AYI NEDJIMI Consultants

SDN Proxmox VE 9 : Zones, VNets, IPAM et Firewalls

Catégorie : Virtualisation Lecture : 6 min Publié le : 22/03/2026 Auteur : Ayi NEDJIMI

Maîtrisez le SDN Proxmox VE 9 : zones Simple/VXLAN/EVPN, VNets, IPAM intégré et VNet Firewall. Configurations CLI et GUI pour clusters multi-tenants.

Le **Software Defined Network (SDN)** de **Proxmox VE 9** transforme profondément la gestion réseau des clusters virtualisés en offrant une abstraction complète des topologies physiques. Ce guide expert détaille la configuration des **zones SDN** (Simple, VXLAN, EVPN, QinQ), la création de *VNets (réseaux virtuels isolés définis par logiciel)*, la gestion **IPAM** intégrée pour l'allocation automatique d'adresses IP, les protocoles **VXLAN** et **EVPN/BGP** pour le routage inter-zones, ainsi que le **VNet Firewall** pour sécuriser vos environnements multi-tenants. Que vous administriez un homelab ou une infrastructure de production multi-nœuds, la maîtrise du SDN Proxmox est indispensable pour isoler les workloads, optimiser le routage et garantir la sécurité réseau. Ce guide couvre chaque composant avec des exemples CLI et GUI concrets, des cas d'usage réels et les meilleures pratiques pour déployer un SDN robuste et scalable sur Proxmox VE 9.

Points clés à retenir

- Le SDN Proxmox VE 9 repose sur une hiérarchie Zones → VNets → Subnets permettant une isolation réseau complète entre tenants et workloads.
- Les zones VXLAN et EVPN/BGP permettent d'étendre les réseaux virtuels sur l'ensemble du cluster avec routage inter-VNets et support multi-site.
- L'IPAM intégré (PHPipam ou NetBox) automatise l'allocation d'adresses IP et élimine les conflits dans les environnements dynamiques.
- Le VNet Firewall applique des règles de sécurité directement au niveau du réseau virtuel, indépendamment du firewall hôte ou VM.

Architecture SDN Proxmox : Zones, VNets et Subnets

L'architecture **SDN Proxmox VE 9** s'organise en trois niveaux hiérarchiques : les **zones** définissent le type de technologie réseau (Simple, VXLAN, EVPN, QinQ), les *VNets (Virtual Networks)* représentent les segments réseau isolés au sein d'une zone, et les **subnets** définissent les plages d'adresses IP avec passerelle et options DHCP. Cette hiérarchie permet une gestion centralisée et scalable de l'infrastructure réseau virtuelle depuis l'interface web Proxmox ou via l'API REST.

La configuration SDN est stockée dans **/etc/pve/sdn/** et répliquée automatiquement sur tous les nœuds du cluster via le **CGFS (Cluster File System)**. Après chaque modification, la commande **pvesh set /cluster/sdn/vnets --apply 1** propage les changements sur l'ensemble des nœuds.

Types de Zones SDN et Cas d'Usage

Zone Simple : Isolation L2 par VLAN

La *zone Simple* est le type le plus basique : elle crée des ponts Linux isolés sur chaque nœud. Idéale pour les environnements homlab ou petits clusters sans exigences de routage inter-VNets. Configuration minimale via GUI : Datacenter → SDN → Zones → Add → Simple, en spécifiant le bridge physique (ex: vmbr0).

Zone VXLAN : Extension L2 Multi-Nœuds

La *zone VXLAN (Virtual eXtensible Local Area Network)* encapsule le trafic L2 dans des paquets UDP pour l'étendre sur le réseau IP du cluster. Chaque VNet reçoit un **VNI (VXLAN Network Identifier)** unique. Cette zone convient aux clusters multi-nœuds nécessitant des réseaux virtuels partagés sans routage centralisé. Prérequis : MTU ≥ 1550 sur le réseau physique pour absorber l'overhead VXLAN (50 bytes).

