Documentation UF infrastructure réseaux
Projet 2

Ynov Campus

Victor-Emmanuel Sedaros

Samy Lacombe

SOMMAIRE

ynov CAMPUS

Problématique

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

- De préférence Open Source
- Redondance des équipements et élimination des SPOF
- Services à mettre en place (portail captif, firewall, DHCP,etc.)
- Gestion de zones réseau (sécurisé/non sécurisé, connecté à internet /isolé)
- Gérer les ressources des machines (Benchmarking).

ynov CAMPUS

Services déployés

- DHCP (Dynamic Host Configuration Protocol)
  Protocole réseau qui assure la configuration automatique des paramètre IP d'une machine.

- FIREWALL
  Un firewall permet la gestion des flux entrant et sortant du réseau.

- FAILOVER
  Permet de basculer automatiquement vers un système alternatif en cas de panne.

- PORTAIL CAPTIF
  Permet aux clients wifi de passer par une page web spécial afin de s'authentifier avant d'accéder au réseau.

- NPS RADIUS
  Permet d'authentifier les utilisateurs via clé WPA2 en se basant sur des comptes AD.

- HONEYPOT
  Méthode de défense active qui consiste à attirer, sur des ressources : serveur, programme, service, etc. des adversaires déclarés ou potentiels afin de les identifier

- HIDS
  Système de détection d'intrusion basé sur l'hôte est un système de détection d'intrusion qui est capable de surveiller et d'analyser les composants internes d'un système informatique

Bonnes pratiques à adopter

Pour garantir une certaine sécurité dans notre infrastructure, il faut mettre en place une politique de bonnes pratiques.

Tous les utilisateurs bénéficieront d'un compte user lier à un object user Active Directory du contrôleur de domaine, ainsi aucun utilisateur ne sera admin local de sa machine.

Ces comptes users seront administrés par le service informatique, les politiques liés à la gestion des droits et de contenu seront appliqués via des stratégies de groupes > GPO (Group Policies Object).

Le service informatique sera le seul à pouvoir accéder au serveur AD DS via des comptes admins du domaine dédiés (chaque administrateur possède un compte admin ainsi qu'un compte user).

L'ensemble des donnés de l'entreprise y compris la documentation IT doit être accessible uniquement via les comptes users.

Les comptes users possèdent le strict minimum en termes d'attributions de droits (ACL), chaque modification de ces attributions doivent-être validé par le SI.

Les comptes admins (domaine et locaux) ne doivent être utilisés que pour des actions d'administration et aucune donnés liés aux documentation IT ne doivent être accessible via ces comptes.

Mettre en place des firewalls afin de filtrer les échanges de flux, interdire les échanges inter VLANs Users (Wifi et Eth), n'autoriser que des flux initiés depuis les VLANs Users vers le VLAN serveur, de plus le service proxy doit être configurer sur le FW afin de mieux limiter les échanges vers le WAN (cf schéma de la topologie réseau ci-dessous).

Chaque poste et serveur de l'organisme doit faire partie du domaine local créer par le Contrôleur de Domaine.

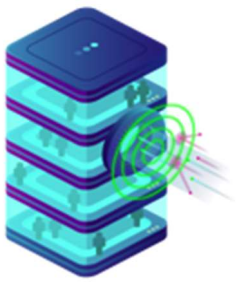
Le FileServeur doit être paramétré avec les attributions de droits (ACL) sur chaque folder afin de limiter l'accès des services à l'ensemble des données. Chaque membre des services ne doit accéder qu'aux informations dédiés à son service.

Vu que nous utilisons des équipements électriques, le risque de surchauffe/incendie reste présent. Une bonne ventilation des machines est à mettre en place, pour éviter tout danger,

Et mettre à disposition des extincteurs en cas de feu.

Un Backup à intervalle régulier (tous les soir à 23h par exemple) devra être mis en place sur un NAS distant du site (peut être hébergé par un service Cloud).

ynov CAMPUS



Recherche et choix des technologies

Après plusieurs recherches, nous avons fait le choix d'utilisé une solution Open source PFSENSE pour le choix du premier firewall avec 3 interfaces (1 pour l'accès au WAN, 1 pour la DMZ puis 1 pour le LAN).

PSENSE nous permet aussi de déployer des services comme le portail captif, DHCP, mise en place de la DMZ, et autres encore.

Cette solution possède une couche logique permettant un meilleur rendu visuel et un meilleur suivi des paramétrages de l'équipement.

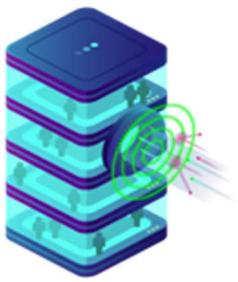
Grâce à la webUI elle est facile à prendre en main et plus agréable à utiliser.

Nous avons fait le choix d'utiliser des routeurs Cisco C3725 pour comme équipement afin d'administrer nos sous-réseaux.

Nous avions aussi trouvé une solution payante plus optimale, FortiGate, n'étant pas open source, nous avons dû laisser cette idée de côté.

Pour la partie Honeypot (méthode de défense active qui consiste à attirer, sur des ressources : serveur, programme, service, etc. des adversaires déclarés ou potentiels afin de les identifier), nous avons choisi l'outil PentBox de la distribution Kali Linux, facile à mettre en place et open Source.

En ce qui concerne le systèmes HIDS, nous avons opté pour la solution OSSEC est un système de détection d'intrusion gratuit et open source basée sur l'hôte. Il effectue l'analyse des journaux, la vérification de l'intégrité, la surveillance du registre Windows, la détection des rootkits, les alertes en fonction du temps et la réponse active.



Documentation d'architecture

Définition des Réseaux

Pour cette architecture, nous avons choisis de mettre en place 3 zones distinctes

- Pour le LAN, les flux sont gérés par le proxy de pfSense, seuls les flux initiés du LAN vers internet ainsi que la DMZ sont autorisés, un portail captif est déployé au niveau de pfSense pour les client WIFI voulant accéder au WAN.

