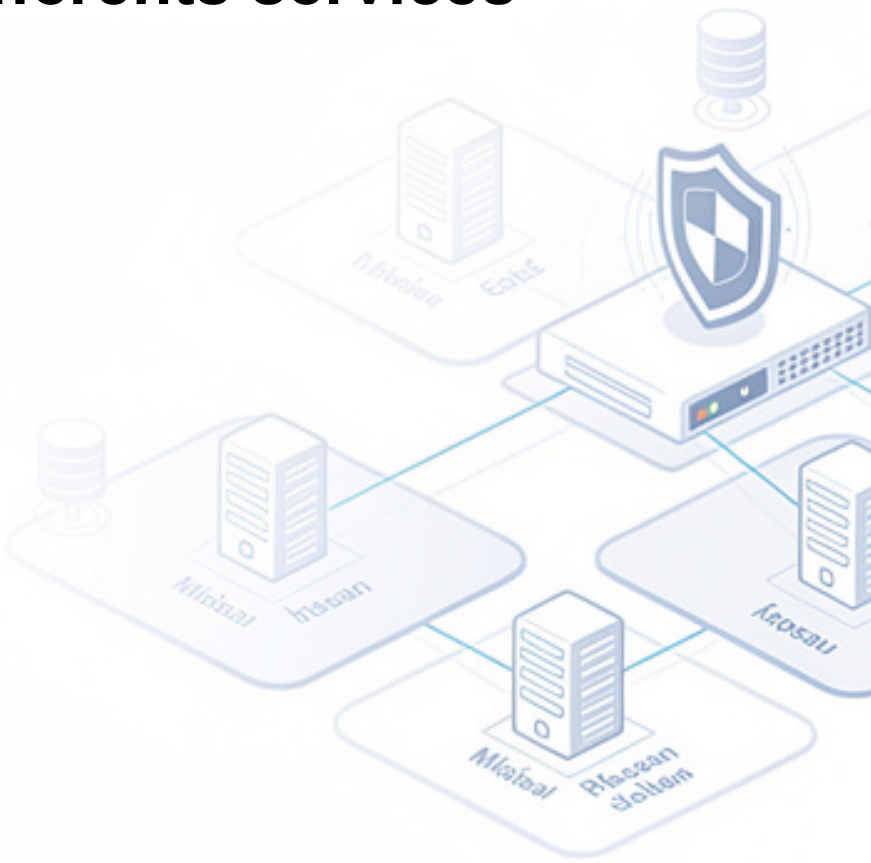
Projet E6 Numéro 1

Mise en place et configuration d'une solution pfSense afin de sécuriser l'accès au réseau de l'entreprise et segmenter les flux entre les différents services



POSTIC Valentin	Promotion 2025 - 2027
BTS SIO SISR	**PICARD SURGELES**

Plan de la situation

1. Cahier des charges

1.1. Expression des besoins

Une PME spécialisée dans le e-commerce utilise actuellement un routeur classique fourni par son opérateur pour gérer son réseau interne et son accès à Internet. Avec l'augmentation de son activité, l'entreprise héberge désormais des données sensibles (clients, paiements) et propose un accès distant à ses employés.

Récemment, plusieurs tentatives d'intrusion et des réductions réseau ont été constatées, mettant en évidence les limites du matériel existant en termes de sécurité et de performance. De plus, la direction souhaite segmenter le réseau (administration, production, invités) afin de mieux contrôler les accès.

Dans ce contexte, le service informatique envisage de remplacer le routeur actuel par une solution plus robuste et configurable comme pfSense, afin d'améliorer la sécurité, la gestion du trafic et la fiabilité globale du système d'information.

1.2. Description de l'existant

Actuellement, le réseau de l'entreprise repose sur un routeur standard fourni par le fournisseur d'accès à Internet, assurant à la fois les fonctions de routage, de NAT et de pare-feu basique.

