Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Exploration d'une infrastructure réseau à grande échelle – Stage au sein de la Région Sud

Jason VACHIER

REGION PROVENCE-ALPES-COTE D'AZUR

Responsable entreprise : Harun Sener

Responsable académique : Cong Tin Nguyen

Table des matières

1 - Introduction

Au cours de mon stage j'ai intégré la Direction des Systèmes d'Information de la Région Sud Provence-Alpes-Côte d'Azur, au sein du pôle réseau et sécurité (DSI-SART). Ce service assure l'exploitation, la maintenance et l'évolution de l'infrastructure réseau régionale, répartie sur plusieurs sites et datacenters.

Durant ces dix semaines, j'ai été amené à participer à un large éventail de missions : gestion de tickets, maintenance de switches et de bornes Wi-Fi, supervision d'équipements, analyse de dysfonctionnements, ainsi que mise à jour de firmware via les outils Cisco Catalyst Center et Panorama. J'ai également contribué à la gestion des règles sur les firewalls, notamment Palo Alto et Fortinet, dans le cadre de la sécurisation des accès.

En parallèle de ces missions quotidiennes, j'ai participé à un projet ponctuel de migration de configuration entre équipements Cisco et Allied Telesis. Ce projet, bien que concentré sur une courte période, m'a permis de gagner en autonomie.

Ce rapport s'articule en trois grandes parties : une présentation du contexte et des outils utilisés, une synthèse des missions réalisées tout au long du stage, puis un focus détaillé sur la migration de Cisco à Allied Telesis. Je terminerai par un bilan personnel et professionnel de cette expérience.

2 - Contexte

2.1 Le Conseil Régional Sud Provence-Alpes-Côte d'Azur

La Région Sud Provence-Alpes-Côte d'Azur est une collectivité territoriale qui joue un rôle majeur dans le développement économique, social et culturel de ses six départements : les Alpes-de-Haute-Provence, les Hautes-Alpes, les Alpes-Maritimes, les Bouches-du-Rhône, le Var et le Vaucluse. Elle est administrée par un Conseil régional composé de 123 conseillers régionaux élus au suffrage universel, présidé par Renaud Muselier depuis 2017.

Le siège de la Région est situé à l'Hôtel de Région, au 27 place Jules-Guesde à Marseille. En plus de ce siège, la Région dispose de plusieurs sites répartis sur l'ensemble du territoire régional, ainsi que d'un Bureau de représentation à Bruxelles, qui sert d'interface avec les institutions européennes.

Figure 1 : Hôtel de Région, 27 place Jules-Guesde à Marseille

La Région emploie environ 5 745 agents, répartis sur l'ensemble du territoire régional. Ces agents sont responsables de la mise en œuvre des politiques régionales dans des domaines variés tels que les transports, l'éducation, la formation professionnelle, le développement économique, l'aménagement du territoire, l'environnement, la culture et le sport.

Dans ce contexte, la Direction des Systèmes d'Information (DSI) joue un rôle important en assurant la continuité et la performance des services numériques de la collectivité. Mon stage s'est déroulé au sein du service réseau et sécurité (DSI-SART), une équipe restreinte de 4 à 5 personnes basée exclusivement à l'Hôtel de Région à Marseille. Cette équipe est responsable de la gestion et de la

maintenance de l'ensemble de l'infrastructure réseau de la Région, couvrant tous les sites. En cas d'incident majeur, l'équipe doit se déplacer physiquement sur les sites concernés, ce qui souligne l'importance d'une infrastructure réseau fiable et stable.

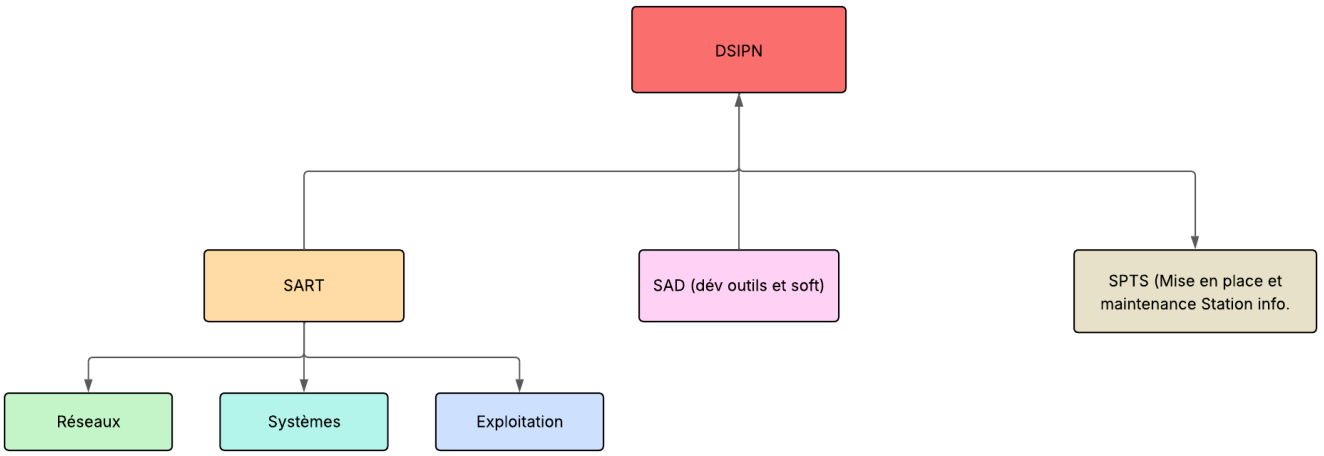


Figure 2 : Organigramme simplifié de la DSI et de ses sous-catégories

Le Président Renaud Muselier accorde une importance particulière à la stabilité du réseau, essentielle au bon fonctionnement des services régionaux. Ainsi, l'équipe réseau doit garantir une connectivité optimale pour l'ensemble des agents et des élus, assurant la continuité des services publics dans toute la région.

Note importante

Dans un souci de respect des règles de confidentialité en vigueur au sein de la Région Sud et de ne divulguer aucune information sensible, les figures et captures d'écran présentes dans les pages suivantes sont fournies à titre d'illustration uniquement. Elles représentent des interfaces similaires à celles utilisées durant le stage, mais ne reflètent pas les configurations réelles des équipements ou des services de production.

Les logiciels, outils et consoles présentés sont bien ceux exploités lors du stage, mais les captures ont été réalisées dans des environnements de démonstration ou reconstitués à des fins pédagogiques.

2.2 Organisation de la DSI-SART et environnement technique

2.2.1 L'organisation du service réseau (DSI-SART)

L'équipe réseau dans laquelle j'ai effectué mon stage fait partie intégrante de la Direction des Systèmes d'Information (DSI), au sein du SART (Service Architecture Réseaux et Télécommunications). Elle est composée d'un nombre restreint de personnes, mais couvre l'ensemble des besoins réseau pour tous les sites de la Région Sud.

- Harun Sener, mon maître de stage, est le chef d'équipe du service réseau. Il assure la coordination technique des projets, tout en intervenant directement sur le terrain.

- Emmanuelle Rome, technicienne réseau, intervient régulièrement sur les mêmes missions réseau que Harun. Elle fait également partie du groupe cybersécurité, qui est chargé d'actions de prévention et de sensibilisation à la sécurité auprès des agents.

- Lucile Gondor est une technicienne polyvalente intervenant sur des missions liées à la téléphonie et aux réseaux. Elle prend en charge des tâches de maintenance ou de support sur l'infrastructure réseau.

- Un apprenti en alternance complète l'équipe, réalisant la plupart des missions techniques du quotidien, notamment les configurations, le support, et les dépannages.

- Enfin, Jérôme Murtas, chef de service adjoint, est principalement orienté vers la gestion administrative (contrats, fournisseurs, etc.), mais dispose d'un fort bagage technique. Il n'hésite pas à intervenir sur les sujets complexes lorsqu'il le juge utile.

L'équipe réseau travaille en étroite collaboration avec de nombreux prestataires extérieurs, notamment les opérateurs télécoms, les entreprises fournissant des équipements ou des solutions techniques (comme SPIE, par exemple). Bien que des équipes intermédiaires puissent intervenir en cas de dysfonctionnements mineurs, l'équipe réseau du SART reste le point de référence pour les incidents majeurs ou les projets structurants.

La coordination avec les équipes systèmes est également quotidienne. De nombreuses actions sont partagées ou dépendent l'une de l'autre : par exemple, l'ouverture de flux réseau pour les applications systèmes, ou la création de machines virtuelles nécessaires à l'administration des équipements réseau.

Enfin, bien que la cybersécurité soit gérée par un groupe à part entière, elle reste étroitement liée aux activités réseau, notamment pour la supervision, les règles de filtrage, et la protection des accès. Le volet cybersécurité s'oriente également vers des actions de prévention utilisateur, comme des campagnes de test de phishing à destination des agents.

2.2.2 Missions globales de l'équipe réseau

Le champ d'action de l'équipe réseau du SART est extrêmement large, car elle est responsable de l'ensemble de l'infrastructure réseau de la Région Sud, répartie sur plusieurs dizaines de sites administratifs et techniques. Ses missions couvrent à la fois l'exploitation quotidienne, la maintenance des équipements, la sécurité réseau, mais aussi la gestion de projets et la relation avec les partenaires externes.

L'équipe assure en particulier:

- La maintenance de l'architecture réseau régionale, avec une connaissance de la topologie et des chemins de communication entre les sites, indispensable en cas d'incident majeur.

