Théo Cabrelli

Rapport projet station F

Contexte :

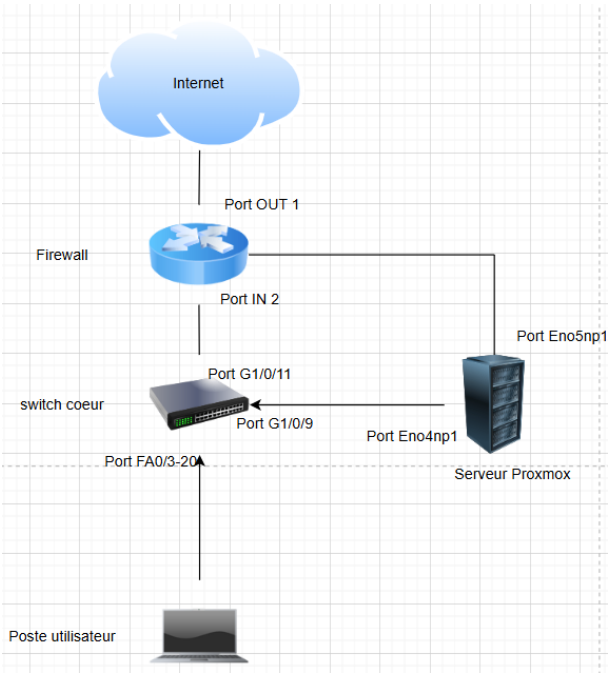
Station F souhaite renforcer ses services web et son infrastructure réseau pour répondre à deux principaux besoins. D'une part, il s'agit de mettre en place une solution d'hébergement web sécurisée pour les startups, tout en séparant les services internes destinés aux collaborateurs de ceux accessibles au public. D'autre part, l'organisation vise à améliorer la gestion et la sécurité de son réseau, notamment via un système d'authentification centralisé, l'automatisation de la configuration réseau et un partage sécurisé des ressources documentaires.

Topologie :

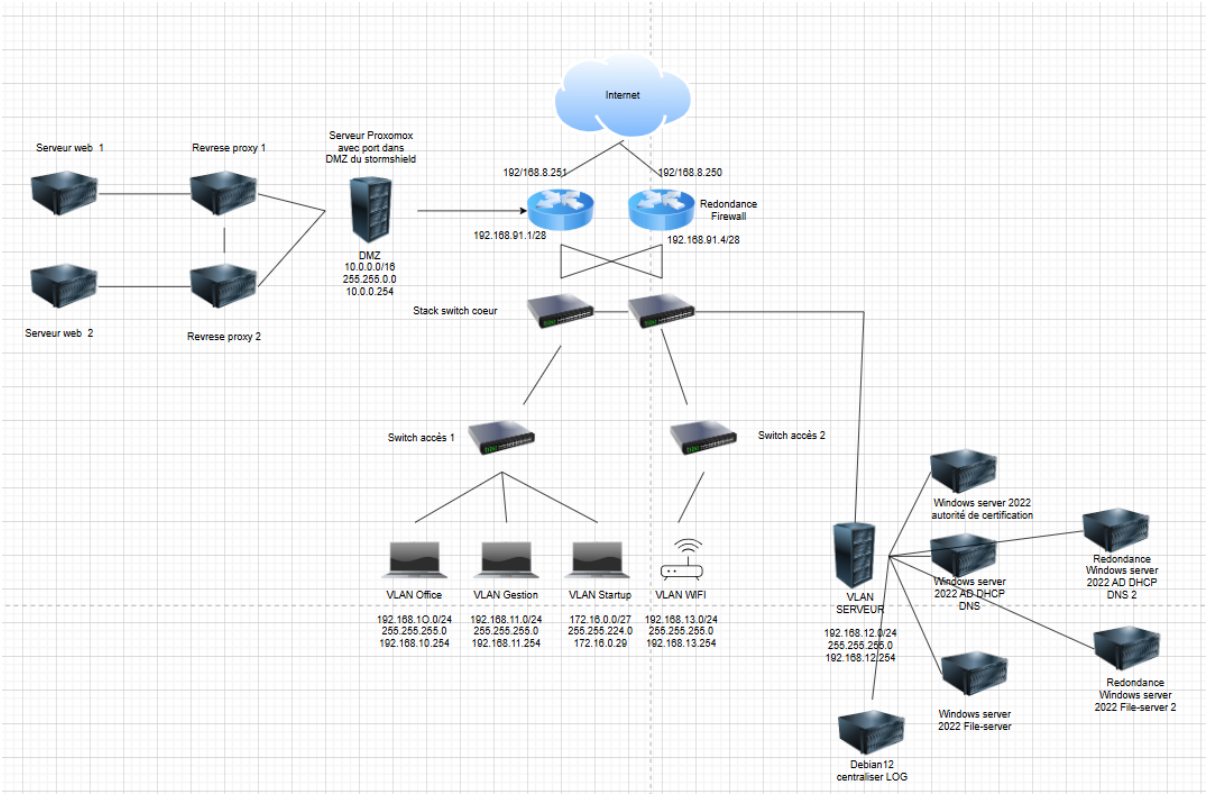
La topologie du réseau est en trois couches avec un routeur pare-feu, un switch cœur, un switch distribution et un switch accès. Tous les équipements réseaux son redondés. Cela permet de correctement segmenter les différents réseaux, améliorant ainsi la sécurité et les performances et la résilience en cas de panne . Le routeur pare-feu assure la communication entre les différents réseaux, le switch cœur gère le trafic à haut débit et router les équipements vers le pare-feu pour pouvoir communiquer avec le réseau externe, le switch distribution assure la répartition du trafic et le switch d'accès connecte les utilisateurs finaux. Cette architecture est idéale pour les réseaux de taille moyenne à grande, offrant une grande flexibilité et évolutivité."