L'ensemble des postes de travail, serveurs internes et équipements (imprimantes, terminaux mobiles) sont connectés sur un même réseau local, sans segmentation. Les règles de sécurité sont limitées et peu personnalisables, ne permettant

pas un contrôle fin des flux entrants et sortants. L'accès distant des employés se fait via des solutions non sécurisées ou peu fiables.

Aucun système de surveillance avancé du trafic ni de journalisation détaillé n'est en place, rendant difficile la détection d'éventuelles anomalies ou attaques. De plus, les performances du réseau se dégradent aux heures de forte activité, ce qui impacte la productivité des utilisateurs.

1.3. Analyse des choix

Plusieurs solutions s'offrent à l'entreprise pour faire évoluer son infrastructure réseau. La première consiste à conserver un routeur classique, éventuellement plus récent et plus performant. Cette option présente l'avantage d'être simple à déployer et peu coûteux, mais reste limitée en termes de sécurité avancée, de personnalisation et de gestion fine du trafic.

La deuxième option est l'intégration d'une solution comme pfSense, un pare-feu/routeur open source basé sur un système dédié. Cette solution offre de nombreuses

fonctionnalités avancées : filtrage précis des flux, gestion des VPN, segmentation du réseau (VLAN), supervision du trafic et globale de la sécurité. Elle nécessite cependant des compétences techniques plus poussées pour l'installation, la configuration et la maintenance.

Enfin, l'entreprise pourrait envisager une architecture sans routeur dédié, en s'appuyant uniquement sur des équipements internes ou des solutions cloud. Cette approche est peu adaptée à ce contexte, car elle réduirait fortement le contrôle sur le réseau local, compliquerait la gestion de la sécurité et augmenterait les risques d'exposition aux menaces externes.

1.4. Solution retenue

Contrairement à un routeur classique, PfSense est une solution open-source basée sur un système d'exploitation dédié, offrant un niveau de contrôle et de personnalisation incomparable. Il permet notamment de créer des VLANs pour segmenter le réseau en zones distinctes, isolant par exemple les postes utilisateurs des serveurs ou du réseau invité, ce qu'un routeur grand public ne sait généralement pas faire de manière fiable.

En matière de sécurité, pfSense intègre un firewall stateful avancé permettant de définir des règles de filtrage très précises entre chaque segment du réseau.

PfSense propose aussi une gestion native des VPN (OpenVPN, IPsec) permettant aux collaborateurs en télétravail de se connecter de manière sécurisée au réseau de l'entreprise. Sa supervision intégrée offre une visibilité complète sur les flux réseau, facilitant le diagnostic et la gestion des incidents.

Enfin, pfSense est une solution évolutive et gratuite dans sa version communautaire, ce qui représente un avantage économique non négligeable pour une PME. Face à toutes ces raisons, pfSense s'impose comme un choix bien plus adapté qu'un simple routeur pour toute entreprise souhaitant professionnaliser la gestion de son réseau.

