MANOLIOS Benjamin *EPSI Montpellier*

N° candidat : 02443855566

Épreuve E6

Situation N°1

Mise en place d'un pare-feu pfSense pour sécuriser le réseau d'entreprise

Sommaires :

Contexte

Je suis actuellement employer à la **Maison des Ligues de Lorraine (M2L)**, un établissement dépendant du **Conseil Régional de Lorraine**. Elle a pour mission de soutenir les **ligues sportives régionales** en leur fournissant des services logistiques, administratifs et techniques. La M2L héberge plusieurs structures dans différents bâtiments, proposant des bureaux équipés, des salles mutualisées (réunion, formation, amphithéâtre) et un accès à un réseau informatique commun.

Le réseau de la M2L dessert un grand nombre d'utilisateurs répartis dans plusieurs bâtiments. Certains sont récents et équipés en **gigabit Ethernet**, d'autres plus anciens, avec des équipements hétérogènes. Le réseau actuel manque de centralisation et de sécurité : la distribution d'adresses IP, le filtrage, et la segmentation ne sont pas uniformisés.

Pour moderniser son infrastructure et renforcer la sécurité, la M2L souhaite mettre en place un **routeur virtuel basé sur pfSense**, capable de gérer :

Le **routage** et la **distribution IP (DHCP)**,

Le **filtrage réseau (pare-feu)**,

La **gestion des VLANs** pour segmenter les flux,

La solution est déployée sur une **infrastructure virtualisée avec Proxmox VE** à l'aide d'un serveur **ASUS PRO Q570M**, intégrant pfSense et plusieurs machines clientes (Windows/Linux). Ce projet permet à la M2L de mieux sécuriser ses services et me permet de mettre en œuvre des compétences clés du **BTS SIO SISR**, notamment en administration réseau, virtualisation et sécurité.

CLIENT :

Maison des Ligues de Lorraine (M2L)

Description :

La Maison des Ligues de Lorraine (M2L) est un établissement public placé sous la responsabilité du Conseil Régional de Lorraine. Elle a pour mission de soutenir les différentes **ligues sportives régionales** en leur fournissant des locaux, des services logistiques, des équipements informatiques, ainsi qu'un accès à une infrastructure réseau partagée.

Avec l'augmentation du nombre de structures hébergées, la M2L doit renforcer la sécurité et la gestion de son réseau interne. C'est dans ce cadre que le projet de mise en place d'un **routeur virtuel pfSense** a été initié. L'objectif est d'assurer une **distribution efficace des services réseau**, tout en garantissant une **bonne séparation des flux** (LAN / DMZ / VLAN), et une **protection renforcée via un pare-feu**.

Redondance et sécurité du réseau avec pfSense

Problème :

Le réseau actuel, bien que fonctionnel, ne dispose pas de règles de sécurité avancées, ni d'un système centralisé pour gérer les accès, le routage et la distribution IP. Cela limite les possibilités de segmentation du réseau et expose l'infrastructure à des risques de mauvaise configuration ou d'attaques.

Solution :

Déployer un **pare-feu pfSense** virtualisé dans **Proxmox VE**, et le configurer comme **routeur principal**.
Les fonctionnalités mises en place incluent :

La **gestion des interfaces LAN et DMZ**,

Le **filtrage du trafic entrant et sortant** à l'aide de règles précises,

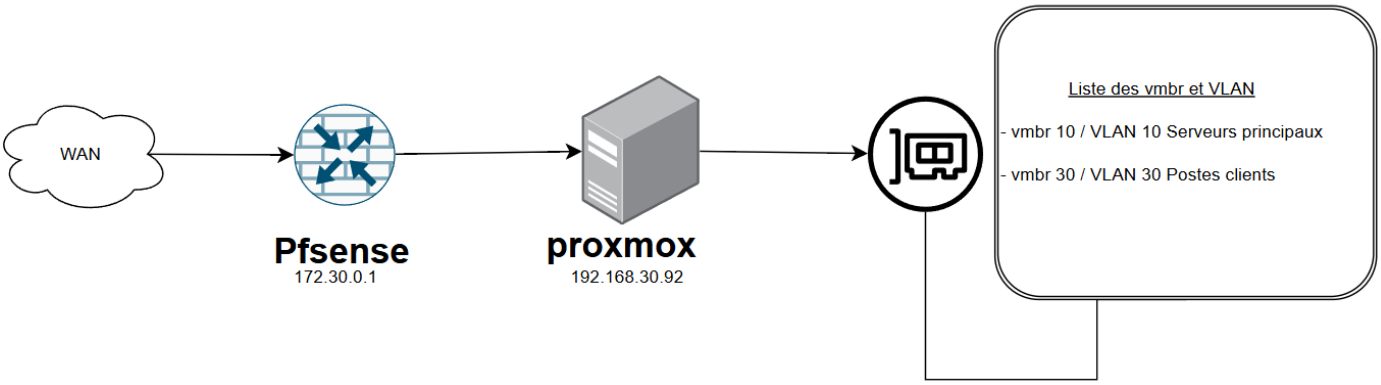
La **distribution des adresses IP** via DHCP,

L'**accès restreint aux bases de données** depuis la DMZ,

Une éventuelle configuration de **VLAN** pour isoler les services selon les besoins.

Cette solution améliore significativement la **sécurité, la gestion et la stabilité** de l'infrastructure réseau de la M2L.

Réseaux avant modification :



On y retrouve :

Un pare-feu pfSense
→ Connecté à Internet (WAN)
→ Adresse IP : 172.30.0.1
→ Gère le routage, le DHCP et la sécurité du réseau

Un serveur Proxmox
→ Adresse IP : 192.168.30.92
→ Contient les machines virtuelles

Deux VLANs configurés :
- VLAN 10 : Serveurs principaux
- VLAN 30 : Postes clients

Malgré la présence de pfSense et de VLANs identifiés, aucune véritable segmentation réseau ni règles de sécurité spécifiques n'étaient mises en place, ce qui justifie la nécessité d'une refonte complète de l'architecture.

