Descriptif du projet

Architecture réseau et sécurité

Mauberger Florian | Bayssié Loïc | Equipe ARS

Sommaire

[Contexte 3](#_Toc41892435)

[Description du sujet 3](#_Toc41892436)

[Schéma complet 3](#_Toc41892437)

[Schéma simplifié 3](#_Toc41892438)

[Matériel utilisé 4](#_Toc41892439)

[Description du réseau 4](#_Toc41892440)

[Plan d’adressage IP 4](#_Toc41892441)

[VLAN 5](#_Toc41892442)

[DMZ 5](#_Toc41892443)

[Connexion 5](#_Toc41892444)

[Protocoles réseaux 6](#_Toc41892445)

[Serveurs 6](#_Toc41892446)

[Bonnes pratiques 7](#_Toc41892447)

[Pare-feu pfSense 8](#_Toc41892448)

[Règles de filtrage : 8](#_Toc41892449)

[Logs : 8](#_Toc41892450)

[NAT : 8](#_Toc41892451)

# Contexte

Lors de cette année de Bachelor 3 au campus d’Ynov Toulouse, nous avons dû réaliser un travail en autonomie avec un sujet libre.

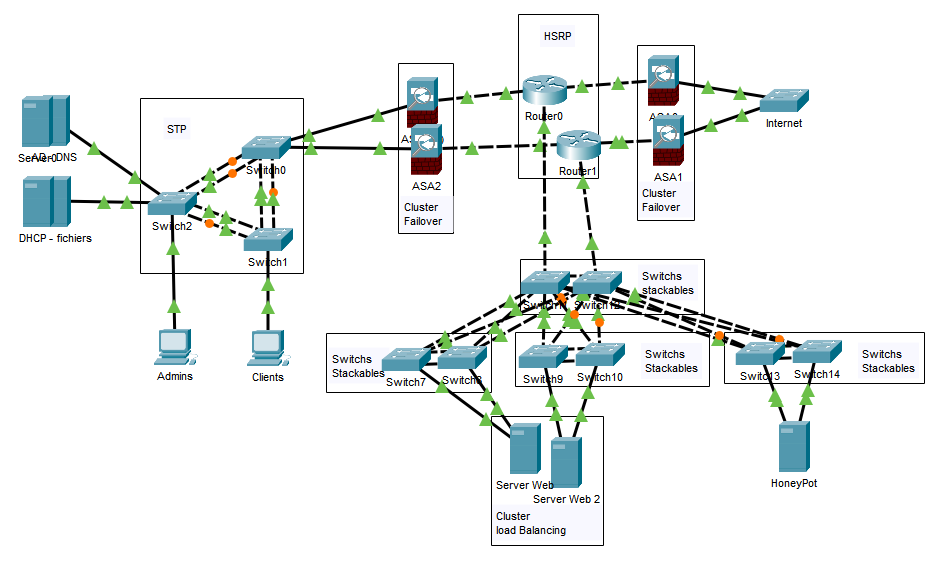
Notre équipe (ARS) est composée de 2 membres : Mauberger Florian et Bayssié Loïc.

Notre sujet est le suivant : Architecture réseau et sécurité

# Description du sujet

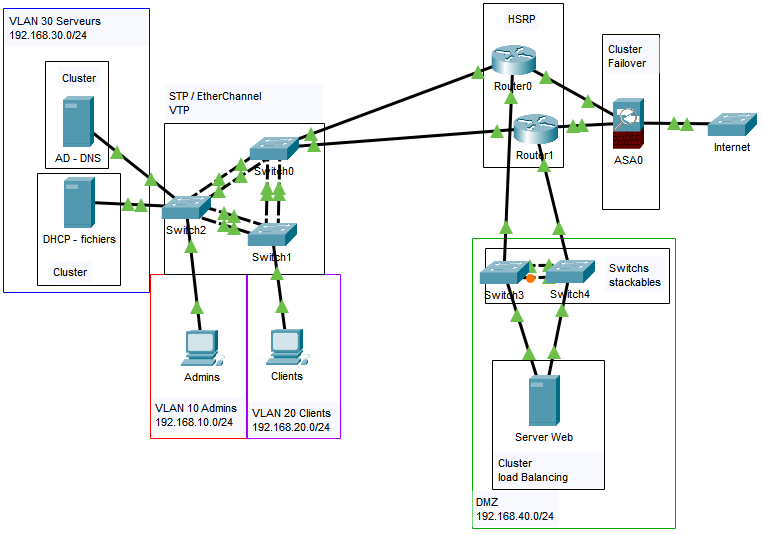
Nous devons créer une architecture réseau la plus sécurisée et robuste possible. Mise en place de la haute disponibilité pour ce faire nous allons devoir mettre en place des solutions de redondance, tant matérielles que des redondances de liens.

