République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene
Faculté d'Informatique
Département des systèmes
Informatique

Spécialité :
Sécurité des systèmes informatique

Rapport :
Réseau d'entreprise sur GNS3

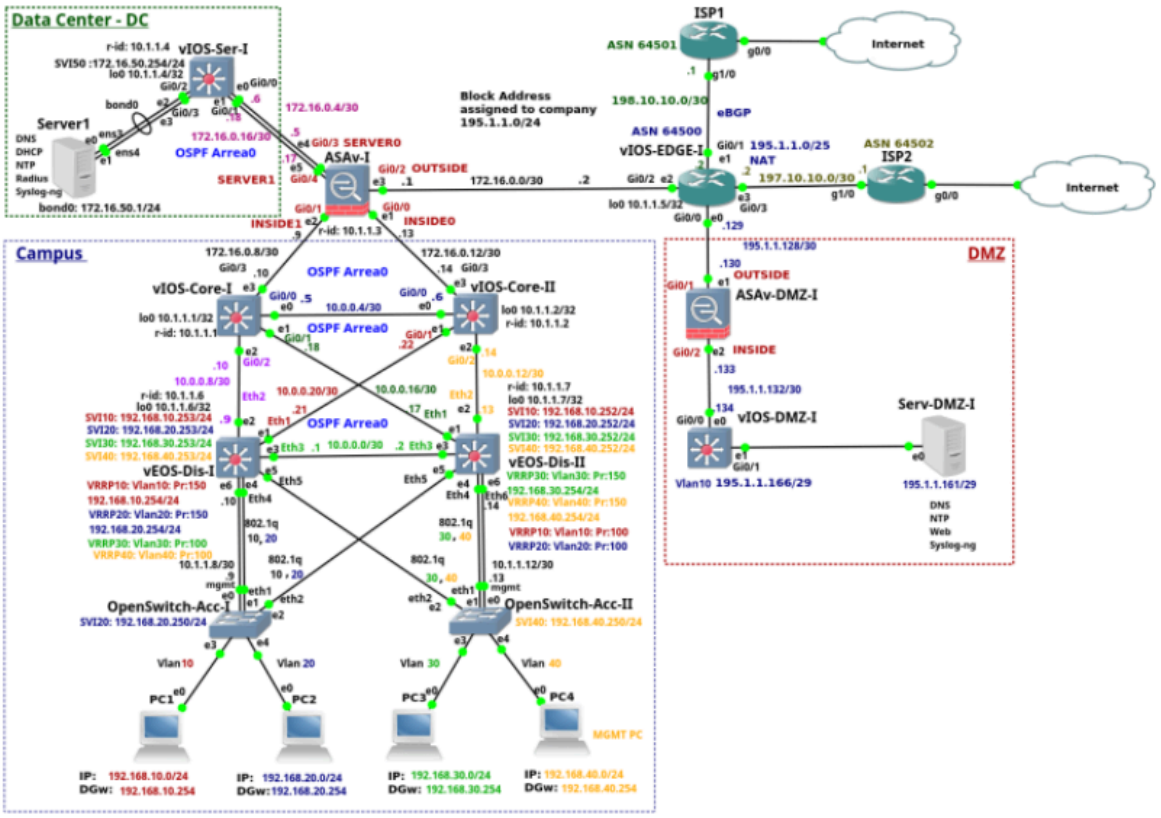
Réalisé par :

- **MEKKI Imene**
- **BENTOUNES Mohammed Rachid Yousr**
- **ZIOUANE Rayane Syphax**
- **TASSADIT Abderrahmane**
- **SEDDIKI Adem**
- **MADANI Mohamed**
- **IOUALALEN Imane**
- **BOUDRIES Karima**
- **CHAABANE Khaoula**
- **AKDIF Khaoula**

Table des matières

Introduction :

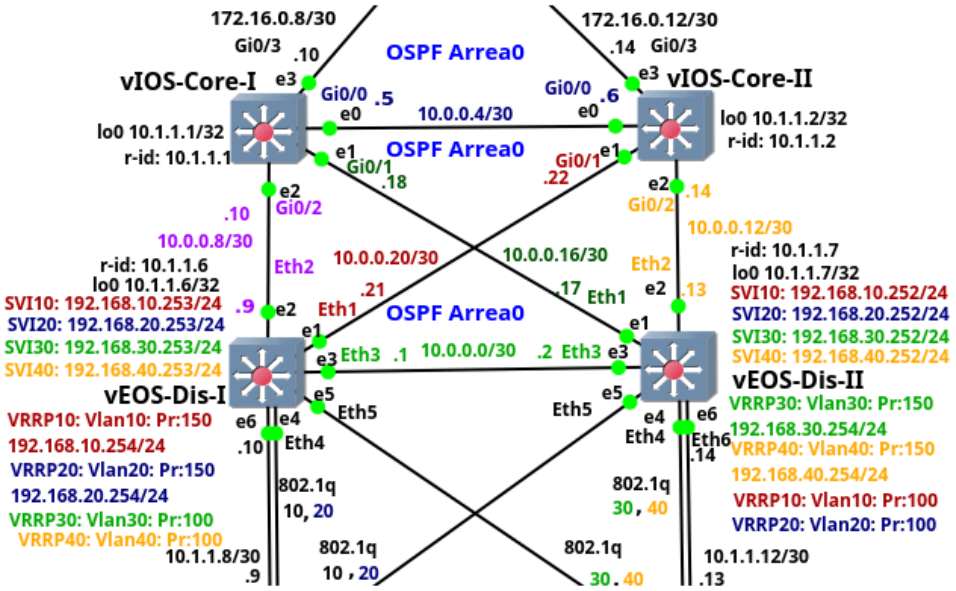
Dans ce projet, nous avons entrepris la configuration d'un réseau d'entreprise qui a été élaboré sur GNS3, une tâche qui a évolué d'un simple laboratoire à une infrastructure complète comprenant un campus, un centre de données, des zones DMZ et des fournisseurs d'accès Internet.