Schémas réseaux physique et logique :

Voici le schéma réseau physique :



Voici le schéma réseau logique :



Plan d'adressage et Vlan :

Nom VLAN	@IP sous-réseau/ MS	@IP SVI Passerelle d	1ère @IP	Dernière @IP	N° de VLAN
VLAN Wifi	192.168.13.0/24	192.168.13.254	192.168.13.1	192.168.13.253	13
VLAN Serveurs	192.168.12.0/24	192.168.12.254	192.168.12.1	192.168.12.253	12
VLAN Management	192.168.11.0/24	192.168.11.254	192.168.11.1	192.168.11.253	11
VLAN Office	192.168.10.0/24	192.168.10.254	192.168.10.1	192.168.22.253	10
VLAN EXIT	192.168.91.0/29	192.168.91.2	192.168.91.3	192.168.91.6	91
VLAN Startup 1	172.16.0.0/27	172.16.0.30	172.16.0.1	172.16.0.29	101
VLAN Startup 2	172.16.0.32/27	172.16.0.62	172.16.0.33	172.16.0.61	102
VLAN Startup 3	172.16.0.64/27	172.16.0.94	172.16.0.65	172.16.0.93	103
VLAN Startup 4	172.16.0.96/27	172.16.0.126	172.16.0.97	172.16.0.125	104
VLAN Startup 5	172.16.0.128/27	172.16.0.158	172.16.0.129	172.16.0.157	105
VLAN Startup 6	172.16.0.160/27	172.16.0.190	172.16.0.161	172.16.0.189	106
VLAN Startup 7	172.16.0.192/27	172.16.0.222	172.16.0.193	172.16.0.221	107
VLAN Startup 8	172.16.0.224/27	172.16.0.254	172.16.0.225	172.16.0.253	108
VLAN Startup 9	172.16.1.0/27	172.16.1.30	172.16.1.1	172.16.1.29	109
VLAN Startup 10	172.16.1.32/27	172.16.1.62	172.16.1.33	172.16.1.61	110
VLAN Startup 11	172.16.1.64/27	172.16.1.94	172.16.1.65	172.16.1.93	111
VLAN Startup 12	172.16.1.96/27	172.16.1.126	172.16.1.97	172.16.0.125	112

Chaque port du switch accès est attribué à un VLAN. Les VLANs permettent de segmenter le réseau en plusieurs réseaux logiques, ce qui permet d'améliorer la sécurité et la gestion du trafic.

