Documentation Pôle Réseaux.

Sommaire

I. Présentation du projet

Pour ce projet, nous avions pour objectif de **mettre en place une architecture réseau** utilisant plusieurs technologies comme : - Les **VLAN** - Le **Routage OSPF** - La mise en place d'un **FireWall** - La mise en place d'un **serveur DHCP/DNS** - Configurer le **NAT/PAT** (avec NAT forwarding service) - Le **VPN**

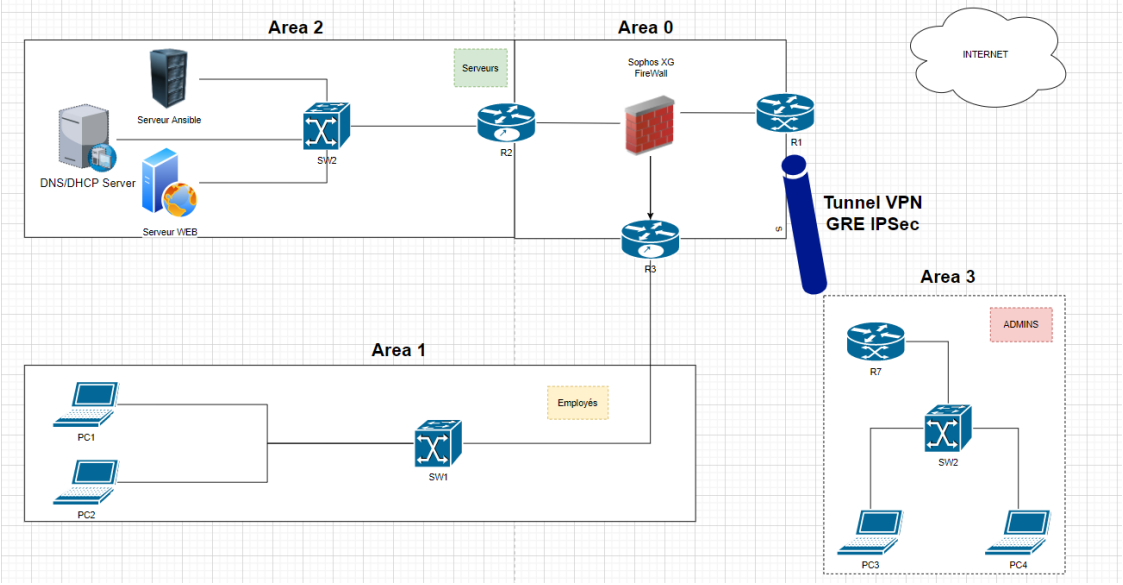
Sur ce repo, vous retrouverez les confs, livrables ainsi que notre projet GNS3.

II. Organisation du projet

Utilisation de Planner

- https://tasks.office.com/ynov.com/fr-FR/Home/Planner/#/plantaskboard?groupId=cf151af7-83e4-4274-96fb-f31bb484b50e&planId=uaQHRlK9z0qpkbb5R1LTp5YAGvj5 ## Utilisation HackMD / Git ### HackMD
- https://hackmd.io/J6xMST0wR9aIFF5Rh60dtQ?both ### Git

- https://github.com/yrlan-montagnier/Labo_Reseaux # III. Livrables ## 1. Schémas des réseaux



2. Tableaux des réseaux

Réseau	Adresse IP + Masque	VLAN	Service
employés	10.10.10.0	10	Réseau privé pour les employés
serveurs	10.10.20.0	20	Salle des serveurs
admins	10.10.30.0	30	Salle pour l'administration
firewall	10.10.40.0	30	Salle pour l'administration

3. Plan d'adressage

Machine	Adresse IP	Réseau
PC1	10.10.10.1	employés
PC2	10.10.10.2	employés
Srv1(DHCP/DNS)	10.10.20.1	serveurs
Srv2(Ansible)	10.10.20.2	serveurs
Web1	10.10.20.3	serveurs
PC3	10.10.30.1	admins
PC4	10.10.30.2	admins
Fw-R1	10.10.40.2	firewall
Fw-R2	10.10.50.2	firewall
Fw-R3	10.10.60.2	Firewall

4. Tableaux des VLAN

	VLAN 10	VLAN 20	VLAN 30
Nom	Employés	Serveurs	Admins
Machines	PC1, PC2	Web1, Srv1, Srv2	PC3, PC4

5. Matrice des flux simplifiés

- **Alias**

Cf. plan d'adressage

Nom	Adresse IP
Google	8.8.8.8

- **Rules**

Port 50000 : NAT forwarding service web ou ansible

Nom	Protocole	@IP src	Port src	@IP dest	Port dest
HTTP	TCP	any	*	any	80
HTTPS	TCP	any	*	any	443
Web1	TCP	Admins	50000	Web1	443
Web1	TCP	Admins	50000	Web1	443
NTP	UDP	any	-	Firewall	123
Ansible SSH	TCP	Admins	-	any	22
DNS ext	TCP,UDP	DNS	-	Google	53
DNS int	TCP,UDP	any	-	DNS	53

IV. Notions obligatoires

Vlan

Un vlan est un réseau local virtuel, qui regroupe plusieurs machines et les isole du reste du réseau en obligeant la comunnication avec divers appareils via un routeur.

