



Rapport de stage : réseaux et sécurité

**Observation et Accompagnement au sein du service Réseaux et Sécurité,
axé sur le déploiement de réseaux clients (LAN, Wi-Fi) et le support réseau
de niveau 1.**

Effectué par :
Emmanuel GRONDIN
Fait du 22/04/2025 au 13/06/2025

Encadré par :

Tuteur de stage : Hugues CHANE-NAM
Enseignant référent : Jean-Pierre FAUCON

Établissement d'enseignement : Institut Universitaire de Technologie de La Réunion
L'organisme d'accueil : NXO OCÉAN INDIEN

REMERCIEMENT

Je souhaite exprimer ma profonde gratitude à **M. Hugues Chane-Nam**, mon tuteur de stage, pour le temps qu'il m'a consacré tout au long de cette expérience professionnelle, malgré la charge importante de projets qu'il mène au sein de l'entreprise. Son expertise, sa disponibilité et sa pédagogie ont été essentielles à ma progression. Grâce à son accompagnement, j'ai pu apprendre de manière concrète et approfondie, tout en découvrant les exigences du métier.

Je remercie également **Mme Erika Jery**, du service Ressources Humaines, pour son accueil chaleureux, sa bienveillance, et son implication constante tout au long de mon stage. Elle s'est montrée disponible et à l'écoute, répondant avec sérieux et réactivité à toutes mes demandes administratives ou logistiques.

Enfin, je tiens à remercier **l'ensemble de l'équipe de NXO Océan Indien** pour m'avoir accueilli dans un environnement professionnel agréable, stimulant et bienveillant. J'ai particulièrement apprécié l'esprit d'équipe, la confiance accordée et les échanges enrichissants avec les collaborateurs, qui ont tous contribué à faire de ce stage une expérience humaine et professionnelle très formatrice.

Sommaire

1- INTRODUCTION	4
1.1- Objectifs du stage	5
1.2- Présentation de l'entreprise (Nxo)	5
- Nom et secteur d'activité	5
- Équipe encadrante	7
1.3- Présentation du service/département d'accueil	7
1.4- Support de niveau 1 - Gestion des tickets (voir annexe 2-fig.1)	8
- Organisation de l'entreprise	8
2. Présentation du stage	9
2.1- Mission confiées	9
2.2- Outils et environnements utilisés	12
1. JIRA - ITSM (IT Service Management) (voir annexe 2-fig.1) :	12
2. GNS3 (voir annexe 2-fig.2):	12
3. Wireshark :	12
4. Console Cisco (Putty via câble console) :	12
5. Interfaces Web (HPE, Fortigate, VMware ESXi) (voir annexe 2-fig.3-5) :	12
6. VMware ESXi & BIOS RAID	13
7. Environnements Datacenter / Matériel physique (voir annexe 5 & 6)	13
8. PatchSee / PatchLight (voir annexe 2-fig.6)	13
9. Étiqueteuse Brady BMP41 (voir annexe 2-fig.7)	13
2.3- Méthodologie	13
1. Progression par paliers	14
2. Documentation et traçabilité	14
3. Outils et équipements adaptés	14
4. Organisation du travail collaboratif	15
5. Méthode d'intervention client	15
2.4- Encadrement	15
3- Projets et interventions réalisées	16
3.1- Interventions techniques réseau	16
- Déploiement et remplacement de switchs Cisco	16
- Mise en place de VLANs, Spanning Tree et autres protocoles en simulation et en physique (voir annexe 3-fig.1)	17
3.2 Interventions sécurité	17
- Installation de pare-feu Fortigate (voir annexe 4-fig.1)	18
Migration MPLS vers SD-WAN(voir annexe 4-fig.2)	18
Analyse de configurations et adaptation sur site	18
3.3 Maquettes et simulations en environnement isolé (voir annexe 2 fig.2 et 3 fig.1)	19
3.4 Cas concrets chez les clients	20
BNP Paribas : remplacement d'un switch défectueux en environnement critique	20

Data center du CHU de Saint-Pierre : installation en baie (voir annexe 5 fig.1)	21
Groupe Père Favron : déploiement de pare-feu Fortigate (voir annexe 4 fig.1)	22
Air Austral : accompagnement technique et infrastructure réseau dans les datacenters de l'aéroport (voir annexe 6 fig.1-3)	22
4. Compétences acquises	23
4.1 Compétences techniques	24
4.2 Compétences méthodologiques	24
4.3 Compétences relationnelles	25
5. Bilan du stage et perspectives	26
 ANNEXES et ILLUSTRATIONS	 27
Annexe 1	27
• Configuration de Switch HPE 1920s avec interface graphique:	27
• Installation et configuration de Serveur HP ProLiant DL360 Gen11 avec RAID 1 :	28
Installation et configuration de Serveur Dell PowerEdge avec RAID 5 :	29
Annexe 2	31
- Outils et environnements utilisés :	31
Figure 3 : Interfaces Web HPE.	32
Figure 4 : Interfaces Web pare-feu fortigate.	32
Annexe 3	34
- Mise en place de VLANs, Spanning Tree et autres protocoles en simulation et en physique :	34
Annexe 4	35
- Installation de pare-feu Fortigate	35
Annexe 5	36
- Data center du CHU de Saint-Pierre : installation de serveur en baie	36
Figure 1 : Photo de serveur en baie et câble QSFP (100 G) dans le datacenter du CHU.	36
Annexe 6	37
- Air Austral : accompagnement technique et infrastructure réseau dans les datacenters de l'aéroport	37
 Tableau des notions :	 40
 Bibliographie / Webographie	 42
1. Gestion de services IT (ITSM)	42
2. Simulation et émulation réseau (GNS3)	42
3. Protocole Spanning Tree (STP)	43
4. SD-WAN sécurisé (FortiGate / Fortinet)	43

1- INTRODUCTION

"Dans un monde où les données circulent à la vitesse de la lumière, le réseau et la sécurité sont devenus les artères vitales des entreprises."

Aujourd’hui, la connectivité est au cœur du fonctionnement des organisations. La qualité, la sécurité et la disponibilité des réseaux conditionnent directement leur performance et leur résilience. Dans ce contexte, les métiers de l’intégration, de l’administration et du support réseau prennent une importance capitale, tout particulièrement dans les domaines en forte évolution comme la cybersécurité, la virtualisation et les infrastructures LAN/Wi-Fi.

C'est dans ce contexte de transformation que s'est déroulé un stage de huit semaines au sein de NXO France (anciennement NextiraOne), une société française spécialisée dans l'intégration, l'exploitation et la sécurisation des infrastructures numériques. NXO intervient auprès d'une clientèle variée – administrations, établissements de santé, grandes entreprises – en tant qu'acteur indépendant, pour les accompagner dans leurs projets de transformation digitale, de migration réseau et de cyber sécurisation.

Au cours de ce stage, une intégration au sein du service Réseaux et Sécurité a permis de collaborer avec des techniciens, des ingénieurs et des chefs de projet, favorisant une immersion directe dans les activités opérationnelles de l'équipe, en m'impliquant dans des missions très concrètes. Le sujet principal de ce stage s'est articulé autour de **l'observation et de l'accompagnement des activités liées au déploiement de réseaux clients (LAN, Wi-Fi) et au support de niveau 1**. Ce positionnement m'a permis d'aborder des problématiques réelles, de manipuler des équipements professionnels (Cisco, Fortinet, HPE, etc.) et de découvrir l'ensemble du cycle de vie d'un projet réseau, de la phase de maquettage à l'intervention chez le client.

Ce mémoire vise donc à retracer l'ensemble des actions menées au cours du stage, en mettant en lumière les compétences techniques mobilisées, les outils utilisés (JIRA, GNS3, Wireshark...), ainsi que les apprentissages tirés des situations rencontrées sur le terrain. Pour structurer cette analyse, trois grands axes seront développés :

1. Maquettage et simulation réseau

Études de cas pratiques en laboratoire (spanning-tree IEEE 802.1D, port-channel IEEE 802.1AX, VLAN IEEE 802.1Q, DHCP **RFC 2131** (IETF), private VLAN), manipulation de maquettes Cisco et simulation sur GNS3.

2. Déploiement réseaux chez les clients

Installation physique d'équipements dans les baies, câblage QSFP, mise à jour de firmware, configuration réseau, adaptation des équipements à l'environnement

client.

3. Support réseau de niveau 1 et interventions sur site

Suivi de tickets via l'outil JIRA, traitement de demandes clients, participation à la résolution d'incidents, changements de switchs ou pare-feux, installation de serveurs et hyperviseurs.

Les résultats obtenus, les compétences développées ainsi que quelques pistes d'approfondissement seront abordés par la suite. Ce stage a constitué une véritable immersion dans le milieu professionnel des réseaux, en cohérence avec les objectifs de la formation et les exigences du terrain.

1.1- Objectifs du stage

Les objectifs de ce stage étaient multiples :

- **Découvrir le fonctionnement d'un consultant réseau** à travers des missions de production et de support.
- **Accompagner à des déploiements et à l'exploitation de solutions réseau** (LAN, sécurité).
- **Développer mes compétences techniques** en configuration de matériel (switchs,, pare-feu), en analyse réseau.
- **M'initier aux méthodes de travail en équipe projet**, à la communication technique et à la gestion de tickets.

1.2- Présentation de l'entreprise (NXO)

- Nom et secteur d'activité

- Fondée en 2007 par Alcatel-Lucent Enterprise sous le nom de NextiraOne, NXO France a d'abord rassemblé les compétences et services d'intégration réseau du groupe pour proposer une offre unifiée d'infrastructures télécoms et digitales. Forte d'une croissance soutenue et de plusieurs acquisitions stratégiques, l'entreprise a opéré un rebranding début 2023 pour devenir NXO France, réaffirmant ainsi son

indépendance vis-à-vis des constructeurs et son positionnement d'intégrateur-opérateur centré sur l'innovation et la proximité client.

- De la conception et mise en place de réseaux LAN/Sécurité, WAN et SD-WAN, à la cybersécurité (audit, intégration de solutions et services managés), en passant par l'infogérance, la supervision et le support de niveau 1, chaque pôle de compétences travaille de concert pour garantir performance, résilience et évolutivité.
 - L'organisation de NXO France repose sur de multiples agences nationales régionales et de centres de services, complété par des entités spécialisées. Parmi elles, **NXO Océan Indien**, où le stage a été réalisé, joue un rôle essentiel dans la prise en charge des projets et du support technique pour les clients de la zone. Ce site compte des équipes dédiées au déploiement LAN/Wi-Fi, à la gestion des flux digitaux et à la maintenance proactive, assurant ainsi une continuité de service optimale dans un territoire aux défis géographiques et climatiques particuliers.
 - Aujourd'hui, NXO Océan indien accompagne ses clients des grands comptes aux collectivités territoriales, en passant par les établissements de santé et les PME tout au long du cycle de vie de leurs infrastructures numériques, voici leur clients à la réunion :



NXO accompagne les plus grands acteurs économiques et institutionnels de l'île de La Réunion, parmi lesquels le **CHU** de La Réunion, **EDF**, la Région Réunion, le **Département de La Réunion**, **E.Leclerc**, **Air Austral**, la **SIDR**, la **SEMADER**, ou encore l'**Aéroport Roland Garros**, témoignant ainsi de la confiance accordée par les piliers du développement local.

