

Projet de fin d'année

Thème

Mise en place d'une architecture réseau avec des fonctionnalités avancées et de haute disponibilité

Présentation de l'architecteur de notre réseau

Spécialité : Infrastructure et système d'information & cybersécurité

Présenté par :

- TAGUEMOUNT Kamelia
- N'GORAN Sonia
- BENTO HATCHA Alvan Jetser

Table des matières

1	Contexte :	4
2	Travail demandé :	4
3	La définition des fonctionnalités :	4
3.1	VLAN :	4
3.1.1	Définition :	4
3.1.2	Typologies des VLANs :	4
3.2	Firewall :	6
3.2.1	Définition :	6
3.2.2	Utilité d'un firewall :	6
3.2.3	Principe de fonctionnement :	6
3.3	Zone démilitarisée (DMZ) :	7
3.3.1	Définition :	7
3.3.2	Firewall avec zone démilitarisée :	7
3.4	Sauvegarde de la configuration réseau :	8
3.4.1	Définition :	8
3.4.2	Importance de la gestion de configuration :	8
3.5	Détection d'intrusion :	8
3.5.1	Définition :	8
3.6	Portail captif :	8
3.7	Honeypot :	9
3.7.1	Définition :	9
3.7.2	Types de honeypots :	9
3.8	SOC :	9
3.8.1	Les avantages à utiliser un SOC :	10
4	Mise en place de notre architecture avec les fonctionnalités :	10
4.1	Le schéma de notre architecture :	10
4.2	Conception et réalisation du réseau sécurisé :	11
4.2.1	Présentation de VMware Workstation :	11
4.2.2	Présentation de Pfsense :	11
4.2.3	Présentation de GNS3 :	11
4.2.4	Configuration des switches et du routage inter-vlans :	12
4.2.5	Installation de Pfsense :	13
4.2.6	Création de la zone DMZ (SRV) sur le pfsense :	15

4.2.7	Création des alias pour les VLANS :	16
4.2.8	Création d'une route :	16
4.2.9	Création de la machine virtuelle serveur 2012 :	17
	Ajouter des règles de filtrage :	18
4.2.10	La sauvegarde de la configuration réseau :	18
4.2.11	Mise en place d'un système de détection d'intrusion sur le pfsense :	20
4.2.12	La configuration de honeypot :	23
4.2.13	Configuration du portail captif :	23
4.2.14	Configuration du SOC :	30
4.2.15	Configuration de la redondance réseau :	30

Introduction

L'infrastructure système et réseaux d'entreprise est le cœur de la majeure partie de l'activité informatique de l'entreprise.

Bien que les infrastructures puissent varier beaucoup en fonction de la taille de l'entreprise et de son activité, le réseau local, outil transversal par excellence et commun à tous les acteurs de l'entreprise, aura toujours une importance capitale au sein de celle-ci.

Ceci est particulièrement vrai pour les entreprises et autres entités qui sont fortement tributaires de leur système d'information pour la conduite des revenus. Les sociétés opérant dans des domaines comme le commerce, le service, la communication, etc. en sont le parfait exemple.

Par ailleurs, le réseau d'entreprise retrace souvent, par son évolution et sa complexité, l'historique et le vécu de toute l'entreprise. En effet, pour répondre au mieux à l'évolution des besoins et en essayant de tirer profit des évolutions de technologies, dispositifs et stratégies, ce dernier évolue considérablement. La virtualisation et les architectures orientées services en sont de parfaits exemples.

La gestion du réseau d'entreprise devient ainsi tout aussi importante dans la mesure qu'il devient essentiel d'en assurer la disponibilité. Ceci est d'autant plus difficile en raison des différentes menaces telles que le piratage, les attaques de déni de service, les virus et autres vols d'informations, etc., synonymes d'indisponibilité, de perte de données voire de baisse de crédibilité et de rentabilité globale.

Notre projet consistera à installer, configurer et mettre en place une architecture système et réseau avec des fonctionnalités avancées et de haute disponibilité afin d'offrir un service informatisé robuste, optimal et fiable qui répondra aux besoins et qui donnera plus de moyens afin de mieux répondre aux exigences de ces projets.

1 Contexte :

Une entreprise nous demande de refaire son architecture réseau avec les fonctionnalités suivantes : firewall, portail captif, DMZ, honeypot, Vlan, redondance réseau, sauvegarde de la configuration réseau, soc, détection d'intrusion, et élimination des SPOF et la redondance des équipements en respectant les besoins clients, et mettre en place un schéma d'architecture agnostique pour pouvoir instancier les éléments de configuration pour plusieurs environnements.

2 Travail demandé :

Mettre en place une architecture avec plusieurs clients au sein d'un réseau, différents équipements réseau comme les switches, le pare-feu, les routeurs, les câbles, et la mise en place des serveurs (Linux ou Windows).

Faire une maquette de l'architecture sur GNS3 avec les fonctionnalités avancées, de haute disponibilité, élimination des SPOF, redondance des équipements et faire une démo sur le traçage de paquets avec routage et filtrage fonctionnel.

3 La définition des fonctionnalités :

3.1 VLAN :

3.1.1 Définition :

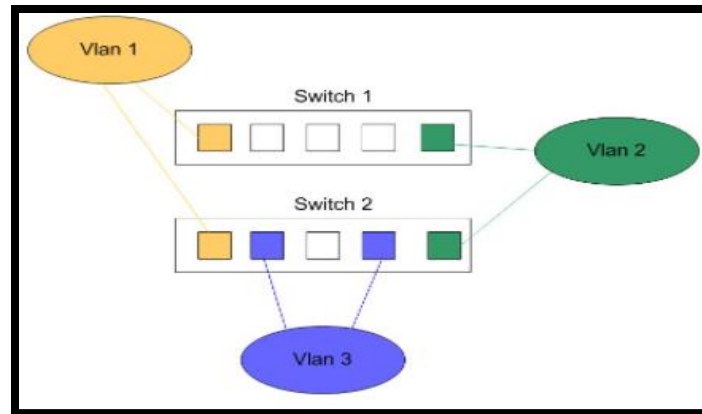
Les réseaux virtuels (VLAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN. Il est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs qui sont les commutateurs VLAN. Ils offrent une solution pour regrouper les stations et les serveurs en ensembles indépendants, de sorte à assurer une bonne sécurité des communications.

3.1.2 Typologies des VLANs :

Les VLANs diffèrent selon les informations utilisées pour regrouper les stations. Il en existe trois modèles :

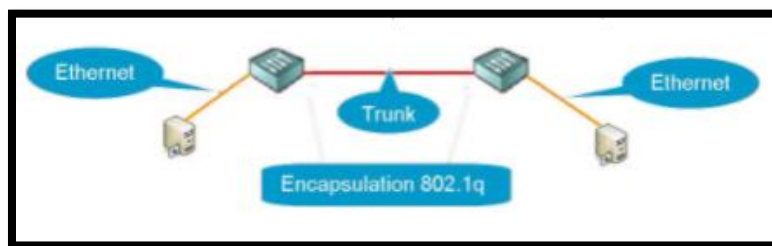
3.1.2.1 VLAN par port :

Les VLANs par port associent un port d'un switch à un numéro de Vlan. On dit alors que le port est tagué suivant le Vlan donné. Le switch entretient ensuite une table qui lie chaque Vlan au port associé. Le taggage des ports peut se faire de manière statique ou de manière dynamique avec la norme 802.1q, l'avantage est qu'une attaque extérieure ne pourra se faire qu'en branchant le pc sur un port tagué, donc le pirate a besoin d'avoir accès à la machine physique pour pénétrer le vlan.



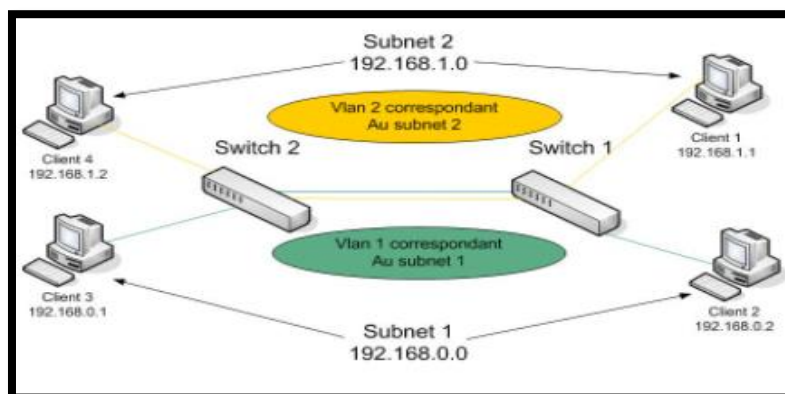
3.1.2.2 VLAN par Adresse IEEE (par adresse MAC) :

Le Vlan de niveau segmente le réseau en fonction de l'adresse MAC de l'utilisateur. On associe ainsi des adresses à des VLANs pour permettre à un utilisateur de se déplacer sans pour autant changer de profil. Ce type de Vlan est généralement utilisé pour regrouper les utilisateurs par service. Ce type de Vlan permet de regrouper au sein d'un même lien et de les transporter sur le réseau. Son avantage est qu'un pirate souhaitant se connecter sur le vlan devra au préalable récupérer une adresse MAC du vlan pour pouvoir entrer.



3.1.2.3 VLAN par protocole et par sous-réseau :

Les VLANs de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent. La mise en place de Vlan de niveau 3 est conditionnée par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...). L'attribution des VLANs se fait de manière automatique en décapsulant le paquet jusqu'à l'adresse source. Cette adresse va déterminer à quel Vlan appartient la machine. L'avantage est qu'il permet une affectation automatique à un vlan suivant une adresse IP.



3.2 Firewall :

3.2.1 Définition :

Un firewall, appelé aussi coupe-feu ou pare-feu a pour but de contrôler et de filtrer l'accès entre un réseau d'entreprise ou l'ordinateur d'un particulier et un autre réseau qui est ici Internet. Le firewall peut être soit un objet matériel ou un programme fonctionnant sur un ordinateur. Dans les deux cas, le firewall doit se placer à la jonction entre le réseau à protéger et Internet. Il examine tout le trafic entre les deux réseaux pour voir s'il correspond à certains critères définis par l'administrateur. Si cela correspond, les données accèdent au réseau, sinon elles sont stoppées. Il filtre aussi bien dans le sens de l'envoi de données vers l'extérieur que dans celui de la réception. Il peut ainsi empêcher un logiciel d'accéder à Internet ou une personne d'accéder à certains services comme le FTP par exemple.