I/- Partie 1 : Enterprise Campus Network

1. Introduction :

La partie "campus" constitue un élément central de notre réseau d'entreprise. Elle abrite une variété de ressources et de services internes essentiels à nos opérations. Cette section se concentre sur la configuration des commutateurs de distribution, qui acheminent le trafic entre les VLAN des utilisateurs finaux et connectent le réseau de couche inférieure à une couche principale. Nous explorerons également l'utilisation du protocole OSPF pour assurer une connectivité L3 robuste. En comprenant le rôle critique de cette partie dans notre infrastructure, nous pourrons mieux appréhender son impact sur la performance et la sécurité globales de notre réseau.



Le rôle:

Dans cette partie, nous allons explorer en détail la configuration et le fonctionnement de cette partie critique de notre architecture.

2. Réalisation :

- **Remplacement des switches de niveau 1 :** En raison de problèmes de sauvegarde des configurations avec les switches ouverts, nous avons opté pour des switches de niveau 3 pour assurer une meilleure stabilité et fiabilité dans la partie "campus" de notre architecture.

- **Utilisation de switches de niveau 3 dans tous les niveaux :** Nous avons choisi des switches de niveau 3 pour tous les niveaux de la partie "campus" en raison de leur puissance et de leur rapidité, comparés aux autres types de switches disponibles.
- **Désactivation de la fonctionnalité "tootch" :** Dans les switches de niveau 3, nous avons désactivé la fonction "tootch" car nous avons constaté qu'elle interférait avec la sauvegarde correcte des configurations que nous avions ajoutées.

En prenant ces mesures, nous avons pu garantir une configuration stable et fonctionnelle de notre réseau dans la partie "campus", ce qui contribue à la performance et à la fiabilité globales de notre infrastructure.

3. Les couches principales du réseau de campus d'entreprise:

A. CORE (Noyau):

Le noyau du réseau, également connu sous le nom de couche de base, est le cœur de l'architecture. Il est responsable du transfert de gros volumes de données à haute vitesse entre différentes parties de l'entreprise et vers des réseaux externes.
Cette couche est généralement constituée de commutateurs et de routeurs hautes performances capables de traiter un trafic intense sans créer de goulot d'étranglement.
Son rôle principal est d'assurer une connectivité rapide et fiable entre les différentes parties de l'infrastructure réseau, y compris les centres de données, les succursales et les autres sites distants.

B. Distribution (Distribution):

La couche de distribution agit comme une **passerelle** entre la couche de base et la couche d'accès. Elle est chargée de redistribuer et de contrôler le trafic provenant des différents segments du réseau.
Les commutateurs de distribution sont responsables de la segmentation du trafic en fonction des besoins de l'entreprise, de l'agrégation des liaisons montantes provenant des commutateurs d'accès, et de l'application de politiques de sécurité et de qualité de service (QoS).
Cette couche contribue également à optimiser les performances du réseau en gérant efficacement les chemins de communication et en évitant les congestions.

C. Accès (Access) :

La couche d'accès est le point d'entrée du réseau pour les utilisateurs finaux et les périphériques. Elle fournit une connectivité aux appareils tels que les ordinateurs de bureau, les téléphones IP, les imprimantes et d'autres périphériques réseau.
Les commutateurs d'accès sont généralement déployés dans les bureaux, les salles de conférence et d'autres zones où les utilisateurs se connectent au réseau. Ils sont responsables de la distribution du trafic vers les segments appropriés du réseau.

Cette couche est souvent conçue pour prendre en charge des fonctionnalités telles que la sécurité des ports, la détection des périphériques, et la gestion des VLAN (Virtual Local Area Networks) pour garantir un accès sécurisé et contrôlé aux ressources réseau

4. Protocoles Utilisés :

Dans la mise en œuvre de l'architecture réseau du campus, plusieurs protocoles sont utilisés pour assurer une connectivité fiable, une gestion efficace du trafic et une sécurité accrue. Voici quelques-uns des protocoles clés utilisés dans notre infrastructure:

- **Protocole de routage OSPF (Open Shortest Path First)** : OSPF est utilisé au niveau de la couche de distribution pour permettre un routage dynamique entre les différents segments du réseau. Il permet aux commutateurs de distribution d'échanger des informations sur les routes disponibles et de calculer les chemins les plus courts vers les destinations.

- **Protocole VLAN (Virtual Local Area Network)** : Les VLAN sont utilisés pour segmenter le trafic au niveau de la couche d'accès, permettant ainsi de regrouper les périphériques en fonction de critères tels que le département, la fonction ou la sécurité. Cela améliore la sécurité du réseau en limitant la visibilité du trafic entre les différentes parties de l'entreprise.
- **Protocole STP (Spanning Tree Protocol) :** STP est utilisé pour assurer la redondance au niveau de la couche d'accès en évitant les boucles de commutation. Il permet de désigner un seul chemin actif à travers le réseau, tout en mettant en attente les chemins de secours pour être activés en cas de panne du chemin principal
- **Protocole DHCP (Dynamic Host Configuration Protocol) :** DHCP est utilisé pour attribuer dynamiquement des adresses IP aux ordinateurs du réseau, simplifiant ainsi la gestion des adresses IP et permettant une configuration automatisée des périphériques réseau.

- **Protocole NTP (Network Time Protocol) :** NTP est utilisé pour synchroniser l'horloge des commutateurs d'accès avec un serveur de temps externe. Cela garantit que tous les périphériques du réseau ont la même heure, ce qui est essentiel pour le bon fonctionnement des applications distribuées et des services basés sur le temps.

5. Conclusion :

En conclusion, les ajustements effectués dans la partie "campus" de notre architecture réseau ont été essentiels pour garantir son bon fonctionnement et sa fiabilité. Le remplacement des switches de niveau 1 par des switches de niveau 3, ainsi que l'utilisation de switches de niveau 3 dans tous les niveaux, ont permis d'améliorer la stabilité et la performance de notre réseau. De plus, la désactivation de la fonction "touch" dans les

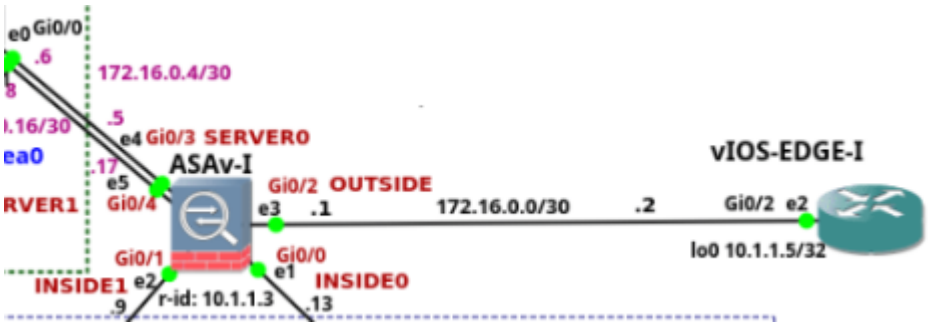
switches de niveau 3 a résolu les problèmes de sauvegarde des configurations, assurant ainsi une gestion efficace des paramètres réseau.