Chaque Vlan possèdent les noms des services auxquelles elles sont attribuées.

- Le vlan 11 est utilisé pour les administrateurs afin d'administrer les équipements sur le réseau (Routeur, switch cœur et switch accès).

- Le vlan 12 est utilisé pour le serveur Proxmox qui héberge différents serveurs. Elle ne possède pas d'adressage IP en DHCP car les serveurs se configurent en IP statique.

- Le vlan 13 est utilisé les équipements systèmes (point d'Accès wifi).

- Le vlan 91 elle ne possède pas d'adressage IP en DHCP car elle permet uniquement de faire sortir les utilisateurs du réseau vers le réseau extérieur afin de pouvoir accéder à internet.

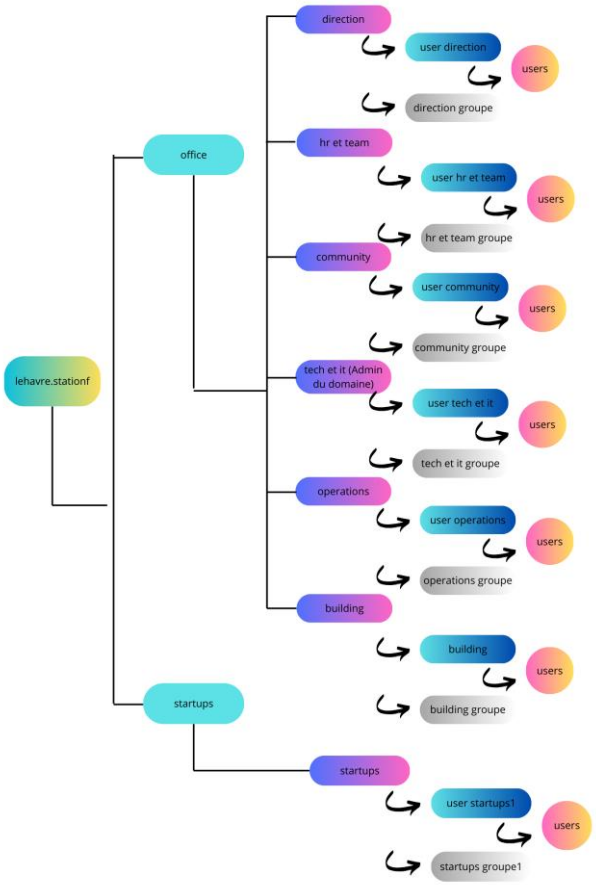
Liste matérielle :

Voici la liste de matériels nécessaire afin de pouvoir réaliser l'infrastructure réseau pour station F :

- 2 switchs cœur
- 2 switchs accès
- 2 Firewall (Stormshield)
- Un serveur afin d'y installer Proxmox
  - Windows server DHCP ADDS
  - Windows server DHCP ADDS 2
  - Windows server Files server
  - Windows server Files server 2
  - Windows server autorité de certification
  - Debain 12 ELK centraliser LOG
  - Debian 12 serveurs web 1
  - Debian 12 serveurs web 2
  - Debian 12 reverse proxy 1
  - Debian 12 reverse proxy 2
- Des ordinateurs configurés dans l'AD pour les startuppers et le personnel.
- Une borne wifi

Arborescence AD :

L'arborescence de l'AD a été réalisé en fonctions des différents services présents à Station F.



Station F est l'unité principale ou la racine, représentant probablement l'organisation globale ou un domaine principal dans un AD.