Solution :

Mise en place de pfSense pour sécuriser et structurer le réseau

Problème :

Le réseau de la M2L n'était pas segmenté et fonctionnait sans règles de sécurité avancées. Tous les équipements étaient connectés au même réseau, ce qui représentait un risque pour la sécurité. De plus, il n'existait aucun moyen de contrôler précisément les communications internes entre les postes, les serveurs et les services réseau.

Solution :

Pour répondre à ces besoins, j'ai mis en place pfSense, un pare-feu open source, en tant que routeur principal de l'infrastructure. Il a été installé sur une machine virtuelle via Proxmox. J'ai ensuite créé deux VLANs : un pour les serveurs (VLAN 10) et un pour les postes clients (VLAN 30). PfSense a été configuré pour gérer le routage entre ces VLANs, attribuer les adresses IP grâce au serveur DHCP intégré, et filtrer le trafic à l'aide de règles personnalisées. Cette configuration permet désormais de mieux organiser les flux réseau tout en renforçant la sécurité.

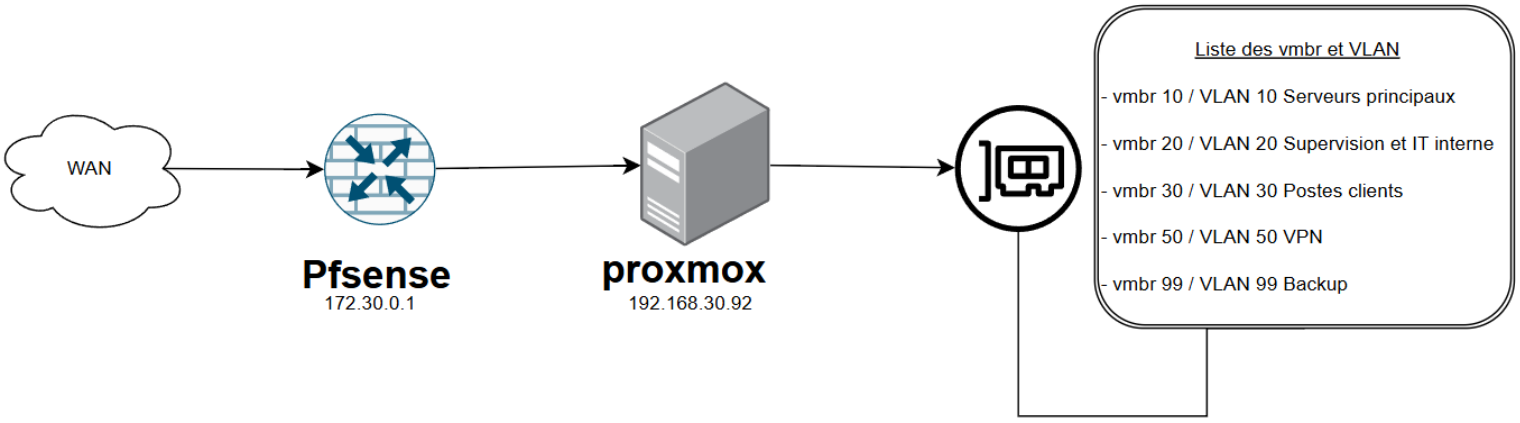
Avantages :

Cette solution permet d'améliorer considérablement la sécurité grâce à la séparation des machines par VLAN. Elle offre aussi une meilleure maîtrise du réseau, car les règles de filtrage peuvent être adaptées aux besoins de chaque zone. En plus d'être fiable, pfSense est une solution gratuite, ce qui en fait un choix économique pour l'organisation. L'administration du réseau est également facilitée grâce à une interface web claire et centralisée.

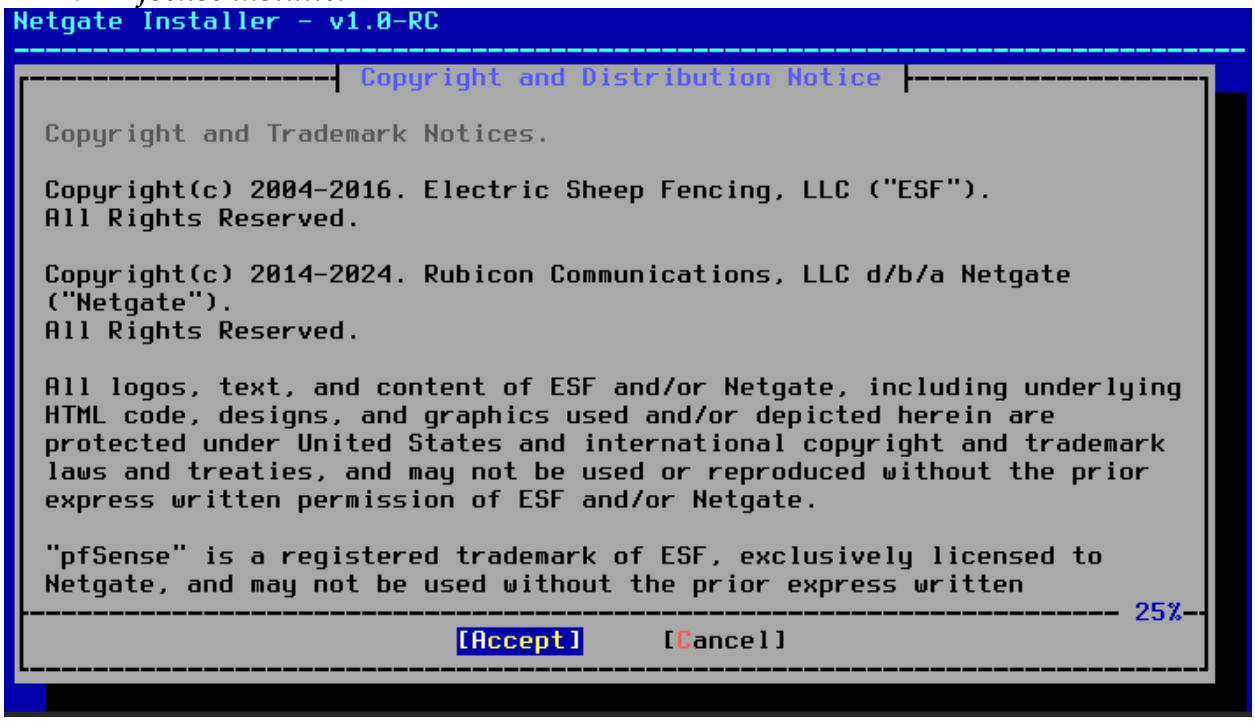
Inconvénients :

La configuration initiale de pfSense demande du temps et des connaissances techniques. Il faut définir manuellement les interfaces, les VLANs, les règles de pare-feu, et s'assurer que tout fonctionne correctement. Une erreur de configuration peut impacter la connectivité. Toutefois, une fois correctement mis en place, pfSense reste stable, puissant et adapté aux besoins de la M2L.