Ces ajustements reflètent notre engagement à maintenir un environnement réseau robuste et performant pour soutenir nos opérations internes. En optimisant la partie "campus" de notre architecture, nous avons créé une base solide sur laquelle reposer nos activités quotidiennes. Nous restons vigilants pour identifier et résoudre tout autre problème potentiel, afin de garantir la continuité et la fiabilité de notre infrastructure réseau dans le futur.

II/- Réseau d'entreprise sur GNS3 -Partie - Cisco ASAv-I :

6. Introduction :

Dans cette section, nous explorerons en détail la mise en place de l'ASAv-I, un dispositif virtuel essentiel au sein de notre infrastructure réseau simulée sur GNS3. L'ASAv-I, basé sur le Cisco Adaptive Security Virtual Appliance (ASAv) version 9.6(1), est déployé sur un disque qcow2 Qemu. Il assure le filtrage et l'inspection du trafic pour notre réseau du campus et le centre de données (DC), tout en assurant la liaison entre ces deux environnements et le routeur de bord vIOS-EDGE-I. Cette configuration garantit une sécurité robuste et une connectivité fiable au sein de notre réseau d'entreprise simulé.



7. Principales notions:

- **Adaptive Security Virtual Appliance (ASAv) :** Un composant virtuel de sécurité de Cisco utilisé pour assurer le filtrage et l'inspection du trafic réseau.
- **GNS3 (Graphical Network Simulator-3) :** Une plateforme de simulation réseau permettant la modélisation et les tests de configurations réseau.
- **Interfaces et niveaux de sécurité :** Les interfaces de l'ASAv-I sont configurées avec des niveaux de sécurité, indiquant le degré de restriction d'accès. Par exemple, les interfaces INSIDE0 et INSIDE1 ont un niveau de sécurité de 100, tandis que l'interface OUTSIDE a un niveau de sécurité de 0.
- **Configuration OSPF (Open Shortest Path First) :** Un protocole de routage utilisé pour l'acheminement du trafic entre le campus et le centre de données (DC). L'ASAv-I redistribue une route statique par défaut vers le processus OSPF pour garantir la connectivité.

- **ACLs (Access Control Lists) :** Les listes de contrôle d'accès définissent les règles pour autoriser ou refuser le trafic réseau. Par exemple, l'ACL "out-to-ins" permet le ping depuis certains sous-réseaux vers les interfaces de l'ASAv-I.
- **NTP (Network Time Protocol) :** Un protocole utilisé pour synchroniser les horloges des appareils du réseau. L'ASAv-I est configuré pour se synchroniser avec un serveur NTP.

- **AAA (Authentication, Authorization, and Accounting) :** Un ensemble de services de sécurité réseau comprenant l'authentification des utilisateurs, l'autorisation d'accès et la gestion des comptes.
- **Inspection des applications :** L'ASAv-I inspecte le trafic réseau au niveau applicatif afin de détecter les violations de protocole et les contenus malveillants.

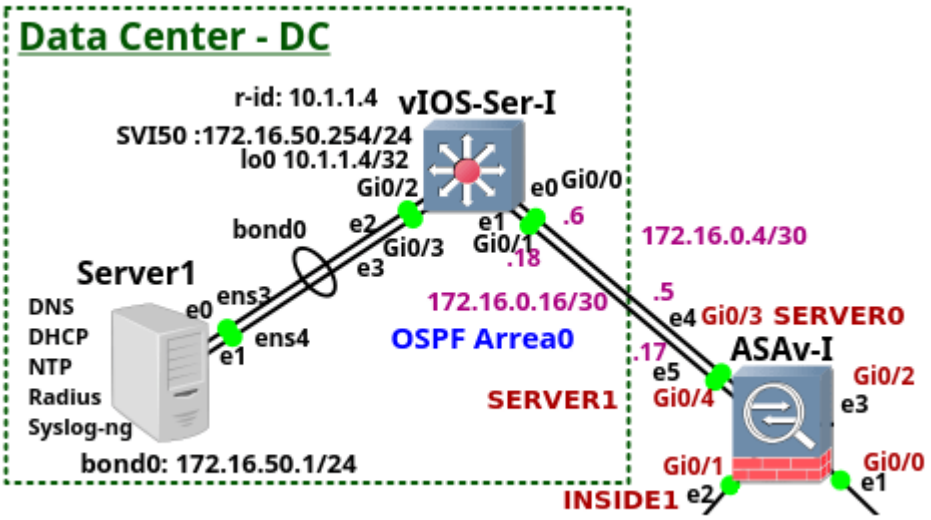
8. Réalisations:

- **Configuration des Interfaces :** On a configuré les interfaces de l'ASAv-I, comme INSIDE0, INSIDE1, SERVER0, SERVER1 et OUTSIDE, avec des niveaux de sécurité appropriés pour permettre le flux de trafic entre les différentes parties du réseau.
- **Configuration du Routage OSPF :** Pour assurer la connectivité entre le campus et le centre de données, on a configuré le protocole de routage OSPF, incluant la redistribution d'une route statique par défaut vers le processus OSPF.
- **Configuration des Listes de Contrôle d'Accès (ACLs) :** On a établi des ACL pour contrôler le trafic réseau entrant et sortant, autorisant notamment le ping depuis certains sous-réseaux, les requêtes DNS et NTP, ainsi que définissant des règles de sécurité pour des communications spécifiques.
- **Configuration du Protocole NTP :** On a synchronisé l'horloge de l'ASAv-I avec un serveur NTP externe pour assurer une gestion précise du temps.
- **Configuration des Services AAA (Authentication, Authorization, and Accounting) :** On a configuré des utilisateurs locaux sur l'ASAv-I pour l'authentification, et un serveur RADIUS pour gérer l'authentification des utilisateurs en cas d'indisponibilité des serveurs RADIUS.
- **Inspection des Applications :** On a activé l'inspection des applications au niveau du pare-feu pour détecter les violations de protocole et les activités suspectes.
- **Création de Zones :** On a regroupé les interfaces associées à des parties spécifiques du réseau en créant des zones, afin d'optimiser le routage et la gestion du trafic.

