**GROUPE 14 - PROJET 2**

**ARCHITECTURE RÉSEAU ET SÉCURITÉ**

**ACHAINTRE Yanis - TIREL Maxime - CÉLESTINE Dorian**



**SOMMAIRE :**

1. Contexte du projet ,
2. Nos solutions ,
   1. Composants logiciels,
   2. Architecture réseau,
   3. Bonnes pratiques,
   4. Sécurité.
3. Conclusion,
   1. Difficultés rencontrées,
   2. Notre ressenti sur le projet.
4. Nos sources.

# Contexte du projet :

L’objectif de notre groupe lors de ce projet est de mettre en place un réseau fonctionnel et sécurisé. Le tout en détaillant le processus de création et de sélection des différentes solutions techniques utilisées tout au long de notre travail.

Le premier axe du projet est de proposer un réseau fonctionnel réaliste qui peut potentiellement répondre aux besoins d’une petite entreprise. Le deuxième axe est que la solution que nous fournissons doit être sécurisée par diverses méthodes pour garantir un réseau fiable. Enfin, la dernière partie de ce travail est de sourcer et justifier nos choix tout en détaillant le processus de mise en place pour qu’il soit facilement reproductible par un potentiel client.

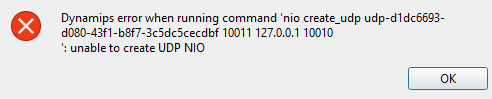
Concernant les besoins du client, il est nécessaire d’isoler et de filtrer les flux entrants et sortants via un firewall ainsi qu’un IDS. Pour garantir la sécurité des serveurs il est aussi requis de créer une DMZ en dehors du VLAN, les deux étant séparés par deux routeurs aux fonctions identiques mais utilisant la redondance pour pallier à d'éventuels incidents. Si l’un des deux routeurs ne fonctionne plus quelle que soit la cause, le deuxième routeur servira de garantie. Afin de centraliser les logs, un système de honeypot est nécessaire sur la machine de l’administrateur qui accueille aussi le portail captif installé sur le réseau.

Lien vers notre dépôt git : <https://github.com/DorianCelestine/projetReseau>

# Nos Solutions :

## **Composants logiciels :**

Dans le cadre de ce projet, nous avons choisi d’utiliser GNS3 pour construire notre réseau et en établir la maquette, la principale raison étant de pouvoir utiliser des outils open source au cours de notre travail. Cependant le mardi 04/05 nous avons eu des problèmes avec GNS 3 et avons dû basculer sur Cisco Packet Tracer pour recommencer.



Erreur sur GNS 3

Les fonctionnalités suivantes sont celles prévues pour GNS3.

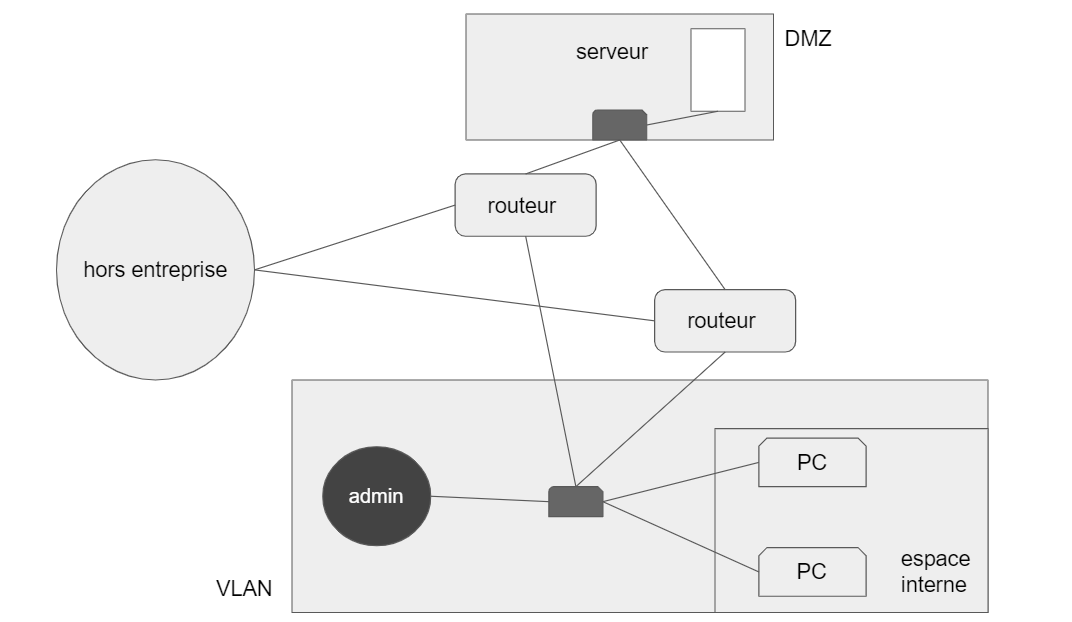
Pour établir un firewall ainsi qu’un portail captif nous avons choisi la solution de pfSense non seulement car c’est une solution connue que nous estimons plus fiable qu’un logiciel méconnu et peu utilisé, mais aussi parce qu’ainsi nous pouvons mettre en place deux fonctionnalités différentes avec un même outil, économisant ainsi des ressources. Notre IPS/IDS servant à détecter les potentielles intrusions sur le réseau est établi grâce à l’open source Snort que nous avons déjà manipulé au cours de l’année. De plus, cette solution est globalement reconnue comme efficace et propose des fonctionnalités adaptées à notre projet.