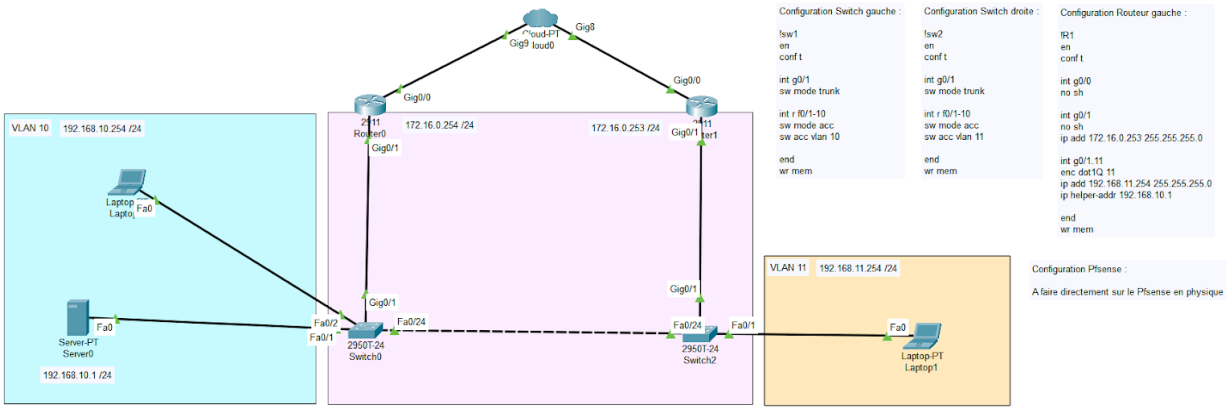
2. Mise en oeuvre technique

2.1. Présentation du matériel utilisé

Un routeur Cisco 1921
Deux switch Cisco Catalyst 2960
Un pfSense (comprenant : écran, trépied, mini tour, clavier, support d'écran, câble HDMI, câble USB)
Cinq câbles RJ45
Trois alimentations
Deux PC portables
Un câble console

Il est important de vérifier l'état du matériel utilisé, notamment l'état des câbles !

2.2. Représentation logique de la situation

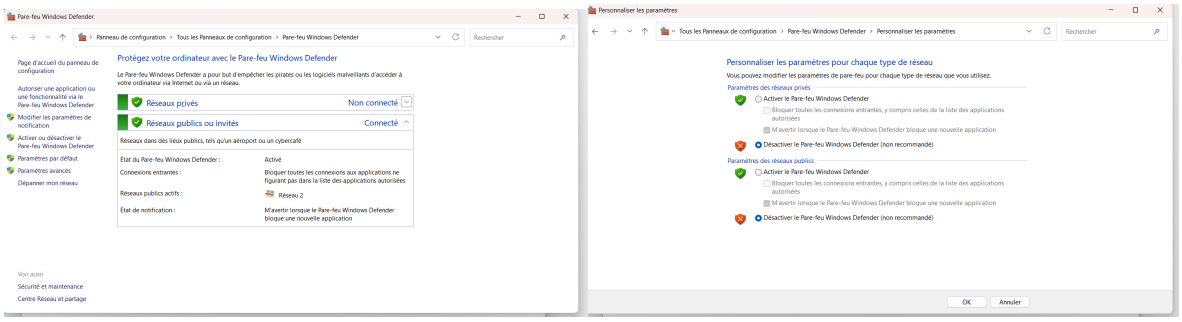


2.3. Préparation physique

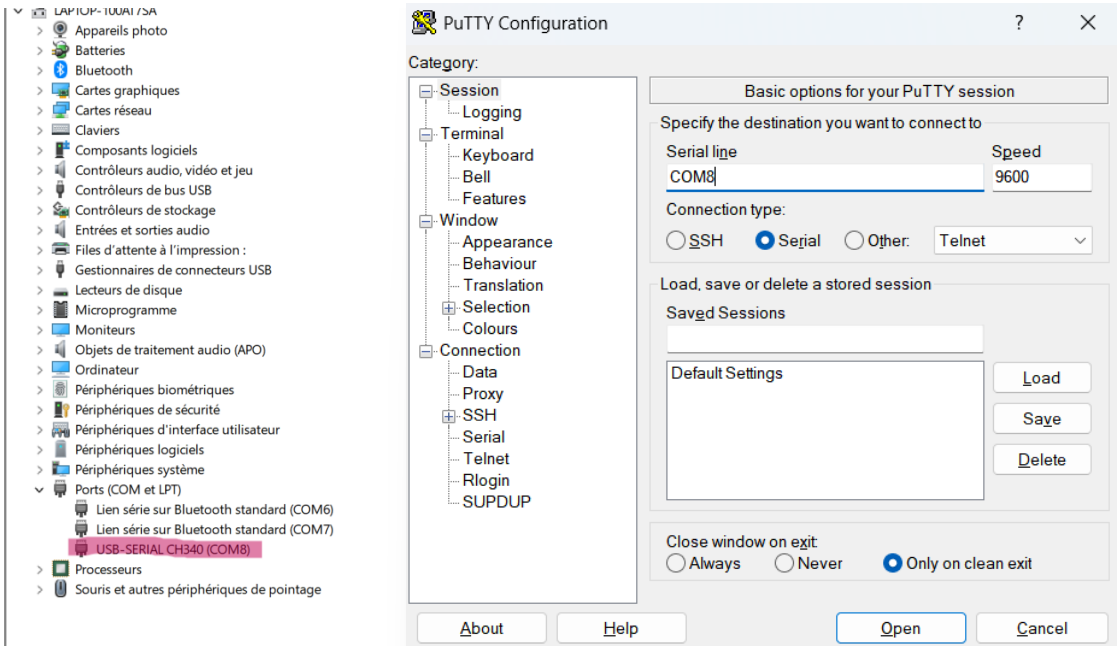
Branchez l'alimentation du routeur sur une prise secteur.
Branchez un câble RJ45 partant d'une prise réseau jusqu'au