III/- Réseau d'entreprise sur GNS3 - Partie – Data Center :

1. Introduction :

Data Center "DC", sont des installations physiques où sont regroupés et interconnectés les équipements informatiques et de stockage nécessaires au traitement, au stockage et à la diffusion de données et d'applications pour une organisation ou une entreprise. Ils jouent un rôle crucial dans le fonctionnement des infrastructures informatiques modernes, offrant un environnement sécurisé et hautement disponible pour héberger les services essentiels.



2. Le rôle du data center :

Le rôle principal d'un DC est de fournir une infrastructure robuste et fiable pour soutenir les opérations informatiques d'une entreprise. Cela comprend le stockage de données, l'exécution d'applications, le traitement des transactions et la diffusion de services en ligne. Les centres de données sont conçus pour offrir une disponibilité maximale, une capacité de montée en charge flexible et une sécurité renforcée pour garantir la continuité des activités et la protection des données sensibles.

3. Les composant :

Les composants principaux d'un centre de données comprennent les serveurs, les systèmes de stockage, les commutateurs de réseau, les routeurs, les pares-feux, les systèmes de refroidissement et d'alimentation, ainsi que les dispositifs de surveillance et de gestion. Ces éléments sont organisés de manière à optimiser les performances, la disponibilité et l'efficacité énergétique du centre de données.

Dans notre architecture de centre de données, un élément crucial est la liaison entre notre serveur et un commutateur de niveau 3 (L3 switch), qui joue un rôle central dans la gestion du trafic réseau au sein de notre infrastructure. Voici un aperçu des fonctionnalités et des services que nous avons mis en place sur ce serveur, ainsi que sa connexion au commutateur de niveau 3 :

1. **Serveur Ubuntu :**
   Nous avons déployé un serveur Ubuntu sur notre infrastructure pour assurer diverses fonctionnalités et services réseau.
   Personnalisation du hostname :
   Nous avons personnalisé le hostname du serveur pour une meilleure identification au sein de notre réseau. Cela permet une gestion plus efficace des ressources et des services hébergés sur le serveur.

0. **Service DNS (BIND) :**
Pour la résolution des noms de domaine au sein de notre réseau, nous avons configuré le service DNS en utilisant BIND. Cette configuration permet au serveur d'agir en tant que serveur DNS interne, offrant une résolution rapide et fiable des noms de domaine.

0. **Service RADIUS (FreeRADIUS) :**
Nous avons également configuré le service RADIUS en utilisant FreeRADIUS sur le serveur. Cela permet une authentification centralisée des utilisateurs et des appareils réseau, renforçant ainsi la sécurité de notre infrastructure.

0. **Serveur DHCP :**
Le serveur Ubuntu agit également comme un serveur DHCP, distribuant automatiquement les adresses IP aux appareils connectés à notre réseau. Cela simplifie la gestion des adresses IP et garantit une connectivité réseau fluide pour tous les périphériques.

0. **Syslog-ng :**
Pour la gestion centralisée des journaux système et des événements de nos dispositifs réseau, nous avons installé et configuré Syslog-ng sur le serveur Ubuntu. Cette solution facilite le dépannage et la surveillance du réseau en permettant la collecte, le filtrage et l'archivage efficaces des journaux.

0. **Serveur NTP :**
Nous avons déployé un serveur NTP sur le serveur Ubuntu pour assurer une synchronisation précise de l'horloge sur l'ensemble de notre infrastructure. Cela garantit une cohérence temporelle cruciale pour de nombreuses applications et services.

0. **Client NTP :**
En plus du serveur NTP, nous avons configuré les périphériques clients pour synchroniser leur horloge avec le serveur NTP central. Cela garantit une synchronisation précise de l'heure sur l'ensemble du réseau, améliorant ainsi la cohérence et la précision des opérations.

0. Connexion au commutateur de niveau 3 :

Le serveur Ubuntu est connecté au commutateur de niveau 3, assurant ainsi une connectivité réseau étendue. Cette liaison permet une gestion efficace du trafic réseau et des communications entre le serveur et les autres dispositifs connectés au réseau.

En intégrant ces composants sur notre serveur Ubuntu et en le reliant à un commutateur de niveau 3 dans notre architecture de centre de données, nous avons établi une base solide pour des opérations réseau efficaces, sécurisées et hautement disponibles. Ces services essentiels contribuent à la stabilité, à la performance et à la sécurité de notre infrastructure, répondant ainsi aux besoins dynamiques de notre entreprise.

4. La connexion entre les différentes parties de l'architecture :

En plus de sa connexion au serveur Ubuntu, le commutateur de niveau 3 (L3 switch) est également relié au pare-feu ASAv-I à l'aide d'un câble Ethernet. Ce pare-feu joue un rôle crucial dans la sécurisation du trafic réseau en filtrant et en surveillant les communications entrantes et sortantes. Sa présence renforce la sécurité de notre infrastructure en permettant une gestion proactive des menaces et des vulnérabilités potentielles.

Le pare-feu ASAv-I est lui-même connecté à deux autres parties essentielles de notre architecture : la partie "campus" et la partie "dmz". La partie "campus" abrite des ressources et des services internes essentiels à notre entreprise, tandis que la partie "dmz" (zone démilitarisée) est dédiée à l'hébergement de services accessibles au public, tels que des serveurs web ou des services de messagerie. Cette segmentation du réseau en différentes zones permet une gestion plus efficace de la sécurité et une isolation des données sensibles, renforçant ainsi la résilience de notre infrastructure face aux menaces externes.