- En 2024, NXO France emploie environ 1 200 collaborateurs dont plus de 200 au sein de la filiale Océan Indien et réalise un chiffre d'affaires de plus de 300 millions d'euros. Parmi ces équipes, on compte aujourd'hui **38 collaborateurs en CDI et 7 apprentis**, gages d'un renouvellement et d'une transmission des compétences permanente.
- Certifiée par les principaux éditeurs (Cisco, VMware, Fortinet, etc.), traite plusieurs milliers de tickets par mois via ses centres de services, avec un niveau de satisfaction client reconnu. Grâce à cette structure agile et à son expertise multidisciplinaire, NXO se positionne comme un partenaire de choix pour conduire la transformation digitale de ses clients, depuis le conseil jusqu'à la maintenance opérationnelle.

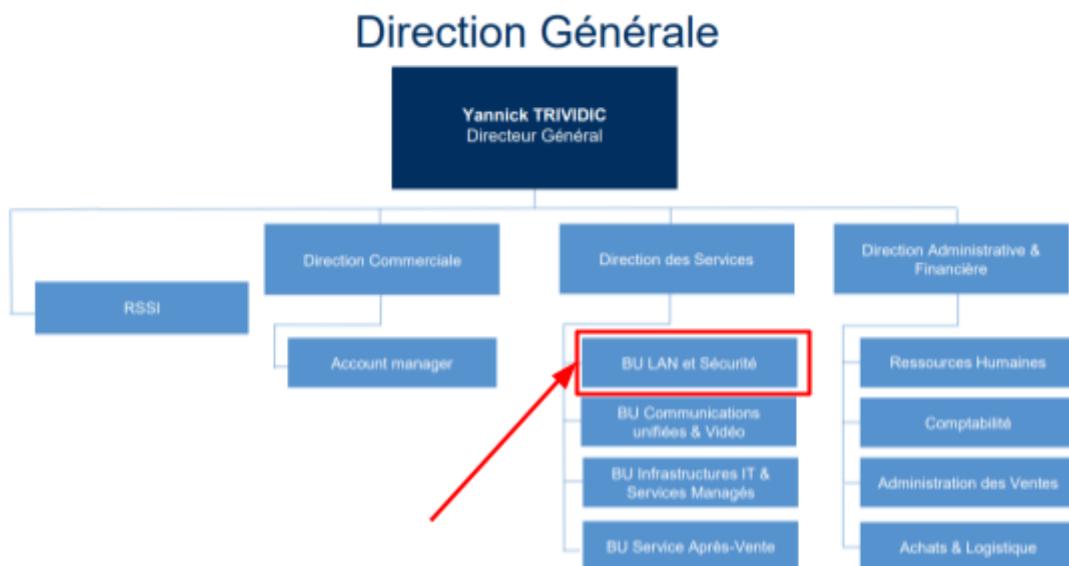
- Équipe encadrante

L'organisation de NXO Océan Indien repose sur une structure hiérarchique claire, détaillée dans l'organigramme disponible ci-dessous.

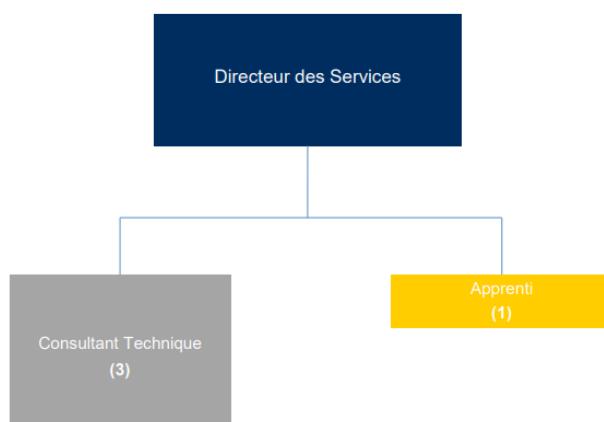
1.3- Présentation du service/département d'accueil

L'encadrement a été principalement assuré par l'équipe du service Réseau, sous la supervision de Hugues CHANE-NAM, consultant réseau. Des collaborations ponctuelles ont également eu lieu avec d'autres membres de l'équipe technique dans le cadre de projets spécifiques.

L'équipe, composée de trois personnes dont un apprenti, est structurée selon les spécialités réseau et sécurité :



BU LAN & Sécurité



1.4- Support de niveau 1 - Gestion des tickets (voir annexe 2-fig.1)

- Organisation de l'entreprise

Durant la période de stage, une participation active a été apportée à la **gestion du support de niveau 1** aux côtés de l'équipe technique, dans le cadre du traitement des demandes clients. Cette activité s'appuyait sur un système de **gestion de tickets structuré**, mis en œuvre via l'outil **JIRA**, utilisé ici comme **solution ITSM (IT Service Management)**.

Les tickets sont créés automatiquement ou manuellement selon plusieurs canaux :

- Via le **portail client** dédié : <https://www.nxo.eu/espace-client/>, réservé aux clients disposant d'un contrat de maintenance.
- À travers le **formulaire de contact en ligne** : <https://www.nxo.eu/contact/>
- Par **appel téléphonique**.

Une fois les tickets enregistrés dans **JIRA** qui est un logiciel qui aide les équipes à gérer et suivre leurs tâches, projets et problèmes. Il permet de créer des tickets pour organiser le travail, suivre leur avancement, et personnaliser les processus selon les besoins. C'est un outil utilisé surtout dans le développement logiciel et le support technique.

Ils sont traités selon leur **niveau de criticité** (P1 à P4) et leur **type** (incident, demande, alerte...). Les missions confiées ont permis de participer aux activités suivantes :

- **Consultation et suivi des tickets**
- **Analyse des demandes simples** : problème d'accès réseau, lenteurs, vérification de lien
- **Transmission ou escalade** vers le bon niveau technique (technicien, ingénieur, chef de projet)
- **Mise à jour des tickets dans JIRA** : commentaires, statut, clôture après validation du client.

2. Présentation du stage

2.1- Missions confiées

De nombreux tickets ont été traités tout au long du stage, portant sur des demandes fréquemment rencontrées au sein de l'entreprise, telles que :

Configuration de Switch HPE 1920s (voir annexe 1-fig.1-3) :

Une intervention a été réalisée sur des problèmes de connectivité réseau affectant des switchs **HPE 1920s**. L'analyse approfondie a permis d'identifier une **incompatibilité de version entre le firmware installé (PD.01.05) et les configurations réseau attendues**, lesquelles nécessitaient au minimum la version **PD.02.12**.

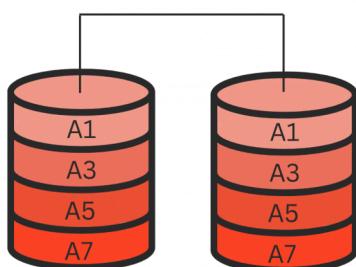
Afin de corriger cette anomalie, une **mise à jour des firmwares** a été effectuée via l'interface web des équipements, conformément aux recommandations du constructeur. Une fois les nouvelles versions installées, les configurations adaptées ont été rechargées, permettant ainsi le **rétablissement complet de la connectivité réseau**.

Installation et configuration de Serveur HP ProLiant DL360 Gen11 avec RAID 1 (voir annexe 1-fig.4-7):

Dans le cadre du déploiement de nouveaux serveurs chez plusieurs clients, une **installation logicielle** de serveurs **HP ProLiant DL360 Gen11** a été réalisée. L'objectif était de mettre en place **VMware ESXi**, un hyperviseur bare-metal permettant la **virtualisation de plusieurs machines**.

Avant l'installation de l'hyperviseur, une **configuration en RAID 1 (miroir)** a été effectuée dans le BIOS des serveurs, afin d'assurer une **redondance des données** : l'hyperviseur détecte alors un **unique disque logique**, tandis que les données sont automatiquement **duplicées sur un second disque dur**. Cette opération garantit une meilleure **tolérance aux pannes** et une **continuité de service** en cas de défaillance matérielle

RAID 1



- **Installation et configuration de Serveur Dell PowerEdge avec RAID 5 et iDRAC (voir annexe 1-fig.8-11) :**

Dans le cadre d'un projet d'intégration, un **serveur Dell PowerEdge** équipé de **7 disques SSD de 2 To chacun** a été configuré en **RAID 5**. Ce type de configuration permet de bénéficier à la fois de la tolérance aux pannes et d'une capacité optimisée, grâce à la répartition de la parité sur l'ensemble des disques.

L'objectif était **d'installer une distribution Debian** sur ce serveur, initialement prévue via une **clé USB bootable**. Cependant, le système échouait à démarrer automatiquement sur la clé. Pour contourner cette contrainte, la solution **iDRAC (Integrated Dell Remote Access Controller)**, composant intégré à la carte mère et actif dès l'alimentation du serveur, a été utilisée.

iDRAC offre une **interface de gestion à distance** avec accès complet au serveur, y compris au BIOS et au système de boot. Grâce à sa propre carte réseau, il a été possible d'y accéder à distance afin de monter directement une image ISO de Debian. Ce procédé a permis de lancer l'installation sans intervention physique supplémentaire, en profitant des fonctionnalités avancées de virtualisation de média qu'offre iDRAC. Cette intervention a ainsi renforcé la maîtrise des environnements de gestion distante et des solutions RAID.

- **Installation physique d'équipement réseaux et serveurs dans les baies :**

Des opérations d'**aménagement de baies réseau** ont également été réalisées, constituant une étape pratique essentielle dans tout projet d'intégration d'infrastructure. Ces interventions comprennent l'**installation des rails métalliques** destinés à supporter les serveurs et les switches, la **mise en place des écrous cage**, ainsi que le **rakkage physique des équipements** dans les baies prévues chez le client.

Ce type de travail requiert une grande **précision**, une **organisation rigoureuse** et le **respect strict des normes de câblage**, afin d'assurer une **accessibilité optimale**, une bonne **ventilation** des équipements et une **sécurité physique adéquate**.

2.2- Outils et environnements utilisés

1. JIRA - ITSM (IT Service Management) (voir annexe 2-fig.1) :

Outil central pour la **gestion des tickets** : suivi des incidents, demandes, alertes clients, priorisation (P1 à P4), et **clôture après validation**. Il permet également la traçabilité des interventions et la collaboration entre les niveaux techniques.

2. GNS3 (voir annexe 2-fig.2):

Environnements de **simulation de réseaux** utilisés pour tester des configurations complexes (VLAN, Spanning Tree, DHCP, Port-channel, etc.).

- GNS3 a été particulièrement utile pour mettre en œuvre des **Private VLAN** non supportés sur les Cisco 2960 physiques empruntés dans le lab et simuler des pare-feu tel que fortinet dont la license provient de l'entreprise.