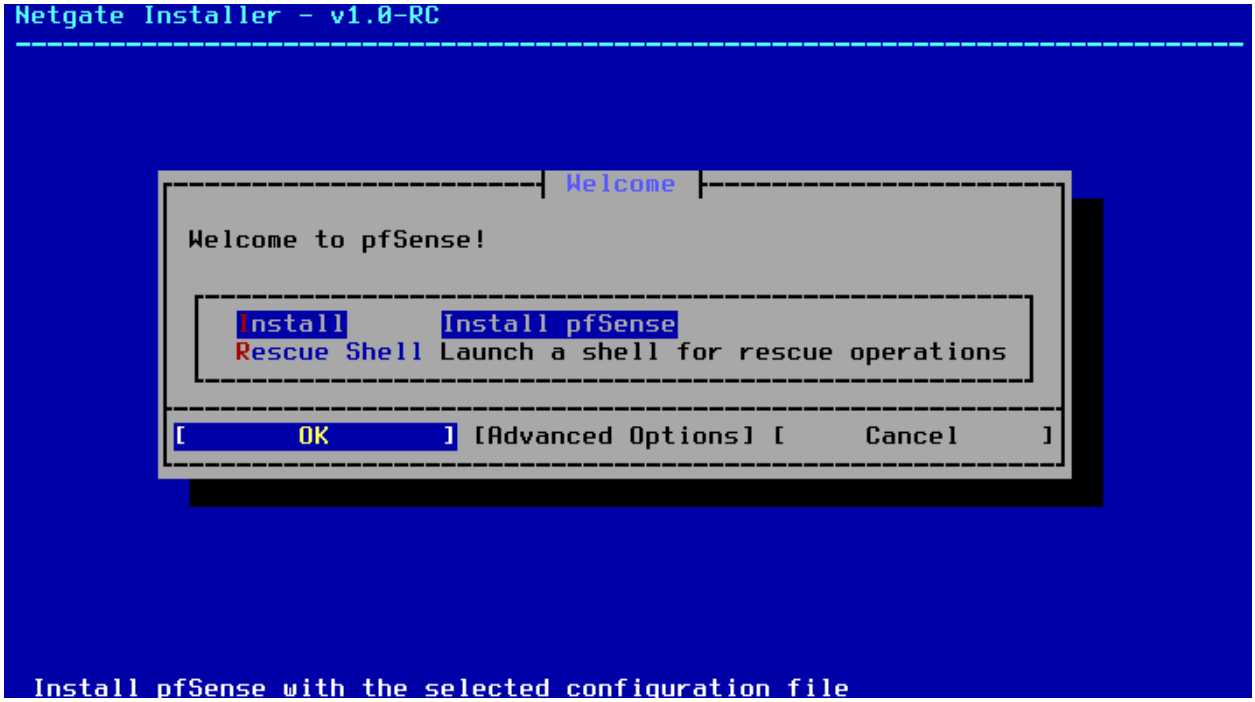
Réseaux après modification :

