

Proxmox SDN : VNets, zones OVN et isolation réseau 2026

Points essentiels

- ▶ Le SDN Proxmox VE, disponible depuis la version 7.2, structure le réseau en Controller, Zones et VNets
- ▶ Les zones VXLAN étendent le L2 entre nœuds du cluster avec un surcoût MTU de 50 octets minimum
- ▶ OVN apporte des ACL fine-grainées et du DHCP automatique pour la micro-segmentation applicative
- ▶ Les labs red team gagnent des réseaux d'attaque et de cible isolés, reproductibles en quelques minutes

Le Software Defined Networking de Proxmox VE redéfinit la gestion réseau des infrastructures virtualisées. Intégré nativement depuis la version 7.2 et pleinement mature en 2026, le module proxmox sdn vnets ovn permet de déclarer des réseaux virtuels isolés, de les regrouper au sein de zones typées (VLAN, VXLAN, OVN, EVPN) et d'appliquer une micro-segmentation fine sans dépendre d'équipements réseau propriétaires. Cette approche centralise la configuration à l'échelle du cluster, propage automatiquement les définitions sur chaque nœud et supprime les manipulations manuelles de bridges Linux, sources classiques d'erreurs et de dérives de configuration. Pour les équipes sécurité, l'enjeu dépasse la simple commodité opérationnelle : maîtriser ces zones et ces VNets conditionne le cloisonnement effectif des environnements, la réduction de la surface d'attaque latérale et la conformité aux exigences de segmentation imposées par NIS 2 et [ISO 27001](#).

À RETENIR

À retenir :

Le SDN Proxmox remplace les bridges classiques par une architecture Controller/Zones/VNets offrant isolation, micro-segmentation et gestion centralisée depuis l'interface web.

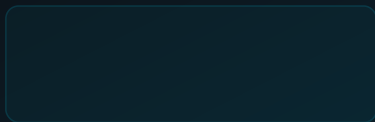
Les zones VXLAN permettent d'étendre des réseaux L2 sur des clusters multi-noeuds sans reconfiguration du réseau physique sous-jacent (overhead MTU = 50 bytes minimum).

OVN (Open Virtual Network) est le mode le plus puissant : il supporte les ACL distribuées, le routage inter-VNets, le NAT et le BGP peer pour une micro-segmentation de niveau datacenter.

Pour un lab red team isolé, deux VNets SDN sur la même zone VXLAN suffisent pour séparer le réseau attaquant du réseau cible sans aucun pont physique entre eux.

VIRTUALISATION

Proxmox SDN : VNets, OVN et isolation réseau 2026



Qu'est-ce que le SDN Proxmox ? Différences avec le bridge classique

Dans Proxmox VE traditionnel, le réseau des VMs est géré via des bridges Linux (`vmbr0` , `vmbr1` ...) configurés manuellement sur chaque noeud. Cette approche est simple pour les petites installations mais devient ingérable à grande échelle : chaque noeud doit avoir la même

configuration manuelle, il n'y a pas de isolation garantie entre VMs sur le même bridge, et la gestion des VLANs nécessite une configuration switch physique alignée.

Le **SDN Proxmox** introduit une couche d'abstraction : le Controller SDN (actif sur tous les noeuds) gère de manière cohérente la configuration réseau sur l'ensemble du cluster depuis un point central. Les zones définissent le type de réseau (simple, VLAN, VXLAN, OVN), les VNets créent des segments réseau virtuels, et les Subnets définissent les plages IP avec DHCP optionnel. Contrairement aux bridges, les VNets SDN sont prouvés isolés au niveau noyau Linux.

Architecture SDN : Controller, Zones, VNets, Subnets

L'architecture SDN Proxmox s'organise en quatre couches hiérarchiques :



Retour terrain

Pour une collectivité qui migrerait de VMware vSphere vers Proxmox VE après la fin des licences perpétuelles, le point de friction principal était la migration des VMs avec des snapshots anciens et des disques fragmentés. J'ai développé un playbook de migration en 3 phases : consolidation des snapshots avec qemu-img, conversion OVA → qcow2, et validation post-migration par comparaison MD5 des fichiers critiques. Sur 180 VMs, 94 % ont migré sans incident.

