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…….…..… 3 - 6

1.1. Expression des besoins…….. 3

1.2. Description de l'existant…….. 3 - 4

1.3. Analyse des choix……. 4 - 5

1.4. Solution retenue……. 6

2. Mise en œuvre……. 7 - 14

2.1. Présentation du matériel utilisé…… 7

2.2. Représentation logique de la situation…….. 7

2.3. Préparation physique…… 8 - 9

2.4. Configuration des commutateurs……. 9 - 10

2.5. Configuration du routeur ……..…..…. 10

2.6. Configuration du Pfsense…… 11 - 12

2.7. Configuration des VLANs…… 12 - 13

2.8. Test et validation…… 14

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.

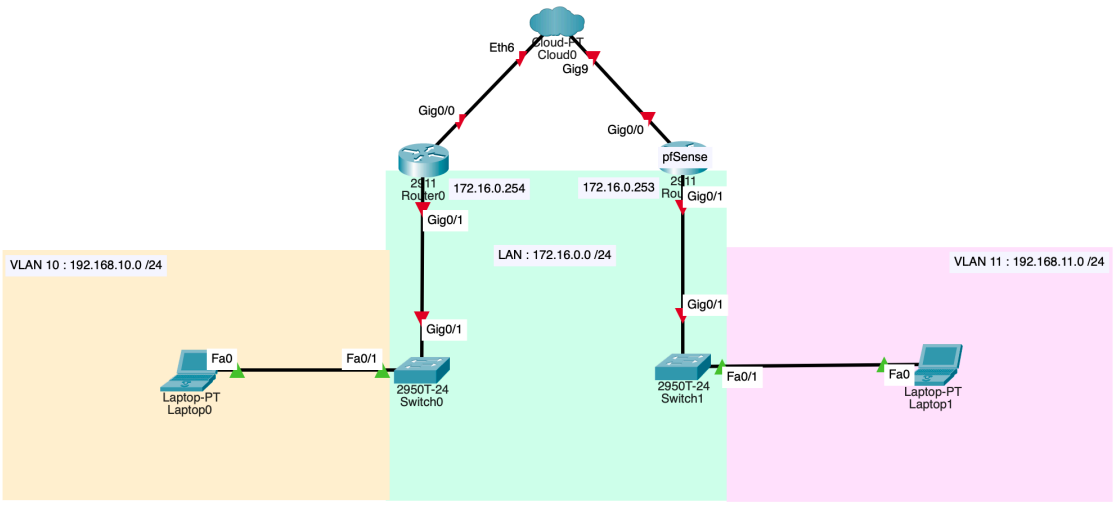
2. Mise en oeuvre technique

2.1. Présentation du matériel utilisé

- Un routeur Cisco 1921
- Deux commutateurs Cisco Catalyst 2960
- Un pfSense (comprenant : un écran, un support d'écran, une mini-tour avec son câble d'alimentation, un clavier, un câble HDMI, un câble USB)
- Huit 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 !

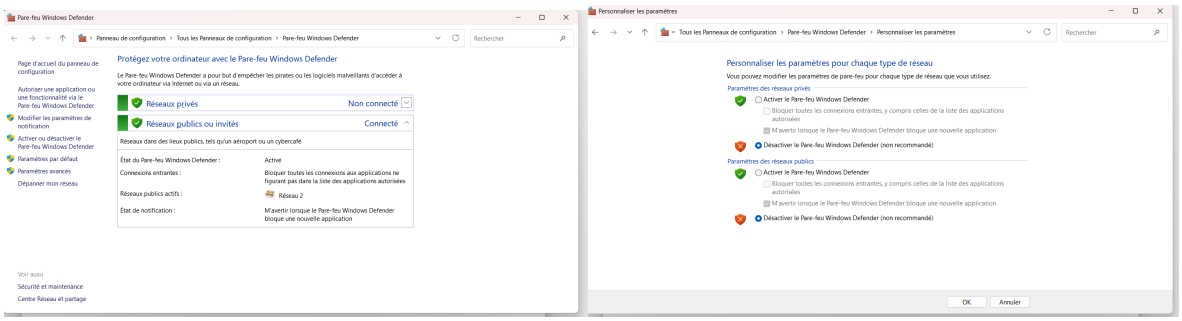
2.2. Représentation logique de la situation