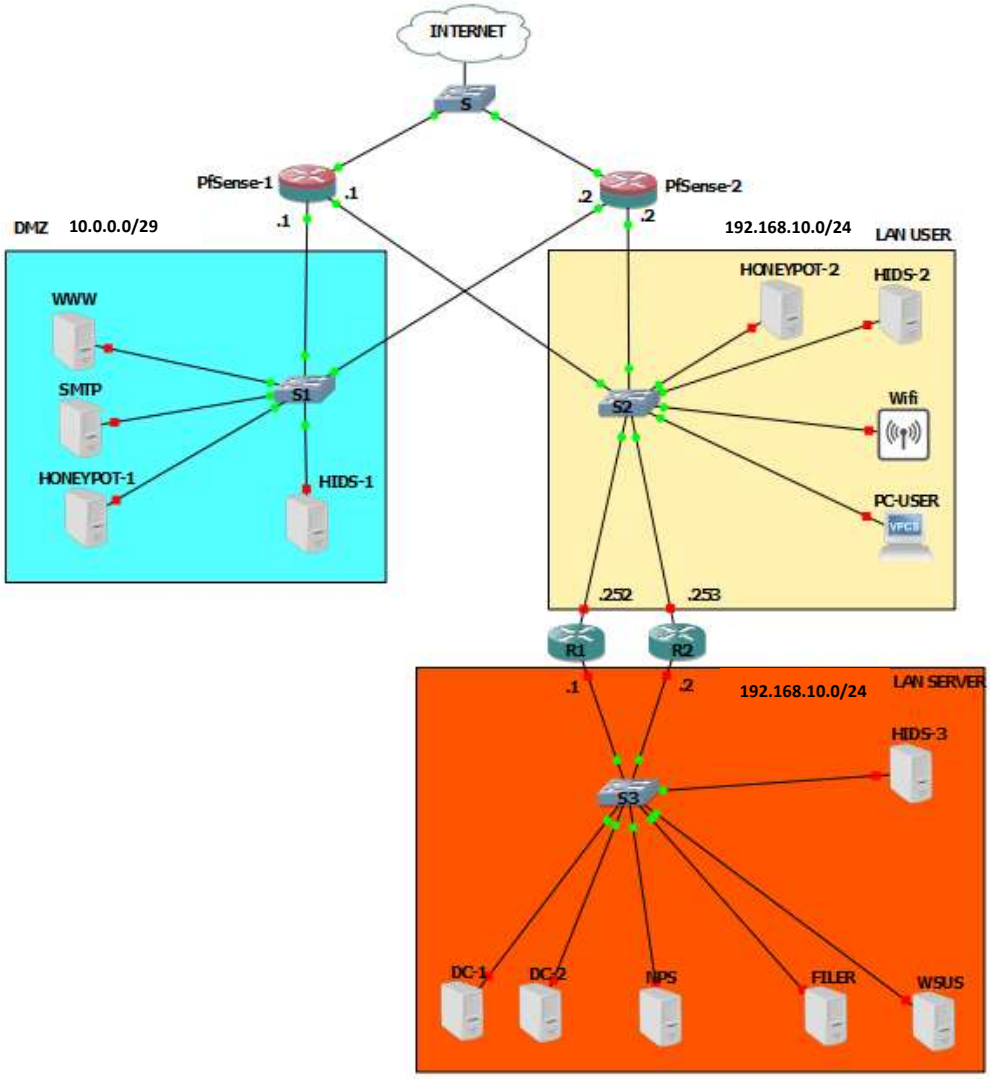
  - Un LAN USER, qui regroupera tous les hôtes user, le modem Wifi, ainsi que plusieurs systèmes de détection d'intrusion que l'on mettra en place avec des honeypots et HIDS afin de détecter si une personne a réussi à passer outre la DMZ.

  - Un LAN SERVEUR, où tous nos serveurs d'infrastructure (AD DS, WSUS, FILER, etc.) seront mis en place, un serveur NPS en tant que proxy radius (pour l'authentification au réseaux WIFI des user en WPA2), ainsi que les systèmes de détection d'intrusion. Ce LAN n'aura pas d'accès direct vers le WAN les flux seront gérer selon le besoin et proxyfiés.

  - Une DMZ, ou seront situé les services susceptibles d'être accédés depuis internet, t'elle qu'un serveur WEB, un serveur SMTP, un DNS.
    La DMZ, zone démilitarisée est un sous-réseau isolé du LAN et d'internet par un pare-feu, Pfsense dans notre cas. Dans notre DMZ, certaines machines sont susceptibles d'être accédées depuis internet, mais n'ont pas besoin d'accéder au LAN, c'est pourquoi nous avons bloqué les flux initiés depuis la DMZ vers notre LAN, ainsi que les flux initiés de la DMZ vers internet. Tous les flux d'internet sont redirigés vers la DMZ pour garantir une certaine sécurité. Cela permettra en cas d'attaque, d'isolé le pirate dans la DMZ, il n'aura donc accès qu'aux machines dans ce réseau et n'aura pas d'accès au LAN. Nous avons aussi installé un honeypot dans la DMZ sur le port 22 pour le service SSH et 80 pour http, afin de détecter toutes intrusions malveillantes.

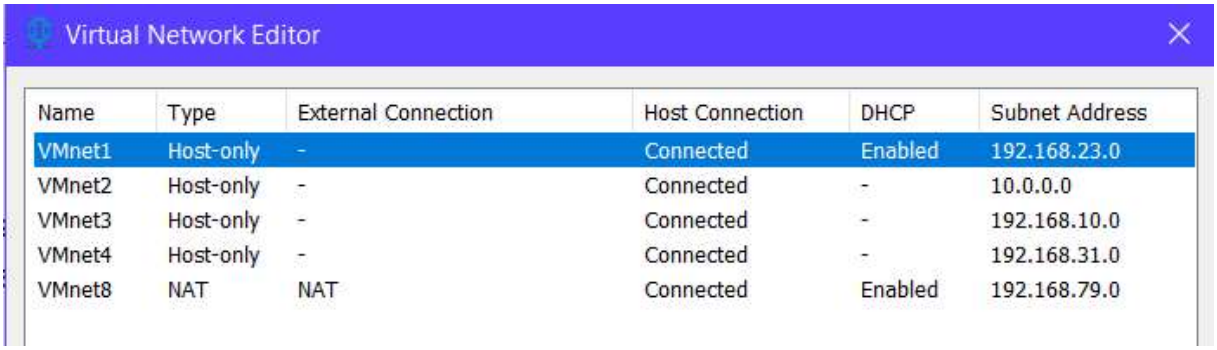
ynov CAMPUS

Architecture réseaux (GNS3)



Configurations

Tout d'abord, nous avons tout d'abord créé de nouvelles cartes réseaux virtuels afin de délimiter nos différents sous-réseaux et de les affilier aux interfaces de nos machines dans Vmware.