OU Principales : Deux OU principales Office et Startups permettent de segmenter l AD et différencier les startups du reste des autres services.

Services : Chaque branche représente un service distinct dans l'organisation (direction, community, tech et IT(admin du domaine), opérations, building, HR et team). Chaque unité est définie par son propre bloc, indiquant une séparation logique des unités organisationnelles au sein de l'annuaire.

OU utilisateurs du service : Chaque service a une OU d'utilisateurs spécifiques à ce service pour stocker les utilisateurs (user direction, user community, user startups...).

Groupe utilisateurs: Chaque service a un groupe d'utilisateurs spécifiques à ce service pour ajouter les utilisateurs du service (direction groupe, community groupe, startups groupe...).

Utilisateurs finaux : Les groupes sont ensuite associés à des utilisateurs finaux (indiqués simplement comme "users"), représentant les membres qui appartiennent à ces groupes dans chaque unité organisationnelle.

Configuration des équipements :

Le SSH est activé en local sur les firewalls, les switchs coeur et les switchs accès. Afin de pouvoir se connecter en SSH. Cependant, l'accès SSH est restreint aux utilisateurs du VLAN 11 uniquement. Cela est réalisé à l'aide d'une liste d'accès, qui est une liste d'adresses IP autorisées à accéder au SSH.

Voici un tableau avec l'ensemble des adressages des équipements :

Elément réseau	Nommage	@ IP/MSR
Stormshield 1 accès gestion		192.168.91.1
Stormshield 2 accès gestion		192.168.91.4
Switch Core 1 stack	SW-CORE1	192.168.11.254/24
Switch Access 1	SW-AC1	192.168.11.253/24
Switch Access 2	SW-AC2	192.168.11.252/24
Serveurs ADDS 1 (AD/DNS/DHCP)	SRV1-ADDS1	192.168.12.1/24
Serveurs ADDS 2 (AD/DNS/DHCP)	SRV1-ADDS2	192.168.12.5/24
Serveurs 3 (FILESERVER 1)	SRV2-FILESERVER	192.168.12.2/24
Serveurs 4 (FILESERVER 2)	SRV2-FILE-SERVER2	192.168.12.6/24
Serveurs 3 (autorité certificat)	SRV3-CERTIFICAT	192.168.12.3/24
Proxmox	PVE	192.168.11.1
Serveur Web 1	WEB1	10.0.0.100
Serveur Web 2	WEB2	10.0.0.101
Reverse proxy 1	SRVRP1	10.0.0.111
Reverse Proxy 2	SRVRP2	10.0.0.112
Reverse proxy virtuel		10.0.0.110
Serveur ELK	ELK	192.168.12.40
Controleur wifi	controleur wifi gr1	192.168.11.249
Borne wifi		192.168.13.253

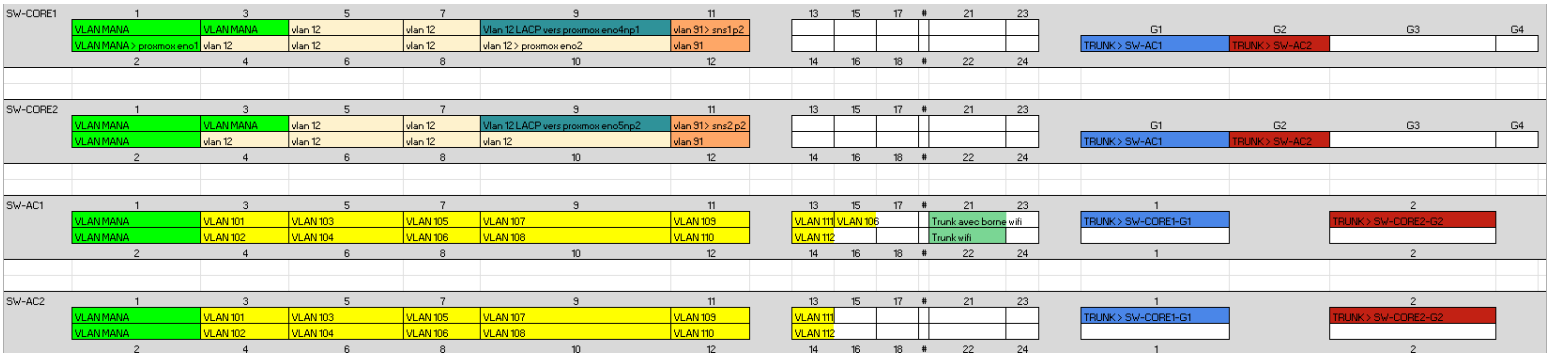
Le pare-feu : Une haute disponibilité est configurée entre les deux Stormshields. Un accès dédier au vlan gestion permet un accès à l'interface web de configuration. Plusieurs règles de filtrage NAT ont été configuré pour que les utilisateurs accèdent aux serveurs web de la DMZ. Les utilisateurs du réseau interne arrivent à accéder à internet. Un Tunnel SSL a été configuré pour que les utilisateurs de l'UO de l'annuaire active directory puissent accéder au Stormshield via un VPN sécurisé depuis n'importe où.

