AKSEL

CAUBEL

RT2 IOM

ADMINISTER

DISCLAMER, DANS LE CADRE DE L'EXERCICE DU PORTFOLIO, SEUL LES PISTES SONT NOTÉES DANS ADMINISTRER/ PROGRAMMER / CONNECTÉ MAIS SI VOUS VOULAIS VOIR DES RAPPORT PLUS REPRÉSENTATIF, ETENDRE ET PLUS PARTICULIÈREMENT EXPLOITÉ ONT ÉTÉ TRAVAILLÉ / APPROFONDI. DE PLUS N'ÉTANT QU'UN BROUILLE POUR LA MISE EN FORME, L'ORTHOGRAPHE N'A PAS ÉTAIT RETRAVAILLÉ.

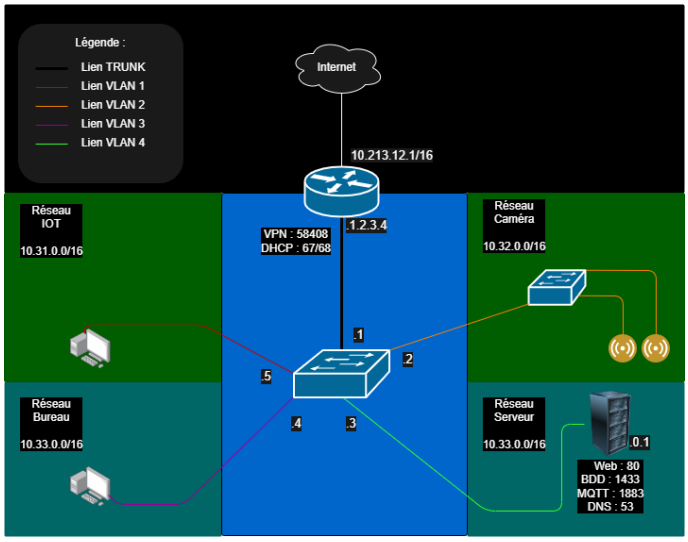
CONFIGURER ET DÉPANNER LE ROUTAGE DYNAMIQUE DANS UN RÉSEAU

- OSPF avec FRR | Exemple de dépannage avec limite dans le cadre de la SAE3I03 avec le multicast qui ne passe pas dans WireGuard

CONFIGURER UNE POLITIQUE SIMPLE DE QOS ET LES FONCTIONS DE BASE DE LA SÉCURITÉ D'UN RÉSEAU

- Parler de la mise en place de VLAN et se renseigner pour mettre en place un faux réseau avec un test de QOS avec débit varier (faire des demandes de matériel)

Lors de la mise en place d'un réseau d'entreprise contant 4 services différents, j'ai pu mettre en place un réseau VLANisé :



Dans ce dernier je n'ai pas eu a géré la Qualité de Service mais cela devrais être vu prochainement.

En revanche j'ai pu me perfectionner dans la mise en place de la sécurité d'un réseau par son FireWall.

Dans ma solution mise en place j'utilise un ordinateur linux comme routeur avec FRR pour la mise en place du protocole de routage dynamique OSPF.

De se fait je me suis penché sur les différents types de FireWall que je pouvais faire et m'en est resorti deux noms : ipTables qui est très utilisé et également très simple syntaxiquement parlant mais il n'est plus mit à jour sans parler qu'il y a beaucoup d'autre extension à installer pour l'utiliser dans toutes les circonstances.

Le deuxième nom et qui est celui que j'ai retenu est NFTables. Plus compliquer syntaxiquement parlant, NFTables est le prédécesseur de ipTables regroupent plusieurs outils que l'on installer autour de ce dernier. Après avoir suivis des cours en ligne pour comprendre son fonctionnement et me perfectionner sur le FireWall que j'avais vu de manière très succin durant ma permière année, j'ai pu mieux comprendre le comportement d'un routeur :

Il existe 5 différents points de "réflexion" dans le routage:

- le Pre-routing qui va agir avant même de diriger le paquet.
- Le Input qui va servir si le paquet doit entrer dans mon interface.
- Le Output s'il sort de mon interface (de manière général, si je sors c'est que je veux).
- Le Forward qui permet de mettre des règles sur les paquets que je dois redirigés.
- Le Post-routing qui va être la modification du paquet après que l'on est regardées toute les règles précédentes.

