SYNTHÈSE GLOBALE DE STAGE – BTS SIO SISR

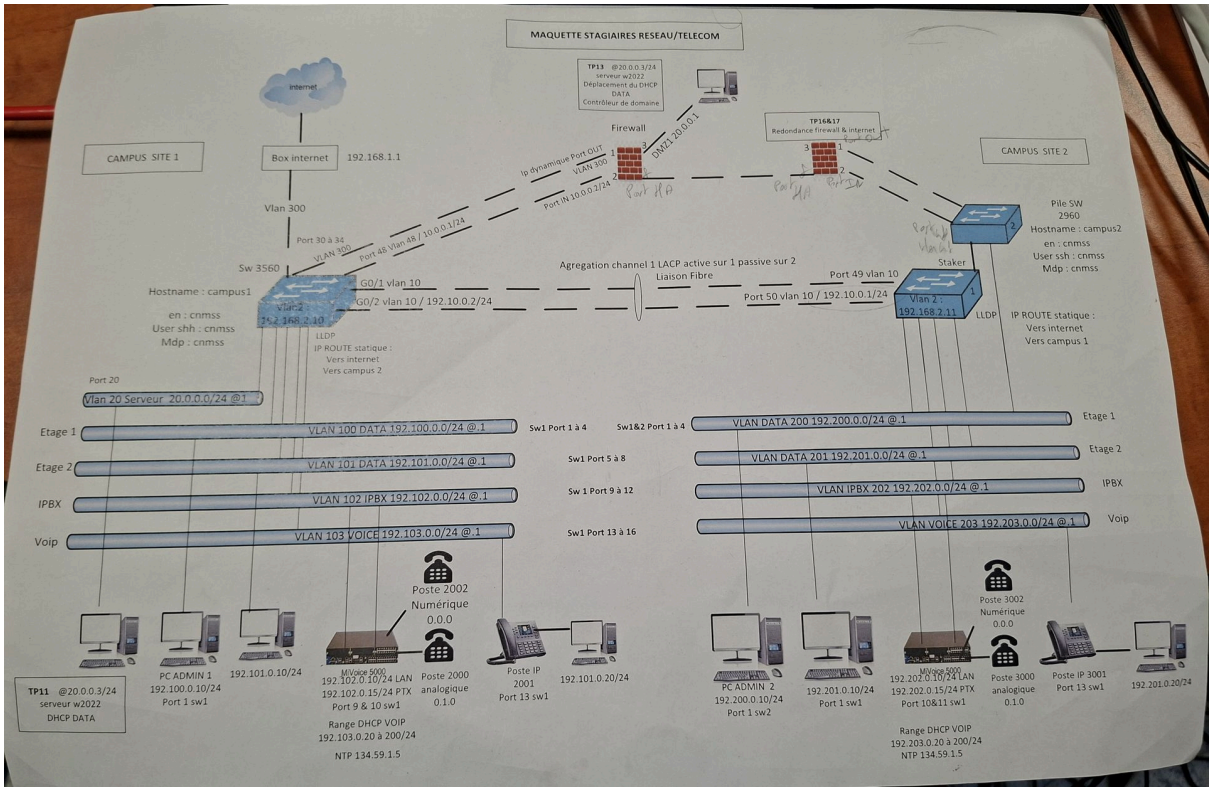
Lieu/Contexte du stage :

J'ai effectué mon stage au sein de la CNMSS (Caisse Nationale Militaire de Sécurité Sociale,) organisme public chargé de la gestion de la protection sociale des militaires.
J'ai intégré le service réseaux et Télécom du Département du Système d'Information,
L'environnement comprend deux campus interconnectés, plusieurs VLAN segmentés, des serveurs virtualisés, IPBX Mitel ainsi que des différents équipements réseaux.

Objectif du stage :

L'objectif du stage était de mettre en place une infrastructure réseau multi-sites simulant deux campus interconnectés. Le projet consistait à configurer les différents VLAN, le routage inter-VLAN, l'agrégation de liens en LACP entre les switches, la mise en place d'un cluster firewall en haute disponibilité (HA).

Il s'agissait également d'intégrer un environnement virtualisé (Proxmox), un contrôleur de domaine Active DIrectory, un serveur DHCP/DNS et une solution de téléphonie IP (Mitel), tout en assurant la cohérence du plan d'adressage et la sécurisation des flux réseau.



Activités réalisées - Bloc 1

1. Conception et mise en place de l’architecture réseau multi-site

Contexte

Dans le cadre du projet, j’ai participé à la mise en place de l'infrastructure simulant deux campus interconnectés (Campus 1 et Campus 2), avec segmentation réseau et sécurisation des flux.

Activité réalisées

- Création et configuration des VLAN
    - VLAN DATA (192.100.0.0/24 - 192.101.0.0/24 - 192.200.0.0/24 - 192.201.0.0/24)
    - VLAN IPBX (192.102.0.0/24 - 192.202.0.0/24)
    - VLAN VOICE (192.103.0.0/24 - 192.203.0.0/24)
    - VLAN Serveurs

- Configuration du routage inter-VLAN
- Mise en place des routes statiques
- Configuration des trunks entre switches
- Mise en place d’une agrégation de lien en LACP
- Vérification de la connectivité entre les différents segments

Compétences Bloc 1 :

- Gérer le patrimoine informatique
- Mettre en place et vérifier les niveaux d’habilitation
- Administrer un réseau local
- Mettre en oeuvre des dispositifs d’interconnexion

2. Mise en place et configuration des équipements de sécurité

Contexte

L’infrastructure nécessitait une sécurisation des échanges entre les deux campus et vers Internet.

