

Preuve de compétence

Épreuve E6

Administration matériel Cisco



20/03/2025

Concevoir une solution d'infrastructure réseau	4
1. Analyser un besoin exprimé et son contexte juridique	4
2. Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique.....	4
3. Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques.....	4
4. Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service	4
5. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue.....	5
6. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue	5
Installer, tester et déployer une solution d'infrastructure réseau	6
1. Installer et configurer des éléments d'infrastructure.....	6
Etape 1 : Configuration du Switch L3B6.....	6
Étape 2 : Configurer le Routeur Rt1B6	8
Étape 3 : Configuration du Switch L2B6.....	10
Étape 4 : Préparation de la machine dans le nouveau réseau	11
Étape 5 : Blocage du réseau 10.4.1.0 pour 172.16.0.0	13
2. Installer et configurer des éléments nécessaires pour assurer la qualité de service	14
3. Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure.....	14
4. Tester l'intégration et l'acceptation d'une solution d'infrastructure	14
5. Déployer une solution d'infrastructure	15
Exploiter, dépanner et superviser une solution d'infrastructure réseau.....	15
1. Évaluer, maintenir et améliorer la qualité d'un service	16

Concevoir une solution d'infrastructure réseau

1. Analyser un besoin exprimé et son contexte juridique

Dans le cadre de la société fictive Littoral, il a été nécessaire de créer un réseau isolé permettant de faire communiquer un poste Windows 7 vers Internet, tout en bloquant l'accès aux serveurs internes. L'analyse a permis de respecter les contraintes de sécurité et d'isolation du système d'information tout en répondant à un besoin fonctionnel de connectivité externe. La mise en place d'un filtrage avec des ACL et des règles PFSense s'inscrit aussi dans le respect des bonnes pratiques de cloisonnement réseau.

2. Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique

La création d'un nouveau réseau (172.16.0.0/24) rattaché au réseau principal de Littoral (10.4.1.0/24) via un routeur Cisco a impliqué une étude d'impact sur la topologie existante, la configuration du routage et la gestion des flux vers le pare-feu. Il a fallu s'assurer que l'ajout de ce nouveau segment n'allait pas compromettre la sécurité ou la stabilité de l'infrastructure.

3. Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques

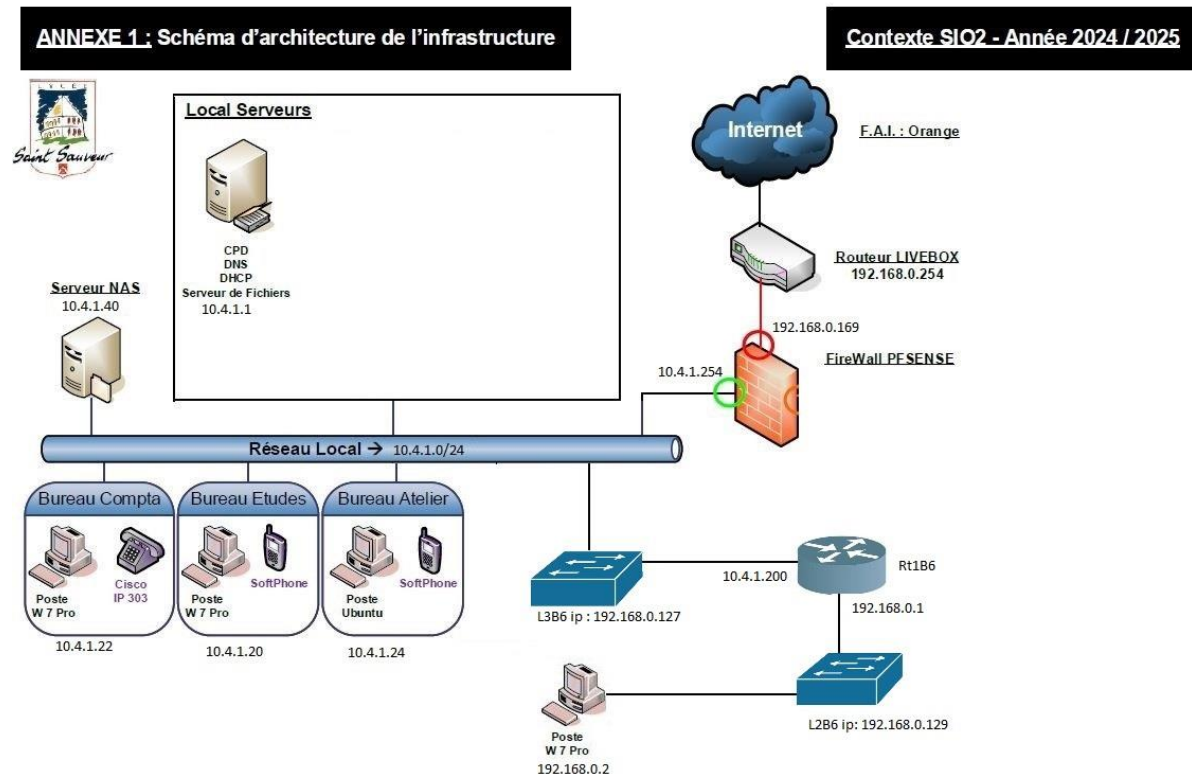
Les choix ont été justifiés entre l'utilisation de VLANs, d'une architecture routeur + pare-feu PFSense, et de la mise en place d'un routage avec filtrage. Le document Preuve Cisco sert aussi de documentation technique, où sont détaillés le plan d'adressage, la configuration des ports, des interfaces, du routage et des filtrages.

4. Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service

Les équipements Cisco ont été choisis pour leur fiabilité. La séparation des réseaux avec des VLANs, un routage précis et des règles claires permet de garantir une disponibilité des services tout en contrôlant les flux. La connectivité Internet est assurée via le PFSense, avec des tests de ping vers 8.8.8.8 pour valider la continuité du service.

5. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue

Une maquette a été réalisée avec un routeur, deux switches (L2 et L3), un PC Windows 7, le tout connecté dans un environnement isolé au sein du lycée. Cette maquette a permis de tester les configurations dans un environnement réel avant validation.



6. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

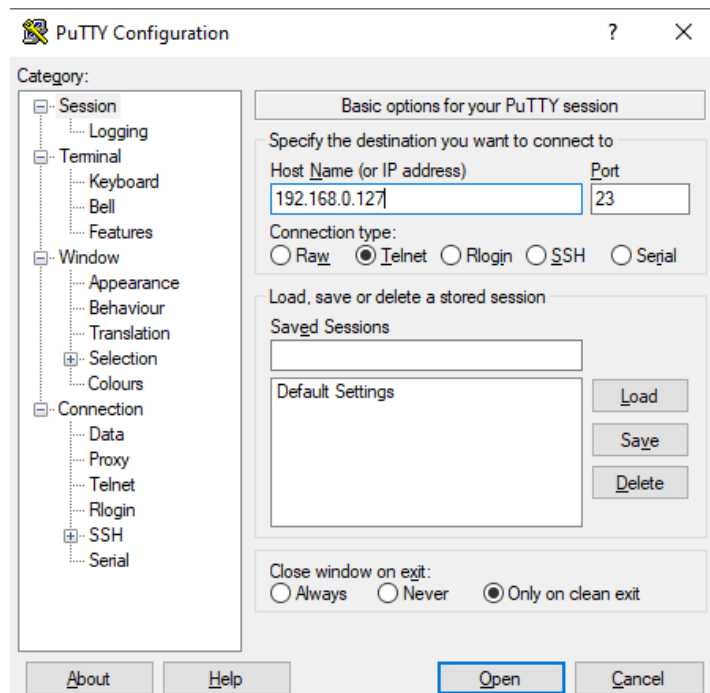
Des tests de connectivité ont été effectués à chaque étape :

- Ping entre les interfaces
- Ping entre le poste Windows 7 et le routeur
- Ping vers Internet
- Blocage volontaire des pings vers le réseau interne pour valider le filtrage