5. Conclusion :

En conclusion, la configuration du centre de données (DC) constitue un élément crucial de notre infrastructure réseau. À travers l'intégration de différents composants tels que le serveur Ubuntu, le commutateur de niveau 3, le pare-feu ASAv-I et les divers services réseau comme DNS, DHCP, RADIUS, Syslog-ng et NTP, nous avons établi une base solide pour des opérations réseau efficaces, sécurisées et hautement disponibles.

La mise en place de ces services essentiels permet d'assurer une connectivité stable et fiable au sein de notre infrastructure, tout en renforçant la sécurité des données et en facilitant la gestion des ressources réseau. La segmentation du réseau en différentes zones, telles que "campus" et "dmz", offre une approche stratégique pour la gestion de la sécurité, en permettant une isolation des données sensibles et une protection contre les menaces potentielles.

En outre, la centralisation de la gestion des journaux système grâce à Syslog-ng facilite le dépannage et la surveillance du réseau, tandis que la synchronisation précise de l'heure via le

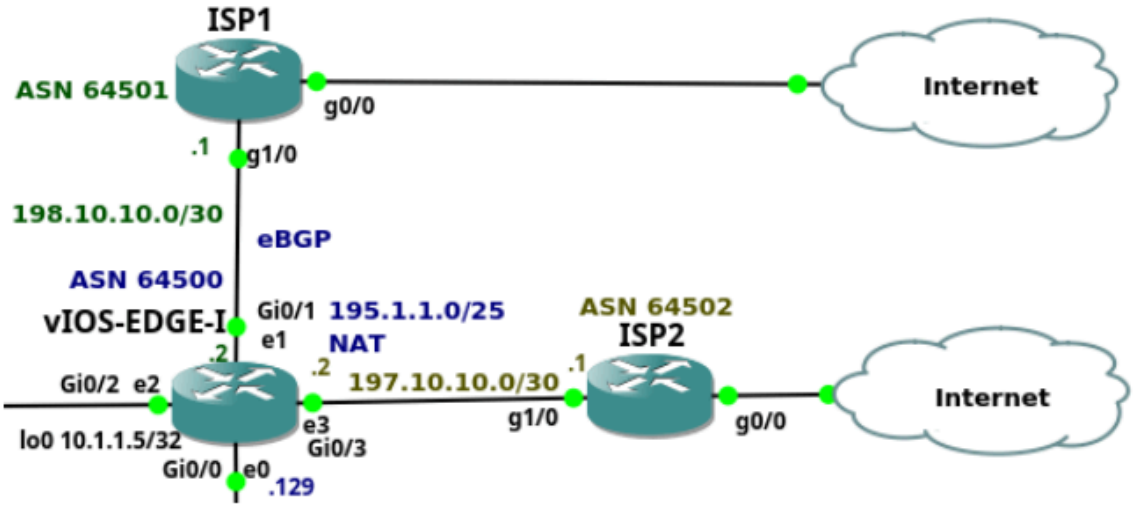
serveur NTP garantit une cohérence temporelle cruciale pour de nombreuses applications et services.

En somme, la configuration du centre de données représente un élément essentiel de notre infrastructure réseau, contribuant à sa stabilité, sa performance et sa sécurité globale. Elle est conçue pour répondre aux besoins dynamiques de notre entreprise, tout en offrant une base solide pour une croissance future et une adaptation aux évolutions technologiques.

IV/- Réseau d'entreprise sur GNS3 - Partie - Routeur Edge et FAI:

1. Introduction :

Pour la mise en place complète du réseau d'entreprise de cette société, nous avons configuré en détail les routeurs vIOS-EDGE-I, ISP1 et ISP2. Ces routeurs sont essentiels pour assurer une connectivité Internet stable et sécurisée à l'ensemble du réseau de l'entreprise.



- **Description du Routeur vIOS-EDGE-I**

Le routeur vIOS-EDGE-I, équipé de la version 15.6(2)T de Cisco IOSv Qemu et disposant de 512 Mo de RAM alloués par GNS3, assure la connectivité à Internet pour trois parties distinctes du réseau de l'entreprise : le réseau du campus, le centre de données et la DMZ (zone démilitarisée).

- **Rôle des Routeurs ISP (Fournisseurs de Services Internet)**

Les routeurs ISP jouent un rôle crucial en fournissant la connectivité à Internet pour le réseau d'entreprise. Connectés au routeur de bord vIOS-EDGE-I via leurs ports Ethernet Gi0/1 et Gi0/3, ils permettent à ce dernier d'annoncer l'ensemble du préfixe 195.1.1.0/24 aux deux ISP grâce au protocole de routage BGP (Border Gateway Protocol). En cas de panne de l'un des ISP, le trafic entrant vers le préfixe 195.1.1.0/24 reste inchangé, car le routeur de bord vIOS-EDGE-I est configuré pour acheminer le trafic sortant principalement via ISP1. Si ISP1 tombe en panne, le trafic est alors routé via ISP2. Cette configuration garantit la continuité de la connexion à Internet du réseau d'entreprise, même en cas de défaillance de l'un des ISP.

2. Réalisations :

D. Configuration du Routeur vIOS-EDGE-I :

- **Changement de Nom d'Hôte :** Le nom d'hôte du routeur est modifié en vIOS-EDGE-I pour faciliter sa gestion.
- **Création d'un Utilisateur Local et Définition du Mot de Passe pour le Mode Exécutif Privilégié :**
  - Un utilisateur local "admin" est créé avec le mot de passe "cisco" pour accéder au routeur.
  - Un mot de passe est également défini pour le mode exécutif privilégié.
- **Configuration des Adresses IP :**
  - Des adresses IP sont attribuées aux interfaces GigabitEthernet du routeur pour chaque connexion (ASA-DMZ-I, ASAv-I, ISP1, ISP2).
  - Une adresse Loopback est également configurée pour la gestion du routeur.
- **Configuration de la Traduction d'Adresses Réseau (NAT) :**

  Le NAT est configuré pour traduire les sous-réseaux du campus et du centre de données en une plage d'adresses IP publiques.
- **Configuration des Routes Statiques :**