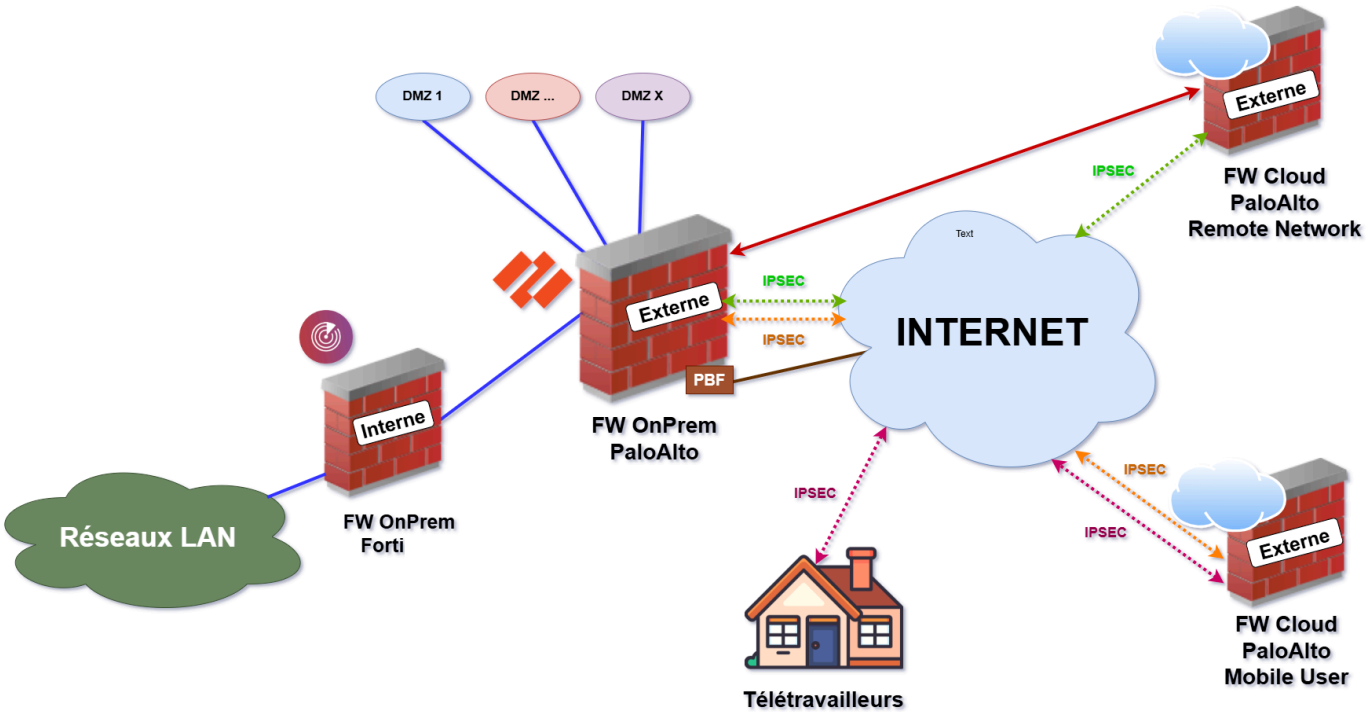


Figure 3 : Schéma simplifié de l'infrastructure réseau de la Région Sud

- La gestion des équipements réseau, incluant les switchs, bornes Wi-Fi, routeurs, firewalls, et autres boîtiers opérateurs présents dans les armoires réseau ou les datacenters.
- La maintenance des datacenters, que ce soit pour la connectivité, la redondance ou la supervision technique.
- La gestion des flux réseau sur les firewalls, une mission récurrente et cruciale, qui consiste à ouvrir ou modifier des règles, en lien avec les besoins métiers ou techniques.
- Le suivi du parc réseau, avec la mise à jour régulière des firmwares, la vérification des équipements actifs, et la supervision en temps réel des incidents ou déconnexions.

- La validation technique des solutions proposées par les partenaires externes (ex : prestataires réseau, éditeurs, intégrateurs), pour s'assurer de leur cohérence avec l'architecture existante.

- La gestion de projets techniques, tels que des migrations de matériels ou de marques (comme le passage de Cisco vers Allied Telesis), ou le déploiement de nouvelles infrastructures (ex. Wi-Fi événementiel).

- L'intervention sur site en cas de panne ou de problème non résolu à distance, que ce soit à Marseille, à Nice, à Gap ou ailleurs.

- La liaison directe avec les opérateurs Internet, notamment pour le suivi des incidents, les retours de matériel, ou la mise en place de nouvelles liaisons fibre.

Au-delà de ces missions techniques, l'équipe assure également un rôle de coordination transverse avec les autres pôles de la DSI, notamment les systèmes et la cybersécurité, afin de garantir une cohérence globale de l'infrastructure numérique.

2.2.3 Les outils et environnement technique

L'infrastructure réseau de la Région Sud est particulièrement vaste et complexe, couvrant plusieurs sites distants, datacenters et environnements métiers très variés. Cela implique une diversité importante d'équipements, d'outils de supervision et de protocoles.

2.2.3.1 Typologie des équipements

L'environnement technique repose principalement sur du matériel réseau de la marque Cisco :

- Environ 200 switchs Cisco, majoritairement de la série 9000, et quelques 3000 encore en service.

- Environ 300 bornes Wi-Fi Cisco, réparties sur l'ensemble des bâtiments administratifs et sites techniques de la Région.

Figure 4 : Catalyst 9166 Series access point

- Deux marques de firewalls :
    - Un firewall interne Fortinet pour la sécurisation du LAN.
    - Plusieurs firewalls externes Palo Alto, connectés en cloud et en physique, avec une gestion des flux inter-sites et des connexions IPsec (télétravailleurs, DMZ, etc.).

| La description détaillée du fonctionnement des firewalls sera présentée dans une section ultérieure afin d'y consacrer une analyse plus approfondie.

- Routeurs et boîtiers opérateurs : équipements RAD, Juniper, Ciena, fournis ou installés dans le cadre de l'interconnexion entre les sites.
- Connexion opérateurs : la Région travaille actuellement avec CELESTE comme opérateur principal. Les équipements précédents étaient fournis par Jaguar Network (Free Pro).

2.2.3.2 Outils de gestion et de supervision

- Cisco Catalyst Center/DNA Center sont utilisés pour la supervision, le déploiement et la maintenance centralisée des équipements réseau Cisco.
- Les firewalls Palo Alto sont administrés via l'interface Panorama, tandis que les firewalls Fortinet ce supervise via leur interface web.
- L'outil SolarWinds Orion est utilisé comme plateforme de supervision transversale pour de nombreux équipements, en complément des outils constructeurs.
- Le VPN GlobalProtect de Palo Alto est utilisé pour la mise en place d'un accès distant sécurisé pour les télétravailleurs ou intervenants externes.

2.2.3.3 Protocoles et fonctionnalités réseau

L'architecture réseau repose sur de nombreux protocoles standard et propriétaires, adaptés à une structure multisite complexe. En voici une liste non exhaustive :

- Virtualisation réseau : usage de VRF sur les routeurs, et VLAN étendus sur les switchs d'accès.
- QoS (Quality of Service) poussée, pour garantir la priorité aux flux sensibles (voix, visioconférence, Teams, etc.).
- RSTP pour la résilience des topologies de couche 2.
- ACLs, DHCP snooping, ARP inspection, port-security, NAC, etc. pour renforcer la sécurité sur les ports d'accès.
- Protocoles de routage : notamment OSPF, largement utilisé pour les échanges dynamiques entre équipements.
- Protocoles propriétaires Cisco : comme VTP pour la distribution centralisée des VLANs.
- Technologies de transport MPLS/VPLS, principalement gérées au niveau du cœur de réseau.

3 - Mes missions réalisées

3.1 Contexte technique préalable aux interventions

Avant de détailler les missions que j'ai réalisées au cours de mon stage, il est nécessaire de présenter brièvement le fonctionnement de l'architecture réseau de la Région Sud, en particulier le rôle des firewalls et des interconnexions entre les différents environnements.

L'infrastructure repose sur un pare-feu interne Fortinet, qui assure la sécurité du réseau local (LAN), et un ensemble de pares-feux externes Palo Alto, à la fois On-Prem (physique, localisé dans les datacenters de la Région) et Cloud (dans les services Palo Alto Remote Network et Mobile User). Ces équipements assurent la protection des DMZ, la segmentation des flux, le traitement des connexions VPN et la redirection des flux utilisateurs, en particulier dans le cadre du télétravail.

Cette compréhension est essentielle pour suivre les différentes missions réalisées, notamment celles impliquant la gestion des flux réseau, les tunnels VPN, la supervision, ou encore les dépannages liés aux accès distants.

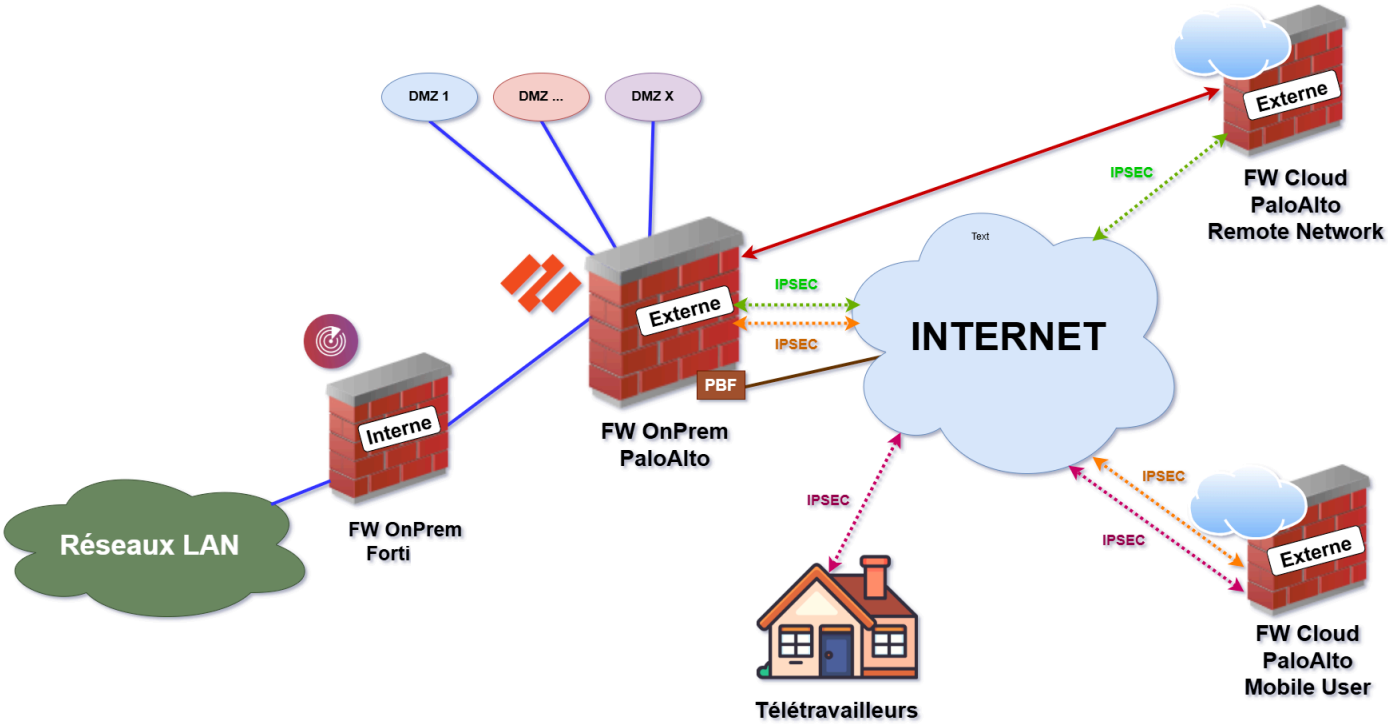


Figure 3 : Schéma simplifié de l'infrastructure réseau de la Région Sud

Le schéma illustre l'infrastructure complète : le réseau LAN est sécurisé par un firewall Fortinet interne. Un firewall Palo Alto OnPrem centralise les accès vers Internet et les flux entrants. Il est interconnecté à deux firewalls Cloud : *Mobile User* pour les télétravailleurs, et *Remote Network* pour l'accès Internet des agents en présentiel. Les DMZ sont également positionnées derrière ce firewall externe.