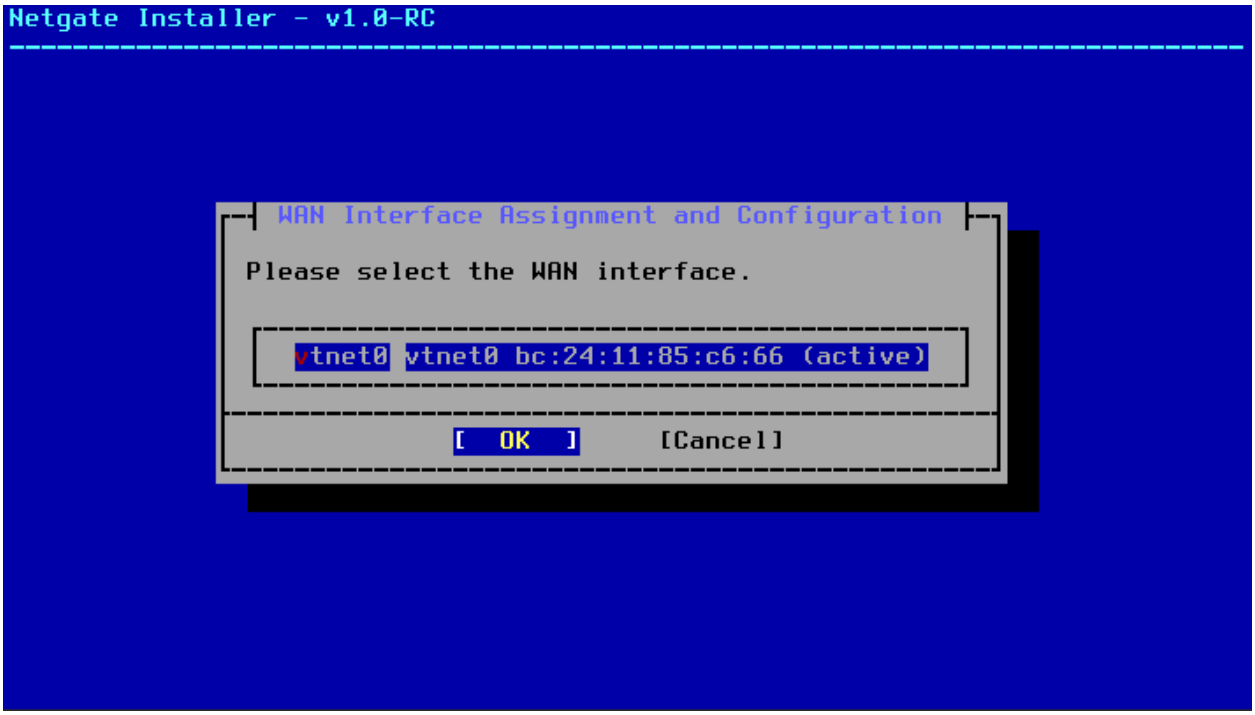


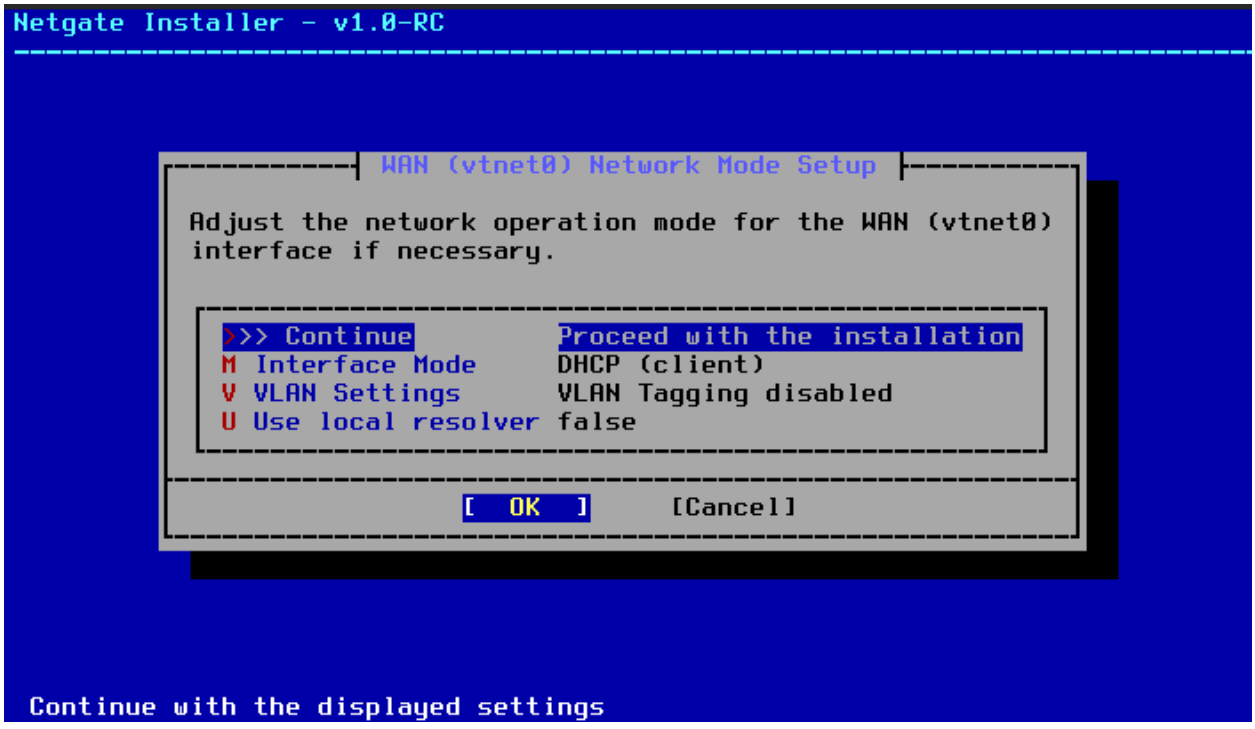
a- *Pfsense installer*

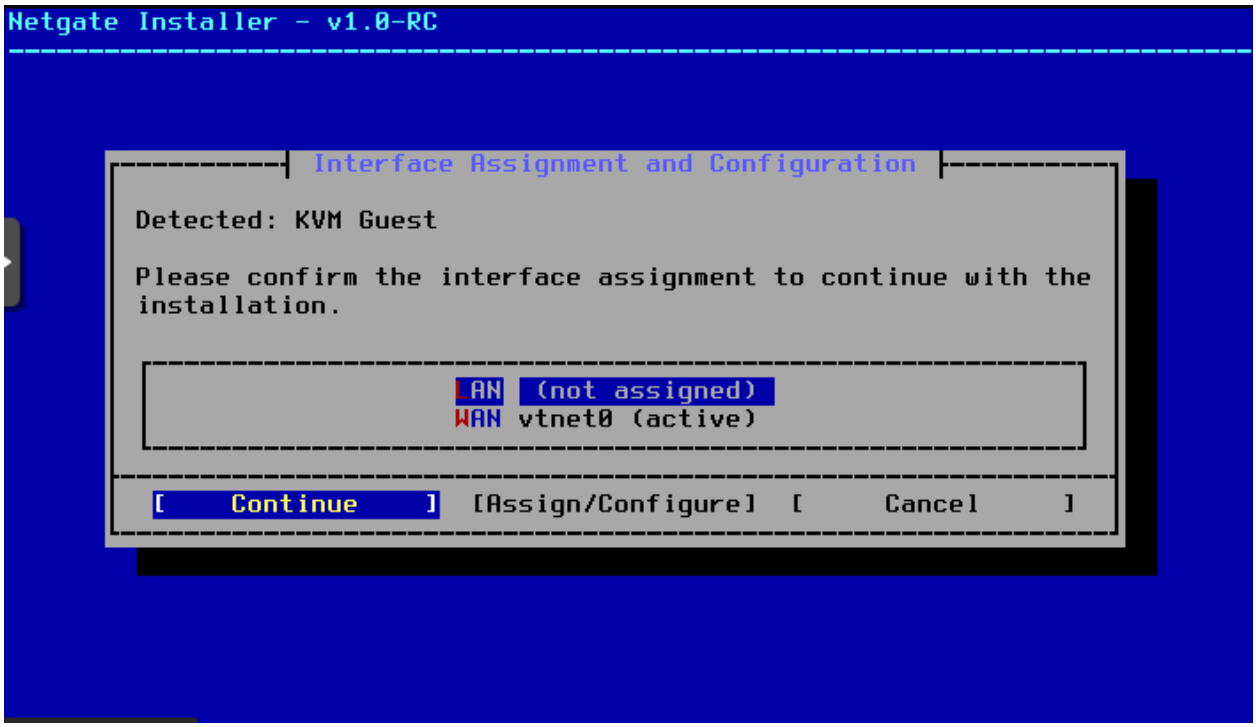


Sur l'écran de démarrage de l'installateur pfSense, il suffit d'appuyer sur Entrée pour accepter les conditions et poursuivre l'installation