routeur sur le port G0/0. Branchez les alimentations pour chaque switch à une prise secteur.
Branchez l'alimentation de la mini tour à une prise secteur. Posez l'écran sur le trépied, le connectez via HDMI à la mini tour ainsi que via USB. Branchez le clavier via usb à la mini tour. Brancher le câble ethernet entre l'un des ordinateurs et le port 2 de la mini tour du Pfsense, ceci nous permettant d'accéder au LAN et de configurer le Pfsense.

Sur les ordinateurs portables, effectuer la configuration suivante :
Afin de désactiver les sécurité Windows : appuyez sur le bouton "windows" du clavier et tapez "vérifier l'état pare-feu". Cliquez sur "activer ou désactiver le pare-feu windows defender", puis cliquez sur "désactiver le pare-feu windows defender" sur les paramètres des réseaux privés et publics.

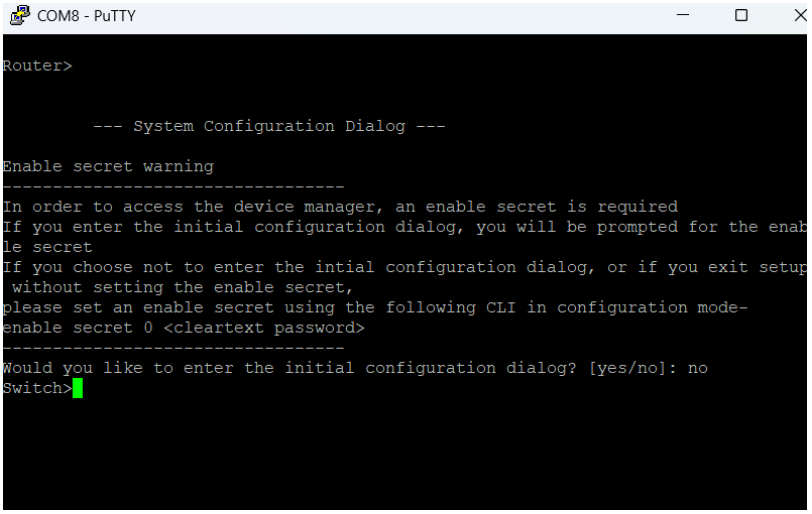


De l'un des ordinateurs portables, brancher le câble console à un commutateur et aller dans le gestionnaire de périphériques. Aller vers "Ports COM et LPT" et cliquez sur "USB SERIAL" pour voir le numéro qui suit "COM" afin de pouvoir utiliser PUTTY. Ouvrez le logiciel PUTTY, puis sélectionnez l'option "SERIAL" et notez le numéro trouvé précédemment dans le gestionnaire de périphériques.



2.4. Configuration des commutateurs

Une fois PuTTY démarré, il est temps d'injecter le code ci-dessous dans l'invite de commandes. Pour cela, il faut voir l'indication "Switch>" comme ci-dessus, indiquant que c'est le commutateur que nous configurons. Copier le code et le coller après "Switch>".