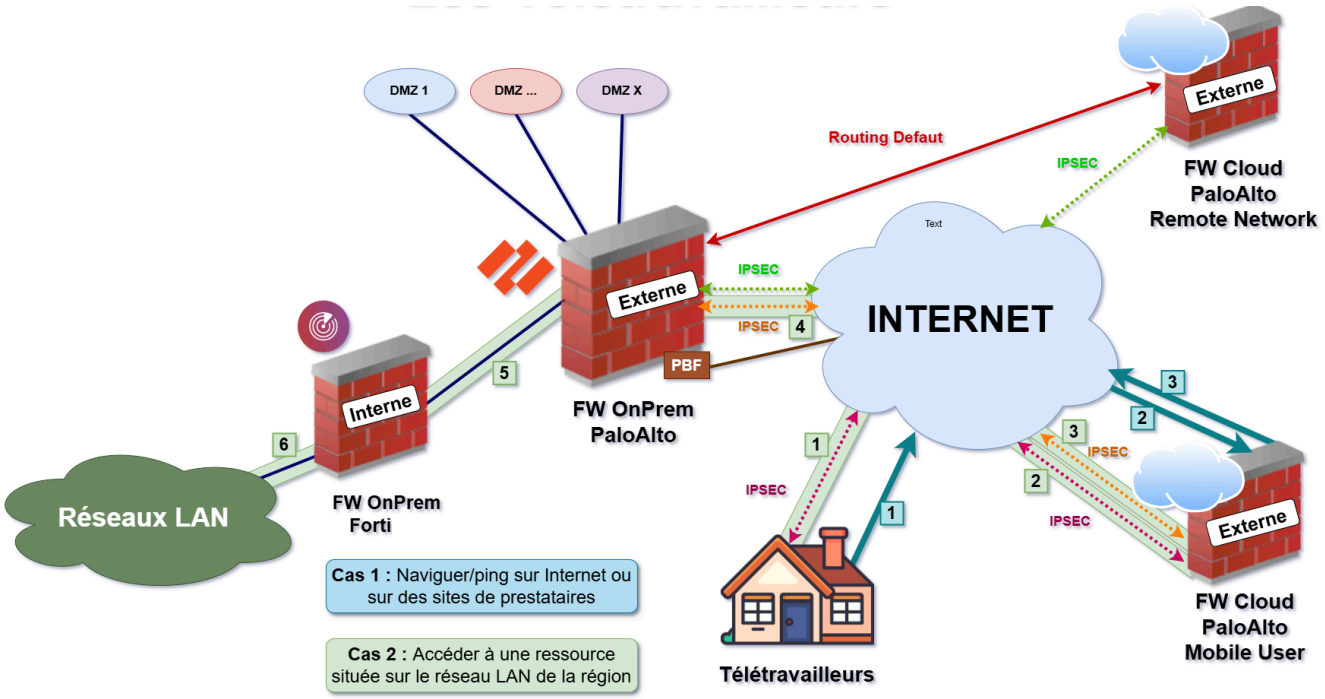


Figure 5 : Cas d'usage – télétravailleurs

Lorsqu'un agent travaille depuis chez lui, il doit se connecter au VPN pour accéder aux ressources internes ou simplement naviguer sur Internet. Sa connexion passe d'abord par le firewall Cloud Palo Alto Mobile User, qui redirige ensuite la requête : soit vers Internet directement, soit vers le firewall OnPrem, pour accéder au réseau LAN.

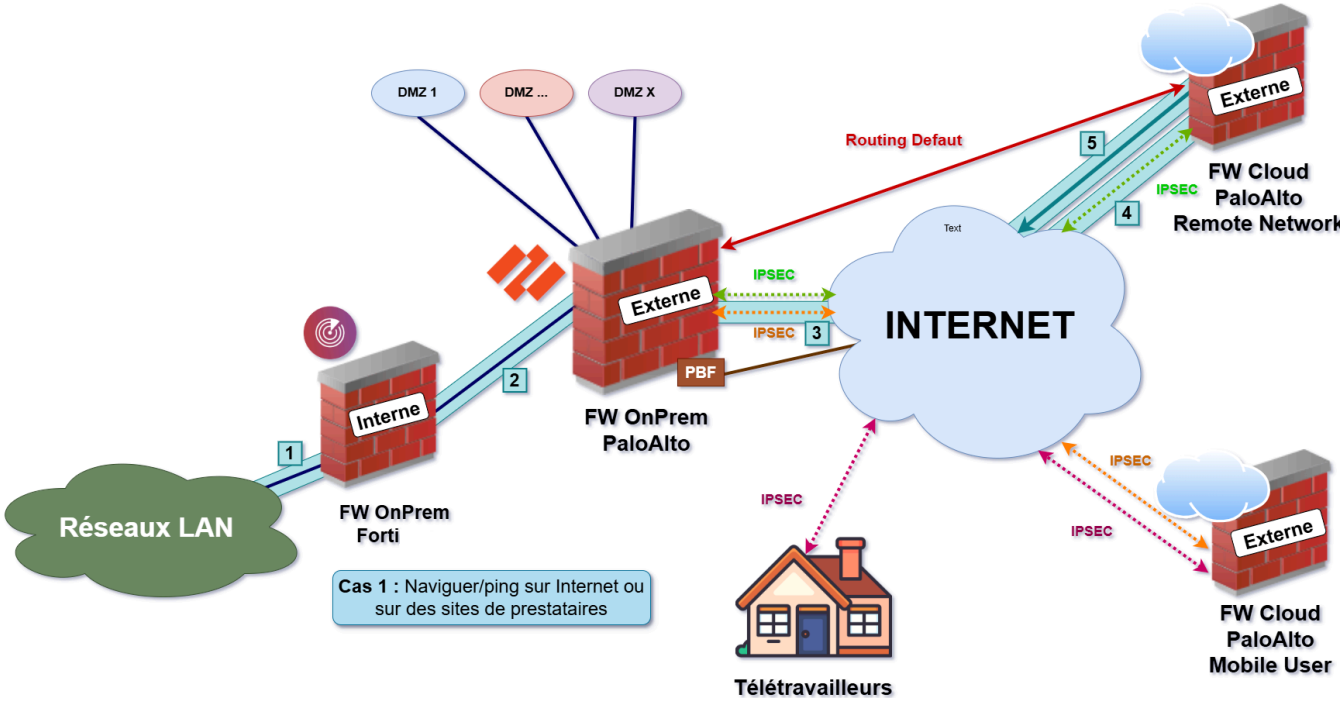


Figure 5 : Cas d'usage – agent sur site

Pour un agent sur site, la requête vers Internet passe d'abord par le firewall externe OnPrem. Mais elle n'est pas envoyée directement sur Internet : un tunnel IPsec est établi vers le firewall Cloud Remote Network, qui prend ensuite le relais pour autoriser la navigation web.

| À noter qu'une PBF (Policy-Based Forwarding) est mis en place sur le firewall Palo Alto OnPrem dans certains cas spécifiques (notamment pour des intervenants externes) afin de bypasser les firewalls Cloud et permettre un accès direct, sans redirection.

3.2 Les Missions

3.2.1 Gestion des tickets et interventions quotidiennes

Une grande partie de mon stage a été consacrée au traitement des demandes utilisateurs et à la gestion quotidienne du réseau. Les tickets proviennent majoritairement par mail, car la plateforme de ticketing interne est peu utilisée. Chaque ticket est une sorte d'enquête : on identifie le problème puis on agit avec les bons outils.

Parmi les interventions les plus fréquentes :

- Création ou modification de règles sur les firewalls, notamment pour ouvrir des flux réseau vers des applications ou services spécifiques.

				Source				
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE
2	testrule	none	universal	gp-clients	net_10.0.1.0	ricardo	any	
3	test2	none	universal	any	any	any	any	any
4	ping	none	universal	any	any	any	any	any
5	allow-ubuntu-s2s-internet	none	universal	inside	ubuntu1	any	any	S2
6	AllowDns	none	universal	global-protect inside	Diskstation net_10.0.1.0	any	any	

Figure 6 : Interface WEB Palo Alto pour modifier des règles de filtrage

- Analyse de connectivité utilisateur, comme des problèmes de VLAN mal affectés ou d'adresses IP non attribuées.

- Diagnostic de ports réseau, souvent avec des commandes classiques comme shut / no shut pour relancer un port bloqué ou instable.

```
swe20-allied#  swe20-allied#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
swe20-allied(config)#int port1.0.4
swe20-allied(config-if)#shut
swe20-allied(config-if)#no shut
```

```
swe20-allied#sh int status
Port       Name               Status      Vlan       Duplex Speed   Type
--------------------------------------------------------------------------------
port1.0.1  prise 162 bur      notconnect           5 auto   auto    1000BASE-T
             reseau
port1.0.2  Jason              connected           50 a-full a-1000  1000BASE-T
port1.0.3  -                  notconnect           5 auto   auto    1000BASE-T
port1.0.4  -                  disabled             5 auto   auto    1000BASE-T
```

Figure 7 : Interface Putty pour sortir un switch d'un disable ou err-disable

- Identification d'erreurs de configuration sur les switchs, parfois liées à des équipements mal câblés ou défaillants.

Chaque matin, nous commencions par consulter le rapport d'exploitation, qui liste les alertes de sécurité ou les incidents en cours sur le site CERT-FR (ANSSI). Ces rapports nous permettent de détecter rapidement les équipements concernés par des failles, comme ce fut le cas pour les firewalls Palo Alto vulnérables à un bug VPN SSL. Dans ce cas précis, nous avons lu la note technique, vérifié les versions, et appliqué les correctifs nécessaires.