# Schéma complet



*Capture d’écran Packet Tracer du schéma réseau complet*

# Schéma simplifié



*Capture d’écran Packet Tracer du schéma réseau simplifié et fonctionnel*

# Matériel utilisé

**Outil de virtualisation :** VmWare Workstation

**Serveurs :** Serveurs Windows 2019

**Clients :** Windows 10

**Commutateurs :** Cisco 2960

**Routeurs :** Cisco 2811

**Pare-feu :** pfSense

# Description du réseau

## Plan d’adressage IP

Serveurs :

* AD-DNS : 192.168.30.1
* DHCP-Fichiers : 192.168.30.2
* IIS main : 192.168.40.1 | IIS secondaire : 192.168.40.2 | Cluster IIS : 192.168.40.3
* Firewall : 192.168.40.10

Postes :

* Admin : 192.168.10.1
* Clients : 192.168.20.1 - 10

Matériel d’interconnexion :

* Switch 0 : 192.168.10.10
* Switch 1 : 192.168.10.11
* Switch 2 : 192.168.10.12
* Router 0 : 192.168.10.252; 192.168.20.252; 192.168.30.252; 192.168.40.252; 11.10.10.10
* Router 1 : 192.168.10.253; 192.168.20.253, 192.168.30.253; 192.168.40.253; 11.11.11.11
* HSRP : 192.168.10.254; 192.168.20.254; 192.168.30.254; 192.168.40.254; 11.12.12.12

## VLAN

|  |  |  |
| --- | --- | --- |
| Numéro | Nom | IP |
| 10 | Admins | 192.168.10.0/24 |
| 20 | Clients | 192.168.20.0/24 |
| 30 | Serveurs | 192.168.30.0/24 |
| 40 | DMZ | 192.168.40.0/24 |

## DMZ

La DMZ est sécurisée d’un côté par le pare-feu et de l’autre par des ACLs sur les routeurs. Ainsi, elle est joignable de l’extérieur du réseau comme de l’intérieur, mais personne ne peut passer les ACLs vers l’intérieur du réseau si la connexion n’est pas à la demande de l’intranet.

# Connexion

**Clients/Serveurs :** AdSuperAdmin | Passw0rd

**Serveurs :** AdAdmin | Passw0rd

**Clients :** AdUser | Passw0rd

**Commutateurs :** mot de passe : cisco

**Routeurs :** mot de passe : cisco

**Pare-feu :** admin | PFSense

# Protocoles réseaux

Liste et description de tous les protocoles réseaux mis en place dans notre réseau :

* **Spanning-Tree Protocol (STP) :** Permet la redondance de lien entre deux éléments réseaux. Si un lien se rompt, l’autre prend la relève.
* **Ether Channel :** Permet de cumuler 2 liens réseau physiques afin de n’en créer qu’un logique ayant la capacité des deux liens physiques additionnés.
* **Vlan Trunking Protocol (VTP) :** Permet le partage de configuration entre les switches.
* **Hot Standby Routing Protocol (HSRP) :** Permet à deux routeurs de travailler en parallèle. Ainsi, si un des deux venait à avoir un problème, le deuxième prend la relève.
* **Trivial File Transfert Protocol (TFTP) :** Permet la sauvegarde de la configuration des différents éléments réseaux. En cas de problème, la configuration pourra être remise en place rapidement.
* **Stackable Switches :** Permet la redondance de commutateurs (switch). Si un switch tombe en panne, l’autre prend la relève.
* **Clustering :** permet à deux serveurs identiques de travailler ensemble. Il existe deux manières différentes :
  + **Load Balancing :** Les serveurs se partagent la charge réseau afin de répondre plus vite.
  + **Fail Over :** Un serveur maître répond à tout le réseau. S’il venait à tomber en panne, le serveur secondaire prend le relais.