3. Wireshark :

Utilisé pour analyser les **trames réseau** capturées, notamment les séquences DHCP (Discover, Offer, Request, ACK), et observer des phénomènes comme les **tempêtes de broadcast**.

4. Console Cisco (Putty via câble console) :

Accès direct aux **équipements Cisco** pour la configuration en ligne de commande. Tu as pu pratiquer sur des switchs Cisco 2960 les configurations réseau classiques et avancées.

5. Interfaces Web (HPE, Fortigate, VMware ESXi) ([voir annexe 2-fig.3-5](#)) :

Administration d'équipements via interface graphique :

- **HPE 1920S** pour les mises à jour de firmware et configurations LAN,
- **Fortigate** pour les configurations SD-WAN et de pare-feu,
- **ESXi** pour l'installation et la gestion de serveurs virtualisés.

6. VMware ESXi & BIOS RAID

Lors de l'installation sur des serveurs **HP ProLiant DL360 Gen11**, tu as utilisé le BIOS pour créer un **RAID 1** (miroir) avant l'installation de l'hyperviseur **VMware ESXi**. Cela garantissait redondance et sécurité des données dès le niveau physique.

7. Environnements Datacenter / Matériel physique ([voir annexe 5 & 6](#))

- **Rackage** d'équipements (serveurs, switchs) dans les **baies informatiques** avec les outils adaptés : rails (U), visserie, écrous cages.
- **Câblage réseau** réalisé avec des liens RJ-45, SFP, et **QSFP+** pour les liaisons **100 Gb** entre équipements cœur et distribution.

- Sites clients visités : **CHU de Saint-Pierre**, **BNP Paribas**, **datacenter FRET**, **Aéroport Roland Garros**, **Père Favron** (EHPADs).

8. PatchSee / PatchLight ([voir annexe 2-fig.6](#))

Outil utilisé pour **identifier facilement les câbles RJ45** dans les baies grâce à un système de **fibres optiques intégrées** dans le câble réseau.

Avec une **lampe PatchLight**, tu peux illuminer une extrémité du câble et voir la lumière guider l'identification de l'autre extrémité, ce qui est très utile pour **le repérage rapide dans les armoires de brassage** lors d'interventions de maintenance ou de migration réseau.

9. Étiqueteuse Brady BMP41 ([voir annexe 2-fig.7](#))

Outil indispensable pour le **marquage et l'identification des câbles** dans les armoires réseau. Cette imprimante portative permet d'apposer des étiquettes durables sur les cordons RJ-45, les ports ou les équipements, facilitant ainsi la lisibilité, la documentation et la maintenance des infrastructures réseau.

2.3- Méthodologie

Au sein de NXO Océan Indien, la méthodologie de travail repose sur une démarche rigoureuse, structurée et évolutive, permettant une intégration progressive dans les missions du service Réseaux et Sécurité. Cette organisation facilite la montée en compétences techniques tout en assurant un cadre opérationnel cohérent et sécurisé, tant en laboratoire que sur les sites clients.

- 1. Progression par paliers

La montée en compétences s'articule en trois étapes :

- **Phase d'observation** : participation à des interventions encadrées et analyse de configurations en production afin de comprendre les environnements clients et les standards appliqués.
- **Phase d'expérimentation** : reproduction de scénarios réels en laboratoire à l'aide de maquettes physiques ou de simulateurs (Cisco 2960, GNS3), permettant de tester les protocoles et d'anticiper les comportements réseau (Spanning Tree, VLAN, DHCP, agrégation de liens, Private VLAN...).
- **Phase de mise en œuvre** : réalisation de tâches sur le terrain ou à distance sous supervision, avec application des bonnes pratiques et vérification systématique avant mise en service.

- 2. Documentation et traçabilité

La gestion rigoureuse de la documentation est un pilier fondamental :

- **Utilisation de JIRA** pour le suivi des incidents et des demandes, avec priorisation (P1 à P4), affectation, commentaires techniques et clôture après validation client.
- **Production de comptes rendus d'intervention**, intégrant les détails techniques et les observations terrain.
- **Archivage de configurations, captures d'écran, trames réseau (via Wireshark)** et schémas explicatifs pour assurer une bonne capitalisation des connaissances.

- 3. Outils et équipements adaptés

L'environnement de travail combine équipements physiques et outils logiciels :

- Outils de simulation : **GNS3, Cisco Packet Tracer**
- Outils d'analyse réseau : **Wireshark, console Cisco, interfaces web HPE, Fortigate, ESXi**
- Matériels physiques : **switchs Cisco / HPE, pare-feux Fortigate, serveurs HP ProLiant, câbles RJ-45, SFP, QSFP+**
- Outils de terrain : **PatchSee, PatchLight, étiqueteuse Brady BMP41** pour le repérage et l'identification des câblages

4. Organisation du travail collaboratif

Chaque action technique est soumise à une **validation systématique par les référents** (techniciens, ingénieurs, chefs de projet). Cette organisation assure une montée en autonomie encadrée, avec des échanges réguliers permettant de :

- Vérifier la cohérence technique des solutions proposées

- Apporter des explications claires aux clients ou à l'équipe
- Prendre en compte les contraintes spécifiques à chaque environnement (bâtiments hospitaliers, aéroport, datacenter...)

5. Méthode d'intervention client

Sur site, les interventions suivent une logique en trois temps :

- **Préparation** : récupération de la configuration, vérification du matériel, mise à jour firmware si nécessaire
- **Déploiement** : installation, câblage, test de fonctionnement
- **Validation** : tests de connectivité, supervision et retour au client

2.4- Encadrement

Durant toute la durée du stage, l'intégration au sein du service Réseaux et Sécurité de **NXO Océan Indien** s'est effectuée sous la responsabilité d'un **consultant réseau** expérimenté. Ce dernier assurait un encadrement quotidien, tant sur le plan technique que méthodologique.

L'accompagnement s' inscrit dans une logique de **transmission progressive des compétences**. Chaque activité débutait par une phase d'explication ou de démonstration, suivie d'une mise en application supervisée. Qu'il s'agisse de configuration d'équipements, d'analyse de trames réseau, de diagnostic d'incidents ou de déploiement sur site, le consultant guidait chaque étape tout en laissant une marge de réflexion et d'initiative.

Le stage s'est déroulé selon une approche structurée : **observation active, expérimentation sur maquettes** (Cisco 2960, GNS3), puis **participation à des interventions clients** réelles, dans des environnements sensibles comme l'aéroport, les établissements hospitaliers, ou les datacenters. Ces contextes exigeants ont mis en valeur la rigueur, la précision et le respect des procédures que le consultant réseau a su transmettre.

L'encadrement a également favorisé une **autonomie progressive**, encourageant l'analyse critique, la reformulation des besoins techniques et la proposition de solutions adaptées. Des temps réguliers de débriefing permettaient de revenir sur les interventions réalisées, d'en tirer les leçons techniques et organisationnelles, et d'améliorer les réflexes professionnels.

Travailler aux côtés d'un consultant réseau a offert une **vision concrète et réaliste du métier**, entre expertise technique, adaptation client et gestion opérationnelle, enrichissant ainsi considérablement l'expérience de terrain.

3- Projets et interventions réalisées

3.1- Interventions techniques réseau

Les interventions réalisées au cours du stage ont permis d'aborder de manière concrète les différentes facettes du métier de technicien et consultant réseau, notamment à travers le **déploiement et la configuration d'équipements actifs**, la **mise en œuvre de bonnes pratiques de sécurisation**, ainsi que la **gestion de la connectivité dans des environnements clients variés**.

- Déploiement et remplacement de switchs Cisco

Plusieurs interventions ont consisté à **remplacer ou installer des switchs Cisco**, en environnement de production, notamment dans les locaux de **BNP Paribas**. À titre d'exemple, un switch défaillant (en mode ROMmon suite à une corruption de la mémoire flash) a été remplacé après un repérage et un étiquetage rigoureux des câbles RJ-45. Une fois le nouveau switch installé, une **mise à jour du firmware** a été nécessaire afin de garantir la compatibilité avec la configuration existante, avant de **réinjecter la configuration sauvegardée**. Cette opération a permis une reprise normale de la connectivité réseau.

D'autres interventions ont concerné des déploiements de switchs en **baies informatiques**, comme au **CHU de Saint-Pierre**, avec des étapes de **racking**, de **brassage fibre (QSFP 100 Gb)**, et de **repérage des unités (U)**. Ces manipulations physiques nécessitent précision, rigueur et une bonne coordination avec les autres pôles (systèmes, sécurité).

- Mise en place de VLANs, Spanning Tree et autres protocoles en simulation et en physique (voir annexe 3-fig.1)

Dans le cadre du **maquettage en laboratoire** avec des switch cisco 2960 et des projets client, plusieurs configurations ont été mises en œuvre :

- **Création de VLANs et Private Vlan** pour la segmentation réseau, avec affectation statique des ports selon les usages (voix, data, management).
- **Configuration du Spanning Tree Protocol (STP)** et de ses variantes (RPVST+, MSTP) pour prévenir les boucles de niveau 2 dans les topologies redondantes.
- **Analyse des BPDU** à l'aide de Wireshark, afin de comprendre le mécanisme de propagation et de détection des chemins actifs dans le réseau.
- **Mise en œuvre du protocole VTP** en mode client/serveur pour automatiser la configuration des VLANs sur plusieurs équipements interconnectés.
- **Port Channel (EtherChannel)** : agrégation de plusieurs liens physiques en un seul lien logique pour **augmenter la bande passante** et assurer une **redondance**.

Ces configurations ont été testées dans un environnement sécurisé avant leur déploiement sur les infrastructures clients. L'objectif était de garantir une **maîtrise des risques** liés à la mise en production et de **renforcer la fiabilité du réseau local (LAN)**.

3.2 Interventions sécurité

Les aspects liés à la **sécurité réseau** ont également été largement abordés durant le stage, notamment à travers des missions de **déploiement de pare-feu Fortigate**, l'accompagnement à la **migration de technologies de communication**, et l'**analyse de configurations** en environnement client.

- **Installation de pare-feu Fortigate (voir annexe 4-fig.1)**

Plusieurs interventions ont consisté à installer et configurer des pare-feu **Fortigate** sur des sites distants appartenant au **Groupe Père Favron**, tels que les EHPAD du Port et de La Possession. Ces déploiements faisaient partie d'un projet global visant à remplacer une infrastructure basée sur **MPLS** par une solution **SD-WAN**, plus flexible, résiliente et adaptée aux usages modernes.

Les équipements déployés étaient préconfigurés en amont selon un modèle standard destiné au siège, mais ont nécessité des ajustements sur site, les structures locales ayant des contraintes spécifiques (liaisons, plages d'adresses, bande passante, etc.). Ces adaptations ont été effectuées en production, en maintenant les services opérationnels.