Stormshield 1	1	2	3	4
FAI 192.168.8.254	OUT 192.168.8.251/24 > FAI	IN 192.168.91.1/29 > sw-core1 p11		
	HA > sns2 p5	HA > sns2 p6	DMZ 10.0.0.254/16 > interf	Mana-gestion 192.168.11.251/24 > sw-core1 p1
	5	6	7	8
Stormshield 2	1	2	3	4
FAI 192.168.8.254	OUT 192.168.8.250/24 > FAI	IN 192.168.91.4/29 > sw-core2 p11		
	HA > sns1 p5	HA > sns1 p6	DMZ 10.0.0.254/16 >	Mana-gestion 192.168.11.248/24 > sw-core1 p2
	5	6	7	8

Stack Switch coeur : Un stack est réalisé entre les deux switchs cœur du réseau en cas de panne de l'un des deux. Le mode IP routing est activé afin de router les machines du réseau interne vers le Stormshield. Deux routes par défauts sont configurées, la principale qui envoie les utilisateurs vers le Stormshield 1 et une secondaire qui envoie vers le Stormshield 2 en cas de panne si le Stormshield 1 ne répond plus. Le vlan exit est configuré afin de pouvoir communiquer avec l'interface IN du routeur.

Switch d'accès 1 et 2 : Il est configuré avec des Vlan attribués aux ports. Cela permet aux équipements connectés à ce port de communiquer uniquement avec les autres équipements du même VLAN. La répartition des ports sur le switch a été réalisé en fonction du nombre d'utilisateur par Vlan. Certains services demandent plus de postes informatiques, plusieurs ports sont nécessaires pour relier le même service a plusieurs endroits. Deux switch accès sont configuré pour créer de la redondance.

Configuration des ports des switchs :



Configuration du serveur Proxmox :

Le serveur Proxmox est attribué au vlan 12 sur le port 4 du switch coeur. Son adresse IP est 192.168.11.1 pour y accéder depuis la vlan gestion. Le serveur contient une template de Windows serveur 2022 et une Debian 12. Une template est une image de machine virtuelle préconfigurée et prête à être utilisée pour créer de nouvelles machines virtuelles.

Les différentes machines virtuelles sur le serveur :