3.2.2 Utilité d'un firewall :

Certains firewalls laissent uniquement passer le courrier électronique. De cette manière, ils interdisent toute autre attaque qu'une attaque basée sur le service de courrier. D'autres firewalls, moins strictes, bloquent uniquement les services reconnus comme étant des services dangereux. Généralement, les firewalls sont configurés pour protéger contre les accès non authentifiés du réseau externe. Ceci, plus qu'autre chose, empêche les destructeurs de se loger sur des machines de vote réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur. Ils sont également intéressants dans le sens où ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux.

3.2.3 Principe de fonctionnement :

Le fonctionnement d'un firewall repose sur le filtrage des paquets cela peut se faire de différentes manières. Il existe deux types de firewall qui sont :

3.2.3.1 Les filtres de paquet :

Le filtrage du trafic de données se fait au niveau des couches 3 et 4 du modèle OSI. Certains firewalls sont des routeurs possédant des fonctions de filtrage de paquets. Avec des règles, l'administrateur réseau peut donc interdire ou autoriser un certain nombre de services ainsi que bloquer les accès aux équipements de son site, tout en permettant à ses machines l'accès aux services de l'Internet. Le routeur doit être configuré avec une liste d'accès

3.2.3.2 Passerelle :

Il existe deux types de passerelles :

- **Passerelles de niveau applicatif (proxy) :** Ces passerelles sont situées entre un client du réseau interne et un serveur du réseau externe.
 - Les proxys filtrent en fonction du service demandé : Telnet, FTP, SMTP, HTTP...
 - Le client se connecte au serveur proxy et demande l'accès au serveur distant.
 - Le serveur proxy vérifie l'adresse du client, authentifie le client à l'aide d'un serveur d'authentification (type RADIUS) et l'autorise à se connecter sur le serveur.
 - Le serveur proxy se connecte sur le serveur distant et relaie les données entre les deux connexions.

- **Passerelles de niveau circuit** : Les passerelles de niveau circuit filtrent au niveau transport. L'avantage est qu'elles sont communes à toutes les applications TCP/IP.
- Le client établit une connexion TCP avec la passerelle en demandant de communiquer avec le serveur.
- La passerelle peut :
 1. Vérifier l'adresse IP du client.
 2. Autoriser une connexion sur un port pour une durée maximale fixée.
 3. N'autorise la réutilisation d'un même port qu'après un certain délai.
 4. Authentifier un terminal.
- La passerelle se connecte au serveur et relaie les données entre les deux connexions TCP

3.3 Zone démilitarisée (DMZ) :

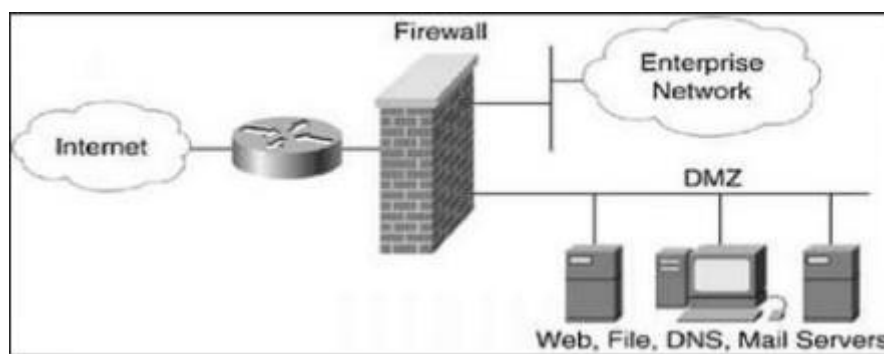
3.3.1 Définition :

C'est un sous-réseau physique ou logique, son but est de séparer un réseau local interne LAN d'autres réseaux non sécurisés tels qu'Internet. Les serveurs sont placés dans cette zone-là pour être accessibles depuis Internet tandis que le LAN n'est pas accessible. Tous les services comme : web, DNS, FTP, messagerie fournis aux utilisateurs sur Internet sont placés sur la zone démilitarisée. Il existe plusieurs façons de mettre en place cette zone avec la méthode du pare-feu.

3.3.2 Firewall avec zone démilitarisée :

Le firewall a pour fonction de surveiller les trames passant sur le réseau et de les bloquer ou de les laisser passer. Le firewall décide de laisser passer ou non une trame en fonction de sa source, de sa destination, et des règles d'approbation définies dans sa table de règles.

La configuration la plus répandue pour un réseau connecté à Internet est une configuration avec firewall et zone démilitarisée (DMZ). Un firewall est placé entre Internet, le réseau local LAN, et une zone spéciale appelée DMZ, qui contient serveurs Web, Extranets, FTP, etc..., qui doit pouvoir être accédée par Internet et du LAN local. La DMZ est une sorte de zone tampon entre l'extérieur et le réseau interne. La figure suivante illustre cette solution :



Firewall permet alors de filtrer les trames et de les diriger vers telle ou telle zone en fonction des règles internes définies par les administrateurs.

3.4 Sauvegarde de la configuration réseau :

3.4.1 Définition :

C'est une méthode qu'est mis en place par la plupart des administrateurs réseau d'une entreprise, a pour but de garder la précédente configuration dans un fichier et si une panne arrive la sauvegarde permet de récupérer le fichier déjà configuré pour une nouvelle configuration des équipements.

3.4.2 Importance de la gestion de configuration :

La gestion de configuration réseau est importante car elle permet de faire évaluer l'infrastructure informatique sans pour autant affecter le personnel administratif à la gestion de ces périphériques.

3.5 Détection d'intrusion :

3.5.1 Définition :

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. Un IDS réagit en cas d'anomalie, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion. C'est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network Based Intrusion Detection System) assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System) assurent la sécurité au niveau des hôtes.

3.6 Portail captif :

Un portail captif est une structure permettant un accès rapide et sécurisé à Internet. Lorsqu'un utilisateur cherche à accéder à Internet pour la première fois, le portail capte sa demande de connexion grâce à un routage interne et lui propose de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page web stockée localement sur le portail captif grâce au serveur HTTP. Ceci permet à tout ordinateur équipé d'un « Web browser » ou navigateur web et d'un accès Wifi de se voir proposer un accès à Internet. La connexion au serveur est sécurisée par SSL grâce au protocole HTTPS ce qui garantit l'inviolabilité de la transaction. Les identifiants de connexion (Login et Mot de passe) sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles de firewall le concernant sont modifiées et celui-ci se voit autorisé à utiliser son accès Internet pour une durée fixée par l'administrateur. A la fin de la durée fixée, l'utilisateur se verra redemandé ses identifiants de connexions afin d'ouvrir une nouvelle session.

3.7 Honeypot

3.7.1 Définition :

Un honeypot est une ressource de l'architecture de sécurité dont le but est de se faire passer pour une cible réelle afin d'être attaquée ou compromise. Autrement dit, les honeypots sont des machines de production destinées à attirer les pirates. Ceux-ci, persuadés d'avoir pénétré le réseau, ont tous leurs faits et gestes contrôlés.

Les différentes implémentations des honeypots reposent sur leur niveau d'interaction. Le terme interaction désigne l'interaction entre le pirate et le système piraté. Les honeypots sont principalement divisés en deux catégories : les honeypots à faible interaction et les honeypots à forte interaction :

- **Les honeypots à faible interaction** : sont les honeypots les plus simples. Ils ne fournissent pas de véritables services, ils se contentent de les simuler par l'intermédiaire de script comme Honeyd le propose, et que nous allons utiliser par la suite.
- **Les honeypots à forte interaction** : cependant fournissent de vrais services sur une machine plus ou moins sécurisée. Néanmoins les risques sont très nombreux puisque la machine est très vulnérable. Il faut donc s'assurer que l'architecture sous-jacente soit bien sécurisée

3.7.2 Types de honeypots :

Un honeypot peut être de production ou de recherche :

- ❖ **Honeypot de production** : Ce type de honeypots a une utilité pour la sécurité active du système pour lequel il est installé. Il dérouté les attaques orientées vers les différents services de production du système, en les attirant vers lui. Ainsi les honeypots de production réduisent le risque, en renforçant la sécurité qui est assurée par les autres mécanismes de sécurité comme les firewalls, les IDS (systèmes de détection d'intrusions).
- ❖ **Honeypot de recherche** : Ce sont des honeypots dont le souci n'est pas de sécuriser un système particulier. Ils sont introduits dans un environnement de recherche pour comprendre et étudier les attaquants et leur façon de procéder. Les renseignements tirés vont servir pour améliorer les techniques de protection contre ces attaques.

Les deux types de honeypots jouent un rôle dans une ou plusieurs composantes de la sécurité qui sont la prévention, la détection, et le recouvrement. Les honeypots de production contribuent à la prévention du système, en provoquant une déception chez les attaquants, après plusieurs tentatives échouées pour atteindre les ressources du système. Et ils sont aussi bénéfiques pour la détection, dans la mesure que toute connexion établie avec un honeypot de production est considérée comme tentative d'intrusion au système, il élimine ainsi toutes les fausses alertes (positives et négatives).