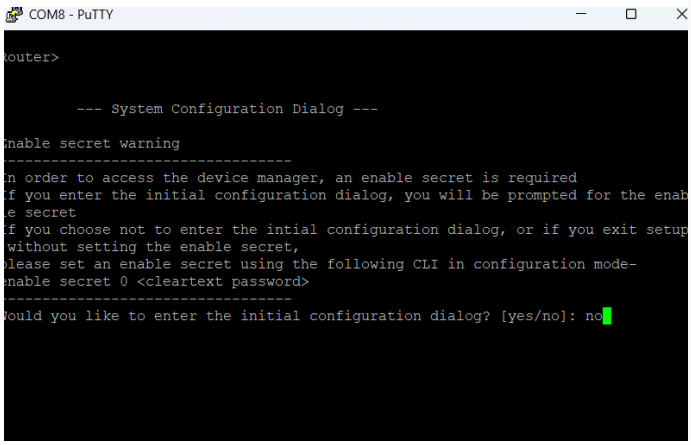
```
!sw1
en
conf t

int g0/1
sw mode tr

int r f0/1-5
sw mode acc
sw acc vlan 10

end
wr mem
```

```
! sw2
en
conf t

int g0/1
sw mode tr

int r f0/1-5
sw mode acc
sw acc vlan 11

end
wr mem
```

2.5. Configuration du routeur

Brancher le câble console sur le routeur. Appuyer sur la touche “entrée” afin de voir apparaître “Routeur>”. Répondre “no” à la question de configuration initiale du routeur, puis appuyer sur “entrée” comme ci-dessous.

De la même manière que pour les commutateurs, injecter le code ci-dessous dans l’invite de commandes.




```
!R1
enable
configure terminal

int g0/0
no sh
ip add dhcp
ip nat outside

int g0/1
no sh
ip add 172.16.0.253 255.255.255.0
ip nat inside

int g0/1.11
enc dot1Q 11
ip add 192.168.11.254 255.255.255.0
ip nat inside

ip dhcp pool tux_vlan10
network 192.168.11.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.11.254

access-list 1 permit 172.16.0.0 0.0.0.255
ip nat inside source list 1 interface g0/0 overload

access-list 3 permit 192.168.11.0 0.0.0.255
ip nat inside source list 3 interface g0/0 overload

router ospf 1
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.255 area 0

end
wr mem
```

2.6. Configuration du pfSense

Appuyer sur le bouton “Power” de la mini-tour. Après le lancement du système, il faut configurer le WAN ainsi que le LAN.

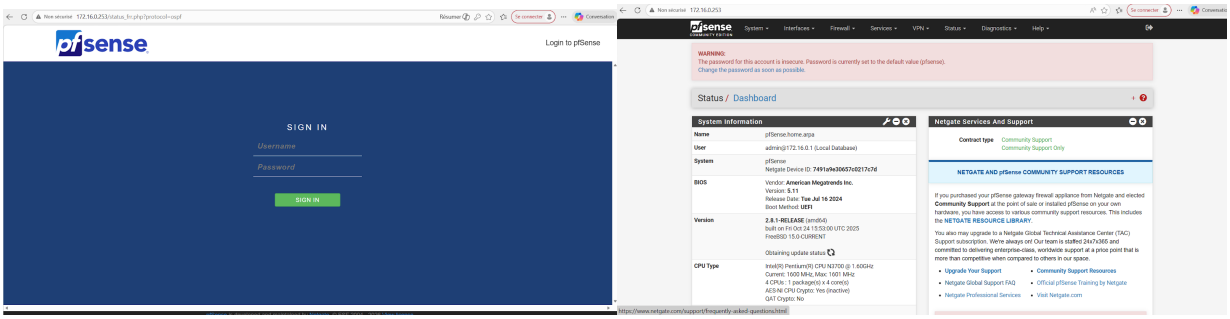
Configuration du WAN :

- Sélectionner l’option “2: set interface IP address”
- Sélectionner l’option “WAN IGC0”. Répondre “y” pour “yes”, à la question “configurer IPv4 address WAN interface via DHCP ?”
- Il faut mettre le nombre “24” à la question “entrez le masque de sous réseau (1 to 32)
- A la question suivante faites “entrer”, mettre “n” pour “no” à la question “voulez-vous configurer une adresse IPv6 ?”
- Faire “entrer” à la question suivante.
- Après avoir rentré ses informations, appuyer sur “entrée” afin de valider la séquence voulue.