- Un Windows serveur 2022 avec l'adresse IP 192.168.12.1. Le DHCP, l'ADDS et le DNS configuré et fonctionnel. Le DHCP a été configuré avec plusieurs étendu en fonction de chaque Vlan sur le réseau. L'ADDS est configuré en plusieurs Unité d'organisation en fonction des différents services du musée ainsi que les différents groupe utilisateur (administrateur, utilisateur, ordinateur utilisateur ...). Les utilisateurs peuvent se connecter aux postes sur le réseau avec comme nom d'utilisateur (première lettre du prénom suivi du nom de famille) ainsi qu'un mot de passe près-définit qui répond aux normes de la RGPD sur la gestion et la création de mot de

passe. Il comprend au minimum douze caractères, une majuscule, deux chiffres, un caractère spécial ainsi que des lettres minuscules. Une rotation des mots des passes est mise en place pour changer tous les 30 jours. Une GPO est mise en place pour certaines restrictions. Elle permet d'exécuter le terminal ainsi que le PowerShell seulement en tant qu'administrateur du domaine, bloque l'accès au panneau de configuration et à la modification des cartes réseau ainsi qu'un mappage réseau pour les utilisateurs de leur startup afin qu'ils puissent échanger ensemble. Une redirection DNS est réalisée afin que les utilisateurs puissent accéder aux sites des startups en internes via le nom DNS définit pour le site web.

- Un deuxième Windows serveur 2022 avec l'adresse IP 192.168.12.5 est ajouté au domaine existant. Le rôle de failover est configuré sur le DHCP en cas de panne du premier serveur, celui-ci prend le relais et permet aux utilisateurs de communiquer avec le serveur de DNS, l'AD ainsi que d'obtenir un bail DHCP.

- Un Windows serveur 2022 File serveur avec l'adresse IP 192.168.12.2. Il permet de stocker les sessions des profils itinérants ainsi que leurs fichiers. Un rôle DFS est configuré pour répliquer les répertoires et leur contenu sur le deuxième file server en cas de panne du premier. Un répertoire Z du serveur est partagé sur le réseau afin que les utilisateurs puissent se connecter à leurs sessions et enregistrer leurs documents. Le répertoire Profiles est configuré pour enregistrer les configurations de Windows enregistré sur la session de l'utilisateur (Fond d'écran ...). Seul un administrateur peut accéder à ce répertoire.

  Le répertoire HomeFolders est partagé aux utilisateurs afin qu'ils puissent enregistrer leurs documents. Celui-ci est segmenté en sous répertoire en fonction des utilisateurs qui enregistrent des documents. Seuls les utilisateurs de leurs répertoires peuvent accéder à son contenu.

  Le répertoire partagé pour chaque startup est aussi configuré.

- Un deuxième Windows serveur 2022 File serveur avec l'adresse IP 192.168.12.6 est configuré avec le rôle DFS en tant que second en cas de panne c'est lui qui prend le relais.

- Un Windows serveur 2022 autorité de certification est configuré avec l'adresse IP 192.168.12.3 et permet de générer des certificats privés pour le réseau interne de station F. Les certificats sont utilisés en interne sur les sites web des startups.

- Une Debian 12 ELK qui permet de centraliser tous les logs grâce à la suite de logiciels Elastic de tous les serveurs du réseau de station F. Ce serveur permet de superviser et peut remonter des alertes en cas de problèmes ou tout simplement avoir une centralisation des logs et pouvoir les consulter facilement grâce à l'interface web.

- Deux Debian 12 reverse proxy sont configurés avec haproxy et keepalived afin de rediriger les utilisateurs vers le bon site web qui se trouve sur le serveur web 1 et 2.Keepalived permet de créer de la redondance de serveur avec une IP virtuelle qui remplace l'IP de la machine. Ainsi, si le maître ne répond plus, le deuxième reverse proxy se voit remplacer son adresse IP automatiquement par l'adresse IP virtuelle afin de pouvoir rendre le service opérationnel en cas de panne. Si le serveur web1 est indisponible ou est surchargé, le reverse proxy renvoie les utilisateurs vers le site web qui se trouve sur web serveur2. Un certificat auto signé est configuré dans haproxy afin de rediriger les utilisateurs en HTTPS sur les sites web des startups. Une redirection DNS est configurée dans haproxy pour que les utilisateurs accèdent aux sites web via le nom DNS définit.