Migration MPLS vers SD-WAN([voir annexe 4-fig.2](#))

Dans le cadre de cette transformation d'infrastructure, la migration vers le SD-WAN a permis d'optimiser la gestion des flux inter-sites, en combinant des liens WAN classiques (fibre, ADSL, 4G) et en utilisant des politiques de routage intelligentes pour prioriser le trafic métier. Ce type de solution, intégré dans les pare-feu Fortigate, assure également un meilleur niveau de sécurité périphérique, grâce aux fonctionnalités natives (filtrage web, contrôle applicatif, IPS...).

L'environnement Fortinet permet de centraliser la gestion via **FortiManager**, une plateforme d'administration centralisée des politiques de sécurité, des configurations réseau, et des mises à jour. Cela permet de gérer plusieurs pare-feu de manière cohérente, tout en gardant un contrôle granulaire sur chaque site. En complément, **FortiCloud** permet un suivi à distance des équipements, des logs et des alertes critiques via une interface en ligne, facilitant ainsi la supervision et la réactivité en cas d'incident.

Le stage a ainsi permis d'assister le consultant dans toutes les étapes : raccordement physique, vérification de la configuration, tests de connectivité et validation avec le client.

Analyse de configurations et adaptation sur site

L'analyse des configurations des pare-feu déjà en place a parfois mis en évidence des incompatibilités ou des erreurs, notamment des règles mal adaptées aux besoins réels des utilisateurs. Il a donc fallu effectuer des diagnostics via l'interface **FortiOS**, consulter les logs, et modifier dynamiquement certaines règles pour assurer la continuité de service.

Ce type d'intervention a mis en lumière l'importance de l'audit régulier des politiques de sécurité, et la nécessité de documenter rigoureusement chaque changement dans un environnement client sensible.

3.3 Maquettes et simulations en environnement isolé ([voir annexe 2 fig.2 et 3 fig.1](#))

Comme dit au dessus avant chaque déploiement en production, des phases de tests et de simulations ont été réalisées dans un environnement isolé afin de valider les configurations et d'expérimenter différentes technologies sans risque pour les infrastructures clientes. Ces essais ont principalement été menés dans le laboratoire de

NXO, à l'aide de switchs Cisco 2960 physiques, ainsi que via le simulateur GNS3, permettant d'utiliser des équipements virtuels plus récents et plus puissants.

Parmi les expérimentations notables figure la mise en place de **Private VLANs**, une technologie de segmentation fine permettant d'isoler certains ports tout en maintenant un accès à des services partagés via des ports "promiscuous". Ce type de configuration, non pris en charge sur les Cisco 2960, a été simulé dans GNS3 avec des équipements de niveau 3.

D'autres mécanismes de sécurité de niveau 2 ont également été étudiés, notamment **DHCP Snooping**, **Dynamic ARP Inspection (DAI)** et **IP Source Guard**. Ces fonctions visent à protéger le réseau contre des attaques de type spoofing et à garantir l'intégrité des communications internes.

Une **étude approfondie du protocole Spanning Tree** a également été menée, avec l'analyse comparative des variantes STP, RPVST+ et MSTP. L'outil Wireshark a été utilisé pour examiner les **trames BPDU** échangées entre switchs, afin de mieux comprendre le rôle de chaque instance dans la prévention des boucles réseau.

Des scénarios de **tempête de broadcast en environnement DHCP** ont été simulés, notamment en injectant plusieurs serveurs DHCP sur le même segment. Cette approche a permis de visualiser, toujours via Wireshark, l'ensemble des échanges DHCP (Discover, Offer, Request, ACK) et d'analyser la rapidité de réponse ou la prise de priorité entre serveurs.

Par ailleurs, **des pare-feu Fortigate ont été testés en simulation avec GNS3** dans des environnements simulés. Cela a permis d'explorer des fonctionnalités avancées telles que le NAT/PAT, le contrôle applicatif, le filtrage web ou encore les VLANs routés, en préparation de leurs déploiements réels sur site.

Enfin, une **comparaison entre le comportement des switchs Cisco 2960** et celui de modèles plus récents comme le cisco 3065 a été effectuée, afin de mesurer les limitations matérielles et logicielles, ainsi que l'impact sur la compatibilité des configurations réseau.

L'ensemble de ces maquettes a joué un rôle crucial dans la **validation des configurations**, **l'approfondissement des concepts réseau**, ainsi que dans la **préparation aux interventions clients**, en réduisant les risques d'erreurs et en améliorant la réactivité lors des missions sur le terrain.

3.4 Cas concrets chez les clients

Plusieurs missions ont été menées directement sur site auprès de clients de NXO, permettant d'intervenir dans des environnements professionnels variés, aux contraintes techniques et organisationnelles spécifiques. Ces cas concrets illustrent la diversité des

besoins en matière de réseau et de sécurité, ainsi que la capacité d'adaptation nécessaire lors de chaque intervention.

BNP Paribas : remplacement d'un switch défectueux en environnement critique

Une intervention réseau a été réalisée sur un site de **BNP Paribas**, à la suite d'une panne majeure ayant provoqué une **interruption complète de l'accès à Internet et aux services réseau pendant plusieurs jours**. L'origine du dysfonctionnement a été identifiée comme étant un **switch Cisco en panne**, incapable de démarrer normalement.

Lors du diagnostic, l'équipement était bloqué en **mode ROMMON (ROM Monitor)**, un mode de secours propre aux équipements Cisco. Ce mode est activé lorsque le **système d'exploitation du switch (IOS)** ne peut pas se charger correctement, généralement à cause d'un **fichier corrompu ou d'un défaut matériel**, comme une défaillance de la **mémoire flash interne**. Dans cet état, le switch ne peut pas exécuter sa configuration habituelle, n'active pas ses interfaces, et ne répond qu'à quelques commandes de bas niveau en mode console.

Dans ce cas précis, la mémoire flash du switch étant défectueuse, aucune tentative de rechargement de l'IOS n'a pu aboutir, et **aucune configuration existante ne pouvait être restaurée**.

L'intervention a consisté à plusieurs étapes clés :

- **Identification des câbles RJ45 actifs**, en repérant minutieusement les connexions critiques vers les différents équipements réseau et serveurs ;
- **Numérotation et documentation des ports utilisés**, pour garantir un positionnement identique sur le nouvel équipement ;
- **Démontage du switch défectueux** ;
- **Installation d'un switch neuf de même modèle**, préalablement préparé ;
- **Mise à jour du firmware (logiciel interne du switch)** sur le nouvel équipement.

Un point de difficulté supplémentaire s'est présenté : **le site ne disposait pas de connexion Internet fonctionnelle** au moment de l'intervention. Cela a empêché le téléchargement classique du firmware depuis les serveurs Cisco. Pour contourner ce problème, **un partage de connexion via données mobiles** a été utilisé afin de récupérer le bon fichier IOS et procéder à la mise à jour en local.

Enfin, la **configuration précédemment sauvegardée** a été injectée dans le nouveau switch, permettant de **restaurer tous les services réseau** (accès Internet, communications internes, liaisons inter-serveurs, etc.).

Cette intervention a mis en évidence l'importance de la **gestion rigoureuse des configurations réseau**, de la **préparation des firmwares compatibles** en amont et de la capacité à **s'adapter à des contraintes d'environnement en situation réelle**, notamment en cas d'absence de connectivité Internet.

Data center du CHU de Saint-Pierre : installation en baie ([voir annexe 5 fig.1](#))

Dans le cadre d'un projet de **migration réseau du CHU de Saint-Pierre**, une phase préparatoire a été menée dans la salle informatique de NXO, où une baie dédiée a été installée pour accueillir l'infrastructure cible. L'objectif était de préparer l'environnement qui serait ensuite déployé sur site.

Les actions menées comprenaient :

- **Le montage physique de plusieurs équipements** (switchs, serveurs) en respectant la disposition en unités U,
- L'utilisation de rails, visseries et écrous cages pour fixer les équipements en baie,
- **Le brassage en fibre optique QSFP** pour établir des liaisons 100 Gb entre les équipements,
- **Le raccordement électrique et le repérage** des interfaces réseau.

Ce travail a permis de valider l'**ergonomie de la baie**, d'organiser correctement les flux réseau et d'**anticiper les problèmes de câblage** pour le déploiement final sur le site du CHU.

Groupe Père Favron : déploiement de pare-feu Fortigate ([voir annexe 4 fig.1](#))

Comme présenté dans la section sécurité, plusieurs établissements du groupe Père Favron ont été équipés de **pare-feu Fortigate** dans le cadre d'un **remplacement progressif des liaisons MPLS** par une architecture plus moderne et nouvelle avec le SD-WAN qui permet de connecter les différents sites d'une entreprise via Internet de façon intelligente et sécurisée, disponible sur le pare-feu. Les sites concernés, tels que les EHPAD de La Possession, du Port et de Saint-Denis, ont bénéficié d'une sécurisation renforcée et d'une amélioration des performances réseau.

L'intervention a exigé :

- La vérification des configurations préchargées,
- L'adaptation aux contraintes spécifiques de chaque site (adresse IP, routage, DNS...),
- Des tests de connectivité et de redondance,
- La validation avec le client une fois les équipements opérationnels.

Air Austral : accompagnement technique et infrastructure réseau dans les datacenters de l'aéroport (voir annexe 6 fig.1-3)

Dans le cadre du suivi de l'infrastructure réseau d'**Air Austral**, plusieurs interventions ont été réalisées sur les différents datacenters situés à l'aéroport Roland Garros, visant à renforcer et interconnecter le réseau entre les différentes baies réparties sur site.

- **Data Center APAX**(voir annexe 6 fig.1) : ce datacenter principal, situé dans les locaux de l'aéroport, héberge une partie centrale de l'architecture réseau d'Air Austral. Une intervention a été menée pour le **branchement de câbles RJ-45 sur les switchs d'une baie dédiée**, dans le but de participer à la migration du **nouveau réseau à l'ancien de l'aéroport**. Ce câblage avait pour objectif d'assurer **cette migration des différents réseaux** de l'infrastructure aéroportuaire. Une attention particulière a été portée à l'organisation et au repérage des ports, pour garantir un câblage structuré et évolutif.
- **Data Center du FRET**(voir annexe 6 fig.2) : localisé dans la zone fret de l'aéroport, ce site secondaire accueille de nombreuses baies utilisées par Air Austral mais aussi par d'autres entreprises. Une mission de **vérification de connectivité des câbles RJ-45** a été effectuée. En raison de la longueur des câbles et du manque de visibilité sur leur trajet exact, un outil spécifique a été utilisé : le **Patchsee Patchlight**. Ce dispositif permet de faire circuler un **rayon lumineux dans les câbles RJ45 équipés de fibres optiques**, facilitant ainsi l'identification de chaque extrémité. Cette méthode a permis de **tracer efficacement les connexions** et de garantir la bonne liaison des équipements réseau. Parallèlement, un **étiquetage rigoureux des câbles** a été réalisé à l'aide d'une **étiqueteuse Brady BMP41**, afin de documenter clairement l'infrastructure.
- **Data Center Witness**(voir annexe 6 fig.3) : situé en **sous-sol de l'aéroport**, ce datacenter fait office de **site technique sécurisé** complémentaire. Il a accueilli une

opération d'installation de **deux bornes Aruba**, dans le cadre du renforcement de la couverture réseau sans fil. À noter que **l'entreprise Atos**, concurrent direct de NXO sur ce marché, est chargée de la mise en place des **serveurs chez Air Austral**. Cette intervention a permis d'observer la cohabitation de plusieurs prestataires techniques autour d'une même infrastructure, tout en suivant un protocole d'accès strict et des consignes de sécurité élevées.