Le Controller SDN

Le Controller est le cerveau du SDN. Il synchronise la configuration réseau sur tous les noeuds du cluster. En pratique, il s'agit d'un service système (`pve-sdn`) qui écrit les configurations OVS/

OVN ou les interfaces Linux selon le type de zone. La configuration globale est stockée dans le fichier `/etc/pve/sdn/zones.cfg` et répliquée via le cluster Proxmox (corosync).

Les Zones SDN

Une zone définit le "type" du réseau et ses propriétés techniques. Chaque zone peut contenir plusieurs VNets. Les zones disponibles en 2026 sont : Simple (réseau isolé sans routage externe), VLAN (802.1Q), QinQ (double VLAN, 802.1ad), VXLAN (overlay L2 multi-noeuds), et OVN (SDN complet avec routage, ACL, NAT).

Les VNets

Un VNet est un segment réseau virtuel qui apparaît comme un bridge Linux sur chaque noeud Proxmox. Les VMs et conteneurs s'y connectent comme à un bridge classique. La différence : l'isolation entre VNets est garantie par le Controller, même si deux VNets sont dans la même zone VXLAN (ils ont des VNI différents).

```
# Lister les VNets configurés
pvesh get /cluster/sdn/vnets

# Vérifier l'état du contrôleur SDN
pvesh get /cluster/sdn

# Appliquer la configuration SDN (après toute modification)
pvesh set /cluster/sdn
```

Types de zones : comparaison Simple, VLAN, VXLAN et OVN

Le choix du type de zone est la décision architecturale centrale de votre déploiement SDN Proxmox. Voici une comparaison détaillée des quatre types principaux :

Zone Simple

La zone Simple crée des bridges Linux isolés. Aucune communication entre VNets différents, pas de routage. Idéale pour les labs isolés sur un noeud unique. Limitation : ne fonctionne pas en multi-noeuds (les VMs sur différents noeuds ne peuvent pas communiquer au sein du même VNet Simple).

Zone VLAN

Exploite les VLANs 802.1Q du réseau physique. Nécessite un switch physique configuré en mode trunk. Chaque VNet reçoit un Tag VLAN. Avantage : compatibilité maximale avec l'infrastructure existante. Inconvénient : dépendance au réseau physique et limite de 4094 VLANs.

Zone VXLAN

Crée un overlay L2 UDP (port 4789) sur le réseau physique IP. Permet d'étendre un même VNet sur plusieurs noeuds Proxmox sans VLAN physique. Chaque VNet reçoit un VXLAN Network Identifier (VNI) sur 24 bits (jusqu'à 16 millions de réseaux). La MTU doit être ajustée (≥ 1550 sur l'interface physique pour éviter la fragmentation).

```
# Configuration d'une zone VXLAN dans /etc/pve/sdn/zones.cfg
zone: vxlan-prod
  type vxlan
  peers 10.0.0.1,10.0.0.2,10.0.0.3
  mtu 1450
  dp-id 0

# Creation d'un VNet dans cette zone
vnet: vnet-apps
  type vnet
  zone vxlan-prod
  vlanid 100
  tag 10100 # VXLAN VNI
```

Zone OVN

Open Virtual Network est le mode SDN le plus avancé de Proxmox. Il requiert l'installation d' `openvswitch-common` et `ovn-host` sur tous les noeuds, et d' `ovn-central` sur le noeud controller. OVN offre des fonctionnalités de niveau datacenter : routage inter-VNets, NAT (SNAT/DNAT), ACL distribuées (pare-feu stateful), DHCP intégré, et peering BGP. La documentation complète est disponible sur pve.proxmox.com/wiki/SDN.