Configuration du LAN :

- Démarrer le Pfsense, après le lancement du système il faut configurer le LAN (IGC1)
- Sélectionner l’option “2: set interface IP address”
- Sélectionner l’option “2-LAN IGC1”. Répondre “n” pour “no”, à la question “configurer IPv4 address LAN interface via DHCP ?” Puis, mettre l’adresse IP suivante : 172.16.0.253.
- Il faut mettre le nombre “24” à la question “Entrez le masque de sous réseau (1 to 32)”
- Appuyer sur “entrée”, puis mettre “n” pour “no” à la question “voulez-vous configurer une adresse IPv6 ?”
- Appuyer sur “entrée” à la question suivante

- Mettre “y” pour “yes” à la question “est-ce-que vous voulez activer le DHCP pour le LAN ?”
- Entrer les adresses IP de départ et finale pour le LAN (172.16.0.1 jusqu’à 172.16.0.253)
- Après avoir rentré ses informations, appuyer sur “entrée” afin de valider la séquence voulue. L’adresse 172.16.0.253/24 devrait apparaître à côté de l’option IGC1.
- Aller sur un navigateur web (ici on utilise Microsoft Edge), et entrer l’adresse 172.16.0.253. Cette adresse nous renverra vers le site Pfsense” comme montré ci-dessous.



2.7. Configuration des VLAN :

Configuration du VLAN 10 :

Le VLAN 10 est déjà configuré via les codes du routeur et du commutateur entrés précédemment. Il suffit de brancher un câble réseau entre le port du commutateur et l’ordinateur portable.

En effet, l’activation du DHCP permet de récupérer une adresse IP automatiquement.

Configuration du VLAN 11 : (sur le site Pfsense)

- Aller dans l'onglet "services" et cliquer sur "DHCP server" (cocher la case Enable DHCP server on LAN interface et le DNS server 8.8.8.8) pour sauvegarder on fait "save" et également "apply changes" afin de sauvegarder les modifications.

- Allez dans l'onglet "interfaces" et cliquez sur "assignments", allez dans l'onglet VLAN et cliquez sur "add". Choisir dans l'option "parent interface" "IGC1-LAN" et faire "save" et "apply changes".

- Allez dans l'onglet " firewall" et cliquer sur "rules", allez dans l'onglet "VLAN 11", cliquez sur "add avec une flèche vers le haut" (choisir "any" dans "protocole"), faire "save" et "apply changes".

- Retourner sur l'onglet "interfaces" et cliquez sur "assignment". Une option "add" permet d'ajouter le VLAN 11 à la configuration.

- Cliquez sur le "VLAN 11" afin de finaliser le paramétrage: cocher la case "enable interface", choisissez l'option adresse IP statique (192.168.11.254 avec /24). Faire "save" et "apply changes".

Sur le Pfsense, appuyer sur la touche "entrée" afin de valider les modifications pour voir apparaître l'option VLAN 11-IGC1.11, avec l'adresse IP : 192.168.11.254/24.

2.8. Test et validation

Connecter chaque PC sur un switch (PC 1 avec switch 1 qui sera dans le VLAN 10 et PC 2 qui sera avec switch 2 dans le VLAN 11). Une fois les ordinateurs connectés à leur commutateur respectif, aller dans l'invite de commande de chaque ordinateur et effectuer une commande "ping", de l'un des PC vers l'autre. Les deux PC peuvent communiquer entre eux, et sont connectés au réseau.

Si le résultat de la commande "ping" ne fonctionne pas, essayez de faire cette commande sur les différentes passerelles par défaut afin de déceler la cause du problème.