Sans VLAN configuré sur le switch, chaque élément du réseau peut communiquer avec l'ensemble du réseau sans passer par un routeur.

A l'aide du VLAN, on va pouvoir isoler certaines interfaces du switch dans un réseau virtuel.

Il permet donc d'améliorer la sécurité du réseau mais aussi d'optimiser la bande passante en séparant les flux de données ### Déclaration des VLAN sur les Switchs - Sur tous les switchs ``` enable conf t vlan 10

name employes vlan 20
name serveurs vlan 30 name admins

```
do wr
```

- Sur `Sw1` ```

  ```

### Routage dynamique OSPF

### Pare-feu au choix (Sophos / pfSense / TNSR)

### Services réseaux (DHCP / DNS)

#### Conf DHCP

- :file_folder:`dhcpd.conf` ### Conf DNS
- :file_folder:`named.conf`
- :file_folder:`dnsdomip.db`
- :file_folder:`dnsipdom.db`

### Accès internet (NAT/PAT)

### Accès aux services internes (NAT/Port Forwarding)

Donner l'accès au serveur web depuis l'ext du rzo https://www.it-connect.fr/pfsense-2-4-creer-une-regle-de-redirection-de-port/

## V. Notions au choix

### Authentification sécurisée sur les équipements réseaux

Dans un réseau il est important de sécuriser l'accès à la configuration des équipements. Pour ce faire, nous avons choisi de mettre en place une authentification par mot de passe sur les switches et routers :

```
Switch#configure terminal
Comm1(config)#line con 0
Comm1(config-line)#password MOTDEPASSE
Comm1(config-line)#login
Comm1(config-line)#end
```

*Ces commandes sont les mêmes que ce soit pour un switch ou un router Cisco.*

Ainsi à chaque fois que l'on accède au terminal de nos équipements, un mot de passe nous est demandé pour passer en mode "enable".
```

```
User Access Verification

Password:
```

Il est donc très simple de mettre en place une sécurité via authentification sur des équipements réseaux ce qui pourrait éviter des manipulations malveillantes via une connexion Telnet.

Port Security (filtrage par adresse MAC)

La fonction s'active en encodant une première fois la commande `switchport port-security` en configuration d'interface.

```
(config)#interface G0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
```

Définition des adresses MAC autorisées

On peut fixer le nombre d'adresses MAC autorisées, ici par exemple 10 :

```
(config-if)#switchport port-security maximum 10
```

Les adresses MAC apprises peuvent être inscrites dynamiquement dans la configuration courante (`running-config`) avec le mot clé "`sticky`" :

```
(config-if)#switchport port-security mac-address sticky
```

Les adresses MAC autorisées peuvent être fixées :

```
(config-if)#switchport port-security mac-address 0000.0000.0003
```

Mode de “violation”

Une “Violation” est une action prise en cas de non-respect d’une règle port-security.

```
(config-if)#switchport port-security violation {protect | restrict | shutdown}
```

- **Mode protect :** Dès que la “violation” est constatée, le port arrête de transférer le trafic des adresses non autorisées sans envoyer de message de log.
- **Mode restrict :** Dès que la “violation” est constatée, le port arrête de transférer le trafic des adresses non autorisées et transmet un message de log.
- **Mode shutdown :** Dès que la “violation” est constatée, le port passe en état err-disabled (shutdown) et un message de log est envoyé.

Diagnostic port-security

Désactivation d’un port `err-disabled` selon la plateforme (shut/no shutdown) :

```
(config)#errdisable recovery cause psecure-violation
```

Diagnostic :

```
#show port-security
#show port-security address
#show port-security interface G0/1
#show running-config
#clear port-security {all | configured | dynamic | sticky}
```

DHCP snooping

- :file_folder:`dhcpd.conf`

Le DHCP snooping est une fonction de sécurité intervenant au deuxième niveau du modèle OSI. Cette fonction est intégrée dans le switch connectant les clients aux serveurs DHCP. En d'autres termes, il s'agit d'un protocole qui contrôle tout d'abord l'ensemble des informations DHCP passant par le commutateur. Seuls les paquets autorisés provenant de serveurs (et interfaces) dignes de confiance sont transmis aux clients.

De cette façon, un serveur DHCP non autorisé peut certes recevoir le paquet DHCPDISCOVER (la requête du client visant à obtenir un serveur DHCP) puisqu'il surveille le broadcast. Il peut aussi envoyer un paquet DHCPOFFER (la réponse à la recherche), mais ce paquet n'atteindra jamais le client. Placé dans le commutateur, le DHCP snooping identifie le fait que le paquet ne provient pas d'un serveur digne de confiance et contient de fausses informations et procède donc au blocage de la transmission.

Déploiement de certains services via Ansible

ansible galaxy

- Serveur Master
- Serveur slave web en HA avec redis + reverse proxy

(Protocol 802.1X (authentification par mot de passe))