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.23.0
VMnet2	Host-only	-	Connected	-	10.0.0.0
VMnet3	Host-only	-	Connected	-	192.168.10.0
VMnet4	Host-only	-	Connected	-	192.168.31.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.79.0

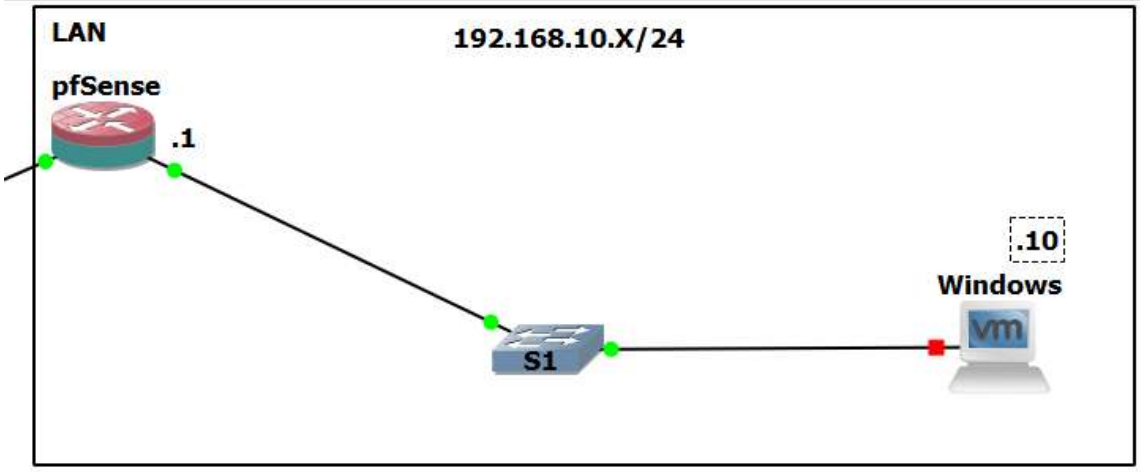
Une fois pfSense installé, nous pouvons déjà paramétrer les interfaces et effectuer quelques configurations via les commandes Shell.

Une adresse IP est assignée en DHCP pour le WAN.

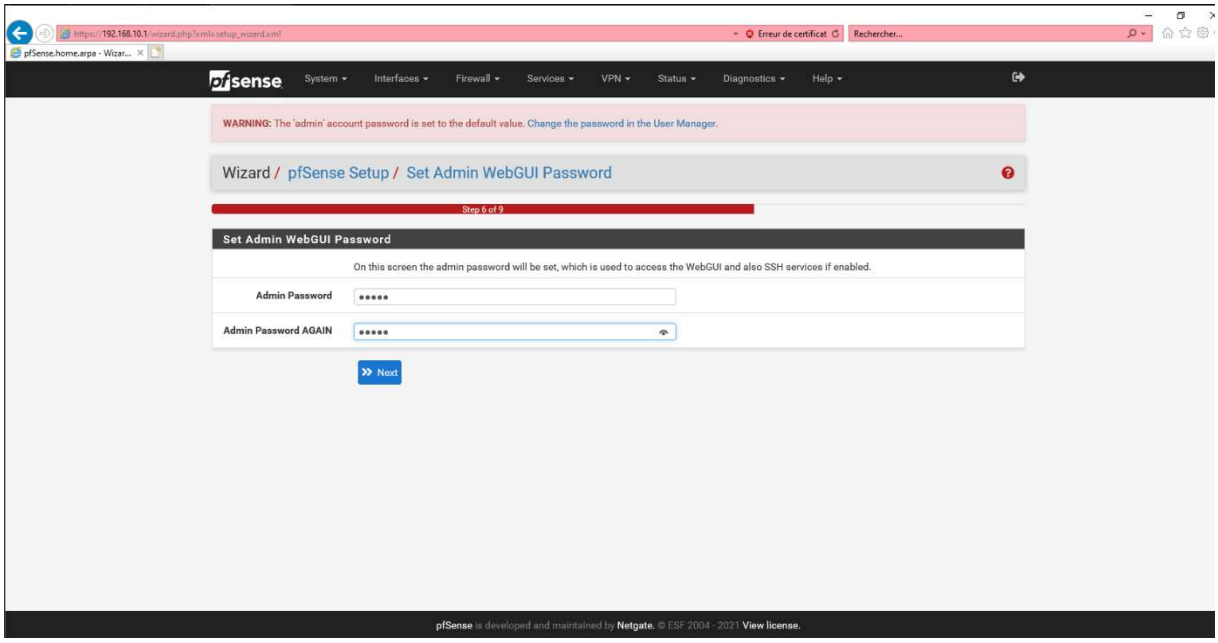
Nous paramétrons donc les deux interfaces voulues (DMZ et LAN) sur nos deux firewalls.

```
FreeBSD/amd64 (pfSense.ynov.local) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 54c6548e2f0ea42c9321

*** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.100/24
 LAN (lan)       -> em1        -> v4: 192.168.10.1/24
 DMZ (opt1)      -> em2        -> v4: 10.0.0.1/29

 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:
```

Nous installons donc un système d'exploitation (Windows en l'occurrence) avec interface graphique possédant une IP fixe dans le LAN afin de pouvoir accéder à l'interface web (gui)



Depuis le client Windows (192.168.10.10) nous accédons à l'interface d'administration du firewall via un navigateur web sur l'IP de l'interface LAN de pfSense (192.168.10.1)



Il est important de modifier le mot de passe admin d'administration de la console de gestion car le mot initial est un mot de passe générique (donc facile d'accès).