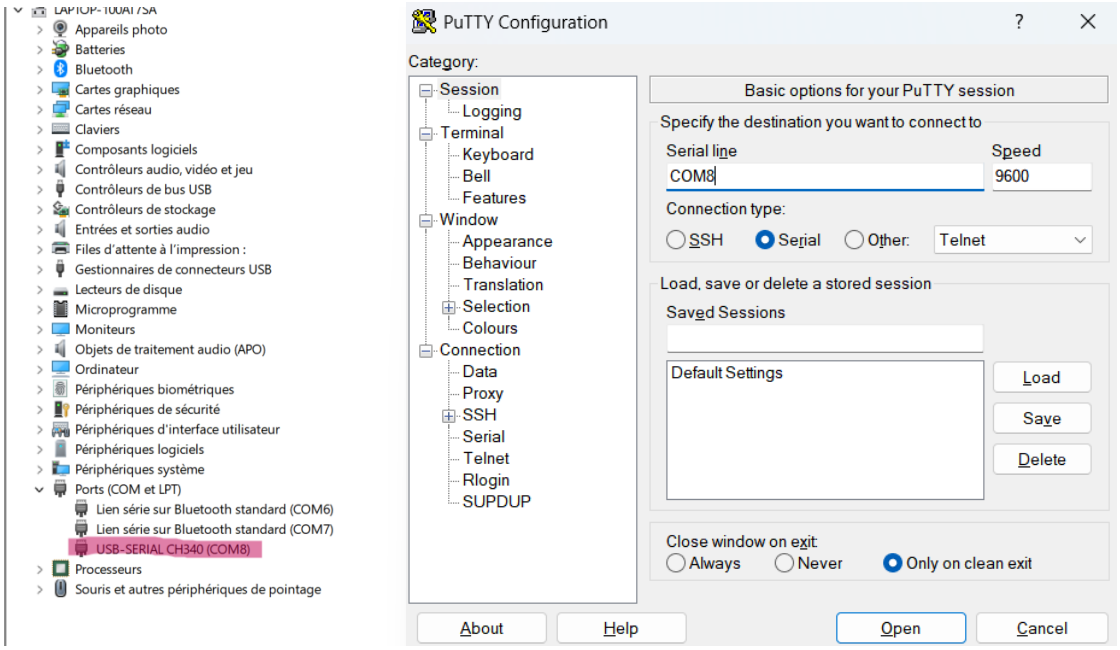
2.3. Préparation physique

Brancher l'alimentation du routeur sur une prise secteur. Brancher un câble RJ45 partant d'une prise réseau jusqu'au routeur sur le port G0/0. Branchez les alimentations pour chaque commutateur à une prise secteur.
Brancher l'alimentation de la mini-tour à une prise secteur. Poser l'écran sur son support, le connecter via HDMI à la mini-tour ainsi que via USB. Brancher 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 : appuyer sur le bouton «Windows» du clavier et taper «Vérifier l'état pare-feu». Cliquer sur «Activer ou désactiver le pare-feu windows defender», puis cliquer sur «Désactiver le pare-feu windows defender» sur les paramètres des réseaux privés et publics.

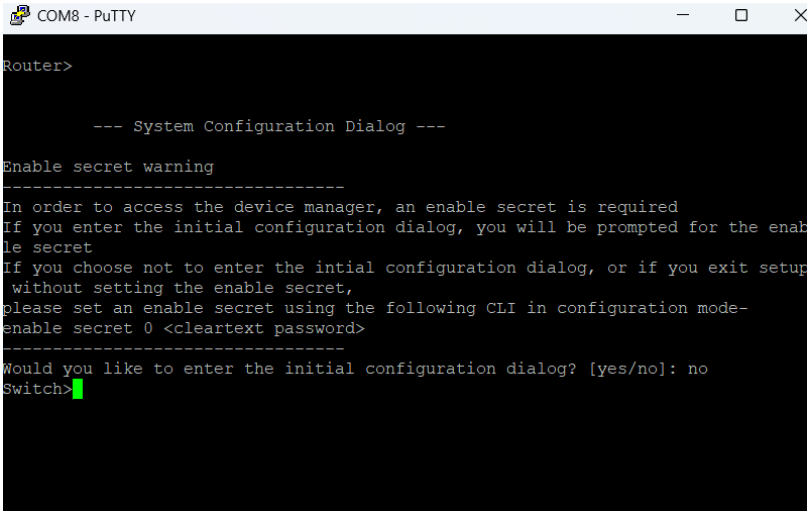


De l'un des ordinateurs portables, brancher le câble console à un commutateur et aller dans le gestionnaire de périphériques. Aller vers «Ports COM et LPT» et cliquer sur «USB SERIAL"» afin de voir le numéro suivant «COM» et de pouvoir utiliser PUTTY. Ouvrir le logiciel PUTTY, puis sélectionner l'option «SERIAL» et noter le numéro trouvé précédemment dans le gestionnaire de périphériques (ici, «COM8»).



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 inscrit l'indication «Switch>» comme ci-dessous, indiquant que c'est le commutateur que nous configurons. Copier le code et le coller après «Switch>».