Objet: [MàJ] Vulnérabilité dans Palo Alto Networks GlobalProtect

GESTION DU DOCUMENT

Référence	CERTFR-2024-ALE-006
Titre	[MàJ] Vulnérabilité dans Palo Alto Networks GlobalProtect
Date de la première version	12 avril 2024
Date de la dernière version	01 juillet 2024
Source(s)	Bulletin de sécurité Palo Alto Networks PAN-252214 du 12 avril 2024

Une gestion de version détaillée se trouve à la fin de ce document.

RISQUE

- Exécution de code arbitraire à distance

SYSTÈMES AFFECTÉS

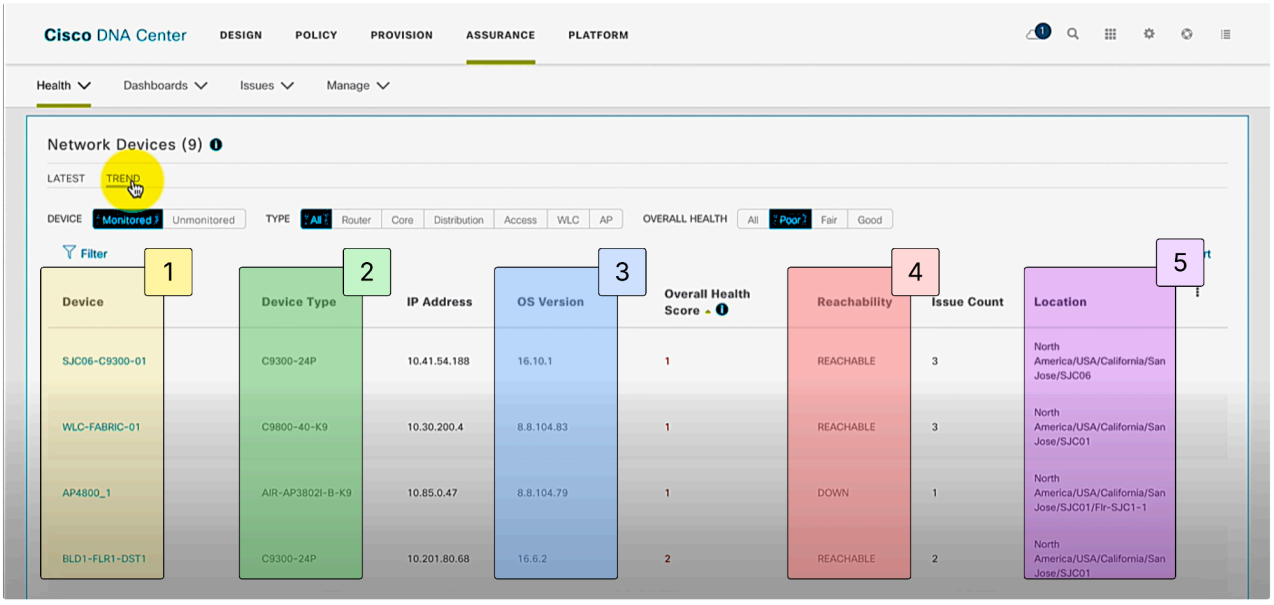
- PAN-OS 10.2.x antérieures à 10.2.0-h3, 10.2.1-h2, 10.2.2-h5, 10.2.3-h13, 10.2.4-h16, 10.2.5-h6, 10.2.6-h3, 10.2.7-h8, 10.2.8-h3
- PAN-OS 11.0.x versions antérieures à 11.0.0-h3, 11.0.1-h4, 11.0.2-h4, 11.0.3-h10 et 11.0.4-h1
- PAN-OS 11.1.x versions antérieures à 11.1.0-h3, 11.1.1-h1 et 11.1.2-h3

Figure 8 : Article sur une Faille Palo Alto - CERT-FR

Enfin, j'ai également eu l'occasion de participer à une intervention en amont d'un événement régional impliquant le président Renaud Muselier. Lors de cette plénière, nous avons vérifié le bon fonctionnement du Wi-Fi pour que tous les élus puissent accéder au réseau sans souci. C'était une mission simple mais importante, avec de la pression en raison du contexte institutionnel.

3.2.2 Supervision et maintenance réseau

L'état de santé des équipements réseau est surveillé en continu à l'aide d'outils de supervision comme Cisco DNA Center et SolarWinds Orion. Lorsqu'une anomalie est détectée, une alerte est automatiquement envoyée par mail, avec le nom de l'équipement concerné, sa localisation géographique.



1 La catégorie ***Device*** correspond au **nom attribué à l'équipement** (hostname). Ce nom permet d'identifier rapidement l'appareil via les filtres. Dans le cadre de la Région, les noms sont choisis de façon à indiquer le **site, le bâtiment**, voire **l'étage** où se trouve l'équipement, ce qui facilite fortement la gestion.

2 **Device Type** indique le **modèle exact de l'équipement** (ex : switch, contrôleur Wi-Fi, etc.). C'est très utile pour filtrer les équipements par catégorie, **notamment lorsqu'on prépare une campagne de mise à jour** : on peut alors se concentrer sur un seul modèle à la fois, ce qui simplifie le déploiement.

3 Cette colonne affiche la **version du système d'exploitation (IOS)** actuellement installée sur l'équipement. Si une version plus récente est disponible (et marquée comme *Golden Image* dans DNA Center), elle est indiquée ici comme **prête à être déployée**.

4 ***Reachability*** indique si l'équipement est actuellement **joignable** ou non. En cas de perte de communication, on peut voir depuis combien de temps le lien est coupé. *Issue Count* donne le nombre de problèmes ou d'alertes associés à cet équipement.

5 ***Location*** correspond à la **zone géographique** (site/bâtiment) où est situé l'équipement. Ces informations sont généralement **renseignées manuellement** lors de l'intégration de l'équipement. Cela permet de localiser rapidement un appareil défaillant sans se perdre dans l'interface.

Figure 9 : Exemple d'écran utilisé pour le suivi d'état et de mises à jour des équipements réseau dans DNA Center (ancienne version de DNA Center)

Un jour nous avons reçu une alerte indiquant qu'un switch situé dans la zone de l'hémicycle n'était plus joignable. Après vérification dans le DNA Center, nous avons constaté que la perte de communication datait de plusieurs heures. Nous nous sommes donc rendus sur place pour inspecter physiquement l'équipement. Ce type de panne est parfois lié à un simple souci d'alimentation (disjoncteur déclenché, câble débranché ou endommagé). Après plusieurs tests (débranchement/rebranchement, changement de baie), le switch restait inactif.

Nous avons ensuite testé l'alimentation en la remplaçant (une cause relativement fréquente de panne) mais cela n'a rien changé. La conclusion était claire : panne matérielle complète. Nous avons donc procédé au remplacement du switch.

Pour ne pas devoir retaper manuellement une configuration de plus de 1000 lignes, nous avons utilisé les CLI Templates disponibles dans DNA Center. Ces modèles permettent de déployer rapidement une configuration préexistante, avec des variables à personnaliser selon le contexte. Une fois ajustée, la configuration est poussée automatiquement sur un fichier texte, ou on colle son contenu sur le nouvel équipement, ce qui permet un redémarrage rapide du service, évitant de bloquer tout un étage.

```
44 ip radius source-interface Vlan${vlan_MGMT}
45 snmp-server trap-source Vlan${vlan_MGMT}
46 snmp-server source-interface informs Vlan${vlan_MGMT}
47 ntp source Vlan${vlan_MGMT}
48 !
```

Figure 10 : Configs avec les variables pour le CLI Templates du DNAC

La supervision inclut également la veille technologique sur les mises à jour des équipements. Le service d'exploitation nous transmet régulièrement des alertes lorsqu'une mise à jour critique est publiée et recommandée par le CERT-FR. Dans ce cas, et après validation, nous téléchargeons l'image via DNA Center, la marquons comme golden Image, puis nous planifions la mise à jour durant une fenêtre de maintenance nocturne (souvent entre minuit et 5h30), afin d'éviter toute coupure de service en journée.

3.2.3 Gestion des équipements Wi-Fi

Comme pour tous les autres équipements réseau, on a une vue complète et en temps réel de l'état de nos 295 bornes Wi-Fi Cisco. Lorsqu'une borne tombe en panne, il est impératif d'intervenir rapidement. Ces bornes assurent la connectivité des agents, mais aussi celle des élus, des prestataires, des journalistes ou d'autres intervenants. Autrement dit, la stabilité du Wi-Fi est primordiale.

Grâce à Cisco WLC, la gestion de ces bornes est simple et très précise. On peut voir en direct leur état, leur nom, leur adresse IP, et même les configurer individuellement. Par exemple, une borne située dans le bâtiment de La Joliette n'a aucun intérêt à diffuser le Wi-Fi du bureau du président.
Chaque borne peut diffuser plusieurs réseaux Wi-Fi différents, chacun avec des niveaux d'accès

spécifiques. Le Wi-Fi Région est destiné aux agents, tandis que le Wi-Fi Invité est utilisé par les visiteurs de passage, comme les journalistes en séance plénière.
Il existe aussi des réseaux événementiels, que l'on active ponctuellement à la demande, via un simple ticket. Par exemple, on peut nous demander d'ouvrir le Wi-Fi "plénière" uniquement le jour d'une session, puis de le désactiver.

Mais dans la réalité, le matériel Wi-Fi est sans doute le plus capricieux. Pendant mon stage, j'ai été amené à changer une dizaine de bornes H.S. Quand ça arrive, il faut :

- récupérer une borne neuve,
- la préconfigurer dans WLC,
- se déplacer sur site,
- démonter l'ancienne (souvent dans les faux plafonds),
- et installer la nouvelle.

Une borne haut de gamme peut coûter jusqu'à 1000 € l'unité, ce qui montre l'importance de bien les suivre.

J'ai aussi eu l'occasion de créer un nouveau réseau Wi-Fi, à la demande du CESER. Le Wi-Fi Invité ne convenait pas à certains intervenants, comme des comptables ou des avocats présents plusieurs jours, car il fallait se reconnecter toutes les X heures. On a donc mis en place un réseau dédié, le Wi-Fi CESER, avec son propre mot de passe et ses propres règles d'accès.