3.8 SOC

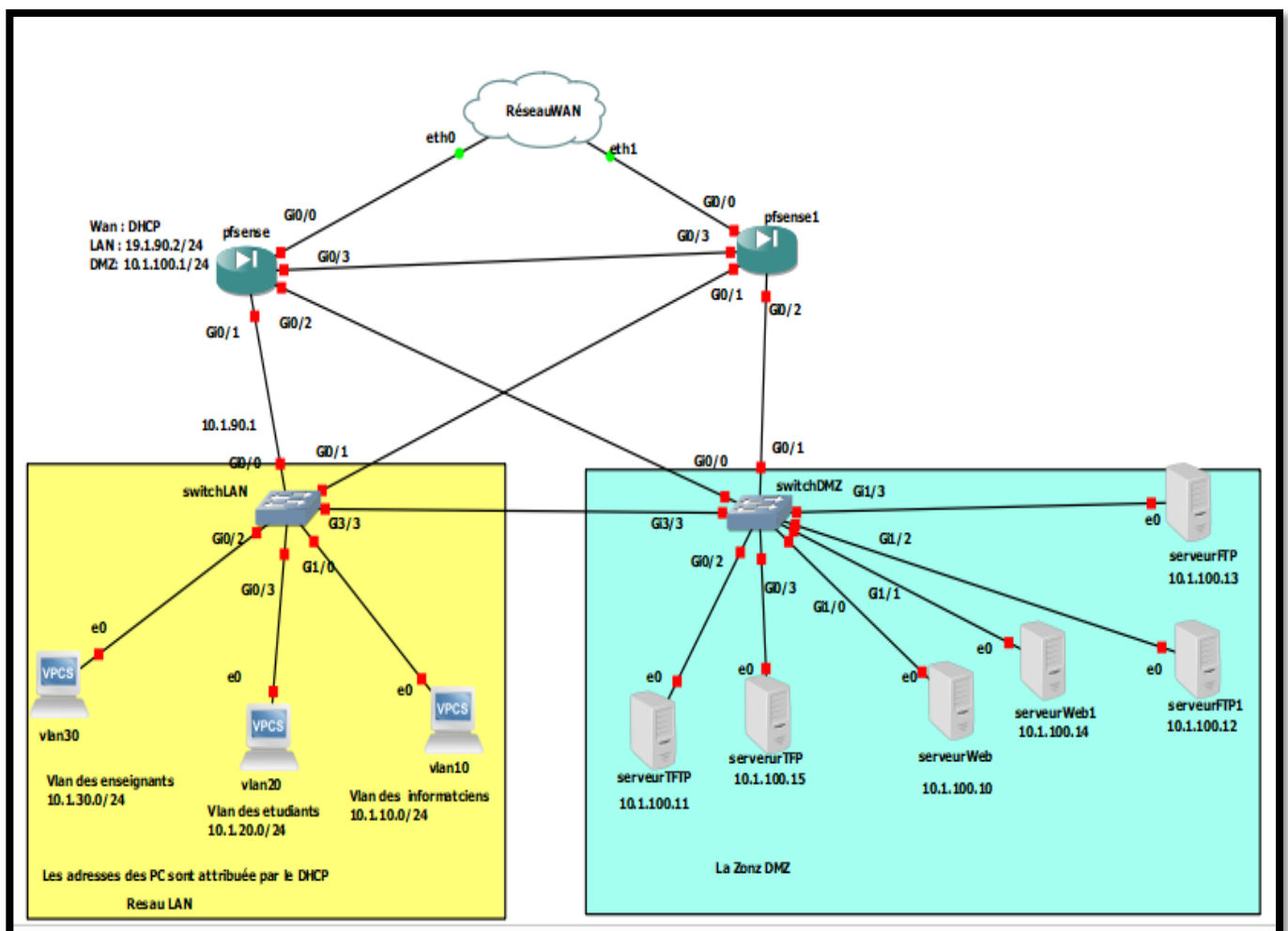
Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

3.8.1 Les avantages à utiliser un SOC :

- Le principal avantage d'avoir un SOC est l'amélioration de la détection des incidents de sécurité par la surveillance et l'analyse continue de l'activité des données. En analysant les réseaux, les terminaux, les serveurs et les bases de données d'une société 24h/24, l'équipe du SOC assure une détection et une intervention rapides en cas d'incident de sécurité.
- La surveillance permanente assurée par un SOC donne aux entreprises l'avantage de pouvoir se défendre contre les incidents et les intrusions, quels que soient leur source, l'heure de la journée ou le type d'attaque.
- L'écart entre le moment où les pirates font des tentatives et le moment où les entreprises sont averties est bien décrit dans le rapport annuel de Verizon intitulé Data Breach Investigations Report. Un SOC aide les entreprises à combler cet écart et à rester au fait des menaces auxquelles leurs environnements sont exposés.

4 Mise en place de notre architecture avec les fonctionnalités :

4.1 Le schéma de notre architecture :



4.2 Conception et réalisation du réseau sécurisé :

Les outils utilisés :

- VMware Workstation
- PfSense
- GNS3

4.2.1 Présentation de VMware Workstation :

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (Machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle pendant son fonctionnement

4.2.2 Présentation de Pfsense :

PfSense (distribution logicielle) est un routeur / pare-feu open source basé sur FreeBSD. Le PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (packet filter), il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre depuis une interface web et gère nativement les VLAN (802.1q).

Les avantages principaux de PfSense sont les suivants :

- Il est adapté pour une utilisation en tant que pare-feu et routeur,
- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement,
- Il offre des options de firewalling / routage plus évolué que IPCOP,
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres,
- Simplicité de l'activation / désactivation des modules de filtrage,
- Système très robuste basée sur un noyau FreeBSD,
- Des fonctionnalités réseaux avancées

4.2.3 Présentation de GNS3 :

GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Vous connaissez peut-être avec VMWare ou Virtual Box qui sont utilisées pour simuler les différents systèmes d'exploitation dans un environnement virtuel. Ces programmes vous permettent d'exécuter plusieurs systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type d'émulation à l'aide de Cisco Internetwork Operating Systems.

4.2.4 Configuration des switches et du routage inter-VLANs :

4.2.4.1 Mise en place des VLANs sur notre architecture réseau :

On a mis en place 3 VLANs qui sont :

- Vlan 10 : c'est le vlan pour les informaticiens avec l'adresse 10.1.10.0/24
- Vlan 20 : c'est le vlan pour les étudiants avec l'adresse 10.1.20.0/24
- Vlan 30 : c'est le vlan pour les enseignants avec l'adresse 10.1.30.0/24

On a configuré le switch de façon à attribuer des IPS automatique avec le DHCP pour les PC clients.

Ci-dessous les images qui illustrent la configuration effectue sur le switch RG (repart:

```
hostname RG
!
boot-start-marker
boot-end-marker
!
!
```

```
ip dhcp excluded-address 10.1.10.1 10.1.10.20
ip dhcp excluded-address 10.1.20.1 10.1.20.20
ip dhcp excluded-address 10.1.30.1 10.1.30.20
!
ip dhcp pool 10
network 10.1.10.0 255.255.255.0
dns-server 10.1.90.2
default-router 10.1.10.1
domain-name ens.isetsf.tn
!
ip dhcp pool 20
network 10.1.20.0 255.255.255.0
dns-server 10.1.90.2
default-router 10.1.20.1
domain-name etd.isetsf.tn
!
ip dhcp pool 30
network 10.1.30.0 255.255.255.0
dns-server 10.1.90.2
default-router 10.1.30.1
domain-name sco.isetsf.tn
!
```

```
interface GigabitEthernet0/2
  switchport access vlan 10
  switchport mode access
  media-type rj45
  negotiation auto
!
```

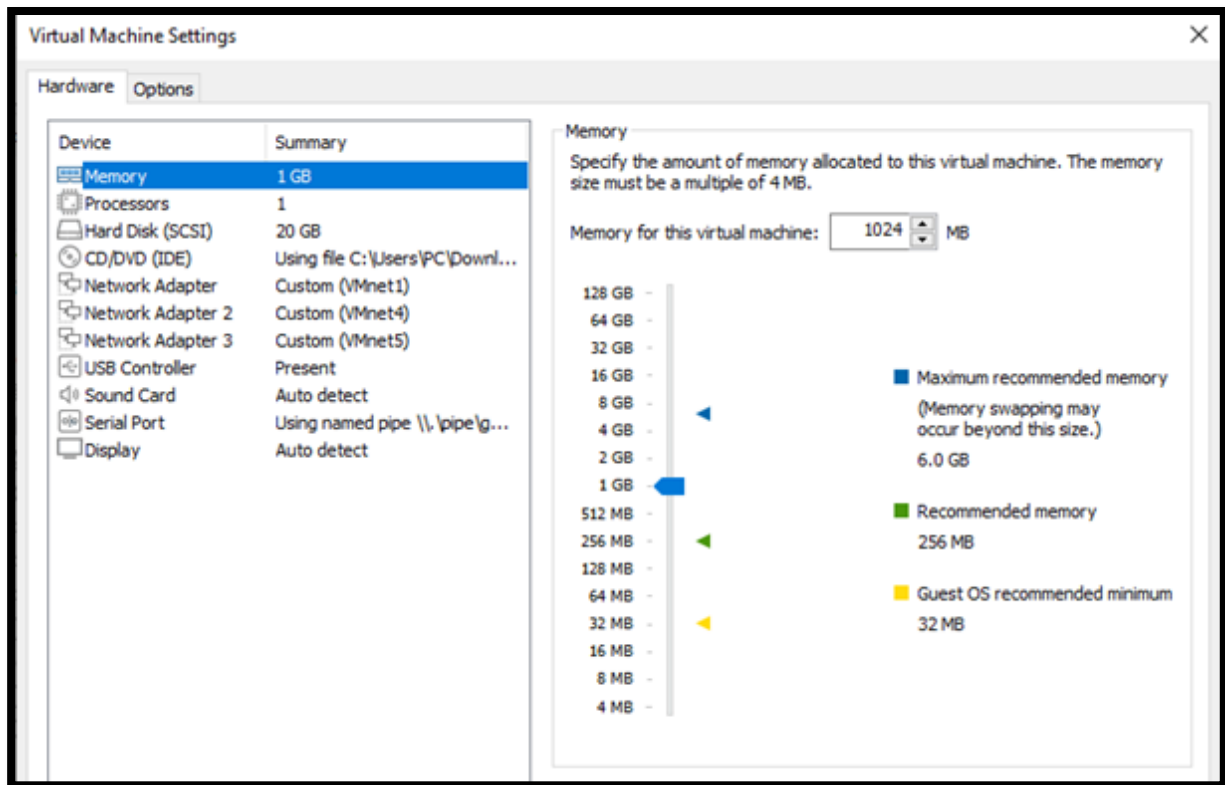
```
interface GigabitEthernet2/2
  no switchport
  ip address 10.1.90.1 255.255.255.0
  negotiation auto
!
```

```
interface GigabitEthernet3/3
  switchport trunk allowed vlan 10,20,30
  switchport trunk encapsulation dot1q
  switchport mode trunk
  media-type rj45
  negotiation auto
!
interface Vlan10
  ip address 10.1.10.1 255.255.255.0
!
interface Vlan20
  ip address 10.1.20.1 255.255.255.0
!
interface Vlan30
  ip address 10.1.30.1 255.255.255.0
!
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 10.1.90.2
!
.
```

4.2.5 Installation de Pfsense :

On crée une machine virtuelle sous VMware et on l'ajoute sur GNS3 pour la faire lier avec notre réseau DMZ et LAN ci-dessous une image de la configuration de Pfsense :



- ❖ Avant de commencer l'installation, notre machine doit avoir au minimum 3 cartes réseaux qui sont :
 - WAN (VMnet1) : pour se connecter à l'internet
 - LAN(VMnet 2) : passerelle du réseau locale
 - DMZ(VMnet 3) : passerelle du réseau DMZ