Ces différentes interventions ont offert une immersion concrète dans la gestion réseau d'une structure critique comme celle d'une compagnie aérienne, tout en permettant de manipuler des outils professionnels (Patchsee, Brady, Aruba) dans des contextes techniques réels et exigeants.

4. Compétences acquises

Au cours de ce stage réalisé au sein de NXO Océan Indien, de nombreuses compétences ont été mobilisées, développées et consolidées dans des contextes concrets et professionnels. Ce stage a permis de renforcer des connaissances théoriques, tout en apportant une expérience significative sur le terrain, tant au niveau technique que méthodologique et relationnel.

4.1 Compétences techniques

Le cœur du stage a porté sur les technologies réseau et sécurité, dans des environnements variés et parfois critiques. Les interventions ont nécessité une bonne compréhension des équipements physiques, des logiciels et des protocoles.

- **Matériel réseau :** Une manipulation régulière d'équipements comme les switchs Cisco Catalyst (série 2960), les pare-feu Fortigate, les serveurs HP ProLiant DL360 Gen11 et Dell PowerEdge, les convertisseurs SFP, ainsi que les outils de test de connectique (PatchSee, PatchLight, testeurs RJ45) a permis d'acquérir une bonne aisance dans les environnements techniques professionnels.
- **Câblage et connectique :** Le câble en baie, l'organisation physique des équipements, l'étiquetage rigoureux des câbles (notamment avec l'étiqueteuse Brady BMP41), ainsi que la gestion des liaisons cuivre et fibre optique QSFP 100G ont été couramment pratiqués.

- **Configuration logicielle** : Plusieurs configurations ont été mises en œuvre : VLANs, Spanning Tree Protocol (STP, RPVST+, MSTP), Port Channels, routage inter-VLAN, NAT/PAT, ACLs, ainsi que des services tels que DHCP, DNS, Web Filtering, Application Control.
- **Environnements simulés** : GNS3 a été utilisé pour tester des scénarios complexes dans un environnement isolé : Private VLANs, DHCP Snooping, Dynamic ARP Inspection (DAI), IP Source Guard, pare-feu Fortigate.
- **Systèmes et virtualisation** : Installation et configuration de VMware ESXi et de systèmes Linux (Debian) sur serveurs physiques, gestion RAID (RAID 1, RAID 5) via BIOS ou iDRAC, gestion d'images ISO, paramétrage de consoles distantes.

Ces expériences ont renforcé la compréhension des interactions entre matériel, protocole et système, avec une approche orientée performance et sécurité.

4.2 Compétences méthodologiques

Le stage a aussi été l'occasion de structurer une approche rigoureuse face aux problématiques techniques et organisationnelles rencontrées sur site ou en laboratoire.

- **Diagnostic et résolution de pannes** : Face à des défaillances matérielles (comme un switch bloqué en mode ROMMON), la démarche a consisté à analyser les causes (problèmes de mémoire flash), à proposer une solution (remplacement, mise à jour firmware) et à valider la remise en service par des tests.
- **Documentation technique** : Chaque configuration, intervention ou scénario a été documenté précisément. La recherche de documentation constructeur (Cisco, Fortinet, Dell), de guides de bonnes pratiques et de schémas réseau a été systématisée.
- **Planification et préparation** : Avant chaque intervention (sur site ou en laboratoire), les configurations ont été testées en maquette afin de réduire les risques d'erreurs en production. Cela inclut notamment la validation d'images firmware, les tests de connectivité, et les sauvegardes de configuration.
- **Autonomie et rigueur** : L'environnement professionnel exigeait précision et fiabilité, notamment dans le câblage, l'attribution des ports, ou encore le respect des procédures de sécurité. La rigueur dans les manipulations et dans le suivi des

tâches a été essentielle.

4.3 Compétences relationnelles

L'intégration dans une équipe technique, les interventions chez les clients et l'accompagnement d'un consultant réseau ont permis de développer des compétences humaines et organisationnelles indispensables dans le monde professionnel.

- **Travail en binôme et en équipe :** L'ensemble des missions a été réalisé sous la supervision ou en accompagnement d'un consultant, ce qui a favorisé l'apprentissage par observation et la coopération dans les prises de décision techniques.
- **Communication avec les clients :** Lors des interventions sur site (BNP Paribas, CHU de La Réunion, Air Austral, Groupe Père Favron), une posture professionnelle était attendue. Il a fallu savoir s'adapter à l'environnement, écouter les besoins, expliquer les actions menées et rassurer sur le bon déroulement des opérations.
- **Adaptabilité :** Plusieurs imprévus ont nécessité des ajustements rapides, comme l'absence de connexion Internet lors de la mise à jour d'un firmware ou la configuration inadaptée d'un pare-feu. La capacité à s'adapter tout en respectant les délais et les contraintes techniques a été fortement sollicitée.

5. Bilan du stage et perspectives

Ce stage m'a permis de mener à bien l'ensemble des missions qui m'ont été confiées, aussi bien en intervention client qu'en environnement de test. Les opérations techniques réalisées sur le terrain, notamment le remplacement de switchs, l'installation en baie, ou encore le déploiement de pare-feu Fortigate, ont toutes abouti à des résultats fonctionnels et conformes aux attentes, malgré certaines contraintes rencontrées, comme l'incompatibilité de configurations pré chargées sur des sites distants.

La diversité des cas rencontrés m'a permis de mieux comprendre le fonctionnement réel d'un réseau d'entreprise, ainsi que les contraintes techniques, logistiques et humaines

liées aux projets d'infrastructure. J'ai également renforcé mes compétences dans la configuration des équipements Cisco, dans la gestion de la sécurité réseau via des pare-feu professionnels, ainsi que dans la démarche d'analyse et de diagnostic.

Cependant, certaines interventions auraient pu être optimisées si une meilleure documentation des infrastructures clients ou un système de gestion centralisée des configurations avait été disponible. Cela pourrait constituer une piste d'amélioration pour les futurs déploiements, notamment dans le cadre de projets de migration technologique comme le passage de MPLS à SD-WAN.

Pour approfondir cette expérience, il serait intéressant d'aborder la mise en place d'une supervision réseau complète (NMS/NOC), ou encore l'automatisation de déploiements via des outils comme Ansible ou Python avec Netmiko/NAPALM. Une étude sur la gestion des logs de sécurité (SIEM) ou sur la mise en place de plans de reprise d'activité (PRA) dans un environnement multi-sites serait également un prolongement pertinent à ce stage.

En résumé, ce stage a été très formateur tant sur le plan technique que professionnel. Il a confirmé mon intérêt pour les métiers de la cybersécurité et des réseaux, et renforcé ma volonté de poursuivre dans ce domaine.

ANNEXES et ILLUSTRATIONS

Annexe 1

- **Configuration de Switch HPE 1920s avec interface graphique:**

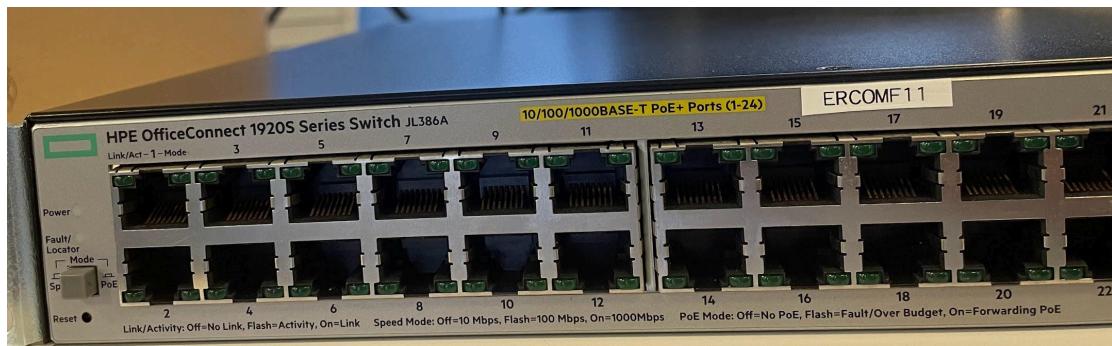


Figure 1 : Photo du HPE 1920s 48 port.

File Transfer		
Transfer Protocol	Backup <i>Transfer a file from the switch</i>	Update <i>Transfer a file to the switch</i>
HTTP	<input type="button" value="Upload"/>	<input type="button" value="Download"/>
TFTP	<input type="button" value="Upload"/>	<input type="button" value="Download"/>
SFTP	<input type="button" value="Upload"/>	<input type="button" value="Download"/>

Copyright © 2010-2017 Hewlett Packard Enterprise Development LP.

Figure 2 : Interface de transfert de fichier de configuration ou de mise à jour.

Copy Configuration Files	
Source File	Running Configuration
Destination File	Running Configuration Running Configuration Startup Configuration Backup Configuration <input type="button" value="Apply"/>

Figure 3 : Choix du type de fichier à transférer.

- **Installation et configuration de Serveur HP ProLiant DL360 Gen11 avec RAID 1 :**



Figure 4 : Photo de Serveur HP ProLiant DL360 Gen11.



Figure 5 : Sélection des disques pour créer le RAID dans le bios.



Figure 6 : Choix du RAID.



Figure 7 : Vérification du disque virtuel RAID 1 .

Installation et configuration de Serveur Dell PowerEdge avec RAID 5 :



Figure 8 : Photo de Serveur Dell PowerEdge.



Figure 9 : Photo de L'IDRAC du serveur DELL et de son port réseau.

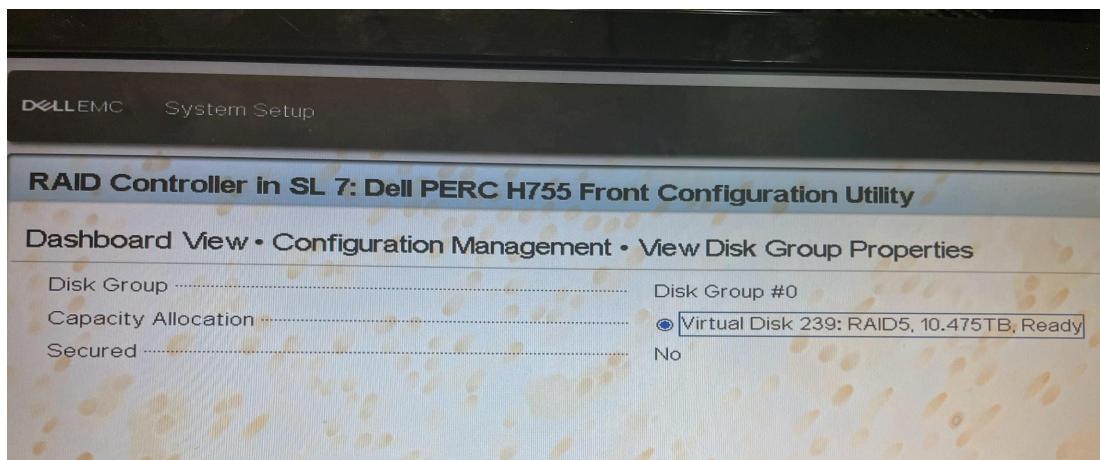


Figure 10 : Vérification du disque virtuel RAID 5.