Enfin, la couverture Wi-Fi doit être la plus complète possible. Dans DNA Center, on a le plan de chaque bâtiment, avec l'emplacement exact de chaque borne et son rayon de diffusion. Le but est de couvrir 100 % des zones de travail, ce qui explique pourquoi il y a parfois plusieurs dizaines de bornes par étage.

3.2.4 Relation avec les prestataires et opérateurs

3.2.4.1 Relations avec les opérateurs : Celeste et Free Pro

La Région était historiquement cliente de Free Pro (anciennement Jaguar Network), mais un changement d'opérateur a été engagé récemment pour passer chez Celeste, suite à l'expiration du contrat. Cette migration a nécessité des audits de l'infrastructure par Celeste, afin d'adapter les nouveaux équipements à notre réseau.

Je n'étais pas encore présent lors de cette migration, mais aujourd'hui, on gère toujours l'après. En effet, comme les équipements opérateurs appartiennent à l'opérateur, nous recevons régulièrement des mails de Free Pro nous demandant de rendre leur matériel, avec les numéros de série concernés. À défaut de retour, des pénalités financières peuvent s'appliquer.

Figure 11 : équipements à renvoyer à Free Pro

En cas d'incident réseau lié à l'opérateur, une hotline technique est disponible pour nous assister au plus vite.

3.2.4.2 Relation avec le prestataire SPIE – Projet Wi-Fi événementiel

Parmi les prestataires techniques, SPIE intervient sur plusieurs sujets. J'ai notamment participé à une réunion avec deux représentantes commerciales de SPIE, aux côtés de mon tuteur Harun, pour faire un point sur la collaboration en cours.

Le thème principal : la gestion du Wi-Fi événementiel. Aujourd'hui, lorsque le Conseil Régional organise un événement, un réseau Wi-Fi dédié est activé manuellement par l'équipe réseau. Il s'agit d'un Wi-Fi isolé, uniquement destiné à fournir un accès internet avec les filtrages classiques, sans accès au LAN.
Cependant, cette activation nécessite :

- une activation manuelle du wifi sur chaque bornes,
- la création d'un mot de passe unique,
- et sa diffusion auprès des invités.

Cela prend du temps à l'équipe, alors que ce sont des tâches qui pourraient être automatisées.

Nous avons donc sollicité une solution “clé en main” auprès des prestataires. L’idée : qu’un simple bouton déclenche tout :

- activation du Wi-Fi,
- génération automatique d’un mot de passe,
- Partage du mot de passe

SPIE a présenté une solution basée sur des scripts PowerShell connectés à Cisco WLC, permettant de piloter les bornes Wi-Fi à distance. Leur proposition comprenait notamment :

- la génération automatique d’un mot de passe,
- l’activation du Wi-Fi,
- la conversion du mot de passe en QR code, qui serait ensuite affiché sur une télévision via un Raspberry Pi pour simplifier la diffusion lors des événements.

À l’issue de la réunion, Harun m’a demandé de lui faire un retour sur cette solution et de voir si cela répondait au cahier des charges global qu’il m’avait transmis en amont.

4 - Migration de cisco vers Allied Telesis

4.1 Contexte et objectifs du projet

Actuellement, l'ensemble du parc de switches réseau de la Région Sud est constitué exclusivement d'équipements Cisco. Cette marque dispose de nombreux avantages, à commencer par une expertise solide acquise au fil des années. Grâce à un important retour d'expérience client, Cisco a pu faire évoluer ses produits pour offrir des solutions toujours plus robustes et complètes.

Sa notoriété mondiale a également permis le développement d'une documentation extrêmement riche et d'une communauté très active, ce qui rend le dépannage ou l'intégration de nouvelles fonctionnalités plus accessibles. En parallèle, Cisco propose des formations et certifications mondialement reconnues, qui permettent aux techniciens et ingénieurs de maîtriser leur environnement réseau de manière approfondie.

Tous ces éléments font de Cisco une solution de référence, souvent considérée comme incontournable lorsqu'on recherche de la fiabilité et de la performance. Cependant, cette position dominante sur le marché implique un certain nombre d'inconvénients, notamment le coût.
Les équipements sont globalement plus chers que la moyenne, et surtout, Cisco fonctionne avec un système de licences payantes, parfois très coûteux, en particulier pour l'accès aux outils de supervision comme DNA Center. À l'échelle de la Région, cela représente plusieurs centaines de milliers d'euros par an, uniquement pour assurer le droit d'utiliser les fonctions avancées de supervision.

Même si des remises et accords commerciaux permettent de réduire un peu ces coûts, ils restent extrêmement élevés, ce qui a logiquement conduit la Région à envisager des alternatives. C'est dans ce contexte qu'une réflexion a été menée sur le remplacement progressif de certains équipements, notamment dans des bâtiments ciblés, par des switches d'une autre marque.

Parmi les fabricants étudiés, c'est Allied Telesis, une entreprise japonaise spécialisée dans les équipements réseau, qui a été retenue pour un premier test grandeur nature. Le principal atout de cette marque réside dans son rapport qualité/prix très compétitif. Leur communication met aussi en avant une proximité syntaxique avec Cisco, avec une CLI (interface en ligne de commande) censée reprendre une logique similaire, ce qui faciliterait la migration pour les équipes habituées à l'environnement Cisco.

Pour évaluer concrètement cette possibilité, la Région a reçu deux switches Allied Telesis en test. Le projet confié à notre équipe (et en partie à moi) consistait à remplacer un switch Cisco en production par un switch Allied Telesis, en migrant l'intégralité de la configuration.

Ce test devait permettre de déterminer si cette solution était réellement compatible avec nos contraintes, et si elle pouvait être déployée plus largement à moyen terme.

La promesse d'Allied Telesis était donc simple : offrir une expérience proche de celle de Cisco, mais à un prix bien plus bas. Mais comme nous le verrons dans les parties suivantes, les différences étaient nombreuses, et cette migration, censée être fluide, s'est avérée plus complexe que prévu.

4.2 Préparation de la migration et environnement de test

Pour ce projet, nous avons pris comme base de travail la configuration d'un switch Cisco Catalyst 9300, un modèle couramment utilisé dans notre infrastructure réseau actuelle. Ce switch est représentatif de l'environnement en production, avec une configuration complète et avancée, ce qui en fait un bon point de comparaison pour évaluer la faisabilité de la migration.

En face, nous avons reçu deux switches Allied Telesis AT-x530L-28GTX, un modèle haut de gamme 24 ports, empilable (stackable), et livré avec l'ensemble des licences nécessaires pour le test. Ce modèle se positionne clairement comme une alternative sérieuse aux switches Cisco de la gamme Catalyst.

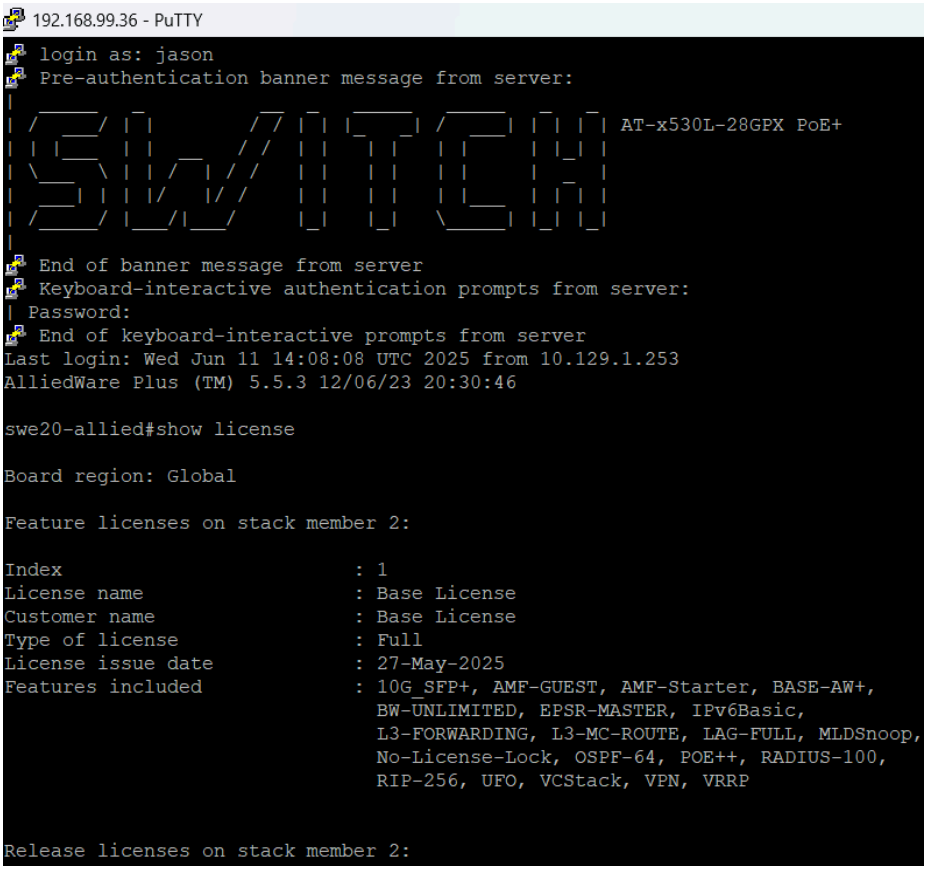


Figure 12 : Console Putty du switch AT - Affichage des licenses

Pour récupérer la configuration du switch Cisco, nous avons utilisé Cisco DNA Center, qui permet d'extraire proprement les configurations en CLI ou sous forme de "template". La procédure exacte est d'ailleurs décrite dans une section précédente.

En ce qui concerne l'équipement Allied Telesis, la configuration initiale s'est faite à l'aide d'un câble console RJ45 vers USB, via le logiciel PuTTY, comme pour n'importe quel équipement réseau CLI. Le but à cette étape était de prendre en main l'environnement CLI propre à Allied Telesis, de vérifier son comportement de base, et de commencer à identifier les similitudes et les différences avec Cisco.

C'est à partir de cette phase que la complexité du projet a commencé à apparaître.

4.3 Réalisation de la migration : erreurs, adaptations et résultats

Pour démarrer la migration, nous avons extrait la configuration du switch Cisco dans un fichier texte. Ensuite, nous avons copié cette configuration bloc par bloc dans le switch Allied Telesis, pour tester directement ce qui fonctionnait… ou non. L'idée était de valider chaque commande, et en cas d'échec, de chercher une équivalence sur le nouvel équipement.