Configuration du cluster de 2 pfSense en failover.

Nous avons mis en place deux pfSense afin d'assurer la redondance réseau et l'élimination des SPOFS.

Ci-dessous les IP de chaque interface des deux équipements ainsi que leur IP virtuelle :

pfSense1 :

WAN : 192.168.1.100 - VIP : 192.168.1.102

LAN : 192.168.10.1 - VIP : 192.168.10.3

DMZ : 10.0.0.1 - VIP : 10.0.0.3

pfSense2 :

WAN : 192.168.1.101 - VIP : 192.168.1.102

LAN : 192.168.10.2 - VIP : 192.168.10.3

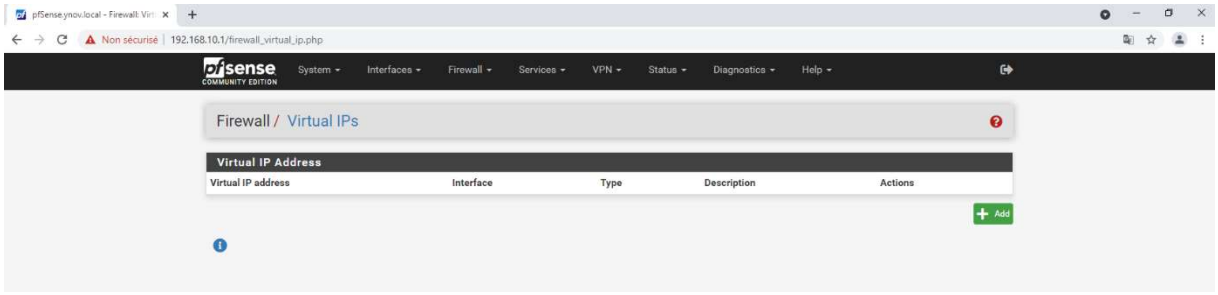
DMZ : 10.0.0.2 -VIP : 10.0.0.3

Nous utilisons deux protocoles présents dans Pfsense afin d'assurer le failover et la synchronisation des deux équipements.

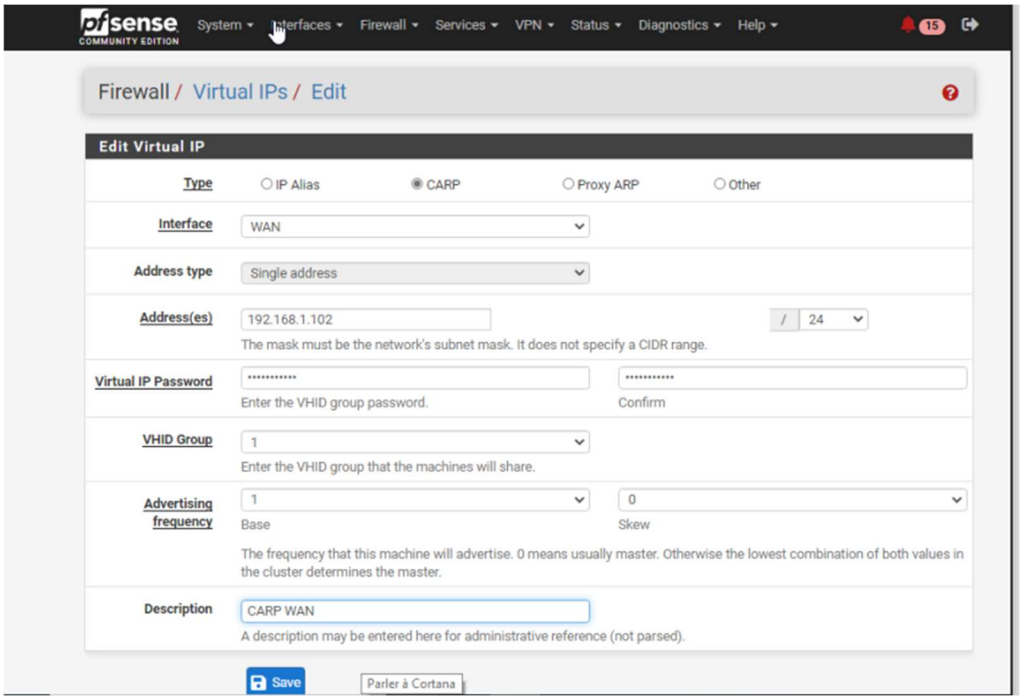
CARP (*Common Address Redundancy Protocol*) est un protocole permettant à plusieurs hôtes présents sur un même réseau de partager une adresse IP.

pfsync est un protocole permettant de synchroniser entre deux serveurs pfSense l'état des connexions en cours