Installer, tester et déployer une solution d'infrastructure réseau

1. Installer et configurer des éléments d'infrastructure

Etape 1 : Configuration du Switch L3B6



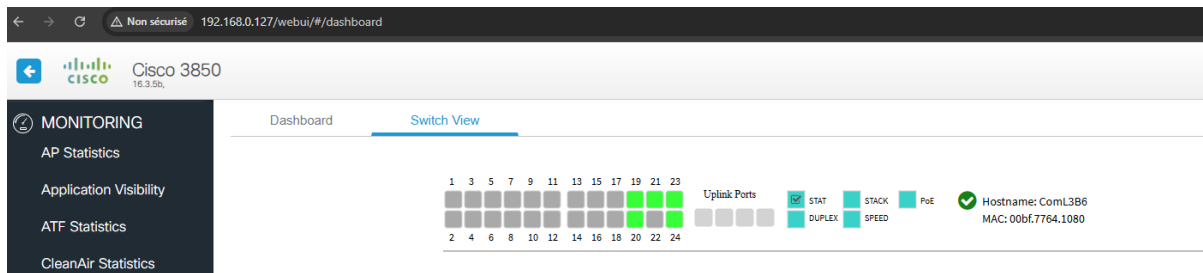
On se connecte via putty en telnet au 192.168.0.127 qui est le switch L3B6

```
User Access Verification

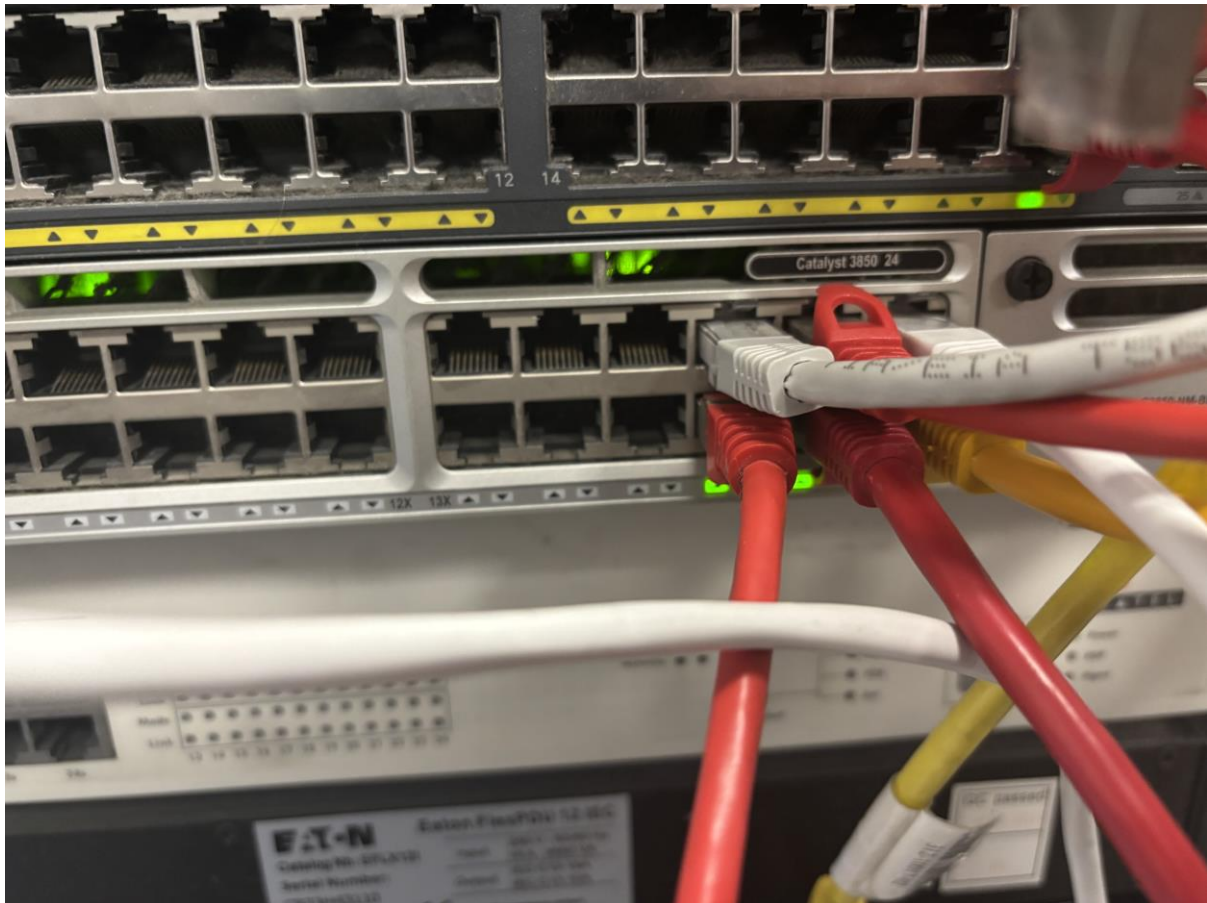
Password:
ComL3B6>enable
Password:
ComL3B6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ComL3B6(config)#in range gil/0/19-24
ComL3B6(config-if-range)#sw m a
ComL3B6(config-if-range)#sw a v 40
ComL3B6(config-if-range)#exit
ComL3B6(config)#exit

ComL3B6(config)#ip default-gateway 10.4.1.254
```