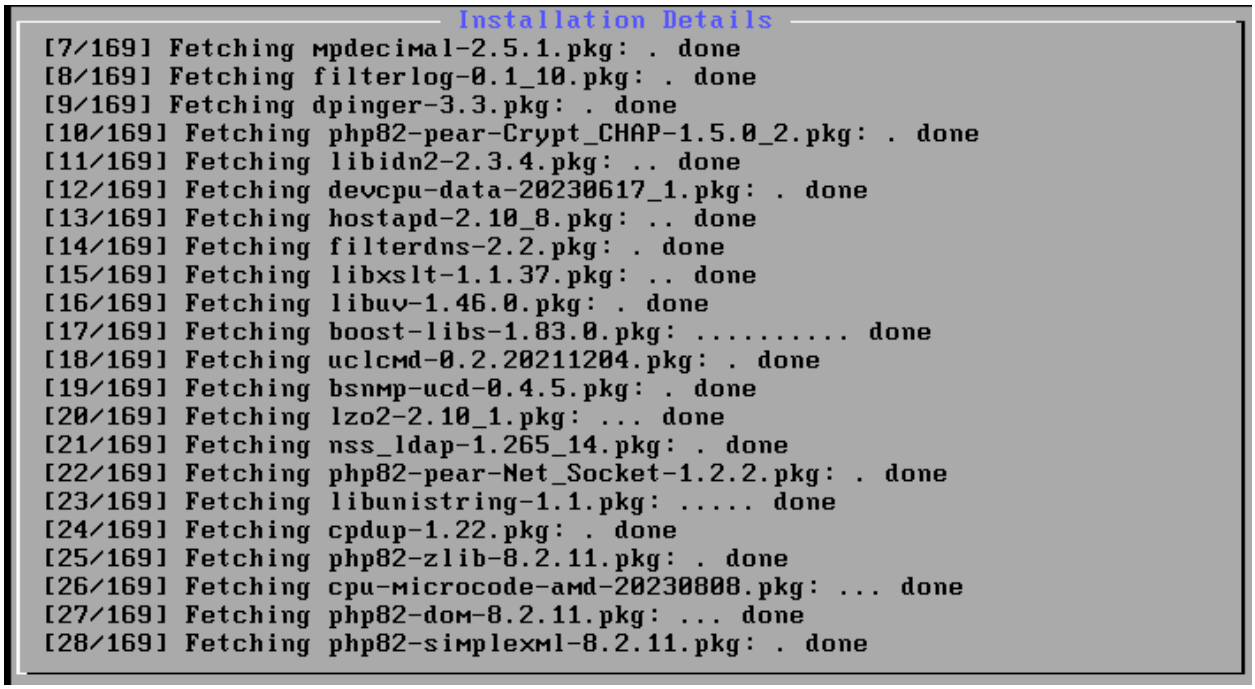

Netgate Installer - v1.0-RC
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
[OK]
[Advanced Options]
[Cancel]
Install pfSense with the selected configuration file


Netgate Installer - v1.0-RC
WAN Interface Assignment and Configuration
Please select the WAN interface.
vtnet0 vtnet0 bc:24:11:85:c6:66 (active)
[OK]
[Cancel]

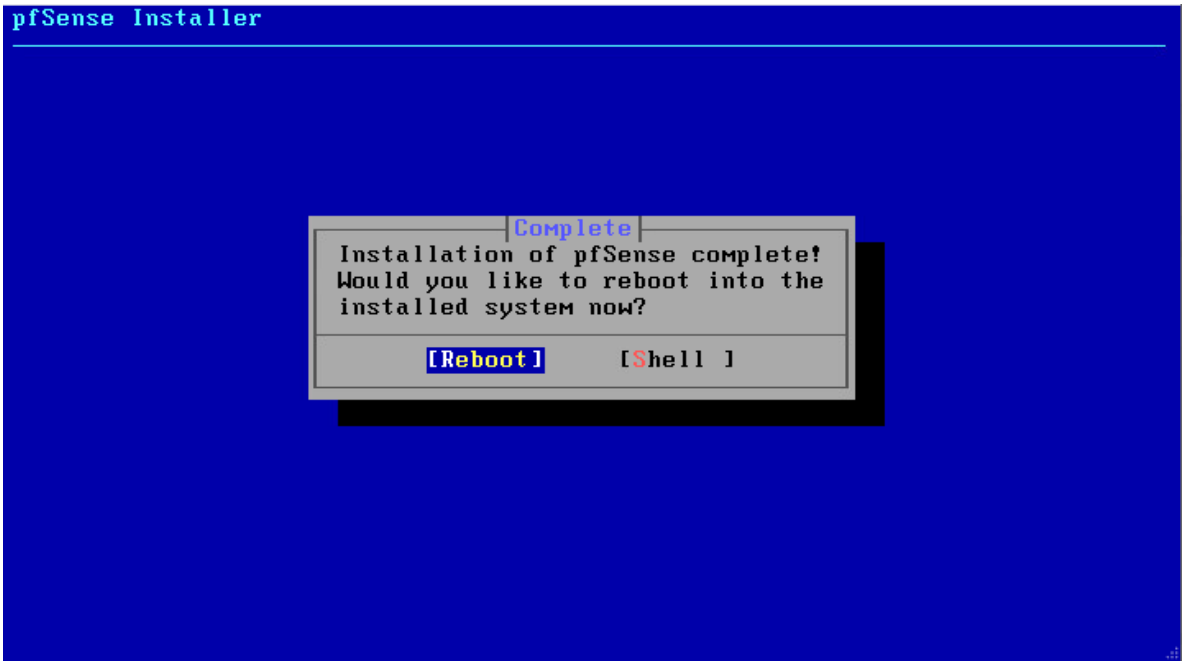

Netgate Installer - v1.0-RC
WAN (vtnet0) Network Mode Setup
Adjust the network operation mode for the WAN (vtnet0) interface if necessary.
>>> Continue Proceed with the installation
M Interface Mode DHCP (client)
V VLAN Settings VLAN Tagging disabled
U Use local resolver false
[OK]
[Cancel]
Continue with the displayed settings



Sur chacune des quatre étapes affichées, il suffit d'appuyer sur la touche Entrée pour poursuivre l'installation de pfSense



L’installation sur le disque s’effectue, notre Pfsense sera bientôt installé sur la machine virtuelle.



