Docker, Ubuntu, Proxmox, IPVlan, trafik mellan containrar och brandväggsregler

Min uppsättning är sådan att jag använder docker (med compose) på Ubuntu-VMar som i sin tur är hostade på Proxmox-hypervisor. Jag tilldelar containrar IPv4-adresser från ett dockernätverk som är av typen IPVlan. Det är ett eget nätverk som finns bakom Ubuntu-hosten. Jag har host-brandvägg aktiverat på VM i Proxmox.

Den här kombinationen av tekniker gör att jag ser trafiken mellan containrarna i Proxmox på host-brandväggen och kan bygga regler där. Jag är inte superbra på hur det funkar, jag har kopierat in ett svar från ChatGPT här:

Svar från ChatGPT

IPVlan *logiskt* kopplar containrarna direkt mot varandra, men i din **Proxmox-miljö** finns ett extra lager som gör att trafiken **ser ut som om den går via hosten**. Låt oss reda ut exakt varför.

Kort svar

Containrarna pratar **inte via Linux-hostens IP-stack**, men deras trafik går ändå **via hostens NIC → Proxmox vSwitch → Proxmox brandvägg**.
Därför syns den i hypervisorns firewall – och det är helt korrekt beteende.

Vad som faktiskt händer i ditt setup

Du har i praktiken detta:

```
[Container A]
     |
   IPVlan
     |
[Ubuntu VM kernel]
     |
  virtio-net
     |
[Proxmox bridge / vSwitch]
     |
[Proxmox firewall]  ⬅️ du ser trafiken här
     |
[Ubuntu VM NIC]
     |
[Container B]
```

Viktig poäng

- **IPVlan gör switching i kernel**
- Men **kernel är i en VM**
- VM:ns nätverksinterface är **virtuellt (virtio)**
- All trafik måste därför passera **Proxmox bridge**

Varför detta inte motsäger hur IPVlan fungerar

“Men IPVlan ska ju vara host-local?”

Ja — på **bare metal**.

I en VM:

- Ubuntu-hostens “fysiska interface” är egentligen **ett virtuellt NIC**
- IPVlan använder detta NIC som *parent*
- All egress/ingress → **Proxmox vSwitch**

Så även:

```
containerA → containerB
```

blir i praktiken:

```
containerA
 → ipvlan
 → VM kernel
 → virtio-net
 → Proxmox bridge (firewall!)
 → virtio-net
 → VM kernel
 → ipvlan
 → containerB
```

Ingen NAT. Ingen routing.
Men **hypervisorn ser L2/L3-trafiken**.

Varför Proxmox brandvägg ser trafiken

Proxmox brandvägg:

- Körs på **bridge-nivå**
- Inspekterar **all VM-trafik**
- Spelar ingen roll om IP-källan och IP-destinationen är “samma VM”

Så:

- Samma MAC ✔
- Olika IP ✔

- Bridge-forwarding ✔
  → Firewall triggeras

Detta är **precis som om två processer i samma VM pratar via nätet**.

Varför detta är *bra* (och varför du gillar det □□)

Du får:

- □ Riktiga IP-adresser
- □ Ingen Docker NAT
- □ Full synlighet i Proxmox FW
- □ Central policy enforcement
- □ Mikrosegmentering utan overlay-nät

I praktiken beter sig containrarna som **mini-VMs bakom samma NIC**.

Detta är en av de *stora* fördelarna med:

> **IPVlan + VM + Proxmox**

Skillnad mot Docker bridge i VM

Med `bridge` hade du ofta sett:

- NAT inuti VM
- Mindre synlig L3-trafik i Proxmox
- Svårare policy enforcement

IPVlan ger dig **ren trafik upp till hypervisorn**.

Mental modell (bra att komma ihåg)

> IPVlan = *”direct attach” till **det interface du har***
> I en VM → det interface ägs av hypervisorn

Så:

- Bare metal → stannar lokalt
- VM → går via vSwitch

Revision #4
Created 3 February 2026 13:58:39 by Jehrlander
Updated 3 February 2026 20:09:40 by Jehrlander