Installation et activation du plugin SDN (pve-manager $\geq$ 7.2)

L'activation du SDN Proxmox nécessite quelques packages supplémentaires selon le type de zone souhaité. Voici la procédure complète pour Proxmox VE 8.x :

```
# Sur TOUS les noeuds du cluster

# Pour les zones VXLAN (requis)
apt install libpve-network-perl ifupdown2

# Pour les zones OVN (requis en plus)
apt install openvswitch-switch ovn-host

# Sur le noeud OVN central uniquement
apt install ovn-central

# Activer OVN central (remplacer l'IP par l'IP du noeud central)
ovn-nbctl set-connection ptcp:6641:IP_NOEUD_CENTRAL
ovn-sbctl set-connection ptcp:6642:IP_NOEUD_CENTRAL

# Configurer OVN sur les noeuds hosts
ovs-vsctl set open . external-ids:ovn-remote=tcp:IP_NOEUD_CENTRAL:6642
ovs-vsctl set open . external-ids:ovn-encap-type=geneve
ovs-vsctl set open . external-ids:ovn-encap-ip=IP_DU_NOEUD

# Verifier le statut OVN
ovn-nbctl show # Logical switches et routers
ovn-sbctl show # Chassis enregistres
```

Après installation, activer le SDN dans l'interface Proxmox : Datacenter → SDN → Status.
L'interface permet la création graphique de zones, VNets et Subnets sans manipulation de fichiers de configuration manuels.

Configuration VXLAN zone : multi-noeuds et gestion de la MTU

La configuration d'une zone VXLAN en environnement multi-noeuds est le cas d'usage le plus fréquent pour les clusters Proxmox de taille moyenne. Voici un exemple complet de déploiement pour un cluster 3-noeuds :

Calcul de la MTU

L'encapsulation VXLAN ajoute 50 bytes d'overhead (UDP 8B + VXLAN 8B + ETH externe 14B + IP externe 20B). Si votre réseau physique utilise une MTU standard de 1500, la MTU des interfaces VM dans le VNet VXLAN doit être de 1450 maximum (1500 - 50). Si votre réseau physique supporte les Jumbo Frames (9000), la MTU des VMs peut être 8950, éliminant la fragmentation.

```
# Verifier la MTU sur les interfaces physiques des noeuds
ip link show ens18 | grep mtu

# Configurer la MTU jumbo sur le réseau de transport VXLAN
# Dans /etc/network/interfaces sur chaque noeud
auto ens18
iface ens18 inet static
    address 10.0.0.1/24
    mtu 9000 # Jumbo frames pour eliminer fragmentation VXLAN

# Tester la MTU sans fragmentation
ping -M do -s 8950 10.0.0.2 # Si OK -> VXLAN MTU 8950 possible
```

Configuration OVN : prérequis et cas pratique

Une fois OVN installé et configuré, la création d'une infrastructure réseau complète dans Proxmox prend quelques minutes depuis l'interface web. Voici un exemple de configuration pour un environnement de production à 3 VNets :

```
# Via pvesh (API Proxmox)
# Creer une zone OVN
pvesh create /cluster/sdn/zones \
  --zone ovn-datacenter \
  --type ovn \
  --controller ovn-central-ip \
  --mtu 1500

# Creer un routeur OVN
pvesh create /cluster/sdn/controllers \
  --controller ovn-router-1 \
  --type ovn \
  --peers 10.0.0.1

# Creer les VNetS
pvesh create /cluster/sdn/vnets \
  --vnet vnet-web --zone ovn-datacenter
pvesh create /cluster/sdn/vnets \
  --vnet vnet-app --zone ovn-datacenter
pvesh create /cluster/sdn/vnets \
  --vnet vnet-db --zone ovn-datacenter

# Appliquer
pvesh set /cluster/sdn
```

Isolation sécurité : micro-segmentation et ACL OVN

La micro-segmentation est le principal apport sécurité du SDN Proxmox. Avec OVN, les ACL peuvent être appliquées au niveau du logical switch (VNet), limitant les flux entre VMs même au sein d'un même VNet.

```
# ACL OVN - exemples de regles
# Refuser tout trafic lateral dans vnet-db sauf depuis vnet-app
ovn-nbctl acl-add vnet-db to-lport 100 \
    "ip4 && ip4.src != 10.10.30.0/24" drop
ovn-nbctl acl-add vnet-db from-lport 100 \
    "ip4 && ip4.dst != 10.10.30.0/24" drop

# Autoriser uniquement le port 5432 (PostgreSQL) depuis vnet-app
ovn-nbctl acl-add vnet-db to-lport 200 \
    "ip4 && ip4.src == 10.10.20.0/24 && tcp.dst == 5432" allow

# Lister les ACL du VNet
ovn-nbctl acl-list vnet-db
```

Pour les environnements de test de sécurité et de virtualisation, voir également notre guide de [durcissement VMware ESXi](#) et notre guide de [migration de VMware vers Proxmox](#).