Pour mettre en place une sauvegarde de nos configurations nous avons choisi d’utiliser Rancid qui est aussi une solution open source qui inclut les CVS, Current Version System, et tous les fichiers utiles peuvent être rapidement trouvés sur Git.

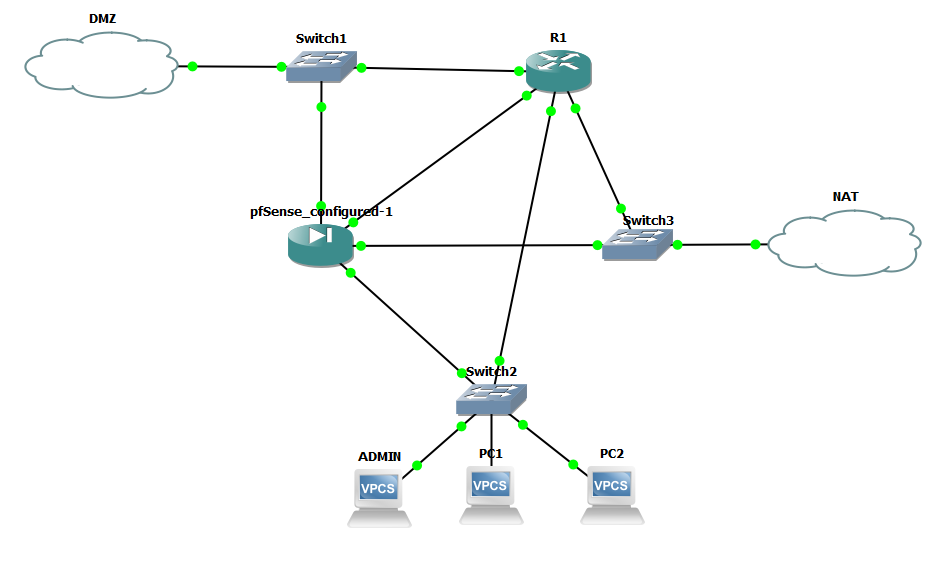
La honeypot que nous avons décidé de mettre en place est Cowrie qui est globalement bien évalué selon les avis que nous avons pu trouver. Cowrie peut surveiller à la fois les connexions SSH et Telnet.