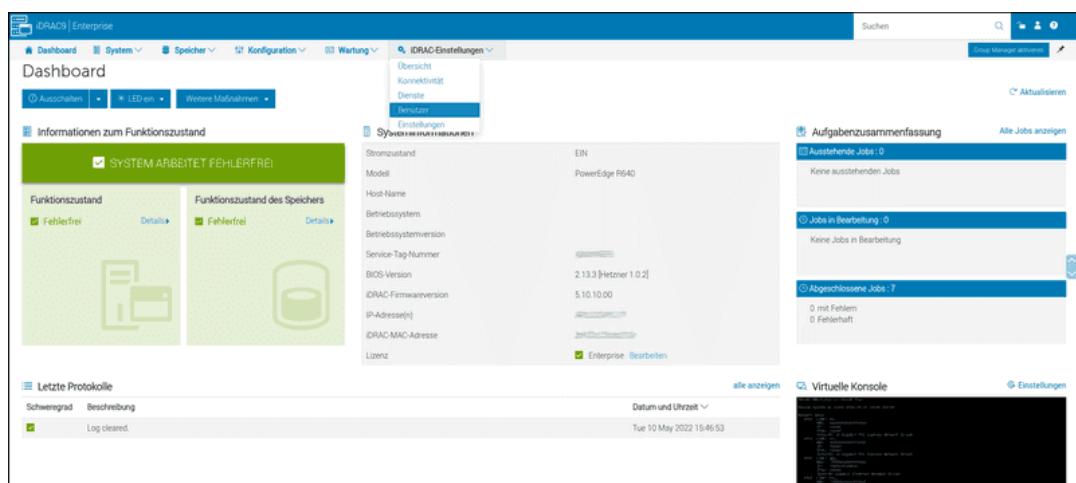


Figure 11 : Interface web de L'IDRAC du serveur DELL.

Annexe 2

- Outils et environnements utilisés :

The screenshot shows the JIRA Service Desk interface under 'Project settings'. On the left, a sidebar lists 'REQUEST TYPES' including 'Service requests', 'Incidents', 'Problems', 'Changes', and 'Unassigned'. The main area displays 'Service requests' with the following details:

Request type and description	Issue type	Portal groups
Create Cloud Site Create your own Cloud Site and choose which products you want created.	[System] Service request	Applications
Fix an account problem Having trouble accessing certain websites or systems? We'll help you out.	[System] Service request	Logins and Accounts
Get a guest wifi account Raise a request to ask for temp wifi access for guests.	[System] Service request	Logins and Accounts
Get IT help Get assistance for general IT problems and questions.	[System] Service request	(Used in 2 grou...)
Request a new account Request a new account for a system.	[System] Service	(Used in 2 grou...)

Figure 1 : Interface web du gestionnaire de ticket “JIRA”.

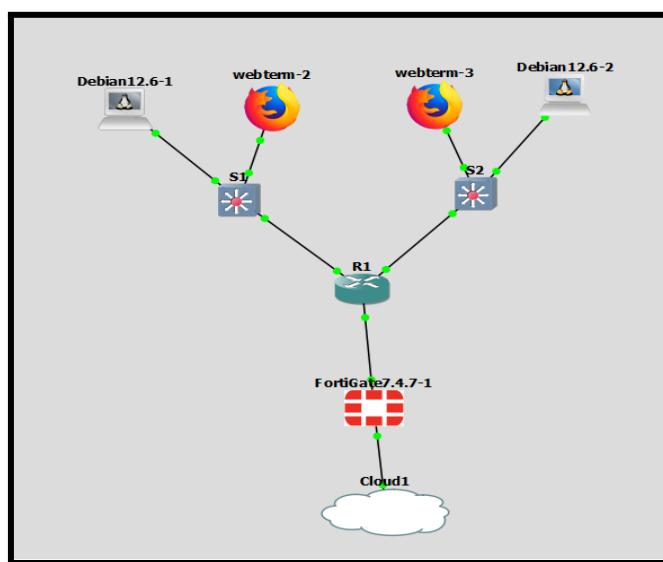


Figure 2 : Maquette réseaux apprentissage pare-feu fortinet sur le simulateur GNS3



Figure 3 : Interfaces Web HPE.

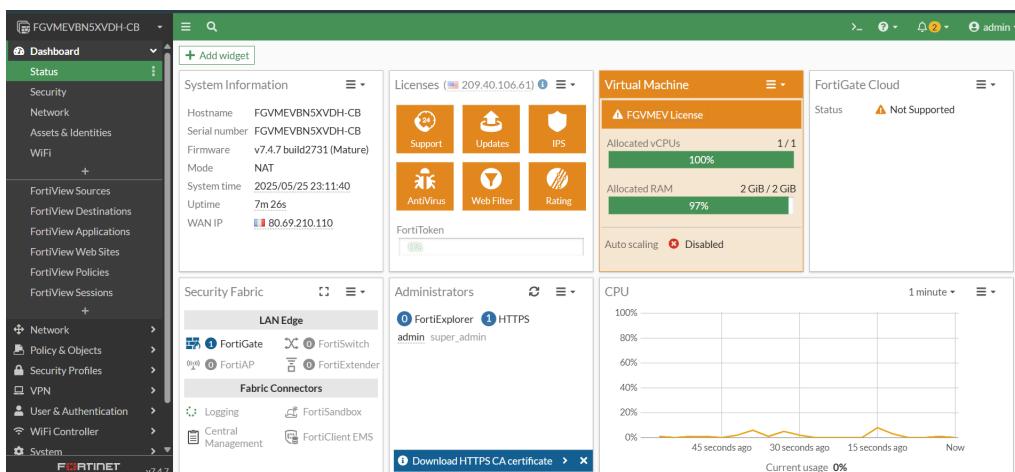


Figure 4 : Interfaces Web pare-feu fortigate.

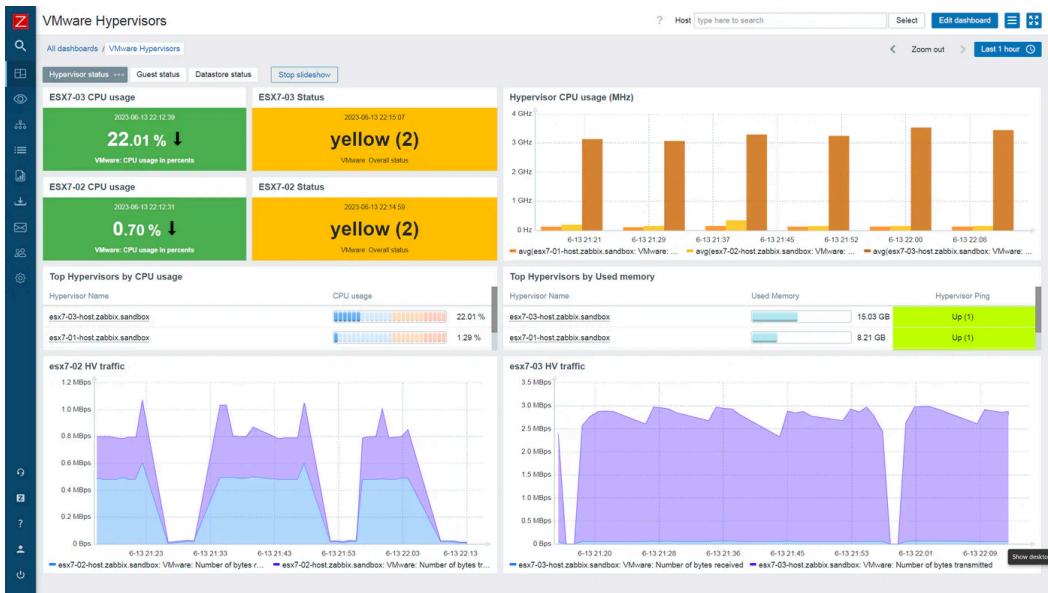


Figure 5 : Interfaces Web VMware ESXi.



Figure 6: Photo PatchSee avec émission d'onde lumineuse.



Figure 7 : Étiqueteuse BRADY utilisée pour nommer les câbles dans les baies.

Annexe 3

- Mise en place de VLANs, Spanning Tree et autres protocoles en simulation et en physique :

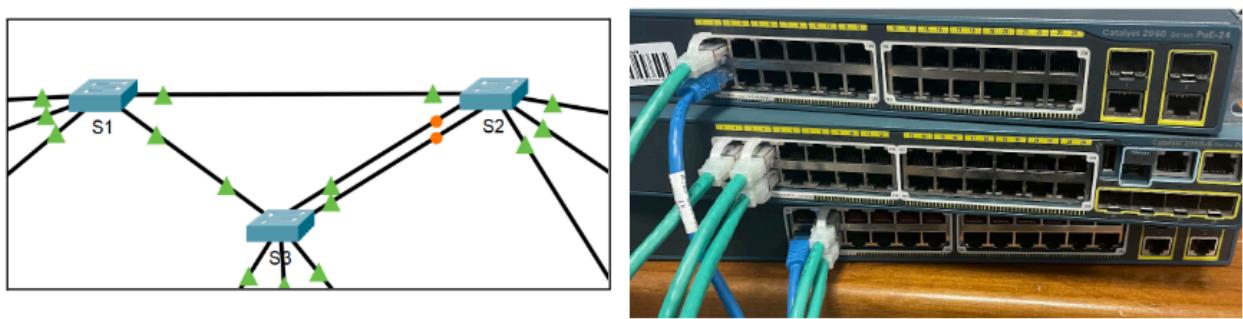


Figure 1 : Maquette en place de Port channel, Spanning Tree et autres protocoles.

