DOCUMENTATION TECHNIQUE

Infrastructure réseau virtualisée sécurisée

Segmentation VLAN - Routage inter-VLAN - Firewall pfSense

BTS SIO - Option SISR

Session : 2026

Étudiant : Alexandre PERZ

Établissement : CFA ESTIAM

Projet : Mise en place d une infrastructure réseau virtualisee

Technologies : Proxmox VE, pfSense, VLAN, NAT, firewalling

Sommaire

1. Présentation du projet

Dans le cadre de ce projet, une infrastructure réseau virtualisee sécurisée a ete déployée afin de reproduire une architecture réseau d entreprise segmentee. L objectif principal etait de mettre en place une architecture claire, evolutive et sécurisée permettant d isoler les differents réseaux, de centraliser les flux et de contrôler les communications via un firewall.

L ensemble de l infrastructure a ete réalisé dans un environnement virtualise sous Proxmox VE avec l utilisation de pfSense comme firewall principal.

Le projet porte uniquement sur la partie réseau de l infrastructure. Les services systèmes comme Active Directory, DNS, DHCP, GLPI ou Zabbix sont traites dans un second projet distinct.

Objectifs principaux

- Segmenter le réseau en plusieurs zones distinctes.
- Mettre en place un routage inter-VLAN centralise.
- Isoler les services critiques et la DMZ.
- Controler les flux réseau avec des règles firewall.
- Permettre un acces Internet aux differents réseaux internes.
- Preparer une base réseau propre pour les services du second projet.

2. Contexte et objectifs

2.1 Contexte du projet

L infrastructure devait reproduire une organisation proche d un environnement professionnel. Dans une entreprise, il est rarement recommande de placer tous les equipements dans le meme réseau. Une segmentation permet de separer les postes utilisateurs, les serveurs internes et les services exposes afin de reduire les risques en cas d incident de sécurité.

Le projet a ete réalisé sur un hyperviseur Proxmox déjà mis a disposition par l etablissement. L installation physique du serveur et l installation initiale de Proxmox ne font donc pas partie du périmètre de cette documentation.

2.2 Objectifs techniques

- Creer plusieurs réseaux isolés dans Proxmox.
- Relier ces réseaux a une machine virtuelle pfSense.
- Configurer pfSense comme routeur et firewall principal.
- Mettre en place les passerelles de chaque réseau.
- Configurer le NAT pour l acces Internet.
- Definir des règles firewall adaptees a chaque zone.
- Valider le fonctionnement par des tests de connectivité et de filtrage.

3. Présentation de l environnement Proxmox

3.1 Role de Proxmox VE

Proxmox VE est utilise comme plateforme de virtualisation. Il permet de creer des machines virtuelles et des réseaux virtuels afin de simuler une infrastructure complete sans disposer de tout le materiel physique correspondant.

- Centraliser plusieurs machines virtuelles sur un meme serveur physique.
- Creer des bridges réseau virtuels, comparables a des switchs virtuels.
- Isoler les flux entre plusieurs segments réseau.
- Faciliter les tests, les modifications et les retours arriere.

3.2 Accès a Proxmox

L administration s effectue depuis l interface web de Proxmox.

```
https://IP-PROXMOX:8006
```

Après authentification avec les identifiants fournis, les actions réalisées dans le cadre du projet concernent la creation des machines virtuelles, la configuration des interfaces réseau virtuelles et l association des bridges aux VM.

3.3 Perimetre de responsabilite

- L hyperviseur Proxmox etait déjà installe par l etablissement.
- Le serveur physique n a pas ete installe dans le cadre de ce projet.
- Le travail réalisé concerne l exploitation de l environnement et la construction de l architecture réseau virtualisee.
- Les ressources etaient limitees a un pool etudiant et a un nombre restreint de machines virtuelles.

4. Conception de l architecture réseau

4.1 Principe general

L architecture repose sur un firewall pfSense connecte a plusieurs réseaux virtuels. pfSense sert de point central pour le routage, le filtrage et l acces Internet. Chaque zone réseau dispose d une interface dédiée sur le firewall.