1. **Architecture réseau :**

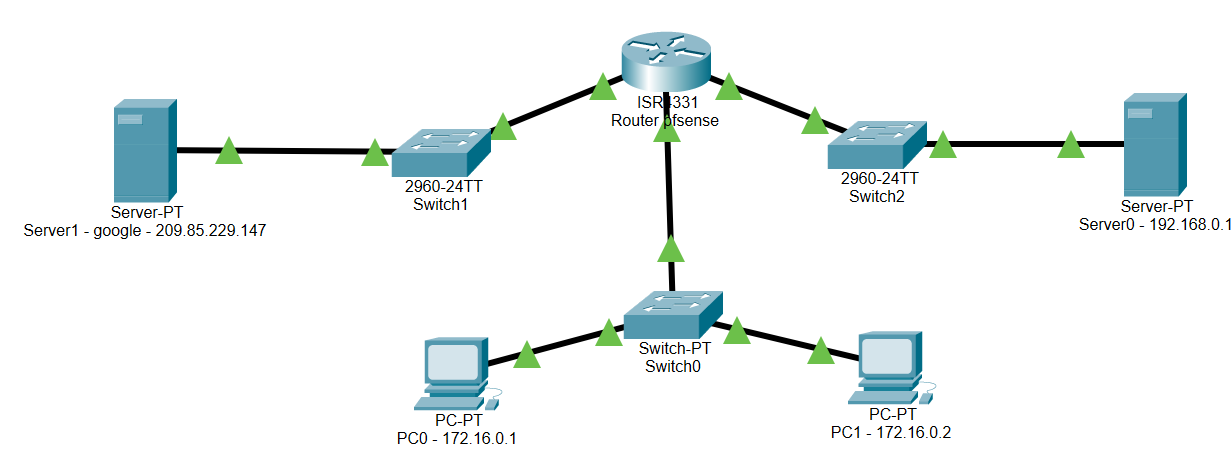
Voici un schéma descriptif de l’architecture réseau créée pour notre projet, le détail de son fonctionnement (firewall, DMZ …) se trouve dans le document d’exploitation.



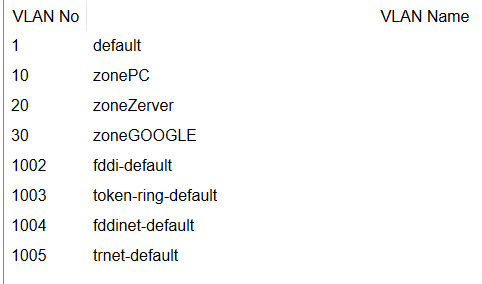
Maquette GNS3 :



Puis passage sur Cisco Packet Tracer où nous avons mis de côté de la redondance à cause de notre gros manque de temps, bien que les pings soient fonctionnels, nous n’avons pas installé d’autres fonctionnalités car nous n’avons pas eu le temps de prendre en main les solutions techniques propres à Cisco.



Sur cette architecture, le routeur est configuré via des VLAN créés spécifiquement pour le routage des différents sous-réseaux :



PS : “zoneZerver” est la zone avec le Server.

1. **Bonnes pratiques :**

Les pratiques que nous avons utilisées pour ce projet concernent la planification, dans le sens où l’architecture du réseau autant que les solutions logicielles ont été prévues en avance. De cette façon, nous nous assurons de ne pas avoir besoin de faire marche arrière après avoir réalisé qu’un de nos choix n’était pas adapté et gagnons ainsi du temps.

La seconde solution utilisée est de centraliser la sortie internet en un seul point pour à la fois limiter les chemins d’accès d’éventuels assaillants et en même temps pour identifier l’accès internet utilisés par les postes internes.

Enfin, nous avons dupliqué notre routeur pour installer un système de redondance permettant de pallier à d’éventuels incidents. Si l’un des deux routeurs venait à avoir des dysfonctionnements, alors le second routeur assurerait les fonctions du premier et inversement.

1. **Sécurité :**

Pour sécuriser notre réseau, nous avons utilisé divers outils qui ont été présentés plutôt. Chacun d’eux à un rôle spécifique en terme de sécurité réseau.

La première barrière installée est le firewall installé sur chaque routeur dans le but de filtrer les adresses entrant sur le réseau créé. De cette façon, il est possible de restreindre les adresses connues comme malfaisantes, de bloquer les adresses inconnues ou jugées non-fiables tout en laissant un accès aux adresses ip reconnues comme étant sans danger.

Nous avons aussi installé une DMZ pour isoler notre serveur du reste du réseau sur lequel se trouvent les postes utilisateurs et le poste de l’administrateur. De cette façon, les services qui doivent être accessibles depuis l’extérieur du réseau le sont tout en isolant ces services du reste du réseau interne pour éviter qu’une faille sur un des serveurs ne permette un rebond vers d’autres postes.

En plus de ceci, nous avons recours à un IDS / IPS pour détecter et bloquer tout type de trafic du moment qu’il est suspect. Il s’agit d’un système à la fois de prévention et de blocage pour sécuriser l’intérieur du réseau depuis des routeurs redondants.