Il ne reste plus qu'à redémarrer la machine en appuyant sur Entrée. Celle-ci démarrera alors sur pfSense fraîchement installé.

Interface console de pfSense

Une fois pfSense démarré, un menu d'administration en ligne de commande s'affiche. Ce menu permet de réaliser différentes actions de configuration de base, utiles notamment en cas de problème d'accès à l'interface web.

Voici les options principales :

- 1) Assign Interfaces : Modifier les interfaces WAN et LAN
- 2) Set interface(s) IP address : Configurer une adresse IP manuellement
- 3) Reset webConfigurator password : Réinitialiser le mot de passe admin
- 5) Reboot system : Redémarrer pfSense
- 8) Shell : Accéder au terminal FreeBSD en ligne de commande

Ce menu peut être consulté directement depuis la VM (Proxmox) ou physiquement si pfSense est installé sur une machine dédiée.

-VLAN 10 Serveurs principaux

-VLAN 20 Supervision et IT interne

-VLAN 30 Postes clients

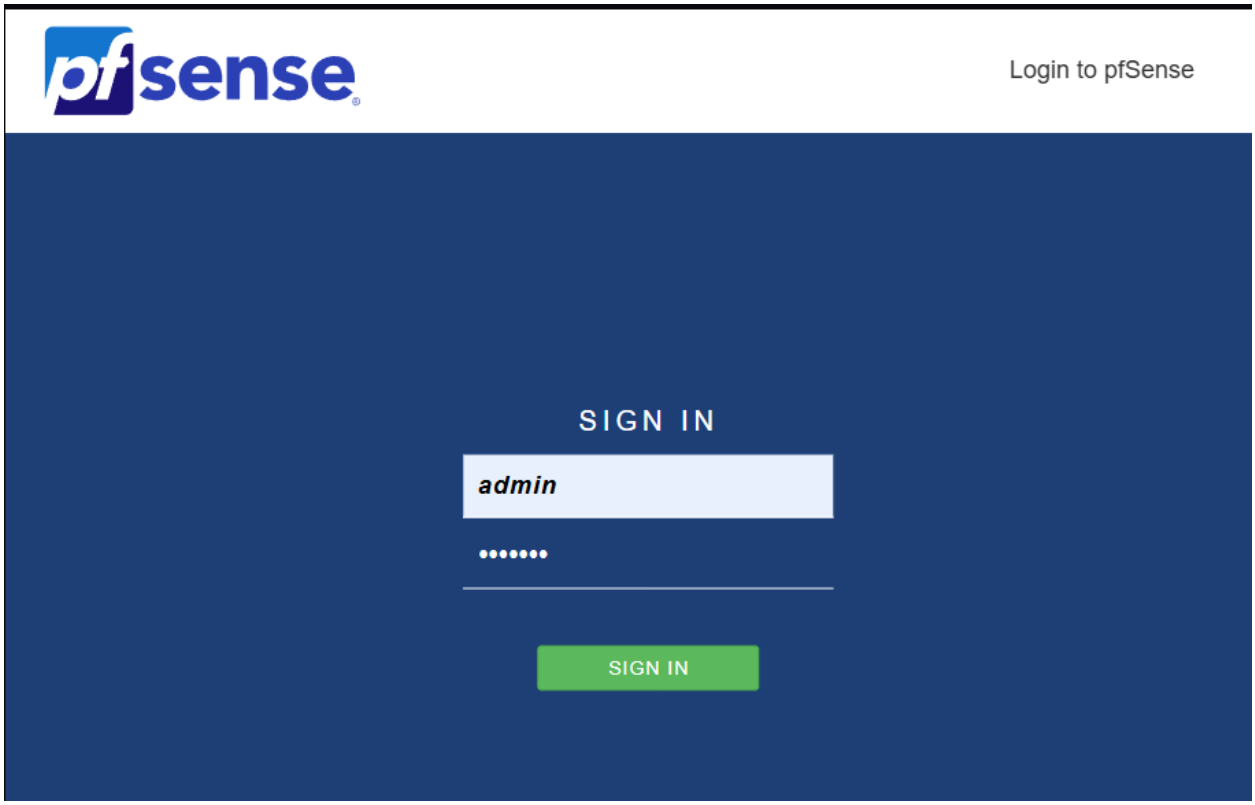
-VLAN 50 VPN

-VLAN 99 Backup

II.Configuration de pfSense

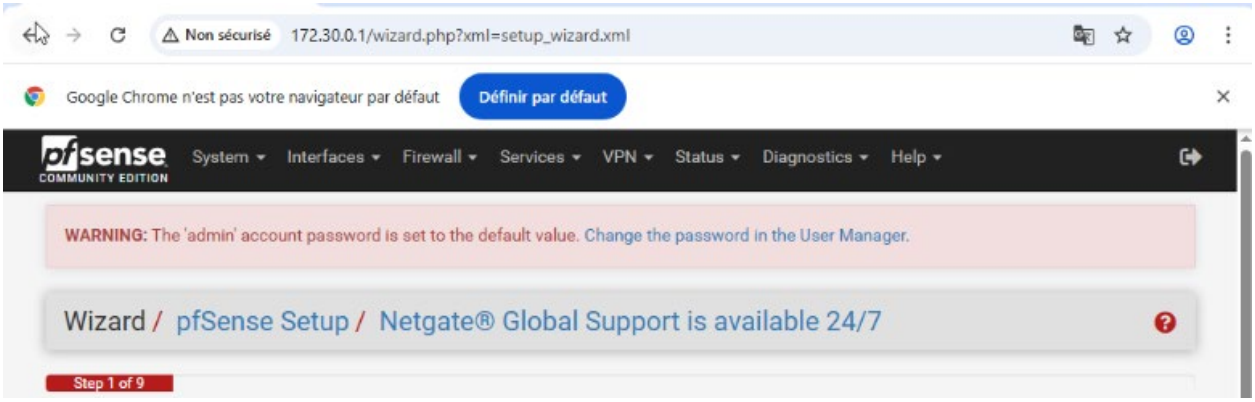
Configuration web

a- *Connexion à l'interface web :*

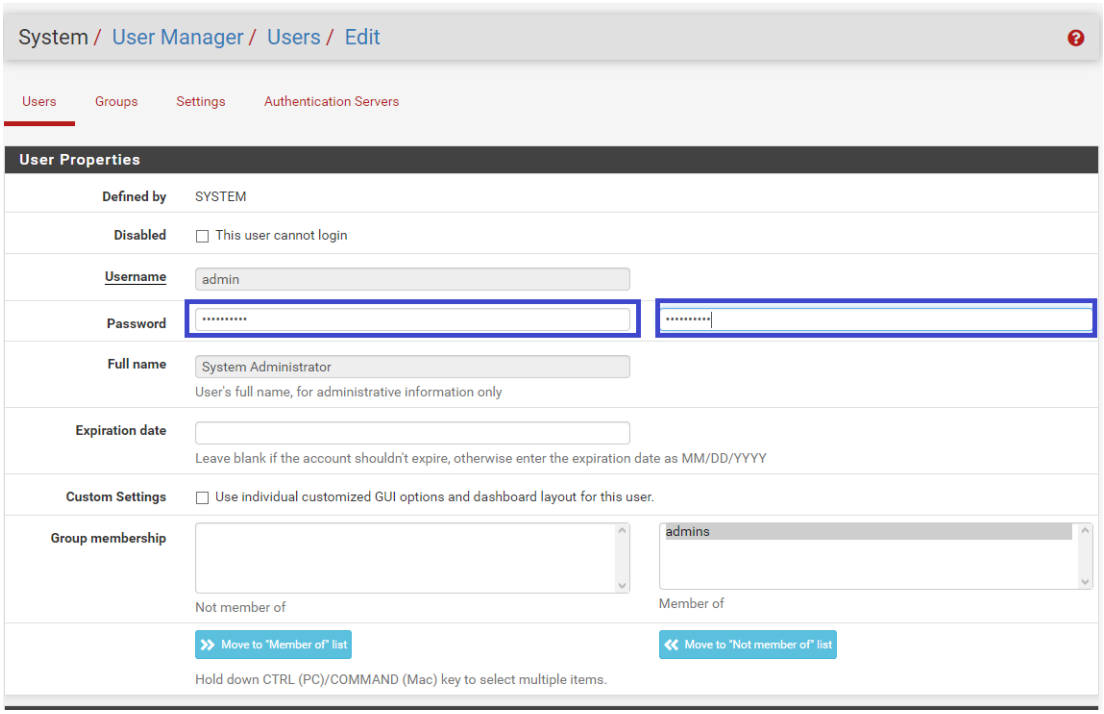


Pour cela, nous nous connectons à l'interface web de pfSense via l'adresse https://172.30.0.1, en utilisant l'identifiant admin et le mot de passe Pfsense.