Pendant tout ce processus, plusieurs documents ont été remplis et partagés sur Teams pour que l'ensemble de l'équipe Réseaux puisse suivre l'avancement en temps réel [voir les annexes 1,2 et 3].

On a commencé simplement, avec le nom du switch et les bannières. Rien de spécial à ce niveau, sauf une première différence : chez Cisco, on utilise *banner motd*, tandis que sur Allied Telesis, c'est *banner login*.

Ensuite, on a attaqué la création des VLANs, une étape cruciale vu la densité de notre réseau et l'importance d'un déploiement sans erreur. La logique est similaire entre Cisco et Allied Telesis, mais la syntaxe change légèrement, et surtout, chez Allied, il faut passer par une base de données des VLANs avant de les configurer.

Exemple de création de VLANs :

Sur Cisco :

- vlan 5
- interface vlan 5
  → description #LAN#VLAN UTILISATEURS
  → no ip address
  → no shutdown

Sur Allied Telesis :

- vlan database
  → vlan 5 name USERS-BAT-E
- exit
- interface vlan5
  → description VLAN utilisateurs
  → ip dhcp snooping
  → arp security

On remarque que, malgré une structure assez proche, la syntaxe est plus stricte chez Allied (pas d'espaces inutiles, blocs à imbriquer proprement, etc.).

Sur le papier, Allied Telesis annonce une compatibilité CLI avec Cisco. En réalité, c'est partiel. L'un des premiers freins a été l'absence d'auto-complétion complète avec la commande [**?**], ce qui nous forçait parfois à deviner les bonnes syntaxes. Et même en cherchant sur Internet, la documentation est souvent difficile à trouver ou mal référencée. Résultat : on perd énormément de temps à chercher les bonnes commandes.

Après plusieurs jours de test, nous avons fini par mettre la main sur une documentation officielle de plus de 5 000 pages. C'est elle qui nous a permis d'avancer concrètement. Mais clairement, le manque de communauté et d'exemples concrets est un point faible majeur de cette marque, surtout comparé à Cisco.

Autres différences notables rencontrées :

- **Comptes utilisateurs :**
  Cisco → username admin privilege 15 secret 8 xxxxx
  Allied → username admin privilege 15 password 8 xxxxx

- **Définition d'un serveur Radius :**
  Cisco :
  - aaa group server radius SRV_RAD
  - server X.X.X.X auth-port 1812 acct-port 1813
    Allied :
  - radius-server host X.X.X.X key xxxxx
  - aaa group server radius SRV_RAD
  - server X.X.X.X

Je ne vais pas détailler toutes les commandes ici, la configuration étant très longue. Ce qu'il faut retenir, c'est qu'il existe de nombreuses différences, et qu'en l'absence de documentation claire et facilement accessible, le travail peut vite devenir laborieux.

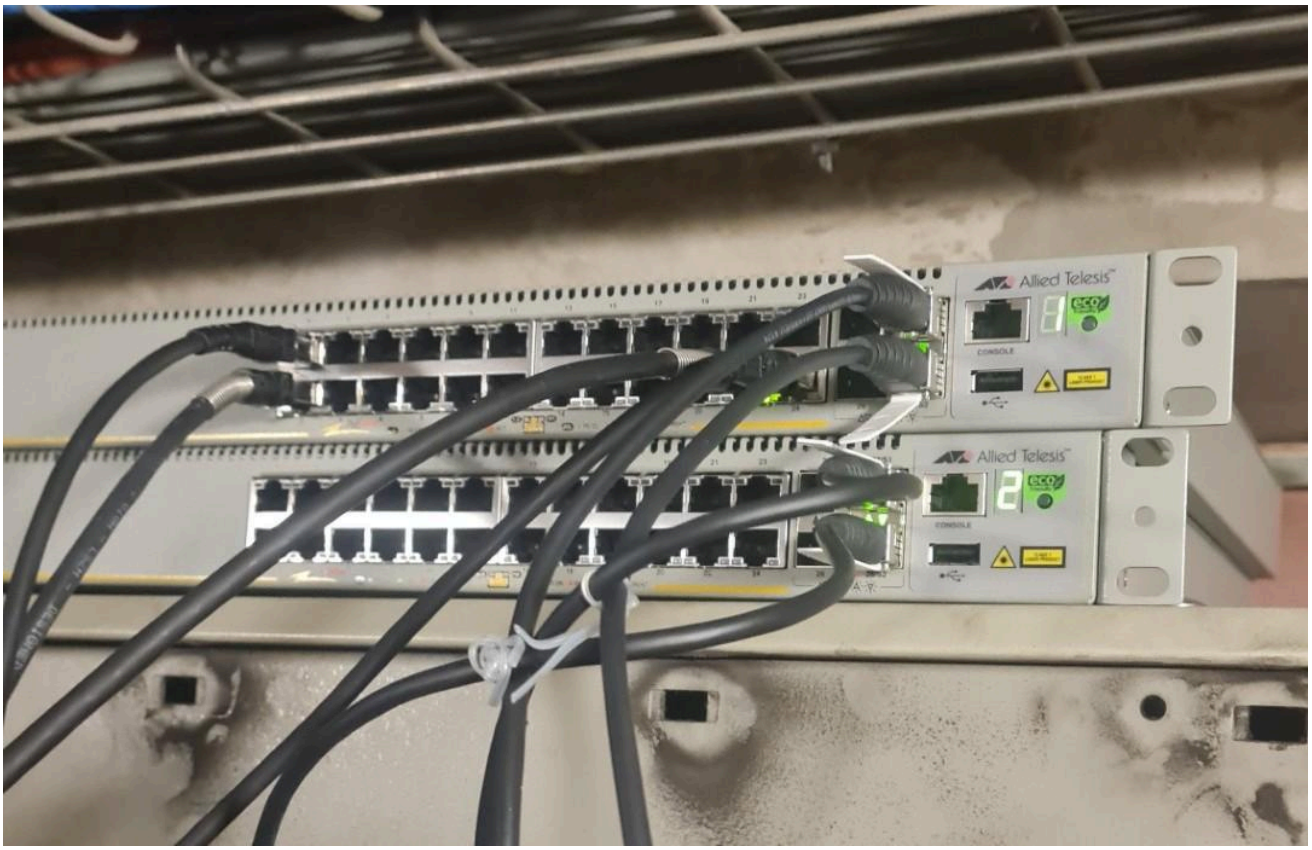


Figure 13 : 2 switchs Allied Telesis test dans la baie de brassage

4.3 Test concret et bilan

Une fois la configuration retranscrite au mieux, nous sommes passés à la phase de test, avec un objectif clair : simuler l'intégration réelle du switch Allied Telesis dans notre environnement réseau.

Le switch a donc été placé dans une baie technique, avec plusieurs ports brassés pour reproduire une situation proche d'un déploiement classique en bâtiment. Et c'est précisément à ce moment-là que nous avons été confrontés au plus gros point de blocage : la gestion de la sécurité des ports, et plus particulièrement le comportement du DHCP Snooping et de l'ARP Security.

À la Région, ces deux mécanismes sont déployés systématiquement sur nos switches. Ils permettent de sécuriser l'accès au réseau en empêchant tout appareil non autorisé d'obtenir une adresse IP ou d'injecter de fausses informations ARP. Sur Cisco, cette sécurité est bien maîtrisée : les ports sont stables, les erreurs rares, et la configuration reste cohérente et prévisible.

Sur Allied Telesis, l'histoire a été toute autre. Très rapidement, plusieurs ports se sont mis en erreur (shutdown), sans logique apparente. Un simple redémarrage d'un ordinateur ou une sortie de veille suffisait parfois à bloquer un port. Il devenait donc impossible de garantir une connectivité fiable à un utilisateur standard.

Nous avons tenté de tester un maximum de scénarios, en imaginant ce qu'un agent ferait au quotidien : allumer ou éteindre son poste, fermer l'écran, ou bien brancher une imprimante ou une borne Wi-Fi, etc. Mais dans quasiment tous les cas, un comportement aléatoire venait perturber le test. Certaines commandes semblaient fonctionner un temps, avant que d'autres erreurs apparaissent sans explication.

La documentation officielle, bien qu'existante, était difficile à trouver et peu claire. Elle varie fortement en fonction de la version du système d'exploitation, et les aides intégrées dans le CLI n'étaient pas toujours fiables (l'autocomplétion avec le caractère ? ne listait pas toutes les options disponibles). Il a fallu beaucoup de temps pour comprendre certaines syntaxes ou simplement deviner comment activer une fonction correctement.

Nous avons contacté le support technique d'Allied Telesis, qui a tenté de nous aiguiller, notamment sur le comportement attendu du DHCP Snooping. Certaines pistes ont permis d'atténuer le problème, mais pas de le résoudre. Le switch restait trop rigide : soit tout passait sans réelle sécurité, soit tout se bloquait dès qu'un comportement sortait du cadre strict.

Au bout d'une semaine de tests intensifs, Harun et Jérôme ont pris la décision de suspendre le projet. Non pas parce que le matériel était mauvais mais parce que la souplesse nécessaire pour intégrer nos politiques de sécurité n'était pas au rendez-vous. Si chaque port défectueux implique d'intervenir manuellement, redémarrer la carte réseau, débloquer le port à distance, ce n'est tout simplement pas viable à l'échelle de notre infrastructure.

La suite ? Une réunion de débriefing est prévue avec le commercial Allied Telesis pour faire le point. Le projet n'est pas totalement abandonné, mais il est clair qu'en l'état actuel, une généralisation sur notre réseau poserait plus de problèmes qu'elle n'en résoudrait.

5 - Conclusion

Ce stage au sein du service réseau du Conseil Régional a été une véritable immersion dans un environnement technique exigeant, à grande échelle. Travailler sur une infrastructure aussi étendue, avec des équipements parmi les plus performants du marché, m'a permis de voir ce que représente la gestion d'un réseau en production dans un contexte où la moindre panne peut impacter plusieurs milliers d'agents, d'élus ou de prestataires.

J'ai eu la chance d'intégrer une petite équipe très compétente, qui assure à elle seule le bon fonctionnement de l'ensemble du réseau régional. Ce fonctionnement en effectif restreint, couplé à un niveau d'exigence très élevé, m'a permis de prendre rapidement des responsabilités et d'être confronté à des situations concrètes, complexes, et parfois critiques. Chaque tâche réalisée avait un impact réel. On n'était pas dans le "stage d'observation" : j'ai été mis en condition de production, et ça m'a énormément fait progresser.