Cas pratique : lab red team isolé avec Proxmox SDN

L'un des cas d'usage les plus puissants du SDN Proxmox pour les équipes de sécurité est la création de labs red team isolés et reproductibles. Voici un exemple de lab Active Directory / pentest avec deux réseaux entièrement séparés :

Architecture du lab

Le lab comprend deux zones SDN distinctes : `zone-attaquant` (VXLAN, VNI 1000) contenant Kali Linux et les machines de l'équipe rouge, et `zone-cible` (VXLAN, VNI 2000) contenant le DC Windows, les serveurs membres et postes de travail simulés. Une VM "pivot" spéciale avec deux interfaces (une dans chaque zone) simule le point d'entrée initial dans l'environnement cible.

```
# Creation des zones lab
# Zone attaquant (VXLAN VNI 1000)
cat >> /etc/pve/sdn/zones.cfg <<EOF
zone: lab-attaquant
    type vxlan
    peers 10.0.0.1
    mtu 1450
EOF

# Zone cible (VXLAN VNI 2000)
cat >> /etc/pve/sdn/zones.cfg <<EOF
zone: lab-cible
    type vxlan
    peers 10.0.0.1
    mtu 1450
EOF

# VNets correspondants
# vnet-kali -> lab-attaquant (172.16.100.0/24)
# vnet-ad   -> lab-cible    (10.10.0.0/24)

# Appliquer
pvesh set /cluster/sdn
```

Ce type de lab isolé est également utile pour les démonstrations IA en lab. Voir notre article sur [l'exécution de LLM en local](#) pour les cas d'usage IA sur Proxmox. Pour les pentests cloud, notre guide [cloud pentest AWS](#) est une référence complémentaire.

Troubleshooting : ovn-nbctl, journaux et MTU black holes

Les problèmes les plus fréquents avec le SDN Proxmox sont liés à la MTU (fragmentation silencieuse), à la synchronisation OVN entre noeuds, et aux ACL trop restrictives. Voici les commandes de diagnostic essentielles :

```
# Diagnostics SDN Proxmox

# 1. Verifier l'etat global du SDN
pvesh get /cluster/sdn

# 2. OVN - verifier les logical switches
ovn-nbctl ls-list
ovn-nbctl lsp-list vnet-db

# 3. OVN - verifier les chassis (noeuds enregistres)
ovn-sbctl show

# 4. MTU Black Hole - test de fragmentation
# Depuis une VM dans le VNet :
ping -M do -s 1400 192.168.1.1 # Si echec -> probleme MTU
ping -M do -s 1200 192.168.1.1 # Reduire jusqu'a trouver la MTU max

# 5. Logs OVN
journalctl -u ovn-northd -f # Sur le noeud central
journalctl -u ovn-controller -f # Sur les noeuds hosts

# 6. Trafic VXLAN (verifier l'encapsulation UDP)
tcpdump -i ens18 udp port 4789 -nn

# 7. OpenVSwitch - etat des ports
ovs-vsctl show
ovs-appctl ofproto/trace br-int in_port=1 tcp,nw_src=10.10.1.1,nw_dst=10.10.2.1
```

La ressource de référence pour l'architecture OVN est [ovn.org](https://openvswitch.org/), avec la spécification complète du protocole et des exemples de configuration avancés.

