the link where the default gateway resides fails switch the default
gateway to another available one. When using default gateway switching use
any available gateway or select a specific gateway group below.
```

System –> Gateways –> Single –> ... –> Mark Gateway as Down

static route from LAN to LAN not working

Problem is that all outgoing traffic on LAN interface is using LAN gateway (autodetected)

```
cat /tmp/rules.debug
pass out route-to ( bge0 192.168.0.242 ) from {bge0} to {!(bge0:network)}
keep state allow-opts label "let out anything from firewall host itself"
pass out route-to ( em1 85.222.100.29 ) from {em1} to {!(em1:network)} keep
state allow-opts label "let out anything from firewall host itself"
pass out route-to ( em0 95.143.241.141 ) from {em0} to {!(em0:network)} keep
state allow-opts label "let out anything from firewall host itself"
```

There are two additional gateways in LAN (bge0) (for OpenVPN remote networks): 192.168.0.231 and 192.168.0.242. From unknown reason OPNSense choose 192.168.0.242 as gateway for non LAN traffic. This firewall rule overrides correct static routing:

```
netstat -nr
192.168.251.235/32 192.168.0.231      UGS         bge0
```

As workaround, firewall rule is needed to force output gateway.

correct workaround

Firewall –> Settings –> Advanced: Tick **Disable force gateway** (Outgoing packets from this firewall on an interface which has a gateway will normally use the specified gateway for that interface. When this option is set the route will be selected by the system routing table instead.)

cannot reach another VLAN from VPN

Check for asymetric routing. Firewall cannot track one way packet flow so packets are blocke by

default rule. Solution is to add pass rule without connection tracking enabled (tracking none).