Le projet de migration de switchs Cisco vers Allied Telesis a été particulièrement formateur. Il m'a obligé à sortir de ma zone de confort, à chercher des solutions là où il n'existait pas de documentation claire, à comprendre en profondeur des mécanismes comme la sécurité des ports, les VLANs, ou le fonctionnement des protocoles DHCP snooping et ARP security. J'ai appris à travailler avec méthode, à faire des tests rigoureux, à documenter mes essais, et à partager les résultats avec l'équipe. Même si le projet n'a pas abouti à un déploiement concret, il reste à mes yeux une réussite en termes d'apprentissage.

Plus globalement, ce stage m'a permis de mieux comprendre les réalités du métier d'ingénieur réseau dans une structure publique. J'ai vu comment les choix technologiques sont aussi des choix stratégiques, budgétaires, organisationnels. J'ai compris ce que signifie "qualité de service" dans un environnement où l'on n'a pas le droit à l'erreur. Et au-delà de la technique, ce stage m'a surtout fait grandir. J'ai appris à poser les bonnes questions, à chercher l'information, à tester, à douter parfois, mais à avancer toujours. J'ai été entouré de professionnels compétents, passionnés, qui m'ont fait confiance et m'ont laissé ma place. Ce n'était pas juste un stage : c'était une vraie immersion dans la réalité du métier.

C'est une expérience que je considère comme un vrai tournant dans ma formation. Elle m'a conforté dans mon envie de m'orienter vers des postes techniques à haute responsabilité, et m'a donné envie de continuer à apprendre, tester, expérimenter. Si je devais résumer ce stage en une phrase, je dirais qu'il m'a donné un vrai aperçu de la réalité du métier, avec tout ce que ça implique : la pression, la rigueur, mais aussi la satisfaction de faire fonctionner une machine aussi grande que le réseau du Conseil Régional.

Remerciements

Je tiens à exprimer ma profonde gratitude envers la Région Sud et tout particulièrement le service réseau pour m'avoir accueilli durant ces dix semaines de stage. Cette immersion m'a permis de travailler dans un environnement technique exigeant, à grande échelle, et d'apprendre au contact de professionnels passionnés.

Je remercie tout spécialement Harun SENER, mon maître de stage, pour sa confiance, son accompagnement et surtout pour le partage de son expertise. Sa connaissance du réseau est aussi impressionnante que inspirante. Il a su me guider tout au long du stage avec rigueur et bienveillance, en m'impliquant pleinement dans les missions de l'équipe.

Je souhaite également remercier Emmanuel ROME, avec qui j'ai eu le plaisir d'échanger quotidiennement. Sa vision complémentaire et son approche du métier m'ont beaucoup appris. Tous deux ont su créer un environnement à la fois professionnel, stimulant et convivial, dans lequel je me suis senti pleinement intégré.

Enfin, un grand merci à l'ensemble de l'équipe réseau pour leur accueil chaleureux et leur esprit d'équipe. C'était un réel plaisir d'évoluer à leurs côtés, d'apprendre au quotidien, et de partager des moments aussi instructifs que sympathiques.

Ce stage restera une expérience marquante dans mon parcours.

Glossaire

ACL (Access Control List) : Liste de contrôle d'accès utilisée pour filtrer le trafic réseau en définissant des règles appliquées sur les équipements réseau (switches, routeurs, firewalls).

ARP (Address Resolution Protocol) : Protocole permettant de faire correspondre une adresse IP à une adresse MAC dans un réseau local.

ARP Security : Fonction de sécurité sur les switches qui permet de valider les adresses ARP entrantes et de prévenir les attaques par usurpation d'adresse (ARP spoofing).

Baie technique : Armoire ou local regroupant des équipements réseau et serveurs.

CLI (Command Line Interface) : Interface en ligne de commande utilisée pour configurer les équipements réseau (switch, routeur, firewall…).

Datacenters : Centres de données hébergeant de nombreux serveurs et équipements réseau, assurant la disponibilité et la sécurité des services numériques.

DMZ (Demilitarized Zone) : Zone tampon entre un réseau interne et Internet, dans laquelle sont placés les services accessibles publiquement (sites web, serveurs mail…).

Firewall : Équipement ou logiciel de sécurité réseau chargé de contrôler les flux entrants et sortants selon des règles définies.

Firmware : Logiciel embarqué dans un équipement (switch, routeur, imprimante, etc.) permettant de gérer son fonctionnement matériel de base.

Flux réseau : Ensemble des données échangées sur un réseau informatique entre plusieurs équipements.

Golden Image : Version validée d'un système ou firmware utilisée comme référence pour les mises à jour sur les équipements.

Hostname : Nom attribué à un équipement réseau pour l'identifier facilement dans une infrastructure.

IPsec (Internet Protocol Security) : Protocole de sécurité qui chiffre et authentifie les échanges IP pour les VPN ou autres communications sécurisées.

LAN (Local Area Network) : Réseau local interne à une organisation ou un bâtiment.

Machines virtuelles : Émulations logicielles d'un ordinateur physique, permettant de faire tourner plusieurs systèmes sur une même machine physique via un hyperviseur.

MPLS (Multiprotocol Label Switching) : Technologie réseau utilisée pour acheminer rapidement les paquets en fonction de labels plutôt que d'adresses IP. Elle est souvent utilisée dans les réseaux opérateurs pour la performance et la qualité de service.

Opérateurs télécoms : Fournisseurs de services de télécommunication (accès Internet, téléphonie)

PBF (Policy-Based Forwarding) : Technique permettant de rediriger les paquets réseau en fonction de politiques personnalisées (au lieu du routage classique).

Phishing : Technique frauduleuse visant à tromper un utilisateur pour qu'il fournisse des informations sensibles (mots de passe, coordonnées bancaires...) via un faux site, email ou message.

Port Security : Mécanisme de sécurité sur les switches permettant de contrôler quels périphériques peuvent se connecter à un port réseau.

QoS (Quality of Service) : Ensemble de mécanismes permettant de prioriser certains types de trafic réseau pour garantir une bonne qualité de service (voix, vidéo…).

Règles de filtrage : Instructions définies sur un firewall ou un équipement réseau permettant d'autoriser ou de bloquer certains flux en fonction de critères (adresse IP, port, protocole…).

RSTP (Rapid Spanning Tree Protocol) : Version améliorée du protocole STP qui permet de prévenir les boucles réseau tout en assurant une convergence rapide.

Switch : Équipement réseau intelligent qui connecte plusieurs périphériques dans un réseau local et transmet les données aux bons destinataires.

Teams : Outil de communication et de collaboration en ligne de Microsoft, utilisé pour discuter, organiser des réunions et partager des fichiers en équipe.

Template : Modèle de configuration réutilisable, permettant de générer automatiquement des fichiers de configuration à partir de variables.

VLAN (Virtual LAN) : Réseau local virtuel permettant de segmenter un réseau physique en plusieurs réseaux logiques pour des raisons de sécurité ou d'organisation.

VPLS (Virtual Private LAN Service) : Technologie permettant de créer un réseau LAN virtuel étendu entre plusieurs sites distants, via une infrastructure MPLS. Elle simule un switch géant entre les sites.

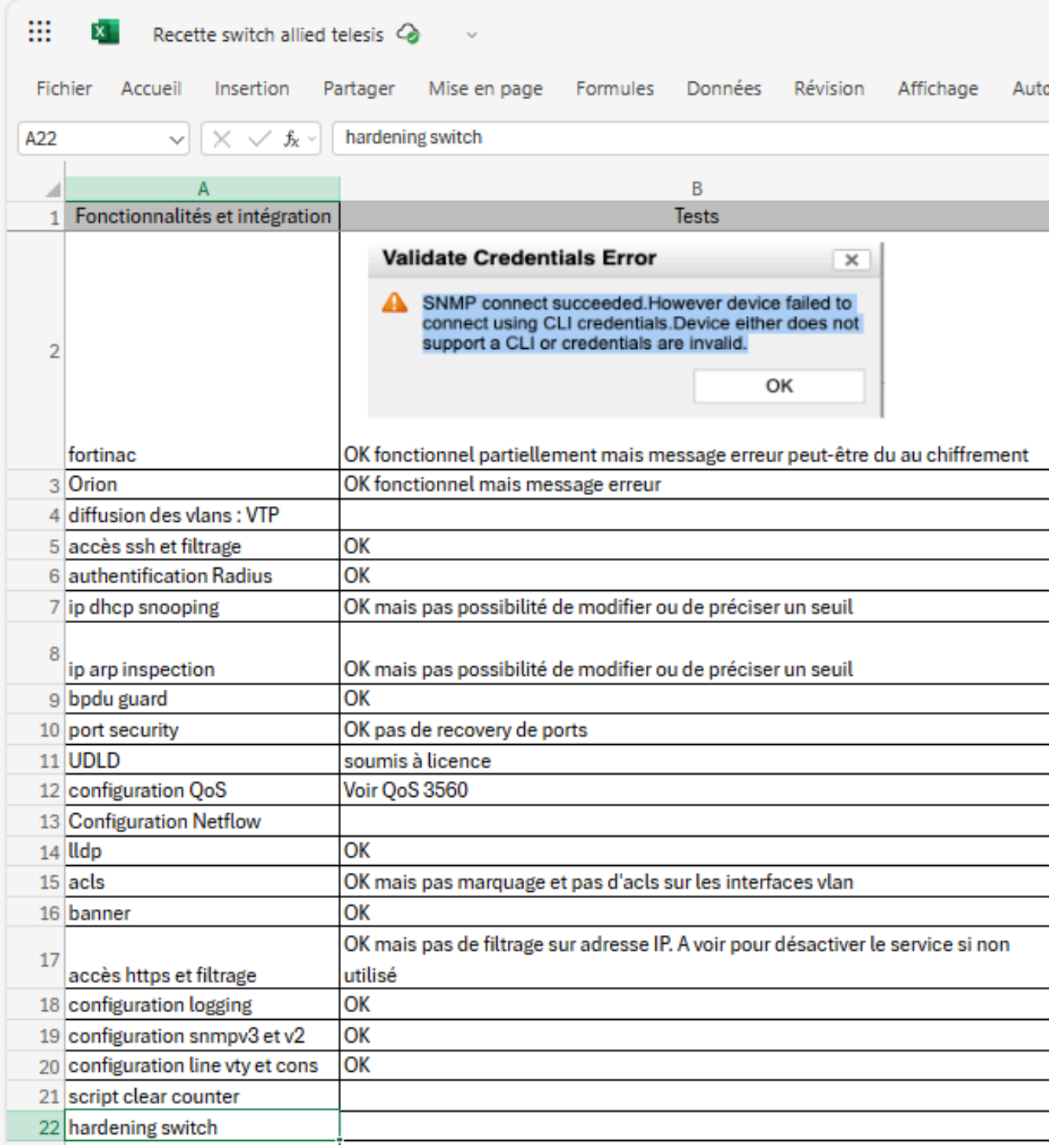
VRF (Virtual Routing and Forwarding) : Technique permettant d'isoler plusieurs instances de tables de routage sur un même équipement.