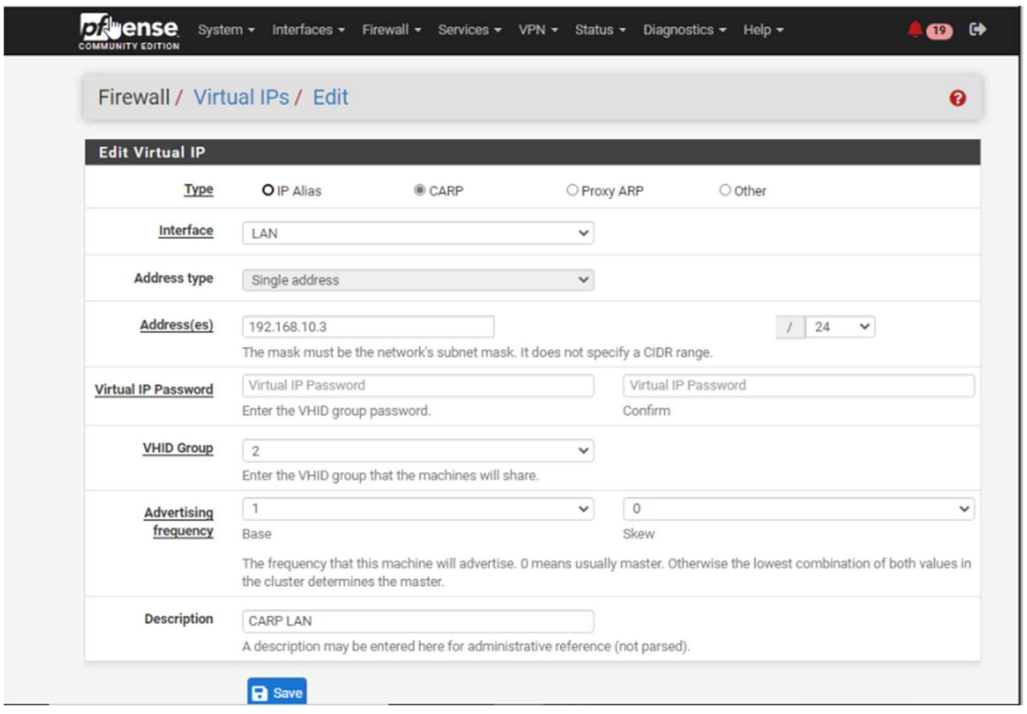
Dans la partie Firewall > Virtual IPs, on crée donc 3 IP virtuels pour chaque interface.



Interface **WAN**

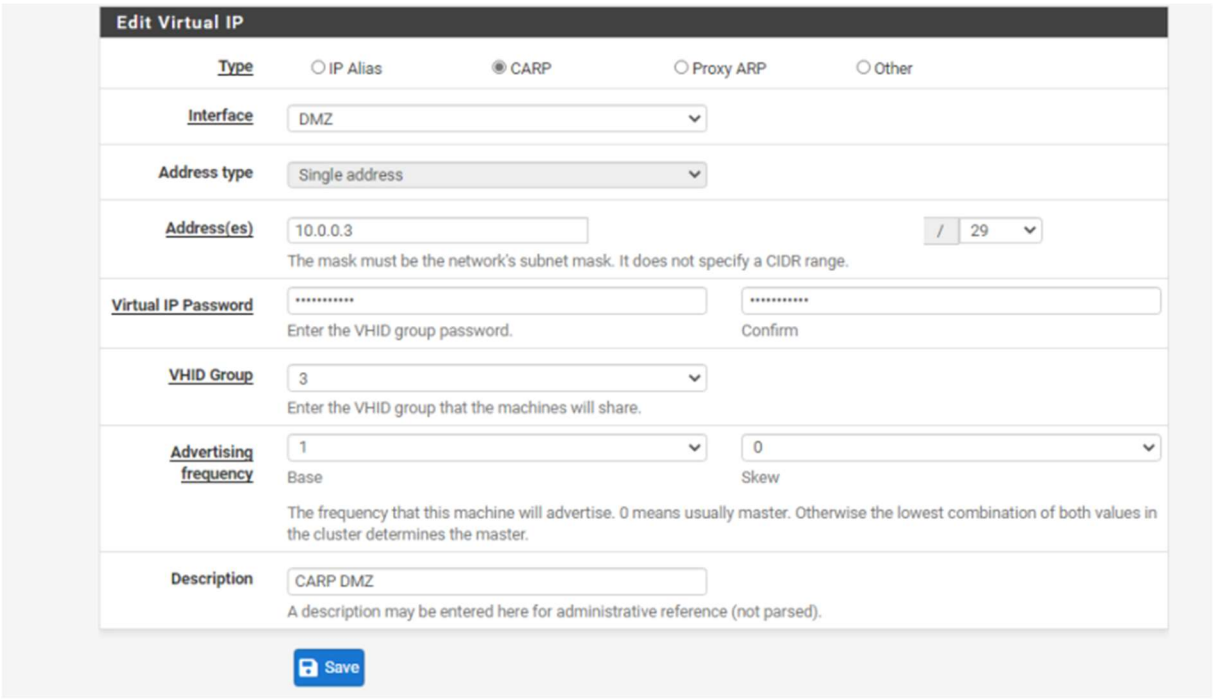


Interface **LAN**



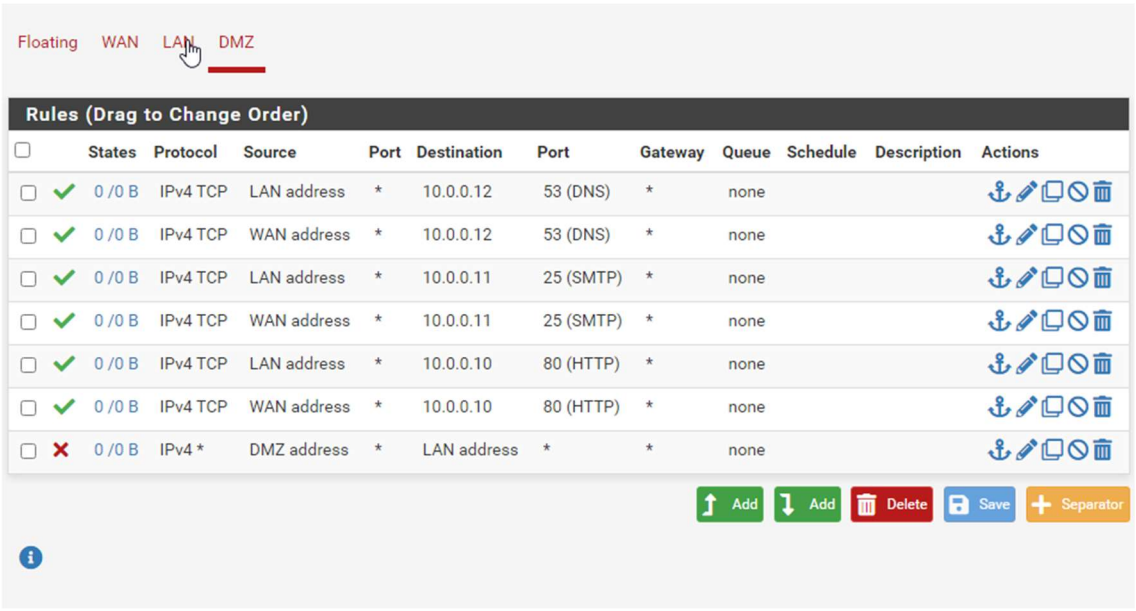
ynov CAMPUS

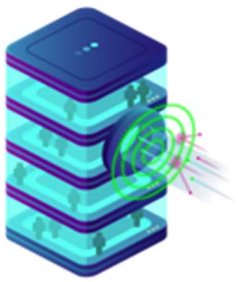
Interface **DMZ**



Dans la partie Firewall > Rules, nous pouvons créer des règles ACL (Access Control List) sur les 3 interfaces.