Selon un cahier des charges données j'ai donc pu établir toutes les règles à faire sur chacun des VLANs ainsi que sur les communications extérieurs. ***re-faire l'illustations des différents accès***

```
# Flush

nft flush ruleset

# NAT

nft add table nat
nft add chain nat prerouting { type nat hook prerouting priority 0 \;}
nft add chain nat postrouting { type nat hook postrouting priority 0 \;}
nft add rule nat postrouting masquerade

# Destination NAT

nft add rule nat prerouting iif eno1 tcp dport 80 dnat 10.34.0.1:80
nft add rule nat prerouting iif eno1 tcp dport 443 dnat 10.34.0.1:80
nft add rule nat prerouting iif eno1 tcp dport 8086 dnat 10.34.0.1:8086

# SetUP

nft add table ip mon_filtreIPv4
nft add chain ip mon_filtreIPv4 forward { type filter hook forward priority 0 \;}
nft add chain ip mon_filtreIPv4 input { type filter hook forward priority 0 \;}

# BASE

nft add rule mon_filtreIPv4 forward ct state established,related accept
nft add rule mon_filtreIPv4 forward iif eno1 accept

        #ICMP
nft add rule mon_filtreIPv4 forward icmp type echo-request accept
nft add rule mon_filtreIPv4 forward icmp type echo-reply accept

        #DNS
nft add rule mon_filtreIPv4 forward tcp dport 53 accept
nft add rule mon_filtreIPv4 forward udp dport 53 accept
nft add rule mon_filtreIPv4 forward tcp sport 53 accept
nft add rule mon_filtreIPv4 forward udp sport 53 accept

        #DHCP
nft add rule mon_filtreIPv4 forward udp sport 67 accept
nft add rule mon_filtreIPv4 forward udp sport 68 accept
nft add rule mon_filtreIPv4 forward tcp sport 67 accept
nft add rule mon_filtreIPv4 forward tcp sport 68 accept

        #VPN
nft add rule mon_filtreIPv4 input udp dport 58408 accept
nft add rule mon_filtreIPv4 forward iif wg0 accept

# INTERFACE IOT

        #MQTT
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 1883 ip daddr 10.34.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 8883 ip daddr 10.34.0.0/16 ct state new accept

        #MQTT Access to Group 2
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 1883 ip daddr 10.24.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 8883 ip daddr 10.24.0.0/16 ct state new accept

        #MQTT Access to Group 4
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 1883 ip daddr 10.44.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan31 tcp dport 8883 ip daddr 10.44.0.0/16 ct state new accept

# INTERFACE CAMERA

        # NO MORE RULES

# INTERFACE BUREAU

nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 443 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 8086 ct state new accept

        # Access to Group 2
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ip daddr 10.22.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ip daddr 10.24.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 443 ip daddr 10.24.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 8086 ip daddr 10.24.0.0/16 ct state new accept

        # Access to Group 4
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ip daddr 10.42.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 80 ip daddr 10.44.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 443 ip daddr 10.44.0.0/16 ct state new accept
nft add rule mon_filtreIPv4 forward iif vlan33 tcp dport 8086 ip daddr 10.44.0.0/16 ct state new accept

# INTERFACE SERVER

nft add rule mon_filtreIPv4 forward iif vlan34 tcp sport 1883 ip daddr 10.31.0.0/16 ct state new accept

        # Access for Group 2
nft add rule mon_filtreIPv4 forward iif vlan34 tcp sport 1883 ip daddr 10.21.0.0/16 ct state new accept

        # Access for Group 4
nft add rule mon_filtreIPv4 forward iif vlan34 tcp sport 1883 ip daddr 10.41.0.0/16 ct state new accept



# End Rule

nft add rule mon_filtreIPv4 forward drop
```

Dans un but de ne pas avoir de faille non pensé, il est important de faire un mur impermeable en bloquant tous le traffic et ajouter des troues pour le traffic que nous avons besoin.