VPN (Virtual Private Network) : Connexion sécurisée permettant à un utilisateur distant d'accéder aux ressources internes d'un réseau comme s'il y était connecté localement.

Wi-Fi : Technologie de communication sans fil permettant aux périphériques de se connecter à un réseau local sans câble.

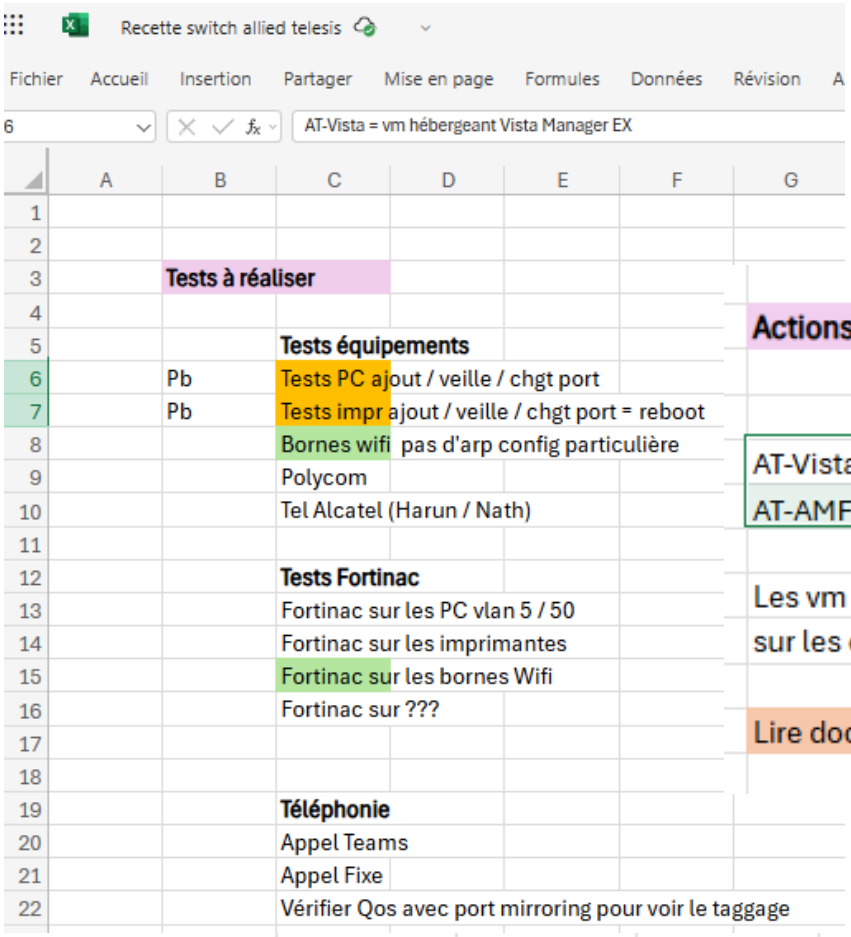
Annexes

Annexe 1 - Cahier de recette Migration configuration Cisco vers Allied Telesis



	A	B
1	Fonctionnalités et intégration	Tests
2	fortinac	OK fonctionnel partiellement mais message erreur peut-être du au chiffrement
3	Orion	OK fonctionnel mais message erreur
4	diffusion des vlans : VTP	
5	accès ssh et filtrage	OK
6	authentification Radius	OK
7	ip dhcp snooping	OK mais pas possibilité de modifier ou de préciser un seuil
8	ip arp inspection	OK mais pas possibilité de modifier ou de préciser un seuil
9	bpdu guard	OK
10	port security	OK pas de recovery de ports
11	UDLD	soumis à licence
12	configuration QoS	Voir QoS 3560
13	Configuration Netflow	
14	lldp	OK
15	acls	OK mais pas marquage et pas d'acls sur les interfaces vlan
16	banner	OK
17	accès https et filtrage	OK mais pas de filtrage sur adresse IP. A voir pour désactiver le service si non utilisé
18	configuration logging	OK
19	configuration snmpv3 et v2	OK
20	configuration line vty et cons	OK
21	script clear counter	
22	hardening switch	

Annexe 2 - Excel des actions à réaliser



Recette switch allied telesis

Fichier Accueil Insertion Partager Mise en page Formules Données Révision A

6 | AT-Vista = vm hébergeant Vista Manager EX

	A	B	C	D	E	F	G
1							
2							
3		**Tests à réaliser**					
4							
5			**Tests équipements**				
6		Pb	Tests PC ajout / veille / chgt port				
7		Pb	Tests impr ajout / veille / chgt port = reboot				
8			Bornes wifi pas d'arp config particulière				
9			Polycom				
10			Tel Alcatel (Harun / Nath)				
11							
12			**Tests Fortinac**				
13			Fortinac sur les PC vlan 5 / 50				
14			Fortinac sur les imprimantes				
15			Fortinac sur les bornes Wifi				
16			Fortinac sur ???				
17							
18							
19			**Téléphonie**				
20			Appel Teams				
21			Appel Fixe				
22			Vérifier Qos avec port mirroring pour voir le taggage				

Actions à réaliser

LG : suivre la création des vm

AT-Vista = vm hébergeant Vista Manager EX

AT-AMF = vm hébergeant le maître AMF

Les vm seront configurées lorsque les tests sur les équipements seront concluants

Lire doc d'install

Switch Cisco swe20			**Switch AT swe20-AT**		
PC Emma	1/0/1	vlan 50	PC Jason	1.0.2	
PC test 22	1/0/7	vlan 50	PC SPTS	1.0.3	1.0.4
PC Jason	1/0/15	Vlan 5			
impr HP canapé	2/0/47	vlan 165	Impr HP SA	1.0.10	
Impr HP SAD	3/0/47	vlan 165			
Impr SPTS ??	2/0/43	vlan 165			
Banc test SPTS	1/0/21	Vlan 5	Borne Wifi	1.0.22	
Banc test 22	1/0/40	Vlan 5	Borne Wifi	1.0.23	
FMinard Tel	3/0/4	vlan 160, visio	Uplink	1.0.24	
GTC_BAT_E	1/0/47	vlan 39			
Polycom Salle réu	A trouver ou 3/0/4 ???				
Banc de travail SI	2/0/39	Vlan 5			
Banc de travail SI	3/0/5	Vlan 5			
Badgeuse					
PC Harun tel Alca	Prendre Netscout				

Annexe 3 - Excel des tests et leurs résultats

PC Jason / refaire le test avec un PC Admin vlan 50				
	le 02/06, pb d'accès au démarrage de l'ordinateur port en err disable, résolu après shut / no shut			switchport
	Vérif config			switchport mode access
	suppression ok arp security drop link-local-arps			switchport access vlan 5
	A tester arp security violation log trap link-down			switchport port-security
				switchport port-security aging
	Pour l'instant, pas d'incidence avec la ligne ip dhcp snooping violation log trap link-down			switchport port-security maximum 3
				switchport port-security violation shutdown
				ip dhcp snooping max-bindings 3
Fermeture Ordi	OK			service-policy input QOS-INPUT
Mise en veille	OK			wrr-queue queue-limit 20 15 15 15 20 5 5 5
Eteindre/allumer	Err-disable	A fonctionné auparavant	arp security drop link-local-arps /// désactivé	snmp trap link-status
Changement de port				snmp trap mac-change add remove
				spanning-tree portfast
				spanning-tree portfast bpdu-guard enable
				switchport voice vlan 205
				ip dhcp snooping violation log trap link-down
				arp security violation log trap link-down
				arp security drop link-local-arps /// désactivé

PC prêt test chez Carole			
		switchport	switchport
		switchport mode access	switchport mode access
Allumer PC avec la config de base	OK port connected // ouvrir la session et vérifier Internet	switchport access vlan 5	switchport access vlan 5
Vérification Fortinac	OK vlan 5 et logo utilisateur	switchport port-security	switchport port-security
Fermeture Ordi		switchport port-security aging	switchport port-security aging
Mise en veille		switchport port-security maximum 3	switchport port-security maximum 3
Eteindre/allumer		switchport port-security violation shutdown	switchport port-security violation shutdown
Changement de port mettre sur le port 1.0.6		ip dhcp snooping max-bindings 3	ip dhcp snooping max-bindings 3
		service-policy input QOS-INPUT	service-policy input QOS-INPUT
		wrr-queue queue-limit 20 15 15 15 20 5 5 5	wrr-queue queue-limit 20 15 15 15 20 5 5 5
Allumer PC sans la ligne link-local-aprs		snmp trap link-status	snmp trap link-status
Vérification Fortinac		snmp trap mac-change add remove	snmp trap mac-change add remove
		spanning-tree portfast	spanning-tree portfast
		spanning-tree portfast bpdu-guard enable	spanning-tree portfast bpdu-guard enable
		switchport voice vlan 205	switchport voice vlan 205
		ip dhcp snooping violation log trap link-down	ip dhcp snooping violation log trap link-down
		arp security violation log trap link-down	arp security violation log trap link-down
		arp security drop link-local-arps	arp security drop link-local-arps /// désactivé

Test : Imprimantes	Test avec impr SAD	Quelle config du port ?
Branchement d'une imprimante	Err-disable	
Mise en veille		
Déplacement port de l'imprimante + reboot		
Test : Borne Wifi		
Vérification borne wifi	OK aire25 à prendre dans la baie du 2ème	
Branchement borne w	OK port AT 1.0.23 connected	
Déplacement port bor	KO sur le port 1.0.22	
Remise sur le port d'or	coneccted mais borne HS, puis shut/ no shut et OK	
Prise en compte Fortin	Le port n'est pas connecté dans Fortinac alors que la borne est pingable et up	
Prise en compte Fortin	OK Fotinac après shut / no shut du port 1.0.23, logo et WAP	
Test : Tel Alcatel Harun		