Annexe 4

- Installation de pare-feu Fortigate

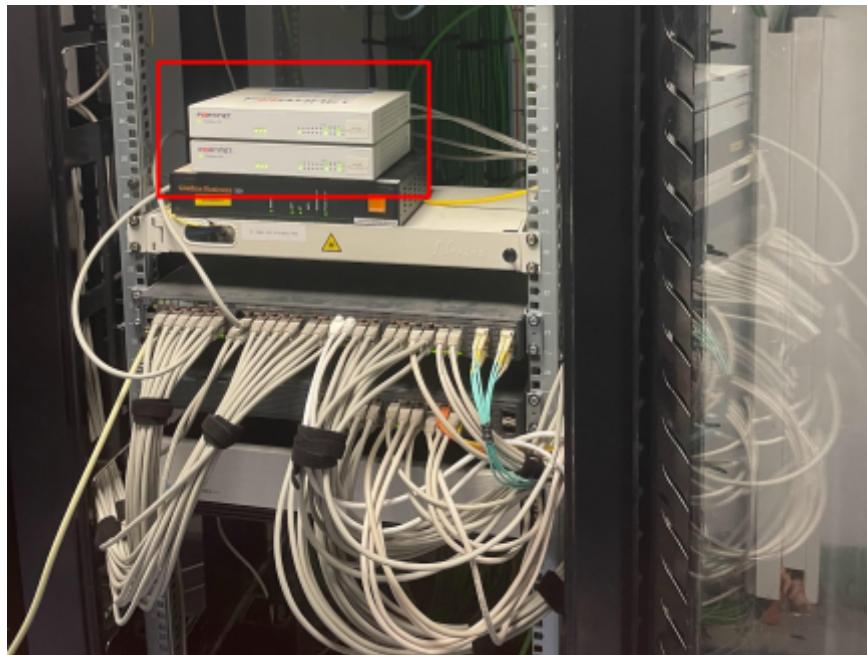


Figure 1 : Photo de deux pare-feu fortinet en redondance dans un baie à l'ehpad de père favron du port.

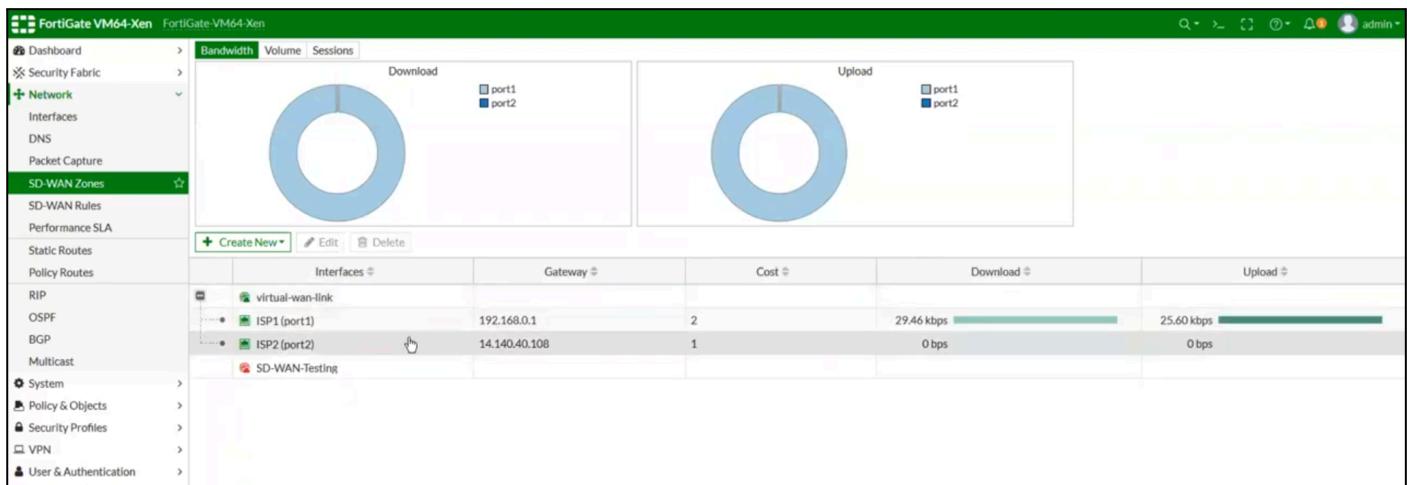


Figure 2 : Dashboard des interfaces SD-WAN configuré sur le pare-feu fortigate.

Annexe 5

- **Data center du CHU de Saint-Pierre : installation de serveur en baie**

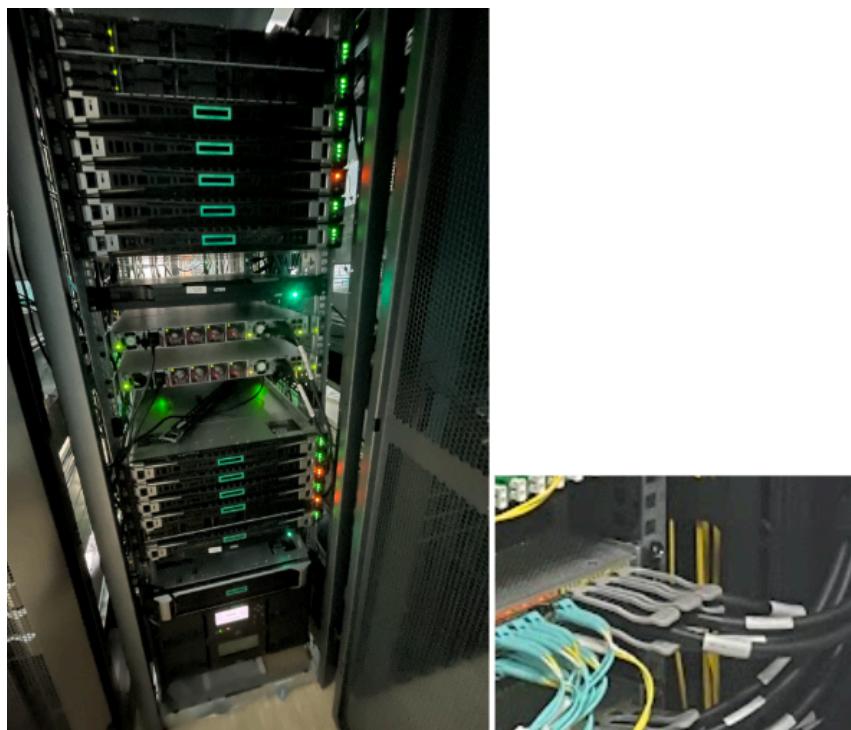


Figure 1 : Photo de serveur en baie et câble QSFP (100 G) dans le datacenter du CHU.

Annexe 6

- **Air Austral : accompagnement technique et infrastructure réseau dans les datacenters de l'aéroport**

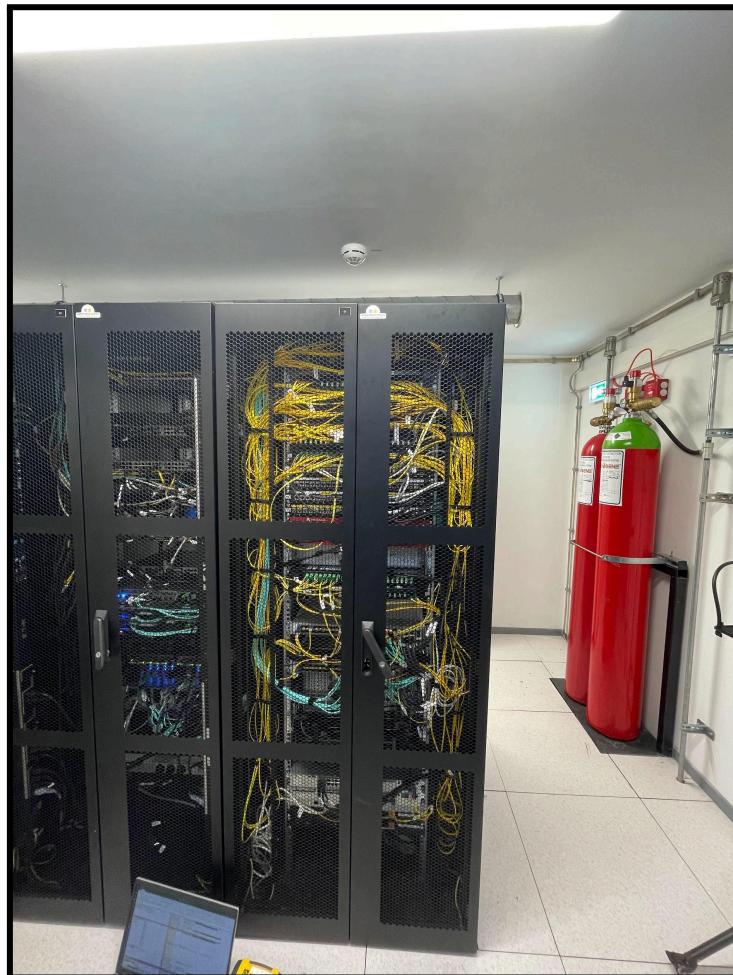


Figure 1 : Photo d'une partie du Data center de l'APAX de Air austral.