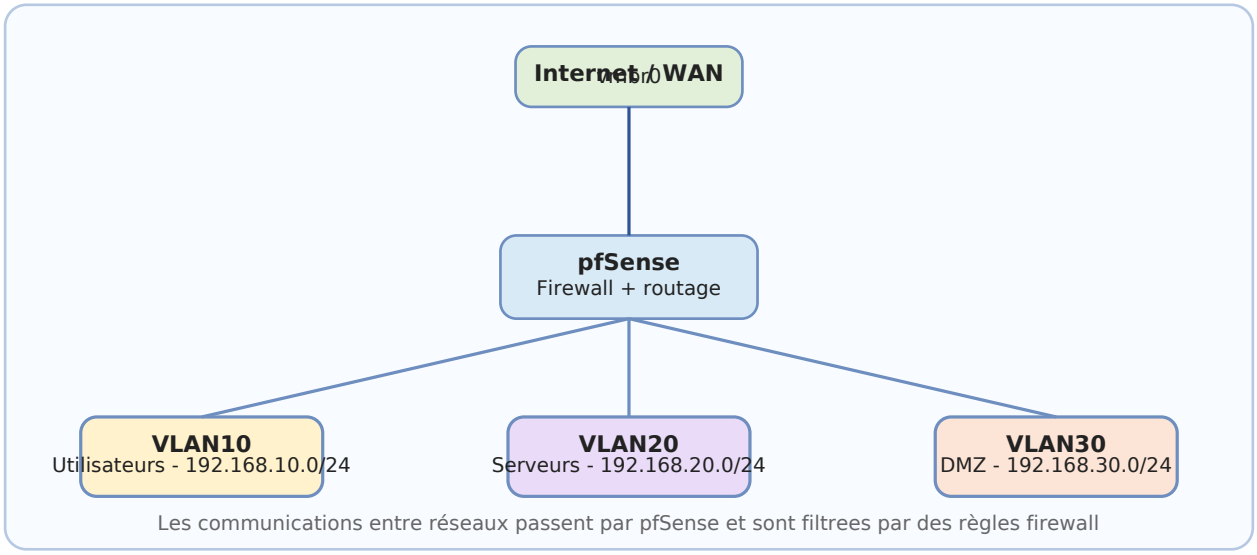

Figure 1 - Schema logique simplifie de l architecture réseau virtualisee

4.2 Zones réseau definies

Zone	Role	Objectif
VLAN10 - Utilisateurs	Postes clients	Accès aux services internes autorises et acces Internet
VLAN20 - Serveurs	Serveurs internes	Hebergement des services critiques du second projet
VLAN30 - DMZ	Services exposes ou isolés	Limiter les risques en cas de compromission d un service

4.3 Interet de la DMZ

La DMZ est une zone separee du réseau interne. Elle permet d isoler les services qui peuvent etre plus exposes que les serveurs internes. Si un service place en DMZ est compromis, les règles firewall limitent les possibilites de rebond vers les autres réseaux.

5. Plan d adressage IP

Le plan d adressage a ete construit afin que chaque réseau dispose d une plage IP lisible et separee. Les adresses de passerelle correspondent aux interfaces pfSense.

VLAN	Usage	Réseau	Passerelle pfSense
VLAN10	Utilisateurs	192.168.10.0/24	192.168.10.1
VLAN20	Serveurs	192.168.20.0/24	192.168.20.1
VLAN30	DMZ	192.168.30.0/24	192.168.30.1

L attribution dynamique des adresses IP n est pas configuree sur pfSense. Elle est prevue sur le serveur Active Directory du second projet afin de centraliser la gestion réseau des postes du domaine.

6. Création de l architecture réseau virtuelle sous Proxmox

6.1 Fonctionnement des bridges Proxmox

Dans Proxmox, un bridge Linux fonctionne comme un switch virtuel. Une machine virtuelle connectee a un bridge peut communiquer avec les autres machines connectees au meme bridge. Cette logique permet de reproduire plusieurs réseaux independants sans switch physique dédié.

6.2 Bridges utilises

Bridge	Usage	Description
vmbr0	WAN	Réseau de sortie vers l extérieur / acces Internet
vmbr1	VLAN10 Utilisateurs	Segment virtuel des postes clients
vmbr2	VLAN20 Serveurs	Segment virtuel des serveurs internes
vmbr3	VLAN30 DMZ	Segment virtuel isole pour la DMZ

6.3 Création d un bridge interne

Pour chaque segment interne, un bridge a ete cree depuis le menu System > Network du noeud Proxmox. Les bridges internes ne disposent pas d adresse IP de gestion, car leur role est uniquement de transporter le trafic des machines virtuelles.

- Acceder au noeud Proxmox.
- Ouvrir System > Network.
- Cliquer sur Create > Linux Bridge.
- Renseigner le nom du bridge, par exemple vmbr1.
- Ne pas renseigner de port physique pour un bridge purement interne.
- Ne pas configurer d adresse IPv4 sur le bridge interne.
- Appliquer la configuration réseau.