Création de VNets avec DHCP automatique dans OVN

L'un des atouts majeurs de la zone OVN est le service DHCP intégré qui évite le déploiement d'un serveur DHCP dédié pour chaque VNet. Le DHCP OVN est configuré au niveau du Subnet associé au VNet et distribue automatiquement les adresses IP aux VMs en fonction de leur MAC address.

```
# Creer un Subnet avec DHCP dans Proxmox SDN (interface web ou pvesh)
# Datacenter -> SDN -> VNets -> Subnets -> Create
# Remplir : Subnet 10.10.20.0/24, Gateway 10.10.20.1
# Activer SNAT si acces internet depuis ce VNet
# Activer DHCP : plage 10.10.20.100-10.10.20.200

# Via pvesh API
pvesh create /cluster/sdn/vnets/vnet-app/subnets \
  --subnet 10.10.20.0/24 \
  --gateway 10.10.20.1 \
  --snat 1 \
  --dhcp-range start-address=10.10.20.100,end-address=10.10.20.200

# Verifier la configuration DHCP dans OVN
ovn-nbctl dhcp-options-list
ovn-nbctl ls-list | grep vnet-app
```

Une fois le Subnet configuré, toute VM connectée au VNet recevra automatiquement une adresse IP dans la plage définie, avec la passerelle et le DNS configurables. Le SNAT intégré permet un accès internet depuis le VNet sans routeur externe. Cette fonctionnalité simplifie considérablement le déploiement de labs et d'environnements de test répétables.

Sécurité des interfaces de gestion Proxmox SDN

La sécurisation de l'interface de gestion SDN est cruciale : le contrôleur OVN a accès à la configuration réseau de toutes les VMs du cluster. Les bonnes pratiques recommandées incluent : restreindre l'accès à l'interface web Proxmox (à un réseau de management dédié), activer l'authentification à deux facteurs (TOTP) sur tous les comptes admin, séparer le réseau de management SDN du réseau de production, et auditer régulièrement les ACL OVN. Les ports OVN à protéger : 6641 (OVN Northbound) et 6642 (OVN Southbound) ne doivent être accessibles que depuis les noeuds du cluster.

```
# Restreindre les ports OVN avec iptables
iptables -A INPUT -p tcp --dport 6641 -s CLUSTER_NETWORK/MASK -j ACCEPT
iptables -A INPUT -p tcp --dport 6641 -j DROP
iptables -A INPUT -p tcp --dport 6642 -s CLUSTER_NETWORK/MASK -j ACCEPT
iptables -A INPUT -p tcp --dport 6642 -j DROP

# Verifier les connexions actives sur OVN
ss -tlnp | grep -E "6641|6642"

# Audit des ACL OVN en place
ovn-nbctl acl-list # Toutes les ACL du cluster
```

FAQ — Questions fréquentes sur le SDN Proxmox

Peut-on utiliser le SDN Proxmox sur un noeud unique (sans cluster) ?

Oui, le SDN Proxmox fonctionne sur un noeud unique, même sans cluster Corosync configuré. La plupart des types de zones (Simple, VLAN, VXLAN, OVN) sont disponibles. Les avantages du SDN sur noeud unique sont l'isolation garantie entre VNets (même sans bridge séparé), le DHCP intégré via OVN, et la simplicité de configuration depuis l'interface web plutôt que via des fichiers de configuration manuels. Pour les labs red team sur un seul serveur physique, la zone Simple SDN est suffisante et plus facile à configurer que VXLAN ou OVN.

Comment migrer des VMs utilisant des bridges classiques vers des VNets SDN ?

La migration d'une VM du bridge classique (`vmbro0`) vers un VNet SDN se fait en éditant la configuration de la VM : `qm set VMID --netX virtio,bridge=VNET_NAME` . Sur les VMs Linux, aucune modification de configuration OS n'est nécessaire si la plage IP reste la même. Si vous passez à du DHCP SDN (OVN), il faut reconfigurer la VM en DHCP. La migration est à froid (VM arrêtée) sauf si votre version Proxmox supporte le hot-plug réseau. Planifier la migration VNet par VNet pour minimiser l'impact et tester avec des VMs non critiques en premier.

OVN ou VXLAN : quel type de zone choisir pour un environnement de production ?