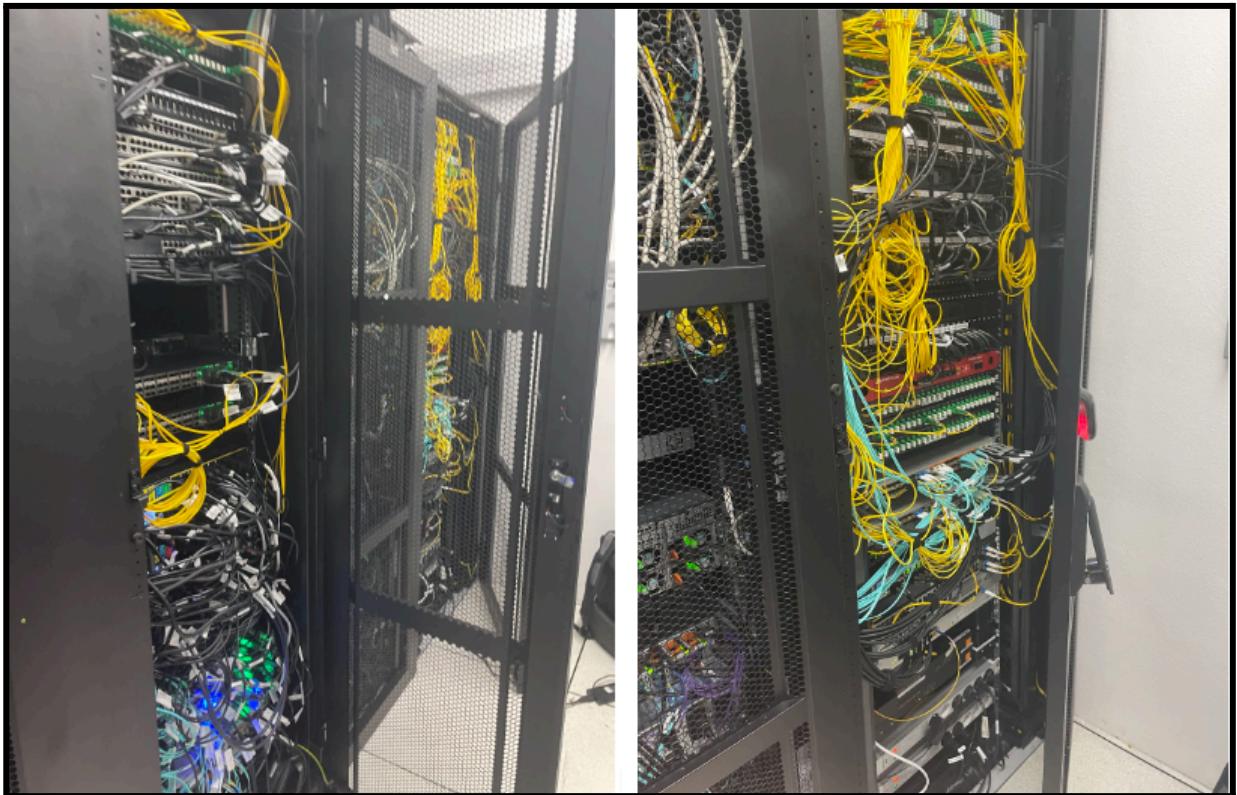


Figure 2 : Photo du Data Center du FRET de Air Austral

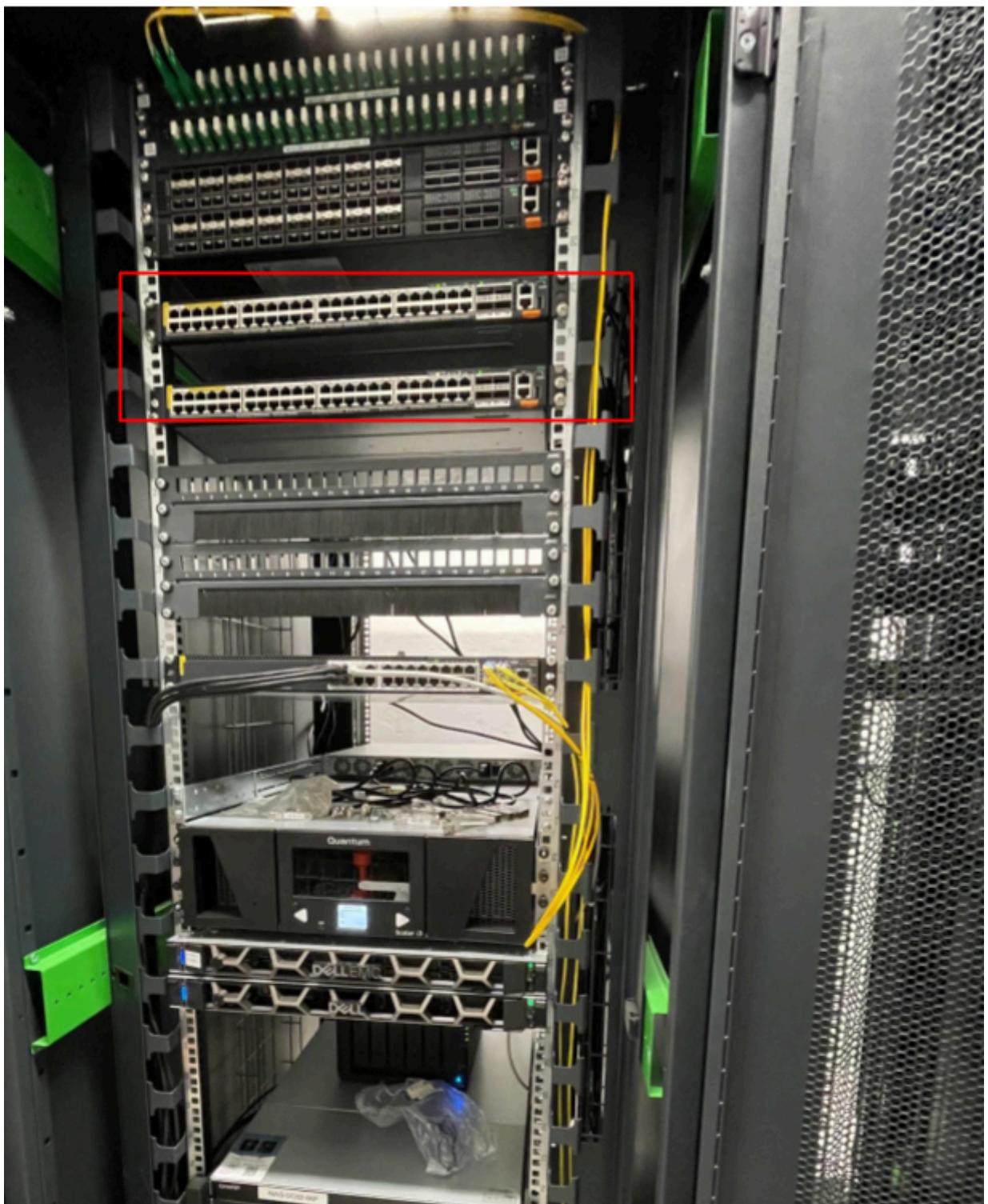


Figure 3 : Photo d'une Installation physique de deux switch aruba 6300M au data center de la salle Witness de l'aéroport Roland Garros.

Tableau des notions :

Catégorie	Notion	Définition	Outil / Application	Exemples concrets
Outils IT	JIRA (ITSM)	Outil de gestion des tickets pour suivre incidents et demandes.	JIRA	Suivi des demandes client, priorisation P1 à P4
Simulation	GNS3 / Cisco Packet Tracer	Simulateurs de réseaux pour tester des topologies virtuelles.	GNS3 / Packet Tracer	Maquettage VLAN, STP, DHCP, pare-feu Fortinet
Analyse réseau	Wireshark	Analyseur de trames réseau (sniffer) pour observer les paquets.	Wireshark	Analyse des échanges DHCP, détection de boucles
Console	Putty (console Cisco)	Terminal pour accéder aux équipements en ligne de commande.	Putty + câble console	Configuration de switch Cisco 2960
Interface web	HPE / Fortigate / ESXi	Interfaces d'administration des équipements via navigateur.	Interfaces Web	MAJ firmware, config SD-WAN, gestion VM
Virtualisation	VMware ESXi	Hyperviseur pour créer des machines virtuelles sur serveur physique.	ESXi	Déploiement sur HP ProLiant en RAID 1
Stockage	RAID 1 / RAID 5	Technologies de redondance disque : RAID 1 (miroir), RAID 5 (parité).	BIOS / iDRAC	Sécurisation données sur serveurs HP/Dell
Matériel & câblage	PatchSee / PatchLight	Câbles RJ45 avec fibre optique interne + lampe pour traçabilité.	PatchSee, lampe PatchLight	Repérage câbles à l'aéroport Air Austral

Identification	Étiqueteuse Brady BMP41	Imprimante pour marquer les câbles et ports en baie.	Brady BMP41	Étiquetage dans baies réseau
Protocoles	VLAN (802.1Q)	Segmentation logique d'un réseau pour isoler des flux.	Switch Cisco / HPE	Création VLAN Voix / Data / Management
Sécurité	Private VLAN	VLAN avec isolement entre ports tout en conservant un accès centralisé.	GNS3	Simulation dans environnement isolé
Boucles réseau	Spanning Tree (STP / RPVST+ / MSTP)	Protocole qui évite les boucles sur les réseaux redondants.	Cisco + Wireshark	Test propagation BPDU en labo
DHCP	DHCP RFC 2131	Protocole pour attribuer dynamiquement des adresses IP.	Serveurs / Wireshark	Analyse DHCP Discover, Offer, Request
Sécurité	DHCP Snooping / DAI / IP Source Guard	Mécanismes de protection contre les attaques de type spoofing.	GNS3 / Switchs	Sécurisation niveau 2 en simulation
Routage	Port Channel (EtherChannel)	Agrégation de plusieurs liens physiques en un seul lien logique.	Switch Cisco	Augmenter débit et redondance LAN
Sécurité réseau	Fortigate	Pare-feu professionnel intégrant filtrage, SD-WAN, VPN, etc.	FortiOS / FortiManager	Déploiement chez Père Favron
WAN moderne	SD-WAN	Technologie de gestion intelligente des flux inter-sites via Internet.	Fortigate / FortiManager	Migration de MPLS vers SD-WAN
Gestion distance	iDRAC	Interface Dell pour gérer un serveur à distance (BIOS, ISO, etc.).	iDRAC	Installation Debian à distance sans USB

Méthodologie	Progression par paliers	Apprentissage structuré : observation → test labo → terrain.	Méthode interne NXO	Observation → GNS3 → interventions CHU
Méthodologie	Documentation & traçabilité	Archivage rigoureux des configs, schémas, logs d'interventions.	JIRA, fichiers internes	Sauvegarde config switch, logs Fortigate

Bibliographie / Webographie

1. Gestion de services IT (ITSM)

- Atlassian. *Jira Service Management documentation*. Support Atlassian. Présente les fonctionnalités clés : gestion des incidents, demandes, changements, SLAs, file d'attente et rapports clemanet.com+10support.atlassian.com+10atlassian.com+10.
- Atlassian. *Revolutionizing ITSM: A Guide to Jira Service Management*. Oxalis. Analyse des fondamentaux et avantages de Jira dans les pratiques ITSM oxalis.io.
- Atlassian. *Getting started with Jira Service Management – ITSM template*. Support Atlassian, juin 2025. Détail du template ITSM et des workflows standard d'ITIL atlassian.com.

2. Simulation et émulation réseau (GNS3)

- GNS3 Documentation. *Getting Started with GNS3*. Guide officiel expliquant l'installation, l'utilisation et la communauté dédiée (800 000+ membres) docs.gns3.com+7docs.gns3.com+7docs.gns3.com+7.
- GNS3. *VPCS – Virtual PC Simulator*. Documentation sur l'émulateur léger de PC utilisé pour simuler DHCP, ping, etc. docs.gns3.com.

3. Protocole Spanning Tree (STP)

- Cisco. *Protocole STP*. Présentation du fonctionnement général : structure sans boucle, BPDU, modes (BPDU, RSTP, MSTP)
ipcisco.com+2cisco.com+2fr.wikipedia.org+2.
 - Wikipédia. *Spanning Tree Protocol*. Décrit l'algorithme IEEE 802.1D, états de port (listening, blocking, forwarding, learning), BPDU
networklessons.com+15fr.wikipedia.org+15cisco.com+15.
 - Cisco. *Introduction to Spanning Tree*. Article sur NetworkLessons détaillant les rôles root, port coût, etc. cisco.com+3networklessons.com+3it-connect.fr+3.
-

4. SD-WAN sécurisé (FortiGate / Fortinet)

- Fortinet. *What Is Fortinet Secure SD-WAN?*. Site officiel Fortinet : intégration SD-WAN + NGFW, SASE, orchestration centralisée
docs.fortinet.com+7fortinet.com+7youtube.com+7.
- Fortinet. *SD-WAN overview*. Guide d'administration FortiOS 7.6.1 – architecte solution, monitorage, consolidation de liens
docs.fortinet.com+2docs.fortinet.com+2docs.fortinet.com+2.
- Wikipédia. *SD-WAN*. Définition en français, classification des flux, utilisation de liens hétérogènes, économies par rapport au MPLS fr.wikipedia.org.