  Des routes statiques sont définies pour les sous-réseaux cachés derrière le NAT et pour la DMZ.
- **Configuration du Protocole de Routage eBGP :**
  - Le routeur annonce le préfixe 195.1.1.0/24 aux FAI via le protocole BGP.
  - Des règles sont définies pour filtrer les annonces BGP et prévenir le transit indésirable de trafic.
- **Configuration du Serveur NTP :**

  Un serveur NTP est configuré pour la synchronisation horaire.
- **Configuration du Journal d'Événements :**

  La journalisation des événements est configurée pour surveiller les activités du routeur.
- **Configuration du Client DNS :**

  Un serveur DNS est défini pour résoudre les noms de domaine.
- **Configuration de l'Accès SSH et de la Liste de Contrôle d'Accès VTY :**
  - L'accès SSH est activé pour la gestion à distance du routeur.
  - Une liste de contrôle d'accès est créée pour restreindre l'accès SSH à partir du sous-réseau de gestion uniquement.

E. Configuration des Routeurs FAI (ISP1 et ISP2) :

Le routeur ISP1 est chargé de fournir la connectivité Internet à l'entreprise. Voici un résumé des principales étapes de sa configuration :

- Attribution des adresses IP aux interfaces connectées au réseau de l'entreprise et à Internet.
- Configuration du protocole BGP pour échanger des routes avec le routeur vIOS-EDGE-I.
- Mise en place du NAT pour traduire les adresses des sous-réseaux internes en adresses publiques.
- Configuration des serveurs DNS pour la résolution des noms de domaine.
- Réalisation de tests de connectivité pour vérifier l'accès Internet depuis le réseau de l'entreprise.
- La configuration du routeur ISP2 est similaire à celle du routeur ISP1, car il remplit le même rôle en tant que fournisseur d'accès Internet.

F. Tests de Connectivité après la réalisation :

- **Test de ping entre ISP1 et ISP2:**

```
ISP1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     192.168.100.14  YES DHCP   up                    up
GigabitEthernet1/0     198.10.10.1     YES NVRAM  up                    up
ISP1#ping 192.168.100.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.15, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 304/312/324 ms
```

```
ISP2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0     192.168.100.15  YES DHCP   up                    up
GigabitEthernet1/0     197.10.10.1     YES NVRAM  up                    up
ISP2#ping 192.168.100.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 376/387/396 ms
```

- **Test de Ping entre vIOS-EDGE et Google :**

```
vIOS-EDGE-I#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/70/164 ms
vIOS-EDGE-I#
```

- **Test de Ping entre PC4 et Google :**

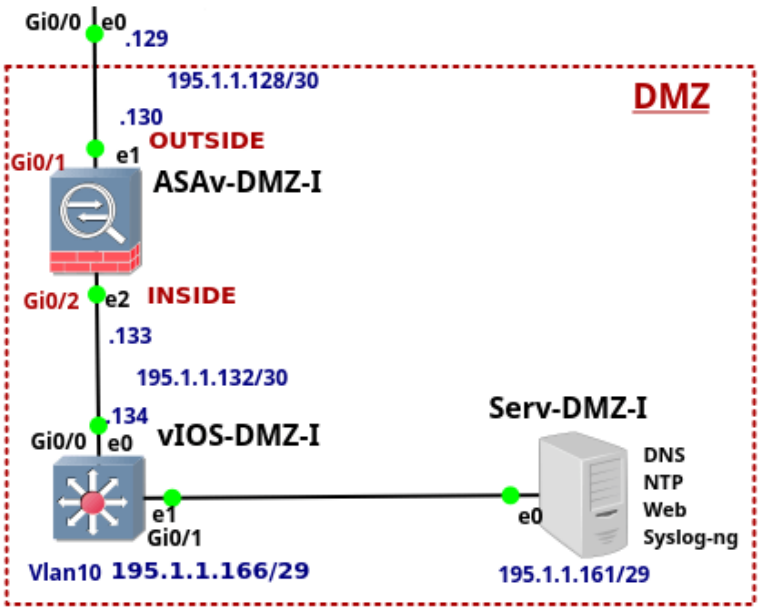
```
gns3@box:/opt$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:DB:BF:6C:00:00
          inet addr:192.168.40.1  Bcast:192.168.40.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:421 errors:0 dropped:0 overruns:0 frame:0
          TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34874 (34.0 KiB)  TX bytes:91958 (89.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

gns3@box:/opt$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=110 time=71.942 ms
64 bytes from 8.8.8.8: seq=1 ttl=110 time=70.286 ms
64 bytes from 8.8.8.8: seq=2 ttl=110 time=64.402 ms
64 bytes from 8.8.8.8: seq=3 ttl=110 time=68.075 ms
64 bytes from 8.8.8.8: seq=4 ttl=110 time=68.019 ms
64 bytes from 8.8.8.8: seq=5 ttl=110 time=67.537 ms
64 bytes from 8.8.8.8: seq=6 ttl=110 time=62.738 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 62.738/67.571/71.942 ms
gns3@box:/opt$
```

V/- Réseau d'entreprise sur GNS3 - Partie – DMZ:

1. Intégration et Configuration de la Zone Démilitarisée (DMZ) au sein du Réseau d'Entreprise:

A. Introduction :

L'implémentation et la configuration stratégique d'une Zone Démilitarisée (DMZ) au cœur de l'architecture réseau de notre entreprise. L'objectif principal de cette initiative est de renforcer considérablement la sécurité de notre réseau d'entreprise. La DMZ est spécifiquement conçue pour isoler efficacement l'accès externe aux services critiques internes, agissant comme une barrière de sécurité robuste qui protège nos ressources informatiques internes des accès non autorisés tout en facilitant une interaction sécurisée avec l'Internet public. Cette configuration permet de mitiger les risques tout en assurant une continuité de service optimale pour tous les utilisateurs autorisés.