On configure les ports occupés par le réseau de Littoral dans le Vlan 40 (il n'y a que le port 24 qui est lié au routeur qu'on configurera après).



On se retrouve avec une interface comme ceci (le matériel du port 22 n'est actuellement pas allumé)

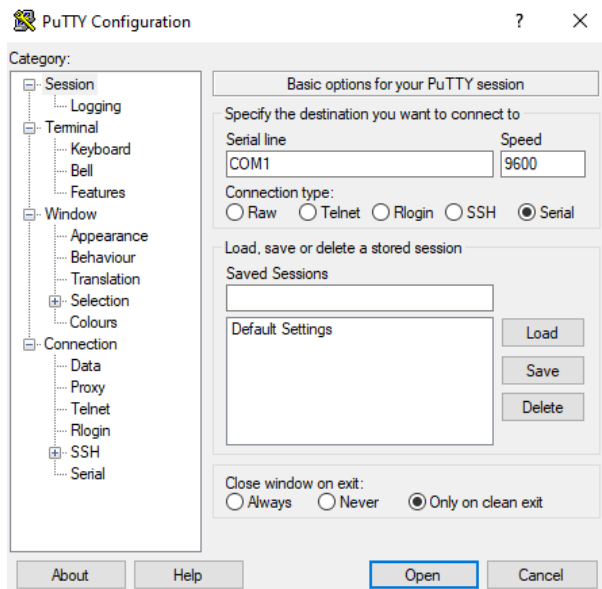


On retrouve le Switch branché de cette manière, avec celui en bas à droite qui va vers le nouveau routeur, et celui en haut à droite qui amène le réseau.

Étape 2 : Configurer le Routeur Rt1B6

Le routeur est branché de manière à ce que le port 0/0/1 est lié au Switch L3B6, qui sera à l'ip 10.4.1.200, donc au réseau Littoral, et le port 0/0/0 va envoyer vers le réseau 172.16.0.0/24, et sera à l'ip 172.16.0.254, et va se brancher au Switch L2B6 plus tard.

Étant donné que nous n'avons accès par aucun moyen au routeur il faut se connecter en port Console.



Tout d'abord il faut donner des IP aux interfaces comme dit précédemment :

```
Rt1B6(config)#int gi0/0/0
Rt1B6(config-if)#no ip address
Rt1B6(config-if)#ip address 172.16.0.254 255.255.255.0
Rt1B6(config-if)#no sh
Rt1B6(config-if)#exit
Rt1B6(config)#exit
```

```
Rt1B6(config)#int gi0/0/1
Rt1B6(config-if)#ip address 10.4.1.200 255.255.255.0
Rt1B6(config-if)#no sh
Rt1B6(config-if)#end
```

Puis configurer de sorte à ce que faire transiter les paquets entre ces deux réseaux et à rajouter une route par default qui est le gateway du pfsense pour Littoral.

```
Rt1B6(config)#ip route 0.0.0.0 0.0.0.0 10.4.1.254
```



Le routeur est monté de cette manière, le cable jaune en haut va vers Littoral, donc 10.4.1.0, et le cable rouge en bas va vers le nouveau reseau donc 172.16.0.0 .