Zone EVPN/BGP : Routage Inter-VNets Distribué

La *zone EVPN (Ethernet VPN)* combine VXLAN pour le transport L2 avec **BGP (Border Gateway Protocol)** pour la distribution des routes L3. Elle permet le routage inter-VNets sans dépendance à un routeur centralisé, avec support de l'anycast gateway pour une redondance optimale. Configuration requise : un routeur BGP par nœud (généralement **FRRouting**), un ASN dédié et un VTEP IP par nœud.

Zone QinQ : Double Encapsulation VLAN

La zone **QinQ (802.1ad)** permet la double encapsulation VLAN (VLAN externe opérateur + VLAN interne client). Utilisée principalement dans les environnements MSP (Managed Service Provider) pour isoler les infrastructures clients tout en partageant une infrastructure physique commune.

Configuration des VNets et Subnets

Un **VNet** est créé via Datacenter → SDN → VNets → Add, en associant un nom, une zone parente et un tag VLAN optionnel. Pour les zones VXLAN/EVPN, un **VNI** est automatiquement assigné. La commande CLI équivalente :

pvesh create /cluster/sdn/vnets -vnet vnet100 -zone vxlan-zone -tag 100

Les **subnets** définissent les plages CIDR avec passerelle (gateway), serveur DHCP optionnel et DNS. Pour activer le DHCP sur un subnet, le service **dnsmasq** doit être configuré sur les nœuds Proxmox. Un subnet avec SNAT (Source NAT) permet aux VMs d'accéder à Internet sans IP publique dédiée.

IPAM Intégré : Gestion Automatique des Adresses IP

L'*IPAM (IP Address Management)* intégré dans Proxmox VE 9 élimine la gestion manuelle des adresses IP. Deux backends sont supportés : **PHPipam** (self-hosted) et **NetBox** (DCIM complet). La configuration s'effectue dans Datacenter → SDN → IPAM → Add en spécifiant l'URL de l'instance et le token API.

Une fois l'IPAM configuré, lors de la création d'un subnet SDN avec l'option IPAM activée, les adresses allouées aux VMs sont automatiquement enregistrées dans la base IPAM. Cela garantit une visibilité centralisée et évite les conflits d'adresses dans les environnements à forte densité de VMs.

Type de Zone	Protocole	Routage Inter-VNets	Cas d'Usage
Simple	Linux Bridge	Non (L2 uniquement)	Homelab, petit cluster
VXLAN	VXLAN/UDP	Non (L2 étendu)	Multi-nœuds sans routage
EVPN	VXLAN + BGP	Oui (L3 distribué)	Production, multi-tenant
QinQ	802.1ad	Non (double VLAN)	MSP, isolation client

VNet Firewall : Sécurité au Niveau Réseau Virtuel

Le **VNet Firewall** de Proxmox SDN applique des règles de filtrage directement au niveau du réseau virtuel, en amont du firewall hôte et VM. Il s'appuie sur **ebtables** (filtrage L2) et **iptables/nftables** (filtrage L3/L4) pour contrôler le trafic entrant et sortant de chaque VNet.

Les règles sont définies dans Datacenter → SDN → VNets → [VNet] → Firewall et s'appliquent à toutes les VMs connectées à ce VNet. Les **IPSets** permettent de regrouper des plages d'adresses pour simplifier la gestion des règles. La politique par défaut (DROP ou ACCEPT) est configurable par VNet.

Pour sécuriser un environnement multi-tenant, la bonne pratique consiste à créer une zone EVPN par tenant avec VNet Firewall activé en mode DROP par défaut, n'autorisant que les flux explicitement listés. Consultez notre guide de hardening Proxmox VE pour une stratégie de sécurité complète.

Déploiement EVPN : Configuration FRRouting et BGP

FRRouting (FRR) est le daemon de routage utilisé par Proxmox pour implémenter EVPN. Il est installé automatiquement avec le plugin EVPN SDN. La configuration BGP générée dans **/etc/frr/frr.conf** définit les sessions iBGP entre les nœuds du cluster, les VNIs à redistribuer et les anycast gateways.