- ❖ Après l'installation de pfSense et l'attribution des adresse IP pour chaque interface, sauf l'interface WAN qui reçoit une adresse IP par le DHCP ci-joint une photo qui montre le pfsense après la configuration :

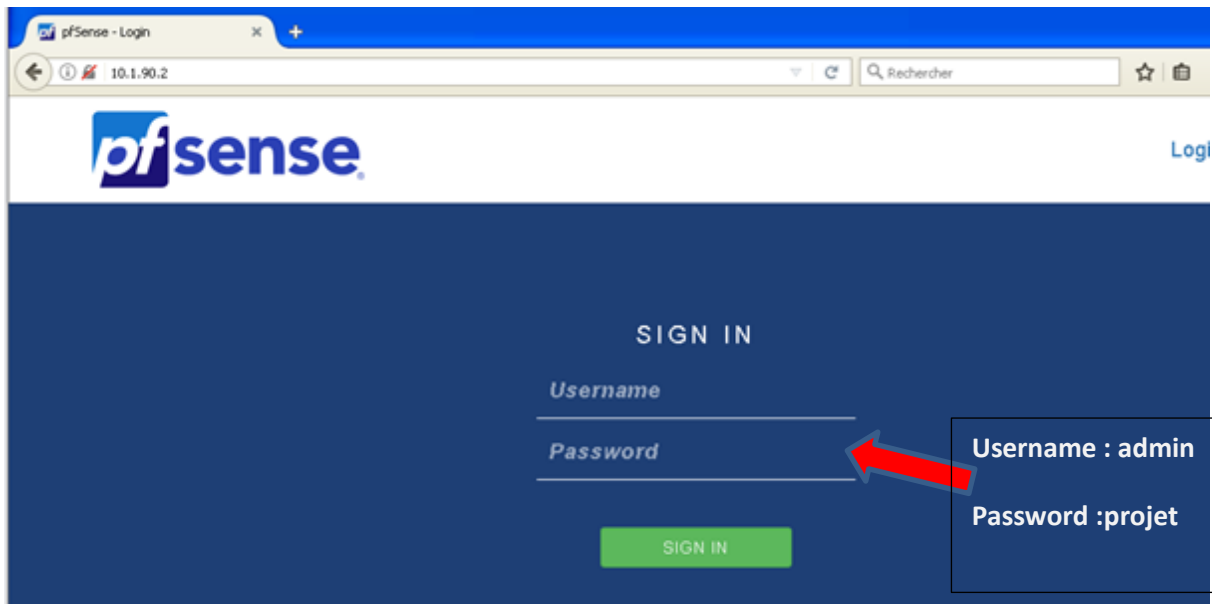
```
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.131/24
LAN (lan)      -> em1      -> v4: 10.1.90.2/24
SRU (opt1)     -> em2      -> v4: 10.1.100.1/24

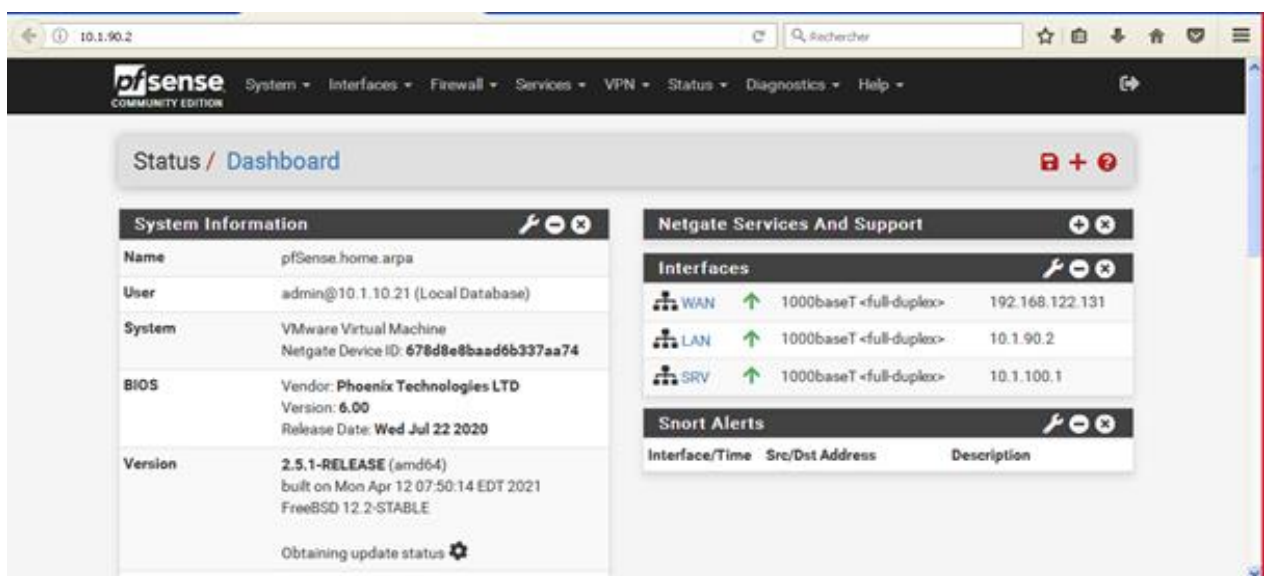
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

- ❖ Pour se connecter à l'interface web de configuration de pfsense on utilise l'adresse ip 10.1.90.2. Cette page s'affiche :



- ❖ Après l'authentification on aura cette interface :



4.2.6 Création de la zone DMZ (SRV) sur le pfsense :

General Configuration

Enable ☒ Enable interface

Description

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

4.2.7 Création des alias pour les VLANS :

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description
A description may be entered here for administrative reference (not parsed).

Type

Network(s)

Hint Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN				
<input type="text" value="10.1.10.0"/>	/	<input type="text" value="24"/>	<input type="text" value="Vlan10"/>	Delete
<input type="text" value="10.1.20.0"/>	/	<input type="text" value="24"/>	<input type="text" value="Vlan20"/>	Delete
<input type="text" value="10.1.30.0"/>	/	<input type="text" value="24"/>	<input type="text" value="Vlan30"/>	Delete

4.2.8 Création d'une route :

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

- ❖ Après la création de la route on a ajouté la route comme une route statique :

System / Routing / Static Routes / Edit

Edit Route Entry

Destination network
Destination network for this static route

Gateway
Choose which gateway this route applies to or add a new one from the list

Disabled ☐ Disable this static route
Set this option to disable this static route without removing it from the configuration

Description
A description may be entered here for administrative reference (optional)

- ❖ Et on a ajouté une règle de filtrage qui va laisser passer le LAN vers le pfSense comme le montre l'image ci-dessous :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	vlangs_	*	*	*	*	none
				internes					

4.2.9 Création de la machine virtuelle serveur 2012 :

- ❖ Après la création du serveur on attribue une adresse manuellement pour la carte réseau :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

4.2.10 Ajouter des règles de filtrage :

- ❖ On a ajouté des règles de filtrage pour notre réseau dans les différentes zones.
- ❖ Dans la zone LAN :

Floating

WAN

LAN

SRV

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2 / 2.68 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 *	WAN net	*	LAN net	*	*	none			
<input type="checkbox"/>	✓ 2 / 2.45 MiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	vlangs_internes	*	*	*	*	none			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

- ❖ Dans la zone DMZ :

FloatingWANLANSRV

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✓</div><div>0 / 0 B</div></div>	IPv4 *	LAN net	*	SRV net	*	*	none			<div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0 / 0 B</div></div>	IPv4 *	WAN net	*	SRV net	*	*	none			<div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div>
<input type="checkbox"/>	<div><div>✗</div><div>0 / 480 B</div></div>	IPv4 *	SRV net	*	LAN net	*	*	none			<div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div></div>

4.2.11 La sauvegarde de la configuration réseau :

Pour la sauvegarde de la configuration réseau on a décidé d'installer un serveur TFTP qui est un protocole de transfert de fichiers il fonctionne en UDP sur le port 69. On a installé le serveur dans zone DMZ.

Après l'installation, on a utilisé une commande sur le switch pour faire le transfert de fichier de configuration vers le serveur.

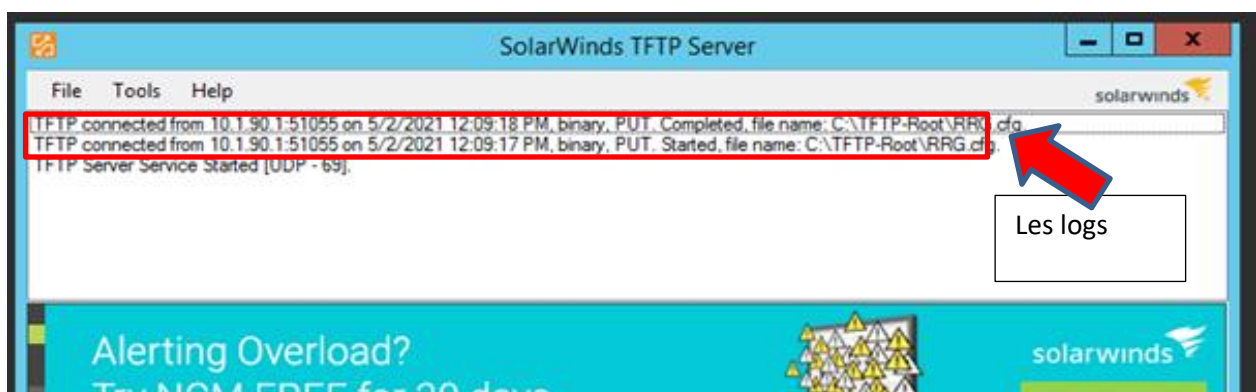
```
RG#ping 10.1.100.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.100.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/39 ms
RG#copy run tftp://10.1.100.10/RRG.cfg
Address or name of remote host [10.1.100.10]?
Destination filename [RRG.cfg]?

-Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8E76A0z 8E
760Ez 7E4E93z 108617Bz 10879ADz F7080Dz F6DFB6z F6D9EEz - Process "Spanning Tree", CPU
hog, PC 0x008FD5B5

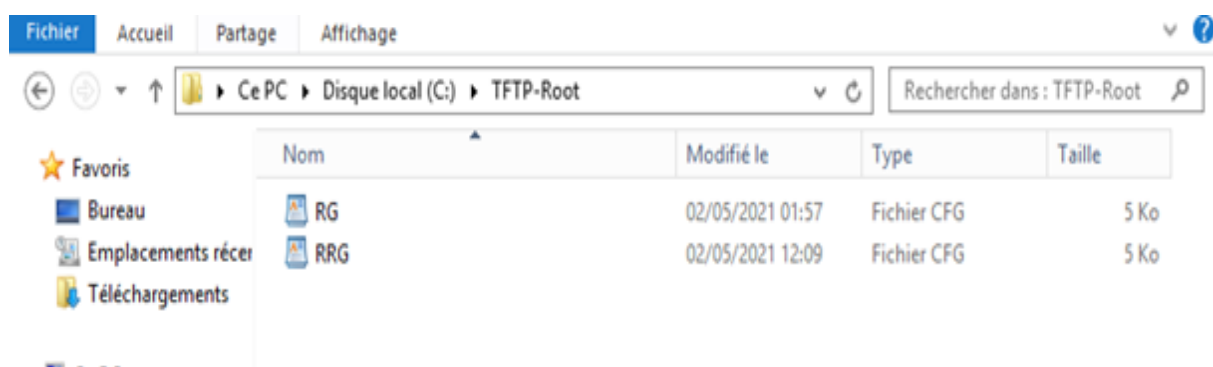
*May  2 09:48:11.598: %SYS-3-CPUHOG: Task is running for (1999)msecs, more than (2000)m
secs (0/0),process = Spanning Tree!!
4421 bytes copied in 184.817 secs (24 bytes/sec)
RG#
-Traceback= 1DBB7C8z 8DBFE5z 90522Ez 904F50z 904D5Dz 900F45z 901B7Bz 901B0Fz 8E76A0z 8E
760Ez 8CE7DAz 7E4E93z 22B2F97z 22B1BC1z 22D2911z 22B98BFz - Process "IP Input", CPU hog
, PC 0x008FD5B5