Ci-dessous les règles appliquées sur l'interface **DMZ**.





On autorise seulement le flux vers la **DMZ** sur des hots spécifiés ainsi que le port de destination lié au service déployé.

On bloque tout flux initié de la **DMZ** vers le **LAN**

Règles appliquées sur l'interface **LAN**

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	0 /1.33 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✔	0 /0 B	IPv4 ICMP any	LAN net	*	*	*	*	none			
✔	0 /0 B	IPv4 TCP	LAN net	*	*	22 (SSH)	*	none			
✔	0 /0 B	IPv4 TCP	LAN net	*	*	53 (DNS)	*	none			
✔	0 /0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			
✔	0 /0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			

On autorise les flux initiés depuis le **LAN** selon les services déployés.

Configuration du système de détection HIDS OSSEC

Une fois le dossier ossec décompressé lancez install.sh

```
ossec-hids-3.1.0/src/win32/vista_sec.txt
ossec-hids-3.1.0/src/win32/win_agent.c
ossec-hids-3.1.0/src/win32/win_service.c
root@user-VirtualBox:/home/user# cd  ossec-hids-3.1.0
root@user-VirtualBox:/home/user/ossec-hids-3.1.0# sh install.sh

  ** Para instalação em português, escolha [br].
  ** 要使用中文进行安装，请选择 [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** A Magyar nyelvű telepítéshez válassza [hu].
  ** Per l'installazione in Italiano, scegli [it].
  ** 日本語でインスト ールします. 選択して下さい. [jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: fr
```

Un utilitaire se lance afin de paramétrer l'installation de OSSEC, ici on nous demande la langue dans laquelle nous voulons installer ossec.

ynov CAMPUS

```
 - Utilisateur: root
 - Hôte: user-VirtualBox


 -- Appuyez sur Entrée pour continuer ou Ctrl-C pour annuler. --


- Quel type d'installation voulez-vous (serveur, agent, local ou aide) ? 1

- Quel type d'installation voulez-vous (serveur, agent, local ou aide) ? serveu


 - Installation du serveur choisie.

- Définition de l'environnement d'installation.

 - Choisissez votre répertoire d'installation de OSSEC HIDS [/var/ossec]:

   - L'installation sera faite sur  /var/ossec .

- Configuration de OSSEC HIDS.

 3.1- Voulez-vous une alerte par email ? (o/n) [o]:
  - Quel est votre adresse email ?
```

Nous avons ajouté une adresse électronique afin d'être alerté en cas de détection d'intrusion.

```
root@user-VirtualBox: /home/user/ossec-hids-3.1.0
  - Lancement de rootcheck (détection de rootkit).

 3.4- La réponse active vous permet d'éxécuter des commandes
      spécifiques en fonction d'évènement. Par exemple,
      vous pouvez bloquer une adresse IP ou interdire
      l'accès à un utilisateur spécifique.
      Plus d'information sur :
      http://www.ossec.net/en/manual.html#active-response

  - voulez-vous démarrer la réponse active ? (o/n) [o]: o

    - Réponse active activée.

  - Par défaut, nous pouvons activer le contrôle d'hôte
    et le pare-feu (firewall-drop). Le premier ajoute
    un hôte dans /etc/hosts.deny et le second bloquera
    l'hôte dans iptables (sous linux) ou dans ipfilter
    (sous Solaris, FreeBSD ou NetSBD).
  - Ils peuvent aussi être utilisés pour arrêter les scans
    en force brute de SSHD, les scans de ports ou d'autres
    formes d'attaques. Vous pouvez aussi les bloquer par
    rapport à des évènements snort, par exemple.

  - Voulez-vous activer la réponse pare-feu (firewall-drop) ? (o/n) [o]:
```

Nous avons choisi d'activer la détection de rootkits (se basant sur l'hôte) ainsi que la réponse active et pare-feu afin d'avoir un retour sur les évènements des équipements réseaux.

```
root@user-VirtualBox: /home/user/ossec-hids-3.1.0
   - Voulez-vous d'autres adresses IP dans votre liste (white list) ? (o/n)? [n]
: n

  3.5- Voulez-vous activer fonctionnalité syslog (port udp 514) ? (o/n) [o]: o

   - Fonctionnalité syslog activé.

  3.6- Mise en place de la configuration pour analyser les logs suivants :
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log
    -- /var/log/apache2/error.log (apache log)
    -- /var/log/apache2/access.log (apache log)

 - Si vous voulez surveiller d'autres fichiers, changez
   le fichier ossec.conf en ajoutant une nouvelle valeur
   de nom de fichier local.
   Pour toutes vos questions sur la configuration,
   consultez notre site web http://www.ossec.net .


   --- Appuyez sur Entrée pour continuer ---
```

Nous renseignons aussi des IP dans la whitelist afin que le système reconnaisse les adresses IP fiables.