Voici une reformulation plus détaillée et professionnelle de cette section du rapport concernant la composition et la configuration de la Zone Démilitarisée (DMZ) :

B. Composition et Configuration des Composants de la DMZ :

La Zone Démilitarisée (DMZ) de notre réseau est structurée autour de trois éléments clés, chacun jouant un rôle essentiel dans la sécurisation et la gestion optimale du trafic réseau :

1.ASAv-DMZ-I : Ce dispositif agit en tant que barrière de sécurité avancée, dédié à la segmentation et à la gestion du trafic réseau. Il est essentiel pour établir des zones de confiance distinctes au sein de notre architecture, permettant ainsi une séparation claire et sécurisée entre les ressources internes et les accès externes.

2. vIOS-DMZ-I : Ce commutateur multicouche est au cœur de notre infrastructure de connectivité. Il gère efficacement les VLANs et assure la distribution optimale des flux de données à travers la DMZ, contribuant à une performance réseau améliorée et à une gestion plus fine des accès réseau.

3. Serv-DMZ-I : Serveur dédié hébergeant les services essentiels tels que DNS, NTP, Web, et Syslog-ng. Ce serveur est configuré pour maximiser la fiabilité et la sécurité de ces services, jouant un rôle dans le maintien de la communication et de la synchronisation au sein de notre infrastructure.

Chaque composant a été méticuleusement configuré pour répondre aux normes les plus strictes en matière de sécurité et de performance. Les adresses IP ont été allouées à partir du sous-réseau 195.1.1.128/25. Des VLANs spécifiques ont été établis pour renforcer le contrôle d'accès, assurant ainsi que seules les communications autorisées traversent la DMZ.

C. Interconnexion avec l'Architecture Edge et les Fournisseurs de Services Internet (ISP) :

La Zone Démilitarisée (DMZ) est stratégiquement connectée à notre infrastructure Edge, intégrant les routeurs vIOS-EDGE-I et II. Cette configuration assure une liaison directe avec deux fournisseurs de services Internet, permettant ainsi une connectivité redondante et robuste. Cette redondance est cruciale pour garantir la continuité des services et une résilience accrue face aux pannes potentielles ou aux fluctuations de performance des réseaux externes.

D. Configuration Avancée des Composants de la DMZ :

La configuration de chaque élément de la DMZ a été soigneusement détaillée afin d'assurer un haut niveau de sécurité et une gestion efficace du réseau :

- Niveaux de sécurité : Des mesures strictes sont appliquées à travers des dispositifs distincts pour créer des barrières robustes contre les menaces externes.

- Segmentation du réseau : Les VLANs et la segmentation du trafic sont configurés pour minimiser les risques de pénétration du réseau interne et pour isoler efficacement les segments du réseau.

- Routes Statiques : Des itinéraires prédéfinis sont établis pour le trafic afin de contrôler et de diriger les flux de données, améliorant ainsi la sécurité et l'efficacité du réseau.

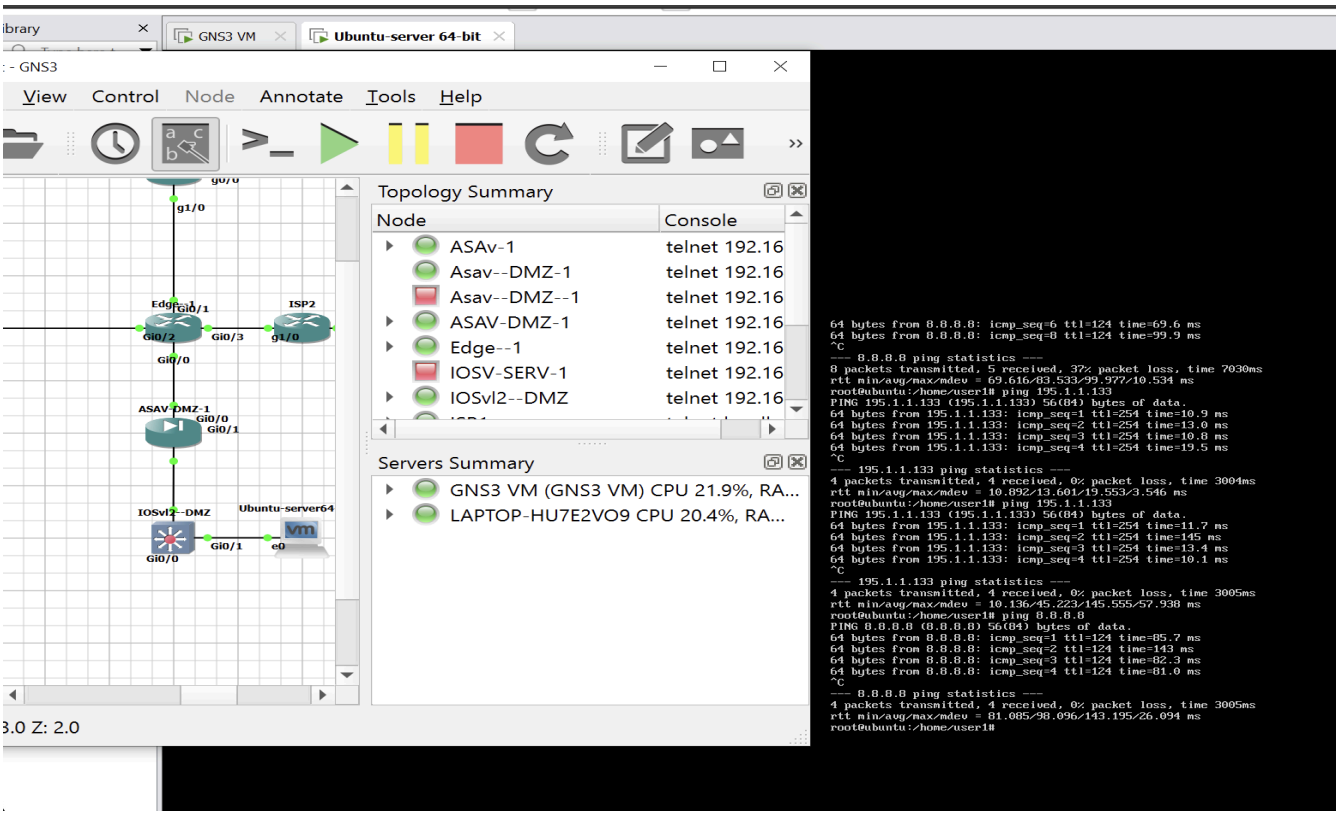
- Protocoles d'Authentification : Des protocoles robustes sont mis en place pour vérifier l'identité des utilisateurs et des dispositifs, renforçant la sécurité des accès.