Activité réalisées

- Installation et configuration des firewalls Stormshield
- Mise en place d'un cluster en Haute Disponibilité (HA)
- Configuration des interfaces (IN, OUT, DMZ, VLAN)
- Création des règles de filtrage (DNS ICMP, flux inter-VLAN)
- Tests de la redondance entre le firewalls actif et passif

Compétences Bloc 1 :

- administrer et sécuriser un réseau
- Mettre en oeuvre une politique de sécurité
- Contrôler les flux réseau

3. Mise en place des services d'infrastructure

Contexte

L'environnement nécessite la mise en place de services essentiels pour le fonctionnement du réseau.

Activités réalisées

- Déploiement d'un environnement virtualisé sous Proxmox
- Installation et configuration d'un serveur Windows Server
- Mise en place d'un contrôleur de domaine Active Directory
- Création d'utilisateurs via script PowerShell automatisé (import CSV)
- Configuration DHCP/DNS
- Intégration d'un serveur GLPI

Compétences Bloc 1

- Installer et configurer un système d'exploitation
- Gérer des comptes utilisateurs
- Automatiser des tâches d'administration
- Assurer la disponibilité des services

4. Mise en place de la téléphonie IP

Contexte

Le projet inclut une infrastructure VoIP inter-campus.

Activité réalisées

- Configuration du VLAN VOICE
- Mise en place du serveur IPBX
- Paramétrage des abonnements sur Mitel
- Configuration du plan de numération
- Tests d'appels internes

Compétences Bloc 1

- Déploiement d'une solution de communication IP
- Assurer la continuité des services

5. Tentative de mise en place du VPN site-à-site

Contexte

Un tunnel IPsec permettant la communication sécurisée entre les deux campus.

Activités réalisées

- Configuration du tunnel IPsec sur Stormshield
- Définition des réseaux locaux et distants
- Création des règles de filtrage associées
- Tests de supervision des tunnels

Le tunnel n'a pas pu être finalisé en raison d'un problème lié à l'agrégation LACP et au fonctionnement en Haute Disponibilité du firewall, empêchant l'établissement correct du tunnel IPsec.

Compétence

- Mettre en oeuvre un tunnel VPN
- Diagnostiquer un dysfonctionnement réseau
- Analyser des logs et états de supervision

Difficultés rencontrées / Solutions apportées

1. Problème d'agrégation de liens (LACP)

Difficulté

Lors de l'interconnexion des switches entre les deux campus, j'ai rencontré des difficultés liées à la configuration du LACP.
L'agrégation ne fonctionnait pas correctement, ce qui impactait la stabilité du lien inter-site et empêchait certains flux réseau de circuler normalement.

Solution apportée

- Vérification des modes actif/passif
- Contrôle des VLAN autorisés sur les trunks
- Analyse des interfaces via `show interfaces trunk` et `show etherchannel summary`
- Tests de connectivité ciblés

Même si l'agrégation fonctionnait partiellement, elle impactait la couche supérieure (VPN).

Ce que j'ai appris :
L'importance de la cohérence de configuration entre équipements et l'impact d'une couche 2 mal maîtrisée sur les services de couche 3 et 4.

Mise en place du cluster Haute Disponibilité (HA)

Difficulté

La configuration du cluster HA Stormshield ajoutait une couche de complexité.
La gestion des interfaces physiques, des rôles actif/passif et des synchronisations de sessions compliquerait les tests réseau.

Solution apportée

- Vérification des états des interfaces
- Analyse de la synchronisation
- Tests de bascule
- Étude de la documentation constructeur

Ce que j’ai appris :
Le fonctionnement concret d’une architecture redondée et les contraintes techniques liées à la haute disponibilité.

Échec du VPN IPsec

Difficulté

Le VPN site-à-site n’a pas pu être finalisé.
Le tunnel ne s’établissait pas correctement malgré la configuration des réseaux locaux/distants et des règles de filtrage.

L’origine probable du problème était liée :

- à la configuration LACP
- au fonctionnement du firewall en HA
- à l’absence ou mauvaise gestion d’une IP virtuelle utilisée comme point d’ancrage du tunnel

Le tunnel IPsec dépendait d’une stabilité parfaite de l’interface OUT, ce qui n’était pas totalement garanti dans cette configuration.

Démarche mise en œuvre

- Analyse de la supervision des tunnels
- Vérification des politiques IPsec
- Contrôle des règles de filtrage associées
- Tests de connectivité
- Comparaison avec la documentation technique

Même si le VPN n’a pas été validé fonctionnellement, toute l’architecture a été configurée correctement et les causes du dysfonctionnement ont été identifiées.

Ce que j’ai appris :

- L’importance de la cohérence entre couche 2 (LACP) et couche 3 (IPsec)
- L’impact d’une architecture HA sur les tunnels VPN
- La méthodologie de diagnostic réseau
- L’analyse des logs et de la supervision