Exemple de vérification de l'état BGP : **vtysh -c "show bgp summary"**. Pour diagnostiquer les routes EVPN : **vtysh -c "show bgp l2vpn evpn"**. En cas de problème de routage inter-VNets, vérifier que le **ip_forward** est activé sur tous les nœuds et que les VNIs sont cohérents entre les zones.

Dépannage SDN et Commandes Clés

Le diagnostic SDN Proxmox repose sur plusieurs outils : **pvesh get /cluster/sdn/vnets** liste les VNets configurés, **bridge fdb show** affiche la table de forwarding L2, et **ip route show table [VNI]** vérifie les routes EVPN injectées. Les logs SDN se trouvent dans **/var/log/pve/tasks/** après chaque apply.

Pour les problèmes de connectivité VXLAN, vérifier les règles firewall sur le port UDP 4789 (VXLAN) avec **iptables -L -n | grep 4789**. Pour EVPN, s'assurer que le port TCP 179 (BGP) est ouvert entre les nœuds. La documentation officielle Proxmox SDN et le wiki Proxmox sont des références indispensables.

Pour aller plus loin sur l'architecture réseau, consultez notre guide d'architecture cluster Proxmox 3 nœuds et notre référence CLI d'administration Proxmox.

Questions fréquentes

Comment choisir entre une zone VXLAN et une zone EVPN dans Proxmox SDN ?

La zone **VXLAN** est recommandée lorsque vous avez uniquement besoin d'étendre des réseaux L2 entre nœuds sans routage inter-VNets. Elle est plus simple à configurer et consomme moins de ressources. La zone **EVPN** s'impose dès que vous avez besoin de routage L3 distribué entre VNets, de support anycast gateway pour la redondance ou d'une architecture multi-site. En production avec plusieurs tenants isolés nécessitant des politiques de routage distinctes, EVPN est le choix incontournable.

Pourquoi l'IPAM SDN Proxmox est-il préférable à une gestion manuelle des IPs ?

Dans un cluster Proxmox avec des dizaines ou centaines de VMs, la gestion manuelle des adresses IP génère inévitablement des conflits et des erreurs. L'**IPAM intégré** (PHPipam ou NetBox) automatise l'allocation, garantit l'unicité des adresses et offre une visibilité centralisée

de toute la plage réseau. Il s'intègre directement avec les subnets SDN pour enregistrer automatiquement chaque VM créée, éliminant le travail de documentation manuelle et réduisant les incidents réseau liés aux conflits d'IP.

Comment sécuriser les communications entre VNets dans un environnement multi-tenant Proxmox ?

La sécurité multi-tenant repose sur l'isolation stricte des zones SDN avec **VNet Firewall** activé en politique DROP par défaut. Chaque tenant dispose de sa propre zone EVPN avec VNIs dédiés, empêchant toute communication non autorisée. Le VNet Firewall applique des règles ebtables/iptables au niveau du bridge virtuel, avant même que le trafic n'atteigne le firewall de la VM. Les **IPSets** permettent de définir des listes blanches précises. Pour le trafic inter-tenants légitimes, des VRFs (Virtual Routing and Forwarding) dédiés dans FRRouting assurent l'isolation des tables de routage.

Sources et références : Proxmox VE Wiki · ANSSI

Articles connexes

- Outils Proxmox VE : Monitoring, IaC et Écosystème 2026

Conclusion

Le **SDN Proxmox VE 9** offre une architecture réseau virtualisée puissante et flexible, de la simple isolation VLAN aux topologies EVPN/BGP multi-sites. La maîtrise des zones SDN, de l'IPAM intégré et du VNet Firewall permet de construire des infrastructures multi-tenants robustes, sécurisées et automatisables. L'investissement dans la compréhension de ces concepts se traduit directement par une réduction des incidents réseau et une agilité accrue dans la gestion des workloads.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr