CPAM Ardèche / Greta Ardèche-Drôme

Mise en place SDWAN

CPAM ARDECHE

Collet Valentin
BTS SIO-SISR / Session 2026

SOMMAIRE

Cahier des charges

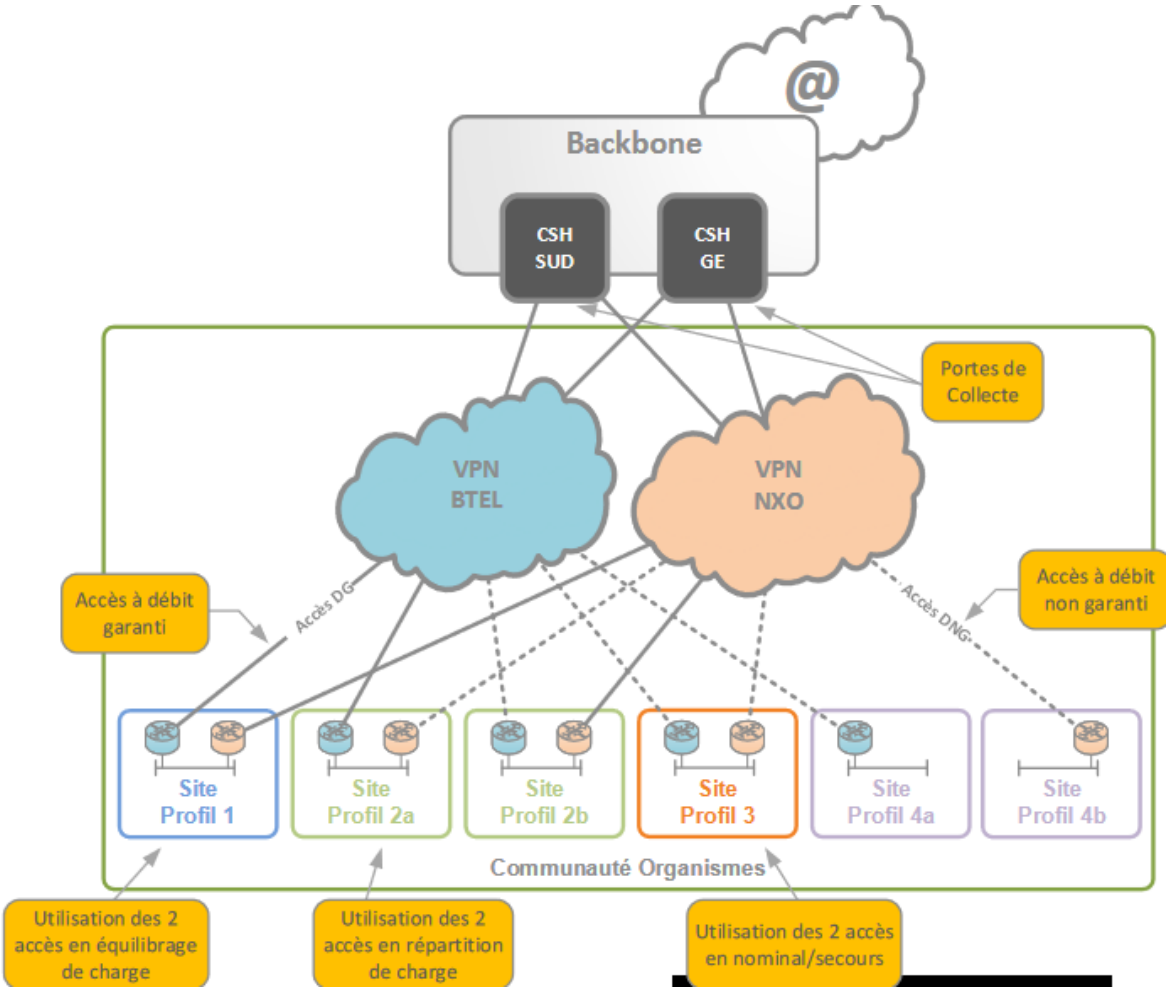
Descriptifs de l'existant

Au sein de la CPAM, l'architecture réseau est actuellement assurée selon plusieurs axes distincts.

⇨ **Au niveau du routage**

L'accès site à site se base actuellement sur une topologie hub & spoke, c'est-à-dire qu'un nœud central (hub) sert de point de connexion pour tous les autres nœuds périphériques (spoke). Toutes les communications entre sites distants (spoke) passent par le hub central, il n'y a donc pas de communications intersites sans passage sur le nœud central.