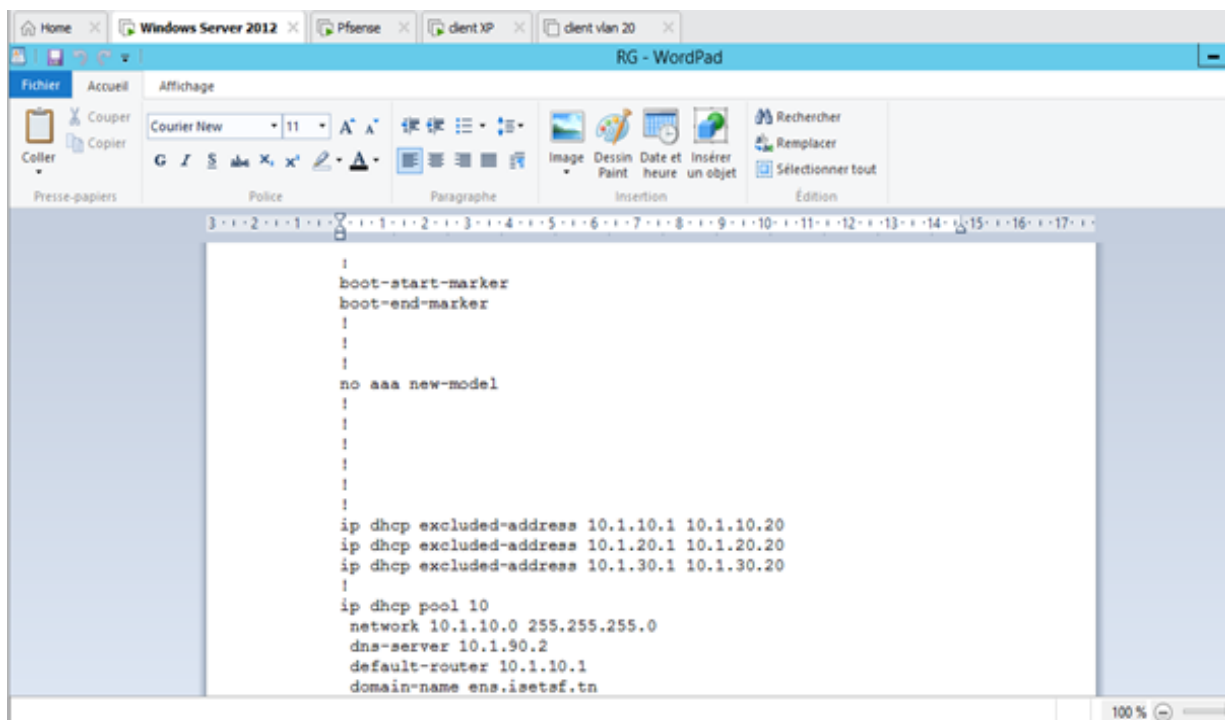
*May  2 09:49:05.942: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)m
secs (0/0),process = IP Input.
```

- ❖ Après l'exécution de la commande on remarque l'ajout de nouveaux logs sur le serveur



- ❖ On peut récupérer le fichier de configuration depuis son emplacement :

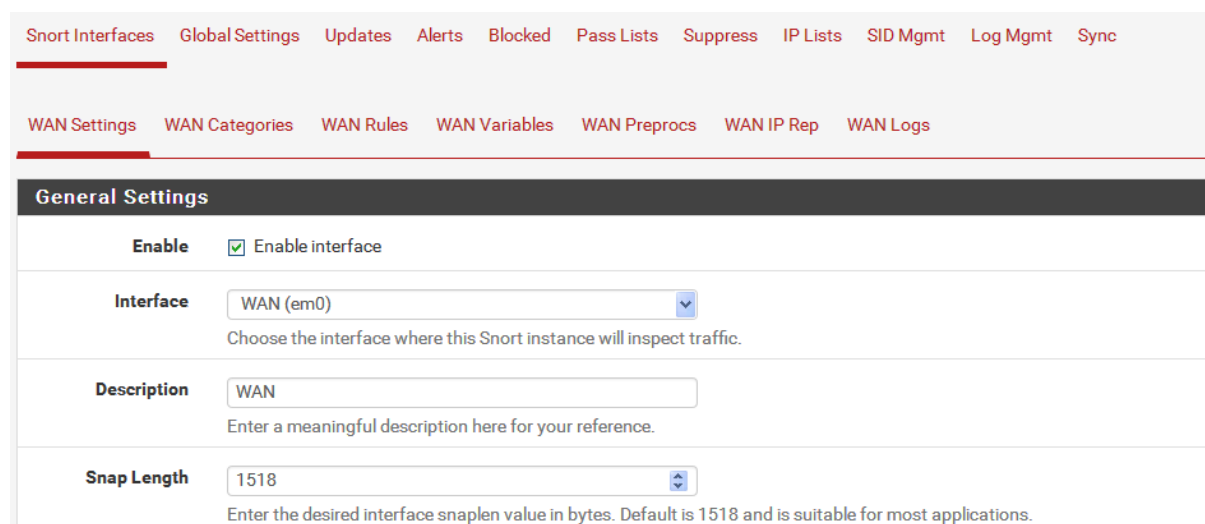




4.2.12 Mise en place d'un système de détection d'intrusion sur le pfsense :

On a choisi d'utiliser **snort** qui est un système de prévention des intrusions open source permettant d'utiliser une série de règle, aidant à définir une activité réseau malveillante et utilise ces règles pour trouver les paquets qui correspondent à eux et génère des alertes pour les utilisateurs.


Après l'installation de snort sur notre pfSense ci-joint des images qui illustre comment on l'a configuré :



Alert Settings	
Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	<div>LOG_AUTH</div> <div>Select system log Facility to use for reporting. Default is LOG_AUTH.</div>
System Log Priority	<div>LOG_ALERT</div> <div>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</div>
Enable Packet Captures	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	<div>128</div> <div>Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em02007 is rotated and a new file opened.</div>
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<div>Legacy Mode</div> <div>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</div> <div>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</div>
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<div>BOTH</div> <div>Select which IP extracted from the packet you wish to block. Default is BOTH.</div>

WAN Settings
 WAN Categories
 WAN Rules
 WAN Variables
 WAN Preprocs
 WAN IP Rep
 WAN Logs

Automatic Flowbit Resolution	
Resolve Flowbits	<input checked="" type="checkbox"/> If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked. Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.
Auto-Flowbit Rules	<div> View</div> <div>Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.</div>

Snort Subscriber IPS Policy Selection	
Use IPS Policy	<input checked="" type="checkbox"/> If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked. Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Balanced

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Select the rulesets (Categories) Snort will load at startup

▲ - Category is auto-enabled by SID Mgmt conf files

▲ - Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Enable

Ruleset: Snort GPLv2 Community Rules



Snort GPLv2 Community Rules (Talos certified)

Enable

Ruleset: ET Open Rules



emerging-activex.rules

Enable

Ruleset: Snort Text Rules



snort_app-detect.rules

Enable

Ruleset: Snort SO Rules



snort_browser-chrome.so.rules

Snort OPENAPPID rules are not enabled.

WAN Settings

WAN Categories

WAN Rules

WAN Variables

WAN Preprocs

WAN IP Rep

WAN Logs

Available Rule Categories

Category Selection:

Auto-Flowbit Rules

Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

Apply

Reset All

Reset Current

Disable All

Enable All

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Note: You should not disable flowbit rules! Add Suppress List entries for them instead by [clicking here](#).

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Snort / Interfaces ?

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (em0)		AC-BNFA	LEGACY MODE	WAN	

Add Delete

4.2.13 La configuration de honeypot :

Pour le honeypot on a choisi d'utiliser le logiciel **KFSensor** qui est un système avancé de pot de miel Windows qui fournit une détection améliorée des intrusions et des menaces internes à notre réseau, il est préconfiguré pour surveiller tous les ports TCP et UDP ainsi que ICMP, après l'avoir mis en place sur notre serveur on a cette interface-là qui s'affiche :



4.2.14 Configuration du portail captif :

Nous avons mis en place le portail captif sur pfsense pour le réseau LAN comme l'indique l'image ci-dessous :

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name
Zone name. Can only contain letters, digits, and underscores (.) and may not start with a digit.

Zone description
A description may be entered here for administrative reference (not parsed).

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

Interfaces

WAN
LAN
 SRV

Select the interface(s) to enable for captive portal.

Authentication Method

Use an Authentication backend

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor without displaying any login page.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically without displaying any login page.

Authentication Server

Local Database

You can add a remote authentication server in the [User Manager](#).
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Idle timeout (Minutes)

30

Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout (Minutes)

60

Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Concurrent user logins

Disabled

Disabled: Do not allow concurrent logins per username or voucher.
Multiple: No restrictions to the number of logins per username or voucher will be applied.
Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected.
First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.

MAC filtering

☒ Disable MAC filtering

If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Services / Captive Portal



Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
Captif_LAN	LAN	0	portail_captif_lan	

Add