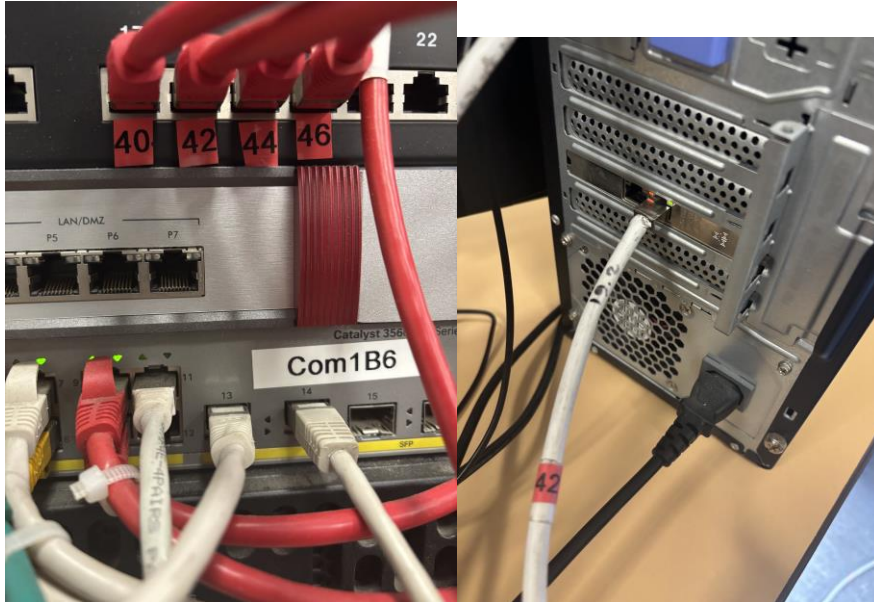
Étape 3 : Configuration du Switch L2B6

Pour ce switch le port 23 servira de lien vers le PC Windows 7, et le port 24 est relié directement au routeur Rt1B6.

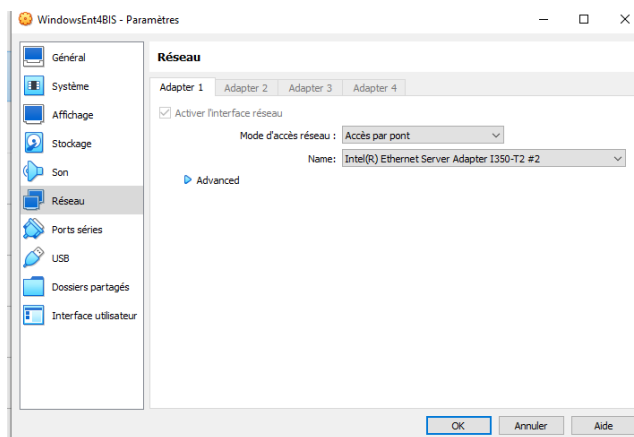


Étape 4 : Préparation de la machine dans le nouveau réseau

Pour ceci j'ai pris une machine Windows 7 pro, qui est connecté par pont de cette manière :

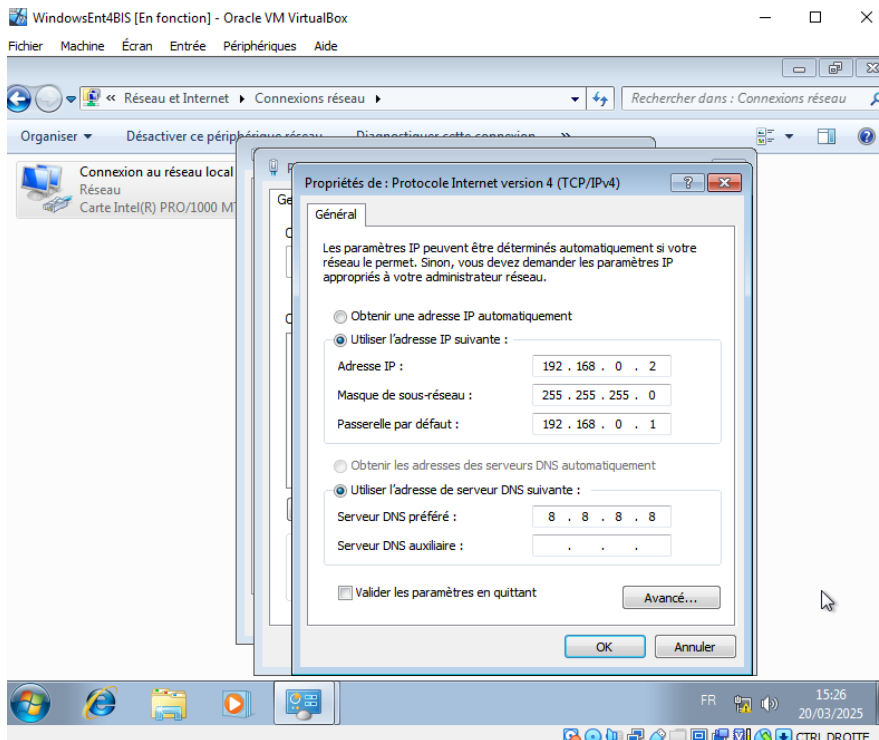


Le port 23 est relié à un switch, qui ressort derrière la table, le numéro 42, qui est ensuite relié à une carte réseau annexe sur le PC,