6.4 Justification technique

Le choix de bridges séparés permet de materialiser les differents réseaux. pfSense possede une interface dans chaque bridge, ce qui lui permet de jouer le role de passerelle pour chaque zone. Sans pfSense, les bridges internes restent isolés les uns des autres.

7. Déploiement de la machine virtuelle pfSense

7.1 Role de pfSense

pfSense est le composant central de l infrastructure réseau. Il assure a la fois les fonctions de firewall, de routeur, de passerelle et de NAT. Toutes les communications entre les réseaux transitent par lui.

7.2 Création de la VM

- Depuis Proxmox, cliquer sur Create VM.
- Nommer la machine virtuelle pfSense.

- Sélectionner l image ISO de pfSense.
- Configurer les ressources matérielles.
- Ajouter les interfaces réseau virtuelles nécessaires.
- Demarrer la machine virtuelle puis lancer l installation.

7.3 Configuration matérielle

Ressource	Valeur retenue	Justification
CPU	2 vCPU	Suffisant pour un firewall de lab
RAM	4 Go	Permet un fonctionnement confortable de pfSense
Stockage	20 Go	Espace suffisant pour le système et les journaux
BIOS	OVMF	Démarrage UEFI moderne
Machine	q35	Compatibilite avec les peripheriques virtuels modernes

7.4 Interfaces réseau ajoutees

Interface VM	Bridge Proxmox	Usage
Net0	vmbr0	WAN
Net1	vmbr1	VLAN10 - Utilisateurs
Net2	vmbr2	VLAN20 - Serveurs
Net3	vmbr3	VLAN30 - DMZ

7.5 Installation de pfSense

- Démarrage de la VM sur l ISO pfSense.
- Choix de l option Install pfSense.
- Validation du partitionnement propose.
- Installation du système.
- Redémarrage de la machine virtuelle.
- Retrait de l ISO apres installation.

8. Configuration des interfaces réseau pfSense

8.1 Attribution des interfaces

Après installation, pfSense detecte les cartes réseau virtuelles. Les interfaces ont ensuite ete associees aux roles WAN, LAN et OPT.

Interface pfSense	Carte virtuelle	Role
WAN	Net0	Accès extérieur / Internet
LAN	Net1	Réseau utilisateurs
OPT1	Net2	Réseau serveurs
OPT2	Net3	DMZ

8.2 Configuration WAN

L interface WAN est configuree afin de permettre a pfSense de sortir vers l extérieur. Dans ce projet, le WAN est configure en DHCP car l adresse de sortie est fournie par l environnement réseau disponible.

- Aller dans Interfaces > WAN.
- Activer l interface.
- Sélectionner le mode DHCP.
- Sauvegarder puis appliquer la configuration.

8.3 Configuration des interfaces internes

Chaque interface interne dispose d une adresse IP fixe. Cette adresse sert de passerelle pour le réseau correspondant.

Interface	Adresse IP	Masque	Role
LAN	192.168.10.1	/24	Passerelle VLAN10
OPT1	192.168.20.1	/24	Passerelle VLAN20
OPT2	192.168.30.1	/24	Passerelle VLAN30

8.4 Gestion du DHCP

Aucun serveur DHCP n a ete active sur pfSense. Ce choix evite de melanger les roles entre les deux projets. Dans l architecture globale, le service DHCP est gere par le serveur Active Directory du second projet. pfSense reste donc dédié aux fonctions réseau : routage, filtrage, NAT et passerelles.

9. Mise en place du routage inter-VLAN

9.1 Principe

Les réseaux etant séparés, les machines d un VLAN ne peuvent pas communiquer directement avec celles d un autre VLAN. Le routage inter-VLAN consiste a faire passer ces communications par un equipement de couche 3, ici pfSense.

9.2 Role de pfSense dans le routage

pfSense possede une interface dans chaque réseau. Il connait donc directement les réseaux 192.168.10.0/24, 192.168.20.0/24 et 192.168.30.0/24. Les machines utilisent l adresse IP pfSense de leur réseau comme passerelle.

- VLAN10 utilise 192.168.10.1 comme passerelle.
- VLAN20 utilise 192.168.20.1 comme passerelle.
- VLAN30 utilise 192.168.30.1 comme passerelle.
- Les communications entre VLAN sont ensuite autorisees ou bloquees par les règles firewall.

10. Configuration du NAT

10.1 Objectif

Le NAT permet aux réseaux internes d acceder a Internet via l adresse WAN de pfSense. Les adresses privees internes ne sont pas routables directement sur Internet, elles doivent donc etre traduites par le firewall.