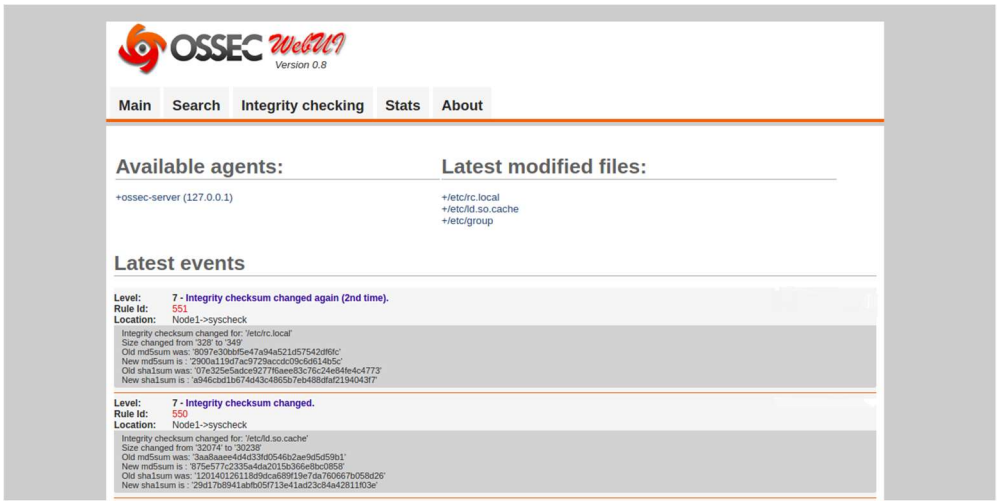
```
root@user-VirtualBox: /home/user/ossec-hids-3.1.0
root@user-VirtualBox:/home/user/ossec-hids-3.1.0# /var/ossec/bin/ossec-control s
tart
Starting OSSEC HIDS v3.1.0 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@user-VirtualBox:/home/user/ossec-hids-3.1.0#
```

```
root@user-VirtualBox:/home/user/ossec-hids-3.1.0# nano /var/ossec/etc/ossec.conf
root@user-VirtualBox:/home/user/ossec-hids-3.1.0# nano /var/ossec/rules/local_ru
les.xml
root@user-VirtualBox:/home/user/ossec-hids-3.1.0# /var/ossec/bin/ossec-control r
estart
Deleting PID file '/var/ossec/var/run/ossec-remoted-16948.pid' not used...
Killing ossec-monitord ..
Killing ossec-logcollector ..
ossec-remoted not running ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
Killing ossec-maild ..
Killing ossec-execd ..
OSSEC HIDS v3.1.0 Stopped
Starting OSSEC HIDS v3.1.0 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@user-VirtualBox:/home/user/ossec-hids-3.1.0#
```

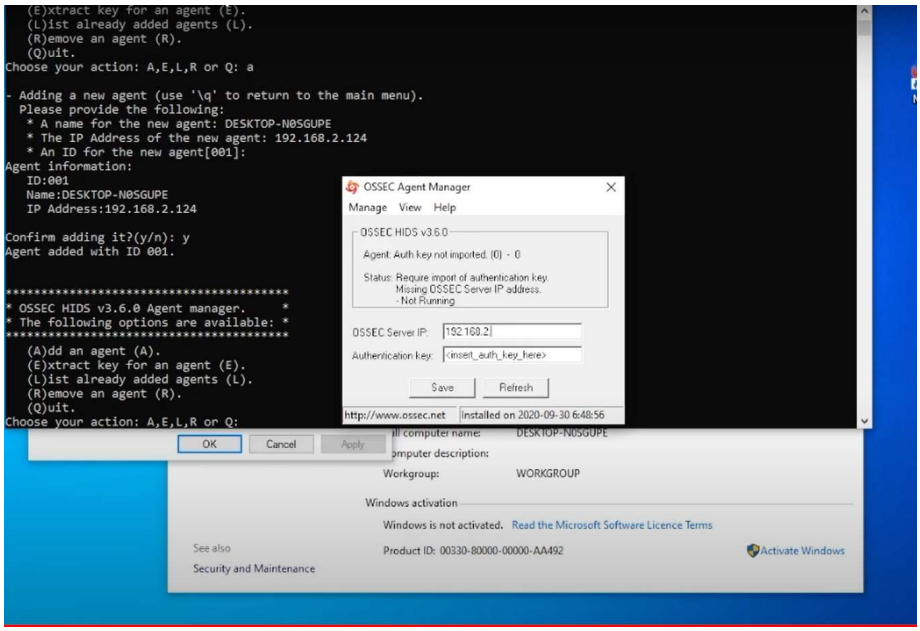
Une fois l'installation terminée, nous pouvons voir les services liés à OSSEC se démarrer avec succès.

On installe après l'interface graphique de Ossec pour une meilleure utilisation.

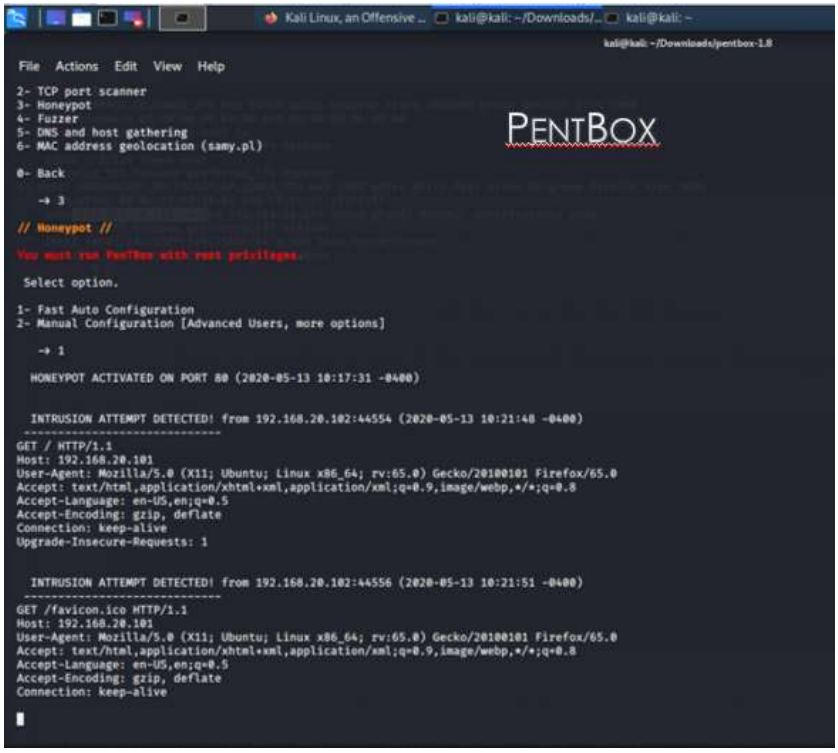
On peut accéder via un navigateur web sur la page ci-dessous à l'adressehttp://your-server-ip/ossec



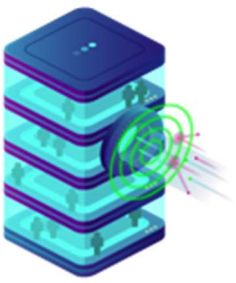
Il faut installer le client OSSEC Agent Manager sur les postes enduser afin de le faire remonter vers le serveur HIDS.