- ❖ Dans le réseau LAN pour accéder à une page web il faut avoir un compte dans la base de données dans notre cas on a créé un compte avec le nom « user » :

System / User Manager / Users

Users Groups Settings Authentication Servers

Users				
	Username	Full name	Status	Groups
<input type="checkbox"/>	admin	System Administrator	✓	admins
<input type="checkbox"/>	user		✓	

+ Add Delete

- ❖ On a créé un groupe pour rattacher tous les comptes à ce groupe pour bénéficier des droits d'accès à internet :

Users Groups Settings Authentication Servers

Group Properties

Group name: GRP_captif

Scope: Local
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description: GRP_captif
Group description, for administrative information only

Group membership: admin (Not members), user (Members)

- ❖ Et on a ajouté un privilège dans ce groupe-là :

Assigned Privileges

Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	

+ Add

- ❖ On a configuré un certificat qu'on a partager avec les utilisateurs pour assurer la sécurité lors de leur connexion à internet comme l'indique les images ci-dessous :

System / Certificate Manager / CAs / Edit ?

[CAs](#)
[Certificates](#)
[Certificate Revocation](#)

Create / Edit CA

Descriptive name

Method

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Lifetime (days)

Common Name

The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

Organizational Unit

Save

System / Certificate Manager / CAs ?

[CAs](#)
[Certificates](#)
[Certificate Revocation](#)

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
portail_captif_lan	✓	self-signed	0	ST=France, OU=info, O=ynov, L=paris, CN=10.1.90.2, C=FR		
				Valid From: Mon, 03 May 2021 21:21:14 +0000		
				Valid Until: Thu, 01 May 2031 21:21:14 +0000		

CA's **Certificates** Certificate Revocation

Search

Search term
Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (60882034a7c43) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-60882034a7c43 Valid From: Tue, 27 Apr 2021 14:31:17 +0000 Valid Until: Mon, 30 May 2022 14:31:17 +0000		
Cert_Portail Server Certificate CA: No Server: Yes	portail_captif_lan	ST=France, OU=info, O=ynov, L=paris, CN=10.1.90.2, C=FR Valid From: Mon, 03 May 2021 21:25:52 +0000 Valid Until: Thu, 01 May 2031 21:25:52 +0000		

Add/Sign

- ❖ Après avoir créé le certificat on va changer la configuration du portail captif pour pouvoir ajouter le certificat qu'on a mise en place :

HTTPS Options

Login ☒ Enable HTTPS login
When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name
This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL/TLS Certificate
Certificates known to be incompatible with use for HTTPS are not included in this list. If no certificates are defined, one may be defined here: [System > Cert. Manager](#)

HTTPS Forwards ☐ Disable HTTPS Forwards
If this option is set, attempts to connect to HTTPS (SSL/TLS on port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

- ❖ Si on n'a pas installé le certificat sur la machine on peut pas avoir accès comme l'indique l'image :

Page de démarrage de Mozilla ... Connexion non sécurisée

https://www.google.com/search?q=youtube&ie=utf-8&oe=utf-8&client=firefox-b

La connexion n'est pas sécurisée

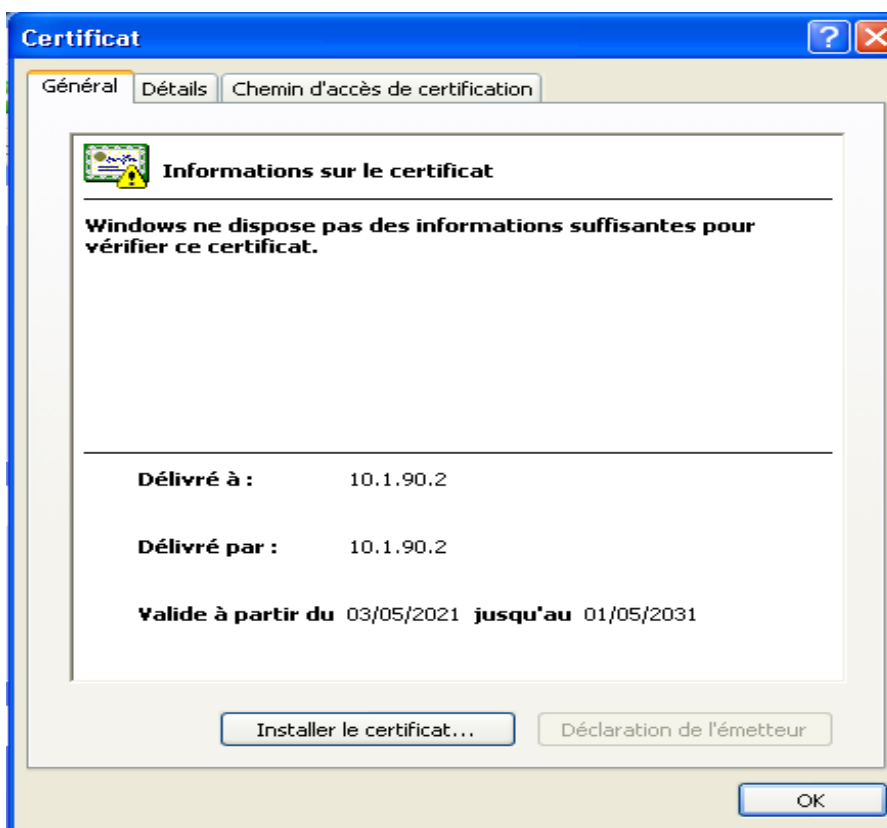
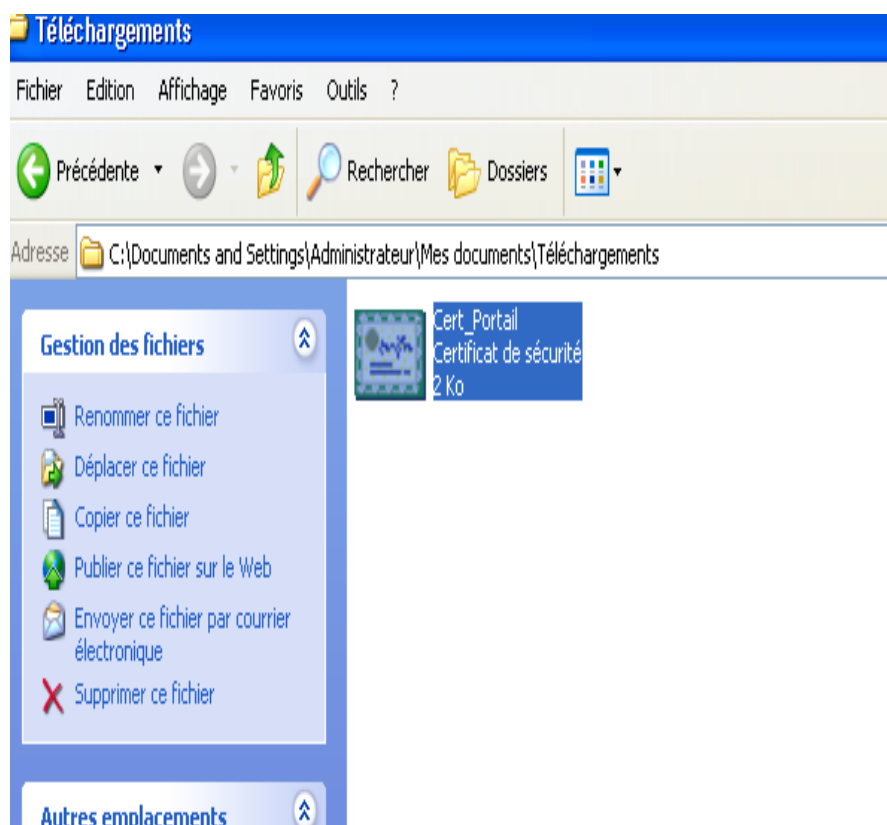
Les propriétaires de www.google.com ont mal configuré leur site web. Pour éviter que vos données ne soient dérobées, Firefox ne s'est pas connecté à ce site web.

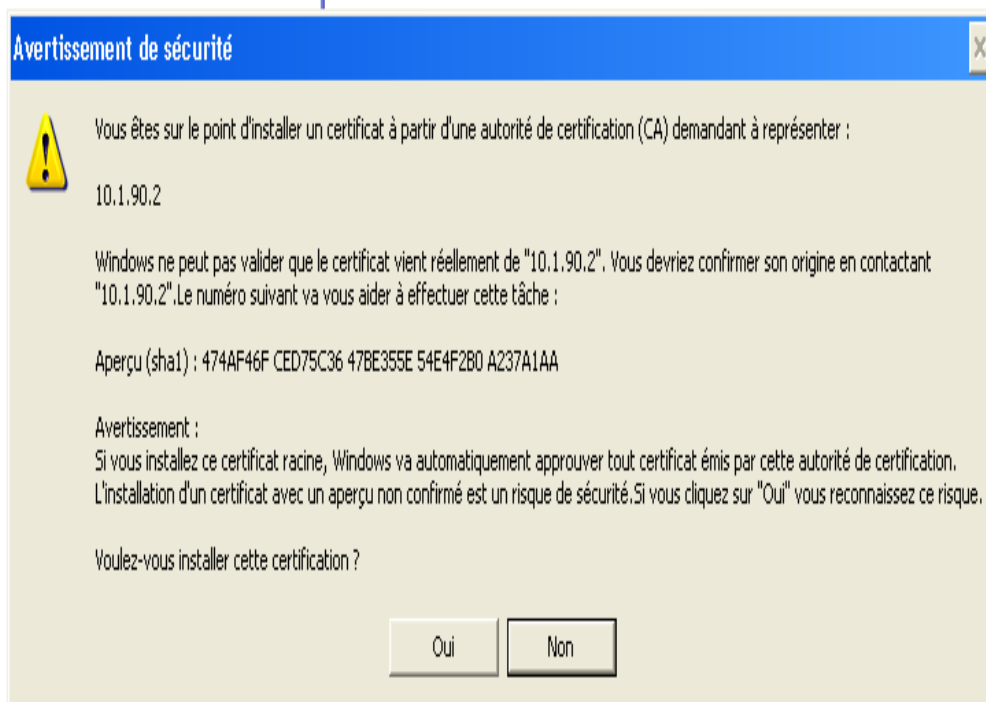
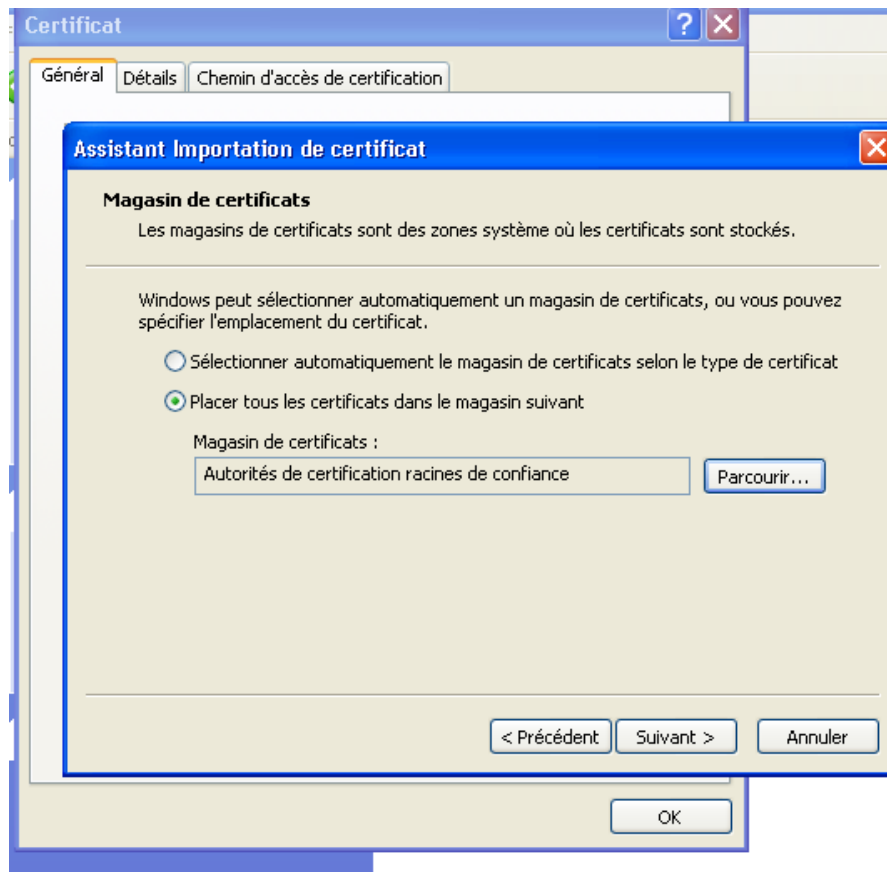
Ce site a recours à HTTP Strict Transport Security (HSTS) pour indiquer à Firefox de n'établir qu'une connexion sécurisée. Ainsi il n'est pas possible d'ajouter d'exception pour ce certificat.

[En savoir plus...](#)

☐ Signaler les erreurs similaires pour aider Mozilla à identifier et bloquer les sites malveillants

- ❖ Après téléchargement et installation du certificat sur la machine :





4.2.15 Configuration du SOC :

Le soc s'appuie sur plusieurs outils pour analyser des sources de logs et garantir une protection cyber plus efficace comme : firewall, ids/ips, web application firewall, anti-malware. Les logs collectés par le soc sont remontés dans le SIEM composé de plusieurs outils d'analyse dans notre cas l'outil qu'on a choisi c'est le snort .

The screenshot shows the 'Services / Snort / Alerts' interface. It includes a navigation bar with links like 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts' (selected), 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Below this is the 'Alert Log View Settings' section with options for 'Interface to Inspect' (set to WAN (em0)), 'Auto-refresh view' (unchecked), and 'Alert lines to display' (set to 250). There are 'Download' and 'Clear' buttons. The 'Alert Log View Filter' section is empty. The '8 Entries in Active Log' section contains a table with columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The first entry is dated 2021-05-04 11:18:35, with a priority of 3, protocol TCP, and a description 'ET INFO WinHttp AutoProxy Request'.

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2021-05-04 11:18:35	!	3	TCP	Generic Protocol Command	192.168.122.131	61617	185.62.136.67	80	1:2022913	ET INFO WinHttp AutoProxy Request

4.2.16 Configuration de la réduplication réseau :

4.2.16.1 Mise en place de la redondance sur pfsense :

NB : Dans ce cas de figure les adresse IP sont différentes car ayant configuré sur une carte réseau différentes pour résoudre le problème de ressource rencontré au niveau de nos PC

4.2.16.1.1 Configuration des cartes réseaux

❖ Pfsense A :