- Deux Debian 12 LAMP qui sont configurés avec apche2 afin d'héberger les sites web des startups avec l'adresse et permettre aux utilisateurs externes et internes d'accéder aux sites web.

Configuration de la borne wifi:

La borne wifi est configurée avec les SSID de chaque startup ainsi qu'aux différents services de station StationF afin qu'ils puissent accéder au réseau en wifi. L'adressage IP utilisée dans la borne wifi est configurée pour attribuer les adresses IP en fonctions des Vlans du service sur lequel l'utilisateur se connecte.

Configuration des postes informatiques :

Les postes sont en adressage IP automatique, le serveur DHCP attribue automatiquement les informations nécessaires au bon fonctionnement du poste sur le réseau. Les utilisateurs peuvent se connecter aux postes sur le réseau avec comme nom d'utilisateur (première lettre du prénom suivi du nom de famille) ainsi qu'un mot de passe près-définit. Des droits administrateurs sont nécessaires pour installer des logiciels ou modifier certains paramètres dans Windows.

Tests réalisés :

Connectivité au réseau filaire et accès Internet

Ouvrir une session en tant qu'administrateur local : La session s'ouvre correctement.

Vérifier l'obtention d'une adresse IP : L'adresse IP est obtenue via DHCP (commande ipconfig).

Vérifier la cohérence de l'adresse IP obtenue : L'adresse correspond bien au bon VLAN.

Tester la connectivité avec une adresse IP statique : Le poste ping la passerelle avec succès.

Tester l'accessibilité de la passerelle : La commande ping vers la passerelle fonctionne.

Tester l'accessibilité des serveurs DHCP : La commande ping vers le serveur DHCP fonctionne.

Tester l'accessibilité du routeur de périphérie : La commande ping vers l'interface interne du routeur fonctionne.

Tester l'accessibilité de l'IP 1.1.1.1 : La commande ping vers cette IP fonctionne.

Tester l'accessibilité du FQDN orange.fr : La commande nslookup réussit à résoudre le domaine.

Connectivité au réseau sans fil et accès Internet

Connecter le poste de travail au bon SSID Wi-Fi : Le poste se connecte correctement au SSID.

Vérifier l'obtention d'une adresse IP : Une adresse IP cohérente est obtenue automatiquement.

Vérifier la cohérence de l'adresse IP obtenue : L'adresse est correcte selon le SSID utilisé.

Tester la connectivité avec une adresse IP statique : Le poste ping la passerelle en IP statique.

Tester l'accessibilité de la passerelle : La commande ping vers la passerelle fonctionne.

Tester l'accessibilité des serveurs DHCP : Le poste obtient une adresse IP en Wi-Fi.

Tester l'accessibilité du routeur de périphérie : Test fonctionnel.

Tester l'accessibilité de l'IP 1.1.1.1 : Test non fonctionnel.

Tester l'accessibilité du FQDN orange.fr : Test fonctionnel.

Ouverture de session utilisateur et hébergement de sites web

Tester l'accessibilité de l'annuaire utilisateur (LDAP/ADDS) : Accès fonctionnel par IP et par nom.

Vérifier le domaine d'appartenance du poste : Vérification du domaine dans la configuration Windows.

Ouvrir une session avec un utilisateur du domaine : L'ouverture de session AD est fonctionnelle.

Accès aux différents sites web : Les utilisateurs accèdent aux sites via un navigateur.

Authentification et accès aux ressources partagées

Accès SSH avec login AD : Fonctionnel.

Accès aux serveurs de fichiers par IP et par nom : Accès à distance fonctionnel avec session AD.

Vérifier les droits d'accès aux ressources partagées : Fonctionnel.