Ainsi sur VirtualBox on met la carte reseau comme entrée de reseau pour la VM de la Windows 7

On retrouve donc une Windows 7 qui est relié au reseau 172.16.0.0 et qui a comme gateway la sortie du routeur donc 172.16.0.254 :



On retrouve ces paramètres-là, avec comme IP 172.16.0.2/24

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\eliaz>ping 192.168.0.1

Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.0.1 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\eliaz>ping 10.4.1.200

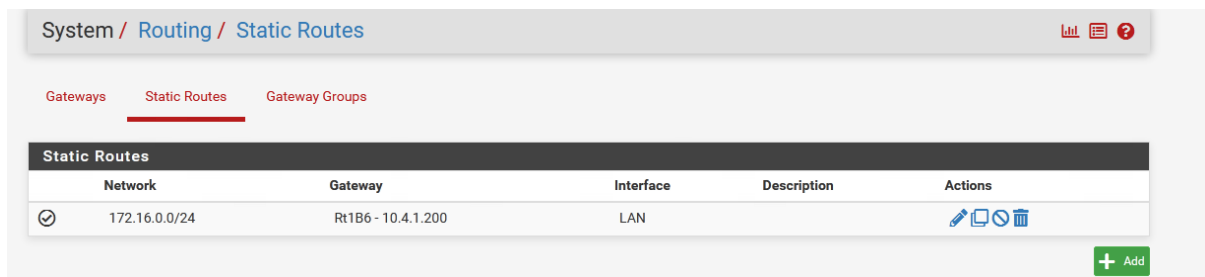
Envoi d'une requête 'Ping' 10.4.1.200 avec 32 octets de données :
Réponse de 10.4.1.200 : octets=32 temps<1ms TTL=255
Réponse de 10.4.1.200 : octets=32 temps<1ms TTL=255
Réponse de 10.4.1.200 : octets=32 temps=1 ms TTL=255
Réponse de 10.4.1.200 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 10.4.1.200:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

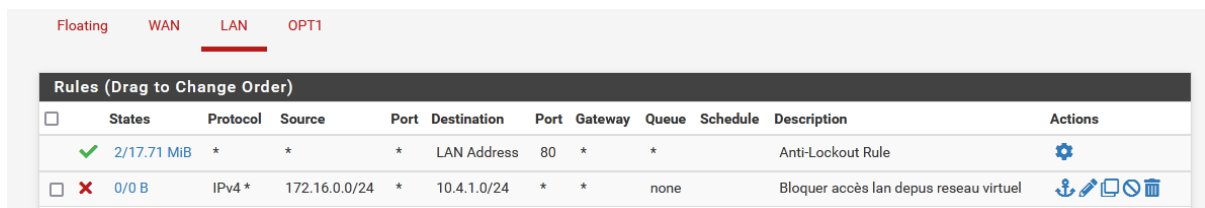
C:\Users\eliaz>
```

Ce qui permet de PING son gateway, ainsi que la sortie l'interface 10.4.1.200 du routeur.

Étape 5 : Blocage du réseau 10.4.1.0 pour 172.16.0.0



Il faut commencer par autoriser la communication du nouveau réseau vers le réseau de Littoral grâce à une route statique dans le pare-feu pfSense.



Dans l'interface LAN il faut bloquer la communication du nouveau réseau sur celui de Littoral, mais que pour le réseau pas pour 8.8.8.8, avec une règle de pare-feu

```
Rt1B6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rt1B6(config)#ip access-list extended BLOQUE_LAN
Rt1B6(config-ext-nacl)#deny ip 172.16.0.0 0.0.0.255 10.4.1.0 0.0.0.255
Rt1B6(config-ext-nacl)#permit ip any any
Rt1B6(config-ext-nacl)#exit
Rt1B6(config)#int gi0/0/0
Rt1B6(config-if)#ip access-group BLOQUE_LAN in
Rt1B6(config-if)#
```

Pareil mais avec une ACL sur le routeur Rt1B6.