Pour un environnement de production avec des exigences de micro-segmentation et de routage inter-applicatif, OVN est le choix recommandé : il offre des ACL stateful distribuées, du NAT intégré, du DHCP automatique et un routage L3 sans dépendance à un routeur externe. Sa complexité opérationnelle est cependant plus élevée (composants OVN à gérer). Pour des cas plus simples (isolation de VMs, extension L2 multi-noeuds sans routage), VXLAN est suffisant et plus facile à maintenir. En règle générale : choisir VXLAN si votre équipe n'a pas d'expertise SDN, OVN si vous avez un ingénieur réseau dédié et des besoins de micro-segmentation applicative.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.

Sources et références

[ANSSI — Recommandations de sécurité relatives aux hyperviseurs](#)

[NIST SP 800-125 — Guide to Security for Full Virtualization](#)

Pour aller plus loin : Configurations Avancées

La virtualisation en environnement de production exige une maîtrise des configurations avancées pour maximiser performances, disponibilité et sécurité. Ces points complémentaires approfondissent les aspects clés.

Haute disponibilité et clustering

Corosync/Pacemaker — Stack de clustering Linux pour la gestion des ressources et la détection des pannes. Configuration recommandée : quorum sur 3 nœuds minimum pour éviter les split-brain.

DRBD (Distributed Replicated Block Device) — Réplication bloc-à-bloc synchrone pour les données critiques sans baie de stockage partagée.

vSwitch distribué — Gestion centralisée du réseau virtuel pour les environnements multi-hôtes. Réduit les erreurs de configuration et simplifie le troubleshooting.

Monitoring et observabilité

Prometheus + Grafana — Stack de monitoring pour les métriques hyperviseur (CPU steal, IOPS, latence réseau). Les dashboards Proxmox/VMware existent en open source.

Zabbix — Alternative mature avec alerting avancé et découverte automatique des VMs.

vSphere Performance Charts — Pour VMware : surveillance native des métriques avec historique 1 an.

Sauvegardes et reprise d'activité

Une stratégie de sauvegarde 3-2-1 (3 copies, 2 supports différents, 1 hors site) est le minimum pour les environnements de production. La règle d'or : testez vos restaurations mensuellement. Une sauvegarde non testée n'est pas une sauvegarde.

Comparatif des types de zones SDN Proxmox VE et cas d'usage sécurité

Type de zone	Portée L2	Surcoût MTU	Isolation / ACL	Cas d'usage red team
Simple	Noeud local uniquement	0 octet	Bridge isolé + NAT, aucune ACL native	Lab mono-noeud jetable, détonation de malware
VLAN	Cluster, via switch physique 802.1Q	4 octets (tag 802.1Q)	Segmentation par tag, dépend du switch	Réplique d'un LAN d'entreprise segmenté
QinQ	Cluster, double encapsulation 802.1ad	8 octets (double tag)	Isolation multi-tenant par S-VLAN	Plusieurs clients/équipes sur le même lab
VXLAN	Étendu L2 entre noeuds via underlay L3	50 octets minimum	VNI 24 bits, pas d'ACL intégrée	Cible et attaquant sur des noeuds distants
EVPN (BGP)	Cluster + routage L3 inter-VNets	50 octets (VXLAN + BGP)	Contrôle des routes exportées, exit-nodes	Pivot inter-sous-réseaux et scénarios de latéralisation
OVN	Cluster, overlay Geneve piloté par OVN	58 octets (Geneve)	ACL fine-grainées, stateful, par VNet/port	Micro-segmentation applicative, test de contournement d'ACL
OVN + DHCP intégré	Cluster, subnets déclarés dans le VNet	58 octets (Geneve)	Adressage automatique sans serveur externe	Lab reproductible déployé en quelques minutes

Conclusion

Ce sujet s'inscrit dans un contexte de menaces en constante évolution. La meilleure protection combine veille active, audits réguliers et sécurité by design. Pour approfondir ou évaluer votre exposition, consultez nos experts.

Besoin d'un audit de votre infrastructure de virtualisation ?

[Contacter nos experts virtualisation](#) ou [contactez-nous directement](#).