```
WAN (wan)      -> em0      -> v4: 192.168.1.181/24
LAN (lan)      -> em1      -> v4: 192.168.100.152/24
```

❖ Pfsense B :

```
browser:
http://192.168.100.153/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 3cacc009426ceccc433d

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.1.182/24
LAN (lan)      -> em1      -> v4: 192.168.100.153/24
```

4.2.16.1.2 Mise en place de notre VIP sur pfsense :

VIPA ou virtual internet protocol address. C'est une adresse IP qui n'est pas connectée à une interface physique. Afin de mettre en place la redondance, il faut que chaque serveur pfsense dispose d'une adresse IP sur l'interface LAN et WAN ce qui a été fait un peu plus haut ainsi qu'une adresse IP virtuelle qui va être partagée entre notre cluster.

Pour ce faire suivons les différentes étapes à savoir :

- ❖ Se rendre dans l'adresse IP virtuelle **"Firewall"** > **"Virtual IPs"** et on clique sur **"Add"**

Les éléments de configurations sont les suivants :

- **Type** : Ici nous avons 4 possibilités :
 - o **IP Alias**
 - o **CARP**
 - o **Proxy ARP**
 - o **Other**

Dans notre cas nous choisirons **CARP** qui est spécialement utilisé pour le clustering.

- **Interface** : l'interface sur laquelle la VIP doit être configurée. Nous configurons la première sur l'interface Wan, puis la seconde sur l'interface LAN.
- **Address(es)** : l'adresse IP et le masque du subnet de l'interface.
- **Virtual IP password** : mot de passe permettant de sécuriser les échanges au sein du groupe d'hôtes se partageant la VIP. Ce mot de passe devra être re-saisie sur les pfsenseB (secondaire).
- **VHID Group** : virtual host identifier. Un serveur peut faire partir de plusieurs groupes de VIP. Afin d'identifier chaque groupe, un ID unique lui est assigné.
- **Advertising Frequency** : la valeur de champs "Skew" à 0 désigne le master (pfsense primaire). Une valeur plus élevée désigne l'esclave (pfsense secondaire). La valeur de "Base" correspond au timeout en seconde au bout duquel l'hôte sera considéré comme étant inaccessible.

4.2.16.1.3 Configuration sur PfsenseA :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☒ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: WAN

Address type: Single address

Address(es): 192.168.100.120 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: Enter the VHID group password. Confirm

VHID Group: 1

Enter the VHID group that the machines will share.

Advertising frequency: Base 1 Skew 0

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: CLUSTER WAN

A description may be entered here for administrative reference (not parsed).

Save

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: WAN

Address type: Single address

Address(es): 192.168.100.120 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password: Enter the VHID group password. Confirm

VHID Group: 2

Enter the VHID group that the machines will share.

Advertising frequency: Base 1 Skew 0

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: CLUSTER LAN

A description may be entered here for administrative reference (not parsed).

Save

4.2.16.1.4 Configuration sur pfsenseB :

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☒ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: LAN

Address type: Single address

Address(es): 192.168.100.120 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password:

Enter the VHID group password. Confirm

VHID Group: 2

Enter the VHID group that the machines will share.

Advertising frequency: 1 2

Base Skew

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: CLUSTER LAN

A description may be entered here for administrative reference (not parsed).

Save

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: WAN

Address type: Single address

Address(es): 192.168.1.120 / 24

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password:

Enter the VHID group password. Confirm

VHID Group: 1

Enter the VHID group that the machines will share.

Advertising frequency: 1 2

Base Skew

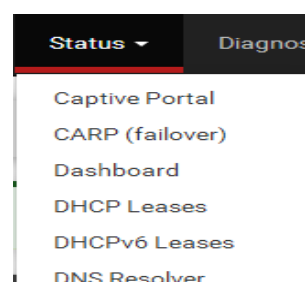
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: CLUSTER WAN

A description may be entered here for administrative reference (not parsed).

Save

Pour vérifier que tout fonctionne bien, rendons-nous dans "status" > "failover"

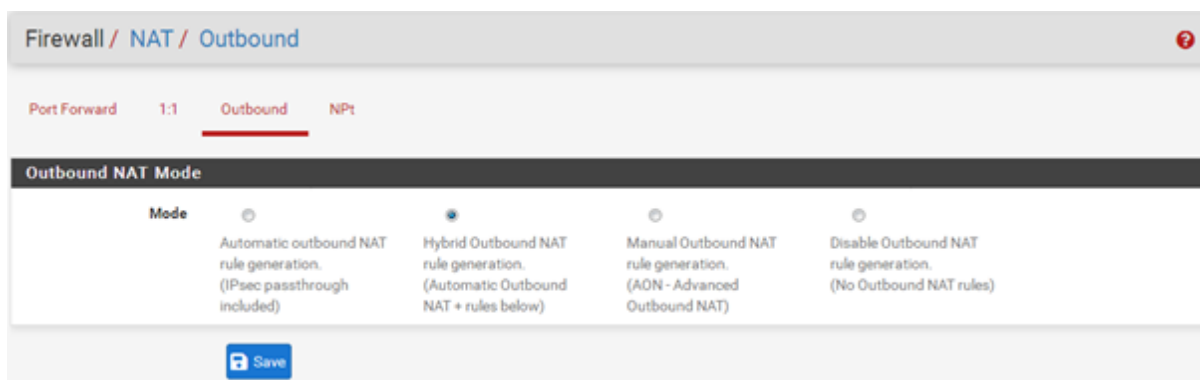


Les adresses VIP sont déclarées, mais non utilisées. Il reste à configurer pfsense pour qu'il utilise les adresses VIP plutôt que les adresses IP attribuées à ses interfaces logiques.

Pour cela, nous devons configurer pfsense pour qu'il utilise l'adresse VIP WAN sur le trafic sortant, l'adresse VIP LAN pour le trafic entrant et configurer les différents services pour qu'ils travaillent avec l'adresse VIP LAN comme adresse par défaut (pour les configurations OpenVPN ou DHCP, par exemple).

4.2.16.1.5 Configuration du NAT :

Rendons-nous dans l'ongle "firewall" > "NAT" et ensuite on clique sur "Outbound", on sélectionne « **Hybrid Outbound NAT rule generation.** »



Le RPC est un protocole qui permet la réplication des données d'un serveur à un autre. Dans pfsense il est utilisé pour recopier la configuration du serveur primaire vers le serveur secondaire.



❖ Maintenant il ne nous reste plus qu'à configurer la Haute disponibilité.

Pour cela se rendre dans "System" > "High Avail. Sync"



Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
 Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
 XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
 Enter the webConfigurator username of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password Confirm
 Enter the webConfigurator password of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin ☐ synchronize admin accounts and autoupdate sync password.
 By default, the admin account does not synchronize, and each node may have a different admin password.
 This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ WoL Server settings
- ☒ Static Route configuration

❖ Après configuration des règles sur le LAN (pfsenseA) :

Firewall / Rules / LAN											
Floating WAN LAN											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 / 5.05 MiB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	⚙️
✓	6 / 2.68 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌✎🗑️
✓	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌✎🗑️

❖ Vérifions dès à présent que ces règles ont été répliquées sur le LAN de notre pfsenseB ce qui est bien le cas :

Firewall / Rules / LAN											
Floating WAN LAN											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 / 1.50 MiB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	⚙️
✓	0 / 197 KB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌✎🗑️
✓	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌✎🗑️

- ❖ Autorisons maintenant le protocole XML RPC entre nos deux firewalls. Pour cela, on doit se rendre dans “firewall” puis “Rules”

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match LAN net Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match This firewall (self) Destination Address /

Destination Port Range HTTPS (443) HTTPS (443)
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

- ❖ La nouvelle règle a bien été prise en compte :

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

Floating WAN **LAN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 5.13 MB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 PFSYNC	LAN net	*	This Firewall	*	*	none		Autoriser PFSync	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Autoriser XML RPC	
<input checked="" type="checkbox"/>	4 / 2.71 MB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

❖ Vérifions maintenant que nos règles ont été prise en compte sur le pfsenseB :

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2/5.13 MB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	⚙️
✓	0/0 B	IPv4 PFSYNC	LAN net	*	This Firewall	*	*	none		Autoriser PFSync	📌🔗🔄🗑️
✓	0/0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Autoriser XML RPC	📌🔗🔄🗑️
✓	4/2.71 MB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	📌🔗🔄🗑️
✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌🔗🔄🗑️

✓ Le résultat obtenu nous confirme que le pfsenseA à bien été répliqué sur le pfsenseB.

4.2.16.2 La configuration de la redondance sur les switches :

La solution aux problèmes de boucles est **STP**, qui signifie **Spanning Tree Protocol**. C'est lui qui a en charge de gérer les chemins physiques vers les segments de réseau. Il fournit la redondance du chemin physique tout en empêchant les boucles dans le réseau. Par défaut, STP est activé sur les switches Cisco.

Les équipements de couche 2, comme les switches, n'ont pas de mécanisme permettant d'éliminer des trames qui tourne en boucle. Contrairement aux équipements de couche 3 comme des routeurs, qui eux, ont un mécanisme qui se nomme TTL pour Time to live, pour limiter la durée de vie d'un paquet.

Sans protocole pour gérer les boucles, les switches retransmettront le trafic indéfiniment, c'est pourquoi le protocole STP a été développé.

4.2.16.3 La configuration de la redondance sur les serveurs :

Tout d'abord entrons l'adresse IP de notre second serveur dans le serveur principal comme l'indique l'image suivant :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) ✕

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 10 . 1 . 100 . 10

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 10 . 1 . 100 . 1

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 10 . 1 . 100 . 10

Serveur DNS auxiliaire : 10 . 1 . 100 . 13

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Maintenant rentrons l'adresse IP du serveur principal dans le serveur secondaire :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) [X]

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 10 . 1 . 100 . 13

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 10 . 1 . 100 . 1

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 10 . 1 . 100 . 13

Serveur DNS auxiliaire : 10 . 1 . 100 . 10

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

Sur la machine client on entre l'adresse IP du second serveur :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) [?] [X]

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 10 . 1 . 100 . 11

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 10 . 1 . 100 . 1

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 10 . 1 . 100 . 10

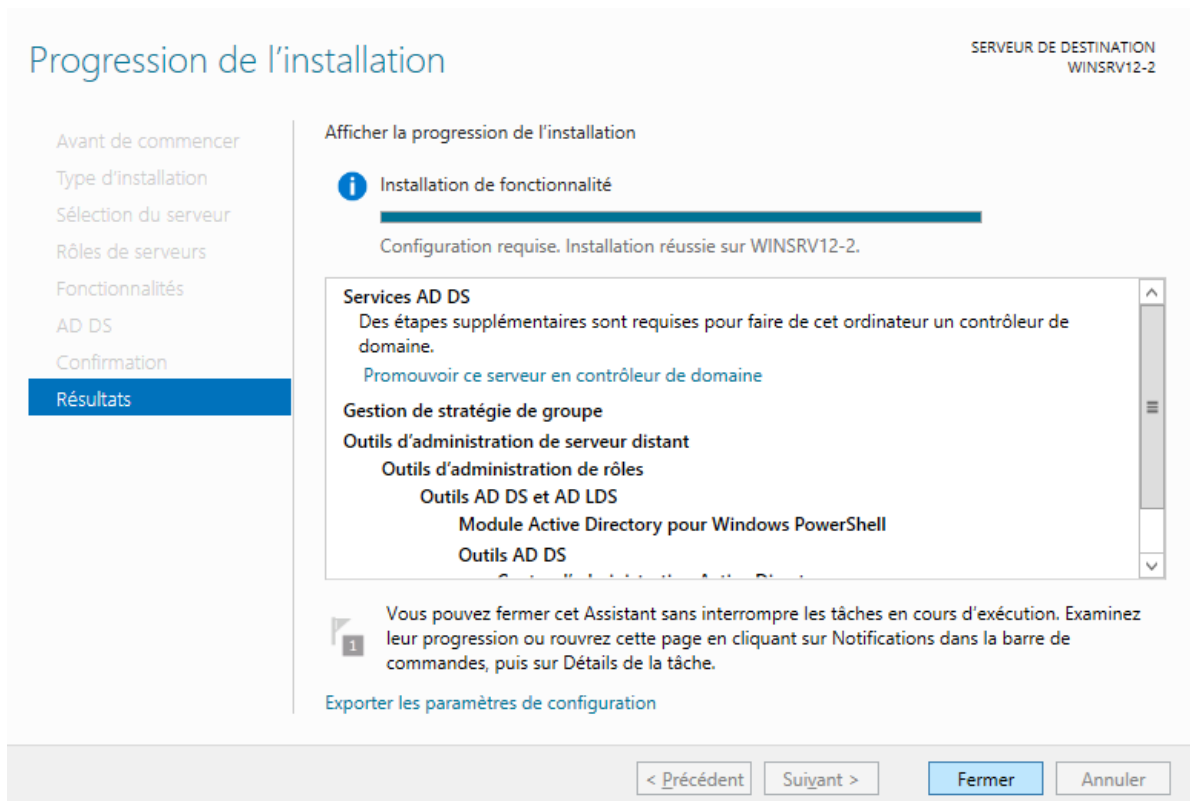
Serveur DNS auxiliaire : 10 . 1 . 100 . 13

☐ Valider les paramètres en quittant

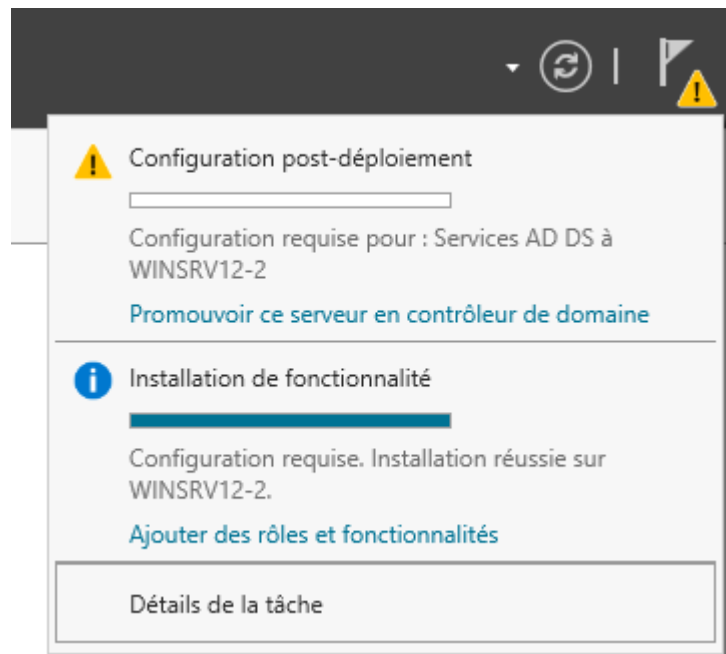
Avancé...

OK Annuler

Sur notre second contrôleur de domaine, ajoutons un nouveau rôle (**Active directory**) :



Ensuite on va promouvoir le serveur :



Puis nous le rajoutons à un domaine existant dans notre cas **ynov.fr** :

Configuration de déploiement

SERVEUR CIBLE
WINSRV12-2

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

☒ Ajouter un contrôleur de domaine à un domaine existant

☐ Ajouter un nouveau domaine à une forêt existante

☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine : ynov.fr Sélectionner...

Fournir les informations d'identification pour effectuer cette opération

<Aucune information d'identification fournie> Modifier...

Sélectionnez un domaine dans la forêt où le nouveau contrôleur de domaine résidera.

ynov.fr

OK
Annuler

Ensuite on décoche catalogue global :

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)

☐ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site : Default-First-Site-Name ▼

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe : *

Confirmer le mot de passe : *

Ensuite on réplique depuis le catalogue global d'**ynov.fr** :

Options supplémentaires

- Configuration de déploie...
- Options du contrôleur de...
- Options DNS
- Options supplémentaires**
- Chemins d'accès
- Examiner les options
- Vérification de la configur...
- Installation
- Résultats

SERVEUR CIBLE
WINSRV12-2

Spécifier les options d'installation à partir du support (IFM)

☐ Installation à partir du support

Spécifier des options de réplication supplémentaires

Répliquer depuis :

WINSRV12.ynov.fr	▼
Tout contrôleur de domaine	
WINSRV12.ynov.fr	