10.2 Configuration réalisée

- Acceder au menu Firewall > NAT.
- Ouvrir l onglet Outbound.
- Sélectionner le mode Automatic Outbound NAT.
- Sauvegarder et appliquer la configuration.
- Vérifier la connectivité Internet depuis les réseaux internes.

Le mode automatique est adapte dans ce contexte car il permet a pfSense de générer les règles NAT nécessaires pour les réseaux internes connus.

11. Mise en place des règles de sécurité firewall

11.1 Objectif des règles

Les règles firewall permettent de contrôler precisement les communications. L objectif n est pas seulement de permettre le trafic, mais aussi de bloquer les flux inutiles ou dangereux.

11.2 Principe applique

La configuration suit le principe du moindre privilege : seules les communications nécessaires sont autorisees. Les autres flux sont bloques par defaut ou par des règles explicites.

11.3 Exemples de règles

Zone	Action	Source	Destination	Objectif
VLAN10	Pass	VLAN10 net	any	Autoriser l acces Internet des utilisateurs
VLAN30	Block	VLAN30 net	VLAN10 net	Empêcher la DMZ d acceder aux postes utilisateurs
VLAN30	Block	VLAN30 net	VLAN20 net	Limiter les rebonds vers les serveurs internes
VLAN20	Pass limite	VLAN20 net	Services nécessaires	Autoriser uniquement les flux utiles

11.4 Isolation de la DMZ

La DMZ est volontairement plus limitee que les autres réseaux. Elle peut recevoir des services exposes, mais ne doit pas pouvoir acceder librement aux réseaux utilisateurs ou serveurs. Cette isolation reduit les risques en cas de compromission d une machine situee en DMZ.

11.5 Application et ordre des règles

Dans pfSense, les règles sont lues de haut en bas. L ordre des règles est donc important : une regle trop permissive placee avant une regle de blocage pourrait autoriser un trafic non souhaite. Après chaque modification, les règles sont sauvegardees puis appliquees.

12. Tests et validation de l infrastructure

12.1 Vérification des interfaces

Une fois la configuration terminee, les interfaces pfSense ont ete contrôlees afin de verifier leur etat, leur adresse IP et leur association au bon réseau.

12.2 Tests de connectivité

Les tests suivants permettent de valider la connectivité locale, le routage et l acces Internet.

```
ping 192.168.10.1
ping 192.168.20.1
ping 192.168.30.1
ping 8.8.8.8
tracert google.com
```

12.3 Tests inter-VLAN

- Depuis un poste utilisateur, test vers la passerelle du VLAN utilisateurs.
- Depuis un poste utilisateur, test vers la passerelle du VLAN serveurs.
- Depuis la DMZ, test vers le réseau utilisateurs pour confirmer le blocage.
- Vérification que les flux autorises fonctionnent et que les flux interdits sont bloques.

12.4 Vérification des journaux pfSense

Les logs firewall de pfSense permettent de confirmer le passage ou le blocage de certains paquets. Ils sont utiles pour diagnostiquer une regle mal placee, une passerelle incorrecte ou un probleme de communication inter-VLAN.

13. Difficultés rencontrées

13.1 Difficultes principales

- Comprendre le role exact des bridges Proxmox.
- Differencier un bridge virtuel d une interface pfSense.
- Comprendre que le routage inter-VLAN ne fonctionne que via pfSense.
- Mettre en place des règles firewall dans le bon ordre.
- Vérifier les flux autorises et les flux bloques.

13.2 Methodes de resolution

- Vérification des interfaces et des adresses IP.
- Tests de ping entre les passerelles.
- Analyse des logs firewall pfSense.
- Correction progressive des règles firewall.
- Validation par tests apres chaque modification.

Ces difficultes ont permis de mieux comprendre le fonctionnement d une infrastructure segmentee et l importance d une méthode de diagnostic réseau progressive.

14. Conclusion

Ce projet a permis de mettre en place une infrastructure réseau virtualisee sécurisée integrant une segmentation par réseaux, un firewall centralise, du NAT, une DMZ et du routage inter-VLAN.

L architecture obtenue permet un meilleur contrôle des flux, une separation claire des roles réseau et une base solide pour accueillir les services systèmes du second projet, notamment l Active Directory, le DNS, le DHCP, GLPI et la supervision.

Le choix de ne pas activer le DHCP sur pfSense permet de conserver une architecture coherente : pfSense assure la partie réseau et sécurité, tandis que le serveur Active Directory du second projet assure la gestion des services d annuaire et d adressage automatique.