- Politiques d'Inspection du Trafic : Des politiques sont appliquées pour surveiller et inspecter le trafic réseau, s'assurant que seules les communications valides et sécurisées sont autorisées à travers la DMZ.

Ces configurations sont essentielles pour maintenir l'intégrité et la sécurité du réseau d'entreprise, tout en facilitant une gestion flexible et sécurisée du trafic de données.

E. Test et Validation :

- **Test de Ping entre le serv-dmz et ASAv-dmz :**



2. Conception et Configuration de la Zone Démilitarisée (DMZ) :

A. Objectif de la Zone Démilitarisée (DMZ) :

La Zone Démilitarisée, ou DMZ, est stratégiquement conçue pour fonctionner comme une barrière de sécurité essentielle entre le réseau interne de l'entreprise et l'internet externe. En établissant cette couche intermédiaire, la DMZ s'assure que toutes les communications entre le réseau sécurisé de l'entreprise et le vaste écosystème d'Internet sont minutieusement contrôlées et surveillées. Cela réduit significativement le risque d'attaques directes sur les ressources vitales de l'entreprise, en maintenant un équilibre optimal entre accessibilité externe et sécurité interne.

B. Dispositifs DMZ et son Roles :

1. ASAv-DMZ-I : Agissant comme pare-feu, il est responsable de la segmentation du trafic entre la DMZ, le réseau interne et Internet.

2. vIOS-DMZ-I : Un commutateur multicouche qui gère la connectivité réseau et les VLAN.

3. Serv-DMZ-I : Serveur sous Linux fournissant des services de DNS, NTP, Web et Syslog-ng

C. Configuration des Dispositifs de la DMZ :

- **ASAv-DMZ-I :**

- Interfaces de Sécurité : Configurées avec des niveaux de sécurité distincts pour une séparation efficace du trafic. Le niveau 100 est assigné pour les interfaces internes (INSIDE) et le niveau 0 pour les interfaces externes (OUTSIDE), assurant une stricte distinction entre le trafic interne sécurisé et celui provenant d'Internet.

- Routes Statiques : Définies pour canaliser les flux de trafic spécifiques vers l'Internet et le réseau interne, optimisant la gestion du trafic et la sécurité.

- Politique d'Inspection HTTP : Implémentée pour examiner minutieusement le trafic HTTP, détectant et prévenant les violations de protocole et les tentatives d'intrusion.

- **vIOS-DMZ-I :**

- Configuration des VLAN : Les VLAN sont définis pour segmenter stratégiquement le trafic au sein de la DMZ, contrôlant ainsi l'accès aux ressources critiques et améliorant la sécurité.

- Désactivation du VTP (VLAN Trunking Protocol) : Pour éviter les modifications non autorisées et maintenir l'intégrité de la configuration des VLAN.

- Sécurité d'Accès : SSH et d'autres protocoles d'authentification robustes sont employés pour sécuriser l'accès administratif aux équipements réseau.

- **Serv-DMZ-I :**

- Services Hébergés : Le serveur héberge les services DNS, NTP, Web et Syslog-ng, tous configurés pour assurer une performance optimale et une haute sécurité.

- DNS : Utilise Bind9 pour une gestion avancée du cache et une résolution efficace des requêtes DNS.

- Serveur Web Apache2 : Configuré pour traiter les requêtes web de manière sécurisée, avec des mesures renforcées contre les attaques web et les abus de protocole.

D. Sécurité et Accessibilité :

- **Listes d'accès (ACL) sur l'ASAv-DMZ-I :** Les ACL sont méticuleusement configurées pour fournir un contrôle précis sur le trafic entrant et sortant. Elles permettent la filtration des données, autorisant uniquement les services spécifiquement approuvés tout en bloquant les autres, ce qui renforce la sécurité en limitant les vecteurs d'attaque potentiels.
- **Mesures d'Authentification Avancées :** Des protocoles d'authentification robustes sont implémentés pour assurer que seul le personnel dûment autorisé puisse accéder aux dispositifs critiques de la DMZ. Cette stratégie prévient les accès non autorisés et les potentielles compromissions de sécurité.
- **Politiques de Sécurité :** Des politiques de sécurité exhaustives sont mises en place pour protéger les services exposés à l'Internet. Ces politiques assurent que les systèmes sont à l'abri des vulnérabilités connues et que les logs sont systématiquement collectés et analysés. Cette analyse aide à détecter rapidement toute activité suspecte ou tentative d'intrusion, permettant une réaction rapide pour sécuriser les ressources.

3. Conclusion:

L'implémentation de notre architecture DMZ a nettement renforcé la sécurité de notre réseau d'entreprise. Grâce à cette stratégie, nous avons atteint une gestion du trafic entrant depuis Internet à la fois plus efficace et plus sécurisée. Les dispositifs et configurations mis en place au sein de la DMZ garantissent une isolation robuste des services internes, protégeant ainsi nos ressources informatiques critiques contre les menaces externes. Cette architecture nous permet non seulement de défendre notre réseau contre les intrusions mais aussi de

maintenir une performance réseau optimale, assurant la continuité et la fiabilité des opérations d'entreprise. En conséquence, la DMZ est devenue un élément central de notre stratégie de sécurité, jouant un rôle crucial dans la préservation de l'intégrité et la confidentialité de nos données.

Conclusion :

En conclusion, la mise en place de ce réseau d'entreprise sur GNS3 a été une expérience enrichissante. Nous avons appris à configurer et à interconnecter les différents éléments d'un réseau, y compris le campus, le centre de données et les zones DMZ.

Ce projet nous a permis de comprendre l'importance de la planification, de la conception et de la configuration pour assurer un fonctionnement efficace et sécurisé du réseau. En plus d'acquérir des compétences techniques, nous avons également développé notre capacité à gérer le temps, à résoudre les problèmes et à collaborer en équipe. En résumé, ce projet nous a fourni une base solide pour comprendre les principes des réseaux d'entreprise et nous a préparés à relever de nouveaux défis dans le domaine de l'informatique et des réseaux.