```
C:\Users\eliaz>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 9ms, Moyenne = 8ms

C:\Users\eliaz>ping 10.4.1.1
Envoi d'une requête 'Ping' 10.4.1.1 avec 32 octets de données :
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 10.4.1.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Ainsi le Windows 7 communique bien avec 8.8.8.8, mais ne communique pas avec le réseau de Littoral.

2. Installer et configurer des éléments nécessaires pour assurer la qualité de service

Le réseau virtuel est isolé pour garantir la sécurité et la stabilité du réseau principal.

Une route statique a été ajoutée dans le firewall PFSense pour que les paquets en provenance du réseau virtuel puissent atteindre Internet.

Une ACL a été mise en place sur le routeur Cisco pour bloquer les communications vers le réseau de l'entreprise, tout en autorisant l'accès à Internet (par exemple 8.8.8.8).

Cela permet de garantir un contrôle fin du trafic, améliorant la sécurité globale tout en assurant un accès stable au réseau externe.

3. Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure

Tout au long du projet, j'ai documenté chaque étape dans ce rapport :

- Schéma de l'architecture réseau
- Commandes de configuration utilisées
- Paramétrages IP des interfaces
- Capture d'écrans de tests ping

Cette documentation technique permettrait à un autre technicien de comprendre, maintenir ou répliquer l'infrastructure facilement.

4. Tester l'intégration et l'acceptation d'une solution d'infrastructure

Des tests ont été réalisés pour vérifier le bon fonctionnement de l'ensemble :

- Ping depuis le PC Windows 7 vers la passerelle (172.16.0.254)

```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\eliaz>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . : 
    Adresse IPv6 de liaison locale. . . . : fe80::8c4e:1fff:ab59:16%11
    Adresse IPv4. . . . . : 172.16.0.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : fe80::7269:5aff:fe20:e930%11
                                   172.16.0.254

Carte Tunnel isatap.{520F878F-A66E-48EF-A2F2-2B1C6C94CB32} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
```

```
C:\Users\eliaz>ping 172.16.0.254

Envoi d'une requête 'Ping' 172.16.0.254 avec 32 octets de données :
Réponse de 172.16.0.254 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.0.254 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.0.254 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.0.254 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 172.16.0.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 2ms, Moyenne = 1ms
```

- Ping vers Internet (8.8.8.8)

```
C:\Users\eliaz>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=108

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 8ms, Moyenne = 8ms
```

- Vérification que les pings vers 10.4.1.0/24 sont bien bloqués

```
C:\Users\eliaz>ping 10.4.1.1

Envoi d'une requête 'Ping' 10.4.1.1 avec 32 octets de données :
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.0.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 10.4.1.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Ces tests ont permis de valider le bon routage, l'isolation du réseau et l'accès contrôlé à Internet. L'ensemble du système a été testé et validé selon les attentes.

5. Déployer une solution d'infrastructure

Une fois toutes les configurations validées, le déploiement a été effectué sur le matériel physique présent dans la salle réseau du lycée.

Le réseau virtuel fonctionne de manière autonome, avec un cloisonnement efficace et une documentation technique complète.

Il est possible d'ajouter d'autres machines dans le réseau 172.16.0.0/24 en conservant les règles de filtrage définies.

Exploiter, dépanner et superviser une solution d'infrastructure réseau

1. Évaluer, maintenir et améliorer la qualité d'un service

La qualité du service a été évaluée à travers des tests de connectivité (ping) depuis le poste Windows 7, en vérifiant l'accès à Internet (8.8.8.8) et le blocage vers le réseau entreprise (10.4.1.0/24).

En cas de dysfonctionnement, la configuration du routeur et du pare-feu PFSense a été vérifiée grâce à des commandes comme `show ip route`, `show running-config`, et à la relecture des règles de pare-feu.

L'ACL sur le routeur permet d'ajuster finement les flux entre réseaux. En cas de besoin, elle peut être modifiée pour affiner le niveau d'isolation.

La documentation du projet permet de retracer l'ensemble de la configuration, ce qui facilite la maintenance et les améliorations futures.

Le système a été conçu de manière modulaire, ce qui permet d'ajouter facilement de nouvelles machines au réseau virtuel tout en conservant les règles existantes.