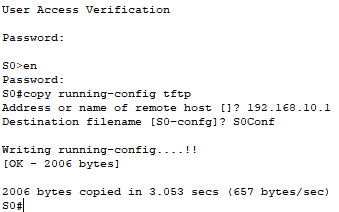
# Serveurs

Liste et description des différents serveurs mis en place dans notre réseau :

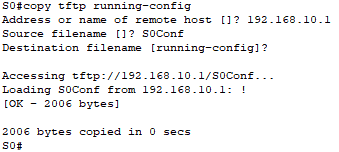
* **Active Directory (AD) :** Centre d’identification et d’authentification des différents clients du réseau.
* **Domain Name System (DNS) :** Annuaire du réseau. Il permet de traduire les noms de domaines en adresse IP
* **Dynamic Host Configuration Protocol (DHCP) :** Détermine l’adresse IP des clients réseaux souhaitant se connecter
* **Fichiers :** Serveurs ayant une grande capacité de stockage. Il permet aux éléments et clients réseau de stocker leurs fichiers.
* **Internet Information Services (IIS) :** Ce sont nos serveurs Web. Ils représentent le site web accessible depuis l’extérieur de notre réseau.
* **Eventualité –** **HoneyPot :** Appât pour les tentatives d’intrusions
* **Firewall :** Pare-feu ayant des règles de filtrage afin de créer une sécurité réseau

# Bonnes pratiques

* **Disponibilité des services :** Tous les services sont redondés et connectés par une architecture redondée elle aussi.
* **Désactivation des services inutiles :** exemple : désactivation du STP sur les ports clients
* **Gestion des autorisations :** Un utilisateur “Super-Admin”, un utilisateur Admin et les clients n’ont aucun droit sur le réseau (accès à internet et à leurs dossiers sur le serveur de fichiers)
* **Sauvegarde de la configuration réseau :**  sauvegarde via TFTP sur le poste Admin (dossier redirigé vers le serveur de fichiers).
  + Sauvegarder une configuration :



* + Restaurer une configuration :



A noter que “running-config” peut être changé par “startup-config”

* **Protection des éléments réseau :** Un mot de passe est défini et encrypté sur chaque élément.
* **Eventualité –** **Politique de mots de passe :** Un ensemble de paramètres permettent une sécurité supplémentaire dans la gestion de l’AD sont possibles, comme : l’utilisation d’un algorithme de cryptage des mots de passe non réversible, l’obligation de création de mots de passe complexes incluant des caractères spéciaux et l’assurance d’un changement de mot de passe tous les 3 mois.

# Pare-feu pfSense

## Règles de filtrage :

Des règles de filtrage réseau sont mise en place grâce au firewall permettant ainsi de limiter le trafic interne au réseau au strict nécessaire. Pour se faire les règles suivantes ont été configurées :

* Autorisation du trafic entrant HTTP/HTTPS provenant de l’extérieur à destination du serveur IIS
* Autorisation du trafic entrant HTTP/HTTPS provenant du serveur IIS à destination de l’extérieur
* Est imposé à tout trafic entrant la redirection vers le serveur IIS
* Tout trafic autre est bloqué

## Logs :

En plus des règles de trafic le pare-feu permet également de récupérer les logs des connexions entrantes et sortantes du pare-feu, notamment les connexions correspondantes aux règles précédemment citées. Permettant ainsi un suivi complet du trafic dans le temps.

## NAT :

Un système de NAT permet aux membres de l'intranet (Admins, Clients, Serveurs) d'aller sur internet à travers la protection du pare-feu sous la forme d'un NAT changeant ainsi leurs adresses IP au profit d'une autre ne permettant pas (ou plus difficilement) de remonter jusqu'au PC à l'origine de la connexion.