Vient ensuite le portail captif que nous voulons installer dans le but d’identifier les utilisateurs tout en filtrant une partie des flux illégitimes ce qui agit en supplément du pare-feu.

L’objectif de la redondance des routeurs est de s’assurer que si l’une des deux machines ne fonctionne plus, qu’elle qu’en soit la raison, une seconde machine pourra assurer les fonctions de routage ainsi que de sécurité, notamment du firewall. Mais cette redondance joue aussi un rôle contre les attaques par déni de service. En effet, avec deux routeurs, les flux externes qui ne sont pas bloqués peuvent être répartis sur les deux machines évitant ainsi une surcharge.

3. Conclusion :

1. **Difficultés rencontrées :**

Ce projet nous a mis face à de nombreux problèmes notamment liés à l'organisation et à la gestion de temps.

Une fois que nous avions choisi notre projet, il a fallu se décider sur les technologies à utiliser, ce qui nous a pris pas mal de temps.

Par la suite, une fois le projet amorcé, nous avons rencontré quelques problèmes techniques concernant le logiciel de virtualisation : certaines images d'équipements d'interconnexions n'ont pas pu être installé, pour celà nous avons dû réorganiser la répartition des tâches et laisser l'hébergement du LAB à une autre personne du groupe.

Aussi, la gestion du temps à été quelque peu problématique : le fait d'avoir largement assez de temps pour réaliser notre travail nous a mis un peu trop en confiance. Nous nous sommes retrouvés à devoir accélérer le pas à une semaine de l'échéance du projet.

Le dernier et plus gros problème est que GNS3 nous a lâché au dernier moment nous contraignant à basculer d’urgence sur Cisco Packet Tracer au détriment de notre travail précédent.

1. **Notre ressenti sur le projet :**

Notre ressenti sur le projet est assez mitigé dans le sens où nous n’avons pas été spécialement attirés par les projets proposés et que nous avons plus choisi par défaut qu’autre chose.

Malgré tout, une fois que GNS3, qui ne nous était pas familier, a été pris en main nous avons rapidement avancé dans notre travail sans rencontrer de soucis jusqu’à la fin où nous avons été brusquement interrompus.

Dès lors, notre moral a chuté et notre objectif est passé de “finir le projet” à “faire ce qu’on peut”. Ainsi, bien que nous n’ayons pas l’impression que le projet soit particulièrement complexe, les aléas on fait qu’il est devenu impossible à terminer correctement.

5. Sources :

En vrac :

<https://hackertarget.com/cowrie-honeypot-analysis-24hrs/>

<https://connect.ed-diamond.com/GNU-Linux-Magazine/GLMF-160/Sauvegardez-vos-actifs-reseaux-HP-Cisco-ou-Juniper-de-maniere-automatisee-avec-RANCID#:~:text=RANCID%20>(Really%20Awesome%20New%20Cisco,suivre%20l'%C3%A9volution%20des%20configurations.

<https://shrubbery.net/rancid/>

<https://www.securiteinfo.com/administration-systeme-et-reseau/outils/cowrie.shtml>

<https://medium.com/threatpunter/how-to-setup-cowrie-an-ssh-honeypot-535a68832e4c>

<https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-a-internet/>

<https://www.ssi.gouv.fr/entreprise/guide/recommandations-et-methodologie-pour-le-nettoyage-dune-politique-de-filtrage-reseau-dun-pare-feu/>

<https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxkYW1pZW5naWNxdWVsMjl8Z3g6NGEwNTAxYjVkMjFmYWZjMw>

<https://www.frameip.com/honeypots-honeynet/>

<https://akerva.com/blog/17-points-essentiels-pour-securiser-vos-infrastructures-informatiques-sensibles-exposees-sur-internet/>

<https://www.ssi.gouv.fr/uploads/2016/08/np_nettoyage-politique-pare-feu.pdf>

<https://www.celeste.fr/5-bonnes-pratiques-de-celeste-pour-la-securite-des-reseaux-informatiques/>

<https://www.hackers-arise.com/post/2018/05/20/snort-ids-part-2-basic-configuration-of-your-snort-ids>

<https://www.linksys.com/fr/r/resource-center/portaif-captif/>