Accès aux différents sites web

Accès aux différents sites web en tapant dans la barre d’adresse d’un navigateur : site.lehavre.stationf : Fonctionne

Rendre hors service un serveur web et essayer d’accéder à un site web : Fonctionnel

Eteindre le reverse proxy maître et vérifier si le second prend le relais : Fonctionnel

Eteindre un serveur web et vérifier si les sites web sont toujours accessibles : Fonctionnel

Redondance du pare-feu

Eteindre le premier Stormshield et vérifier que les utilisateurs arrivent toujours à accéder aux sites web des startups ainsi que internet : Fonctionnel

Redondance du stack

Eteindre le switch cœur 1 et vérifier si le switch cœur 2 prend correctement le relais : Fonctionnel

Redondance serveur DHCP, AD

Eteindre le serveur DHCP 1 et vérifier si les utilisateurs obtiennent bien un bail DHCP du serveur DHCP 2 : Fonctionnel

Eteindre le serveur DHCP 1 et vérifier si les utilisateurs arrivent à ouvrir leur session AD : Fonctionnel

Journalisation des LOG :

Vérifier si tous les serveurs envoie correctement leu log au serveur ELK : Fonctionnel

Plan PCA et PRA :

Un plan PRA est mis en place avec la sauvegarde de configurations de différents serveurs et matériels de l'infrastructure réseau. Ce plan permet lors d'un incident sur l'infrastructure d'avoir une sauvegarde et pouvoir refaire fonctionner le réseau correctement et le plus rapidement possible grâce à la sauvegarde de la configuration des équipements.

Le plan PCA correspond à la redondance des serveurs et services mis à dispositions sur le réseau. En cas de panne d'un équipement redondé le second prend le relais afin d' éviter les coupures d'activités des startups.

Conclusion :

En tant que chef de mon groupe, j'ai distribué les tâches à réaliser à mon équipe. Toutes les tâches ont été réalisées équitablement par l'équipe. Chacune des personnes de l'équipe a pu contribuer à la réalisation de chacune des tâches citées précédemment afin d'apprendre à mettre en place une architecture réseau. De mon côté j'ai réalisé la configuration de la SVI exit, l'ajout d'adresse IP en guise de Gateway dans le switch coeur pour les Vlans. J'ai configuré sur le switch coeur, le IP Routing afin de router les vlan vers la vlan exit et le IP Helper-Address pour permettre au DHCP de se diffuser sur le réseau. J'ai installé le serveur Windows server et File-Server sur le serveur Proxmox. J'ai configuré

une partie des étendu du DHCP ainsi que l'ADDS. J'ai aidé mon équipe dans leurs tâches afin de montrer et expliquer les configurations. À la suite d'un problème de dernière minute qui a rendu le serveur DHCP hors service, j'ai réalisé la reconfiguration totale du serveur DHCP et ADDS.

L'architecture réalisé par l'équipe apporte une meilleure évolutivité et bien plus sécurisé. Elle implémente la segmentation en VLANs qui permet une gestion efficace du trafic et renforce la sécurité, avec des attributions claires pour différents services et utilisateurs. La configuration des équipements, notamment l'activation du SSH restreint aux administrateurs, montre une attention particulière à la sécurité. Le déploiement du serveur Proxmox, avec ses machines virtuelles dédiées permet de centraliser plusieurs services en un seul serveur Proxmox et ainsi réaliser des économies d'argent, de place dans le cas de notre petite infrastructure de test. Pour l'infrastructure réel, des serveurs seront utilisés afin de pouvoir subvenir aux besoins du nombre conséquent d'utilisateur. De la redondance sera mis en place avec plusieurs switch, switch coeur et routeur afin d'éviter toutes panne sur le réseau. Toutes les tâches ont été réalisées équitablement par l'équipe. Chaque startup est attribuée à une personne. Chacune des personnes de l'équipe a pu contribuer à la réalisation de chacune des tâches citées précédemment afin d'apprendre à mettre en place une architecture réseau pour le bon fonctionnement de sa startup ainsi que du réseau. Un plan PCA ainsi que PRA est mis en place avec la sauvegarde de certains équipements certains jour de la semaine afin de pouvoir restaurer les données en cas de pertes ou de panne temporaire du système informatique.

Photo de l'infrastructure réalisé :