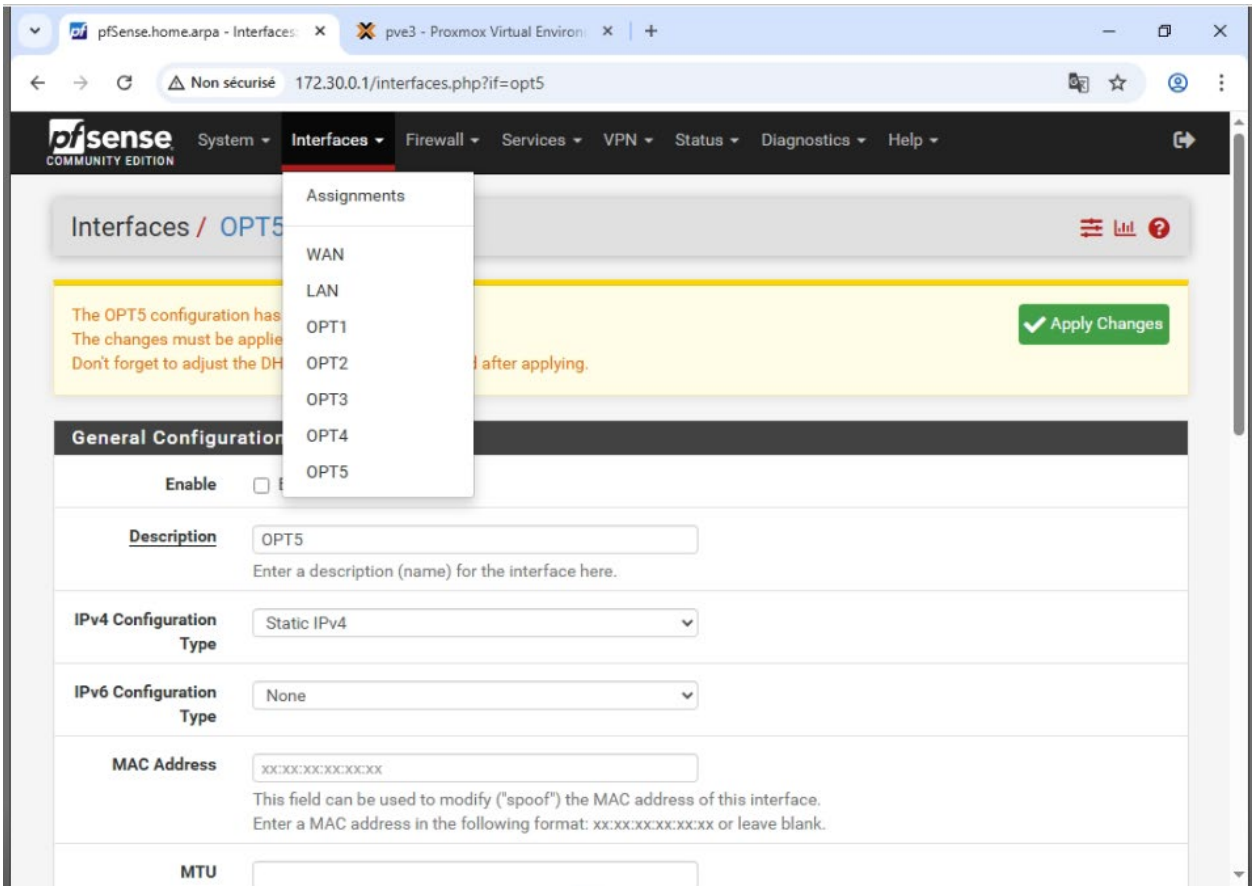
b- *Changement mot de passe :*



Une fois connecté, nous accédons à la section "User Manager" afin de modifier le mot de passe administrateur via l'option "Change the password".



Nous remplaçons ensuite le mot de passe administrateur par un mot de passe sécurisé, puis nous validons la modification en cliquant sur le bouton "Save" en bas de la page.


pfSense.home.arpa - Interfaces
pve3 - Proxmox Virtual Environ
Non sécurisé
172.30.0.1/interfaces.php?if=opt5
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
OPT1
OPT2
OPT3
OPT4
OPT5
Interfaces / OPT5
The OPT5 configuration has
The changes must be applie
Don't forget to adjust the DH
after applying.
Apply Changes
General Configuration
Enable
Description
OPT5
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU

Conclusion _

Ce projet de mise en place d'un pare-feu pfSense au sein de la Maison des Ligues de Lorraine (M2L) s'est inscrit dans une démarche de **renforcement de la sécurité réseau** et de **modernisation de l'infrastructure informatique**. Avant cette réalisation, le réseau de la M2L souffrait d'un manque de segmentation, d'un routage centralisé insuffisant, ainsi que d'une absence de règles de sécurité précises, ce qui exposait l'infrastructure à des risques importants.

En installant et configurant pfSense sur un environnement virtualisé via **Proxmox VE**, j'ai pu proposer une solution fiable, évolutive et économique, qui répond aux besoins de l'organisation. Cette solution a permis :

La **création de VLANs** pour segmenter les flux réseau selon les usages (serveurs, postes clients, etc.) ;

L'**attribution dynamique des adresses IP** grâce à un serveur DHCP interne ;

La mise en place de **règles de filtrage précises** pour contrôler les accès entre les différentes zones ;

La séparation entre les zones sensibles comme la **DMZ** et le **réseau interne**, garantissant une meilleure protection des données.

Cette infrastructure offre à la M2L une meilleure visibilité sur le trafic, une plus grande flexibilité en cas d'ajout de nouvelles machines ou services, et un **niveau de sécurité renforcé**, tout en restant accessible grâce à l'interface web intuitive de pfSense.

Sur le plan personnel, ce projet m'a permis de **mobiliser plusieurs compétences clés** du référentiel BTS SIO option SISR :

L'installation et la gestion de machines virtuelles (hyperviseur Proxmox)

La configuration d'un pare-feu open source avancé (pfSense)

La gestion des VLANs et des plans d'adressage IP

La mise en œuvre de règles de sécurité réseau adaptées aux besoins métiers

Au-delà des compétences techniques, ce projet m'a également permis de développer ma **rigueur**, mon **autonomie**, et ma **capacité d'analyse**, des qualités essentielles dans les métiers de l'administration système et réseau.

En conclusion, cette réalisation constitue une **expérience professionnelle enrichissante**, concrète et représentative des missions qu'un technicien SISR peut être amené à gérer. Elle m'a permis de contribuer à la sécurité d'une véritable organisation tout en renforçant mes compétences techniques et méthodologiques dans un contexte professionnel.

ANNEXE BTS :

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation** : 01
Nom, prénom : MANOLIOS Benjamin	**N° candidat** : 02443855566
☑ **Épreuve ponctuelle** ☐ **Contrôle en cours de formation**	**Date** :

Organisation support de la réalisation professionnelle

La Maison des Ligues de la Lorraine, établissement du Conseil Régional de Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées. Elle assure l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région.
M2L souhaite mettre en place un routeur virtuel pour gérer ses réseaux.

Intitulé de la réalisation professionnelle

Installation et configuration d'un routeur pfSens

Période de réalisation : 01/10/2024 - 22/11/24 **Lieu :** EPSI MONTPELLIER

Modalité : ☐ Seul ☑ En équipe

Compétences travaillées

- ☑ Concevoir une solution d'infrastructure réseau
- ☑ Installer, tester et déployer une solution d'infrastructure réseau
- ☑ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation [1] (ressources fournies, résultats attendus)

Ressources fournies :

- Cahier des charges M2L
- Serveur Asus PRO Q570M
- Proxmox VE 8.2
- ISO pfSense
- VM client Linux/Windows

Résultats attendus :

- Gestion des réseaux
- Filtrage par les regles de securite
- Sécurisation du réseaux (pare-feu)

Description des ressources documentaires, matérielles et logicielles utilisées [2]

- Schéma réseau M2L
- Documentation d'installation et configuration de pfSense
- Documentation d'installation et configuration de VM client Linux/Windows
- Documentation d'installation et configuration de Proxmox VE

Modalités d'accès aux productions et à leur documentation

Lien de production : lnsh.xyz/ed11ef
Lien de documentations :

- **pfSense :** lnsh.xyz/0690a7
- **Proxmox** : lnsh.xyz/ddf77c
- **Client** : lnsh.xyz/48f056

1 En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
2 Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.
3 Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.
4 Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.