- Un accès intersites via un tunnel VPN passant par les CSH (Centre de Services Hébergés)
- Avantage de centraliser les connexions à un seul hub, simplifiant ainsi son administration, contrairement à une topologie maillée qui nécessite beaucoup plus de tunnels pour chaque site



Le routage se fait via le protocole BGP (Border Gateway Protocol). Les équipements ne sont pas uniformes : routeurs (couche 3) et commutateurs (couche 2/3) différents selon les sites, entraînant plusieurs problèmes tels que des fabricants différents, versions d'OS variées, besoins de formations spécifiques et problèmes d'incompatibilité. La gestion s'effectue de la Direction

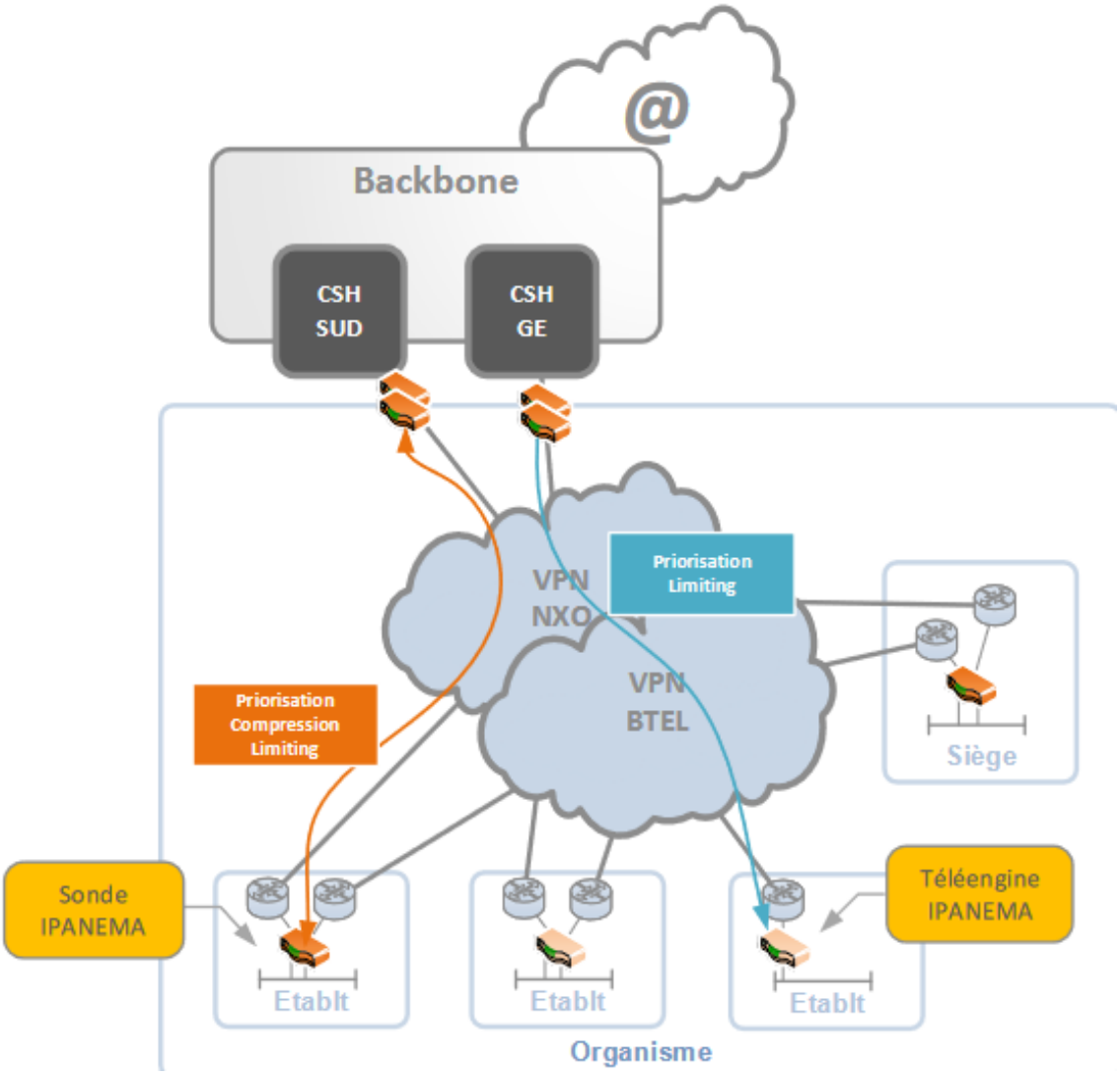
régionale vers les organismes, puis vers les individus, ce qui implique une absence de gestion centralisée et de procédure universalisée.

⇨ **Au niveau applicatif**

Chaque site est équipé d'une sonde IPANEMA permettant la répartition des flux et la QoS (Quality of Service). Ces sondes assurent une performance applicative optimale en garantissant la qualité de l'expérience utilisateur lors de l'utilisation d'applications métier (latence, disponibilité, bande passante). Les sondes IPANEMA sont des équipements réseaux dédiés à la surveillance, l'analyse et l'optimisation du trafic, avec une sonde sur le Hub et une pour chaque Spoke.

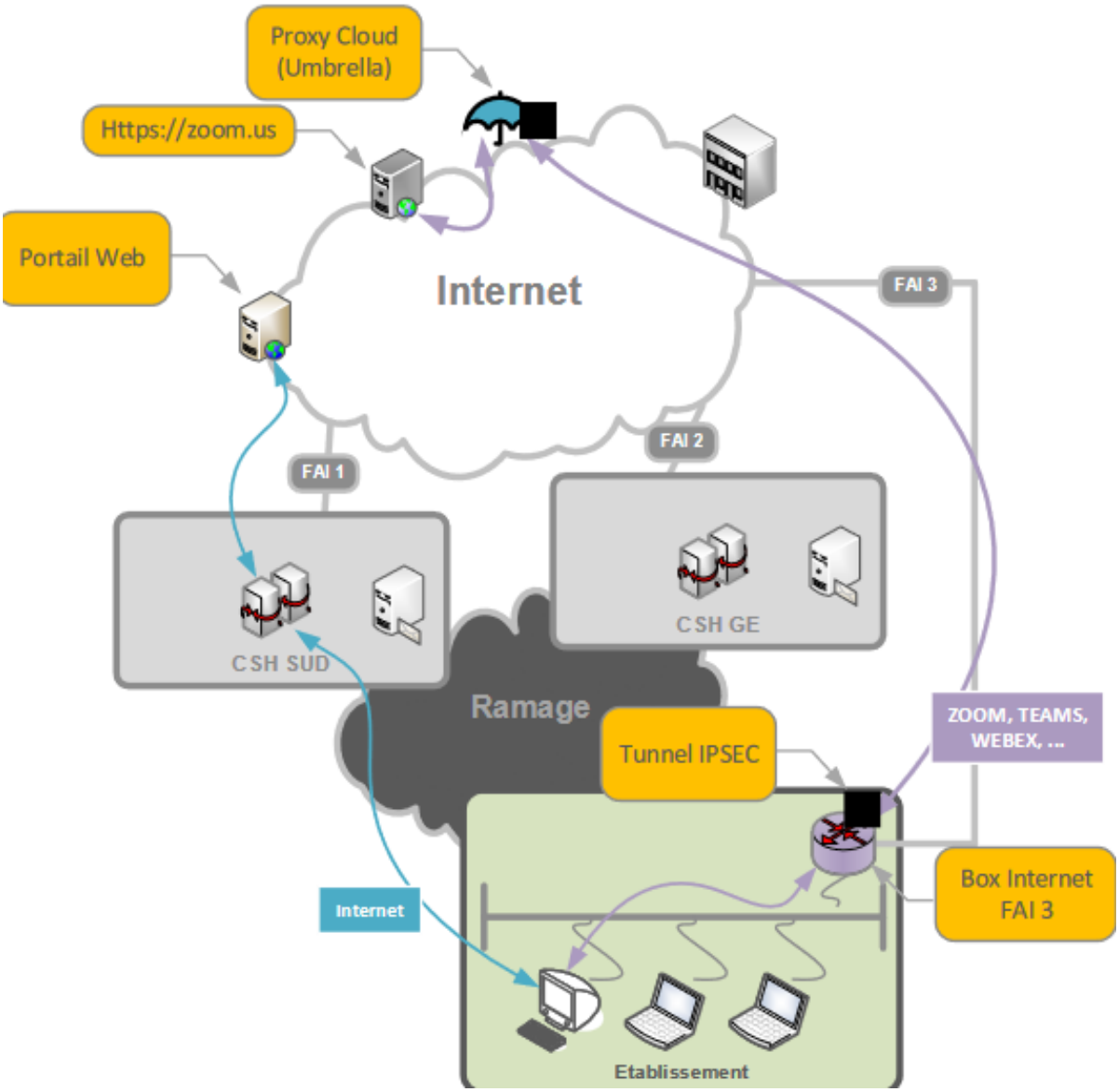
Elles permettent plusieurs fonctionnalités clés :