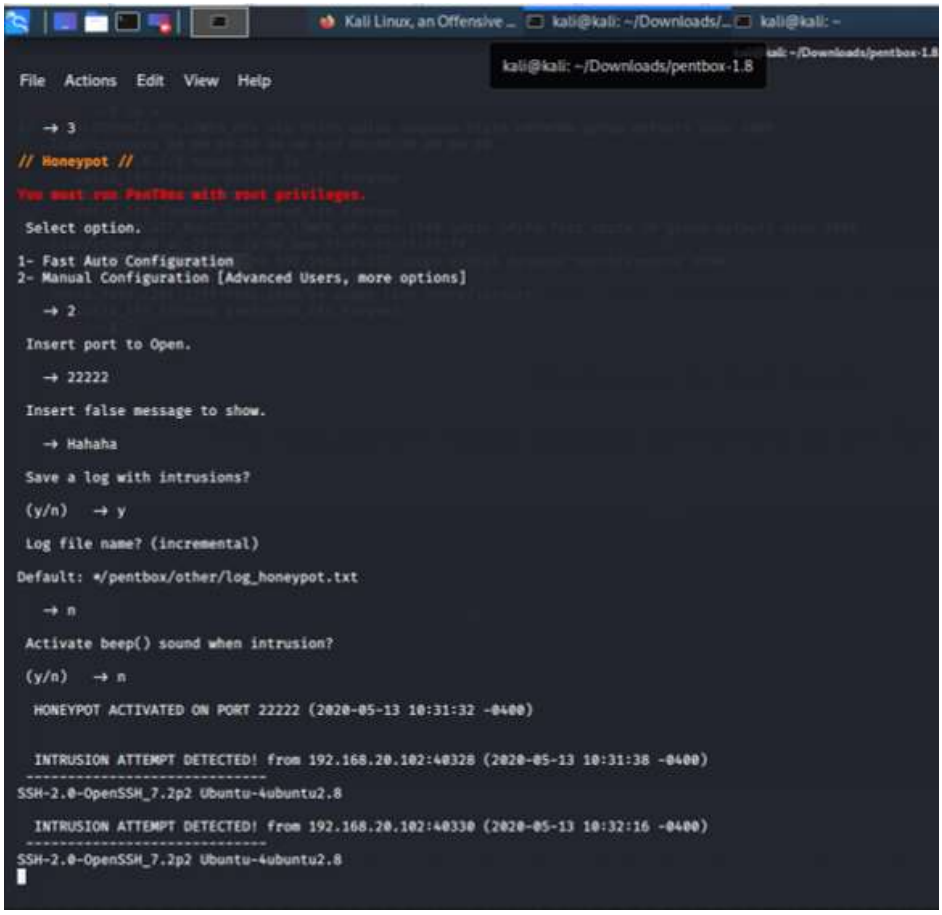


Configuration du Honeypot sur le port 80 avec l'outils **PentBOX**



Sur le Port 22





Problèmes rencontrés

Durant notre projet, nous avons rencontré plusieurs problèmes pendant nos configurations de VM avec le logiciel GNS3.

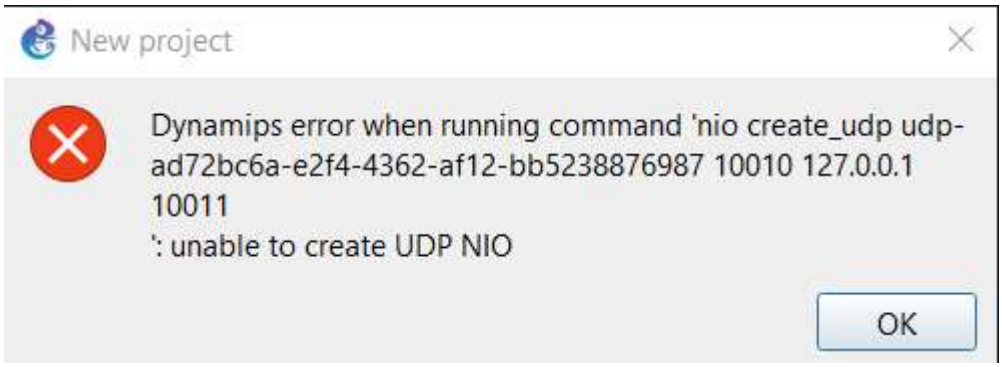
En effet, nous avons eu plusieurs problèmes de compatibilités entre GNS3 et nos machines, que ce soit avec nos cartes réseaux où carte graphique.

Dans plusieurs cas, sous GNS3 l'accès au WAN utilisant une carte réseau Intel été inaccessible en mode bridge, nous devions donc mettre la carte en mode NAT, ce qui n'était pas notre choix de base.

Nous avons aussi eu des problèmes de compatibilités entre GNS3 et la carte graphique Nvidia.

ynov CAMPUS

Lors de l'ouverture du projet sous GNS3, une erreur apparait, ce qui rend l'ouverture du projet impossible (Voir screen ci-dessous).



Après plusieurs recherches, le seul moyen que nous avons trouvé est de désinstaller tous les Drivers graphiques Nvidia, cela permet ensuite de pouvoir ouvrir le Fichier de topologie GNS3.

Plusieurs erreurs liées à Winpcap ont été rencontrés, souvent lors de l'établissement de liens entre une carte réseaux sur un Cloud et des VM.