A savoir que les règles mises en place ne sont pas permanant, il est necessaire de faire une crontab qui au démarrage de l'ordinateur (routeur) exécute le script.sh que vous vouyez si dessus.

DÉPLOYER DES POSTES CLIENTS ET DES SOLUTIONS VIRTUALISÉES

- Se baser sur la première année pour les postes clients car pas refait depuis | Solution virtualisés, se basé sur la SAE 21

DÉPLOYER DES SERVICES RÉSEAUX AVANCÉS ET DES SYSTÈMES DE SUPERVISION

- VPN (Wireguard)
- FireWall (nftable)
- DNS (bind9)

Lors de la mise en place d'un réseau d'entreprise multi-sites, j'ai du mettre en place divers services réseaux "basiques" mais également "avancée".

Ne sachant pas qu'elle service est "avancé" ou non j'ai donc fait la recherche pour trancher.

IDENTIFIER LES RÉSEAU OPÉRATEURS ET L'ARCHITECTURE D'INTERNET

- Non fait a ce jour

TRAVAILLER EN ÉQUIPE

Dans un projet et même dans la vie en général le travaille d'équipe est important car il permet de soulager les charges de travail d'une part mais il permet surtout de faire monter en compétence tous les parties s'il est bien réalisé.

Pour le travail d'équipe je vais commencer par les échecs pour ensuite partir sur mes réussites.

De manière général à l'IUT je dirais que le travail d'équipe est une échec et je vais expliquer pourquoi.

Très régulièrement, dans un groupe tous les parties n'ont pas la même implication.

Lors de mise en situation professionnel comme la SAE3I04 qui est la seule ou je me suis retrouver en binôme cette année, je me suis retrouvé dans un groupe de 3 personnes.

Certaine les personnes avec qui j'étais été un choix mais cela n'est pas forcément synonime de réussite. Mon choix et ce qui fût une des raisons de complication était porté sur une groupe constitué d'amis rendant alors la communication de manque de travail fournit par certain difficile.

Dans le groupe les niveaux était très hétérogène ce qui n'était en aucun cas dérangeant et même plaisant. J'aime beaucoup apprendre au autre mes connaissances (disclamer : Uùniquement celle que je métrise de manière sûr).

Mais le vrai problème comme énoncé plus haut est l'investissement de certain, lorsque nous arrivons à devoir reprendre le travail de tous le monde car les personnes de s'investisse pas ce n'est pas du travail d'équipe.

Pour en revenir a la compétence, j'estime que j'ai encore à travailler sur la partie de comment donner l'envie a mes collaborateurs de travailler et réussir à transmettre cette amour pour le travail que j'ai même si je suis un bourreau du travail et que je comprend totalement que se ne soit pas la philosophie de tous le monde bien au contraire.

Pour ce qui est de mes réussites en collaboration car oui il y en a :

Lorsque tous les parties travailles avec sérieux même s'il y a forcément des moments de relachement sinon nous ne serions plus capable de faire la différence entre un 0 et un 1, tous se passe bien et dans c'est cas là en général nous fonctionnons de cette manière :

- Discution de la mise en place du projet.
- Réflection des solutions possibles avec une mise en commun pour mettre en confrontation nos idées pour choisir la meilleur ou même en trouver une autre meilleur grâce à nos points de vue différent.
- Un répartition des tâches en fonction de nos préférences / compétences. Dans le but également que nous gagnons en compétence j'essaie personnellement si le temps nous le permet de faire ensemble ou d'avoir des explications de la personne sur les points que je ne connais pas et que lui oui et inversément quitte a sortir du sujet principale pour bien comprendre le système.
- résolution des bugs ensembles.

De manière générale nous utilisons aussi Github pour rassembler le travail et ainsi avoir la possibilité de faire du versionning tout-en aillant un travail disponible même si certain membres ne sont pas présent momentanément.

Cela permet si les tâches sont asynchrones de pouvoir évoluer dans des espaces séparés tout en aillant un merge des travaux réalisés.

Dans le cas d'un travail qui nécessite de modifier le même fichier en même temps pour créer des fonctions ou des comptes rendu par exemple, j'utilise l'option de Live Share de Visual Studio Code qui nous permet de partager notre sessions avec nos collaborateurs.