Si la question «Would you like to enter the initial configuration dialog ?» Est posée, toujours répondre «no»

```
!sw1
en
conf t

int r g1/0/47-48
sw mode trunk

int r g1/0/1-5
sw mode acc
sw acc vlan 10

end
wr mem
```

```
! sw2
en
conf t

int r g1/0/47-48
sw mode trunk

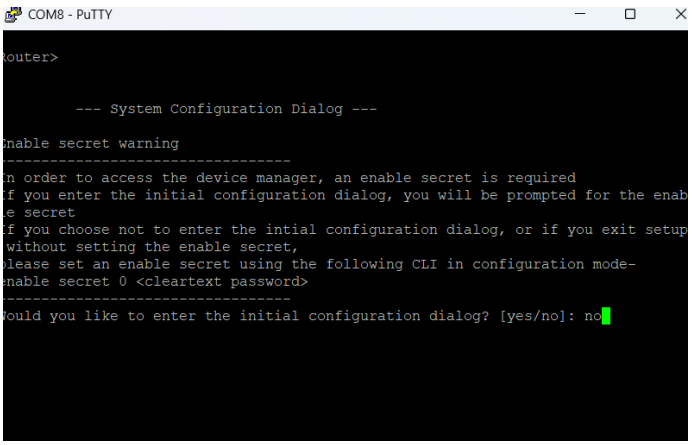
int r g1/0/1-5
sw mode acc
sw acc vlan 11

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 172.16.0.254 255.255.255.0
ip nat inside

int g0/1.10
enc dot1Q 10
ip add 192.168.10.254 255.255.255.0
ip nat inside

ip dhcp pool tux_vlan10
network 192.168.10.0 255.255.255.0
dns-server 8.8.8.8
default-router 192.168.10.254

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 192.168.10.0 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 «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 «Entrer le masque de sous réseau (1 to 32)»
- A la question suivante, faites «Entrée», puis mettre «n» pour «no» à la question «Voulez-vous configurer une adresse IPv6 ?»
- Appuyer sur «Entrée» à la question suivante
- Appuyer sur «Entrée"» afin de valider la séquence de tâches et de voir apparaître l'adresse IPv4 du WAN

Configuration du LAN :

- Sélectionner l'option «Set interface IP address»
- Sélectionner l'option «LAN IGC1». Répondre «n» pour «no» à la question «Configurer IPv4 address LAN interface via DHCP ?», puis rentrer l'adresse IP suivante : 172.16.0.253
- Il faut mettre le nombre «24» à la question «Entrer 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 ?»

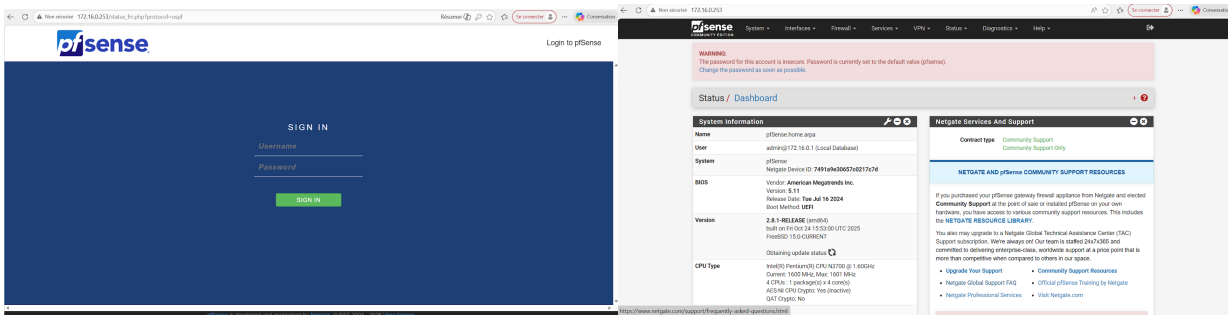
- Entrer les adresses IP de début et de fin pour le LAN («172.16.0.1» comme départ et «172.16.0.253» comme fin)
- Appuyer sur «Entrée» afin de valider la séquence de tâches et de voir apparaitre l'adresse IPv4 du LAN

2.7. Configuration des VLANs :

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.



Faire attention à la version utilisé du pfSense : il faut utiliser la version 2.8 car la 2.7 ne fonctionnera pas correctement !

Configuration du VLAN 11 : (sur le site Pfsense)

- 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-dessus
- Aller dans l'onglet «Interfaces» et cliquer sur «Assignments». Aller dans l'onglet «VLANs» et cliquer

sur «Add». Choisir dans l'option «Parent interface» «IGC1-LAN», appuyer «Save» et «Apply changes».

- Dans l'onglet «Interfaces», cliquer sur «Assignment». Une option «Add» permet d'ajouter le VLAN 11 à la configuration.

- Aller dans l'onglet «Services» et cliquer sur «DHCP server» : cocher la case «Enable DHCP server on LAN interface» et rentrer le DNS server «8.8.8.8», puis appuyer sur «Save» et «Apply changes» afin de sauvegarder les modifications.

- Aller dans l'onglet «Firewall» et cliquer sur «Rules», puis sur l'onglet «VLAN 11». Cliquer sur «Add» (avec une flèche vers le haut) puis choisir «Any» dans «Protocol». Appuyer sur «Save» et «Apply changes».

- Cliquer sur le «VLAN 11» afin de finaliser le paramétrage : cocher la case «Enable interface», puis choisir l'option «Static IPv4 adress» («192.168.11.254» avec «/24»). Appuyer sur «Save» et «Apply changes».

Sur le Pfsense, appuyer sur la touche «Entrée» afin de valider les modifications et 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 avec switch 2 qui sera 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 «ipconfig» et «ping», afin de connaitre la configuration IP de chaque PC et de vérifier qu'ils peuvent bien communiquer entre eux et reçoivent bien Internet.

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