- Monitoring et visibilité applicative : identification des applications métiers utilisées, mesure en temps réel de la qualité d'accès, détection des goulots d'étranglement
- Optimisation du trafic via compression en temps réel des données réseau (économie sur la bande passante)
- Priorisation intelligente : protection et garantie de la performance des applications critiques pour chaque utilisateur, sur chaque site



⇨ **Au niveau sécurité :**

La sécurité repose sur des équipements spécifiques tels que des pare-feu et IPS (Intrusion Prevention System). Un IPS est un équipement de surveillance du trafic en temps réel permettant de détecter et bloquer automatiquement les activités suspectes ou malveillantes. Ces équipements sont centralisés au niveau des CSH (nœuds centraux), avec peu de solutions déployées au niveau local.



Besoins

La mise en place d'une solution au sein de la CPAM doit permettre d'agir sur plusieurs points critiques de l'infrastructure existante.

⇨ **Routage**

Une solution permettant de gérer facilement différents types de liens WAN, capable de mettre en œuvre une solution de routage avancée prenant des décisions basées sur la performance des liens. Cette solution doit être apte à décider s'il est préférable d'utiliser le réseau MPLS pour les applications critiques ou de basculer sur le réseau fibre si le MPLS est saturé. Elle doit également simplifier l'ingénierie de routage, incluant la définition des chemins réseau, la configuration des routeurs, la création des tunnels VPN, ainsi que le routage et la maintenance.

⇨ **Performance applicative**

Remplacer la solution IPANEMA pour la priorisation et la compression des flux
Offrir une visibilité applicative des flux transitant sur le réseau capillaire

⇨ **Sécurité**

Chiffrer les flux de bout en bout
Pouvoir distribuer des fonctionnalités de sécurité dans le réseau (IPS/Firewall)

Contraintes

Plusieurs contraintes techniques et organisationnelles encadrent ce projet de déploiement.

- Contrainte humaine : nécessité d'être deux techniciens pour effectuer le rackage des routeurs
- Les routeurs sont préconfigurés par la Direction Régionale et les CSH. La configuration côté switch est gérée localement, nécessitant le respect d'un ordonnancement précis au niveau du câblage
- Contrainte temporelle majeure : fin du support IPANEMA prévue en juillet 2026, imposant un déploiement complet avant cette échéance

Schéma de câblage requis :

- Liaison Back To Back : Port Gi0/0/2 Routeur SD-WAN Master vers Port Gi0/0/2 Routeur SD-WAN Slave
- Liaison WAN : Port Gi0/0/0 Routeur SD-WAN Master vers Port Gi0/3 Routeur Opérateur 1
- Liaison WAN : Port Gi0/0/0 Routeur SD-WAN Slave vers Port Gi0/4 Routeur Opérateur 2 (Juniper)
- Liaison LAN : Port Gi0/0/1 Routeur SD-WAN Master vers Switch N3 du site (port libre à définir)
- Liaison LAN : Port Gi0/0/1 Routeur SD-WAN Slave vers Switch N3 du site (port à définir)
- Raccordement idéalement sur un stack switch : un boîtier par switch niveau 3, sur des ports 1G
- Infrastructure électrique : nécessité de 4 prises ondulées

Ressources

Ressources humaines

- Mon référent d'alternance est disponible pour m'aider et répondre à mes questionnements

Ressources matérielles locales

- Poste de travail avec accès SSH pour la configuration
- 5 câbles Ethernet Cat 6a
- 2 routeurs Cisco Catalyst 8300 : ces équipements intègrent la fonctionnalité d'optimisation qui remplacera la compression des sondes IPANEMA

Ressources gérées par la Direction Régionale

La Direction Régionale prend en charge plusieurs aspects critiques de la configuration :

- Configuration des switches N3 : déploiement automatique d'un nouveau master de configuration incluant un nouveau VLAN d'interconnexion avec les boîtiers SD-WAN
- Mise en place d'un nouveau protocole de routage dynamique OSPF en remplacement de BGP
- DNS : création des entrées DNS pour les boîtiers SD-WAN
- Bastion : ajout des boîtiers dans le bastion de sécurité
- SD-WAN : préparation et préconfiguration des boîtiers avant livraison

Ressources documentaires:

- Cisco Catalyst SD-WAN
- Cisco Catalyst SD-WAN Getting started guide
- Introduction to Cisco Catalyst SD-WAN
- Page produit Cisco Catalyst 8300

Analyse

Descriptif des solutions

Solution Cisco Catalyst SD-WAN

Cisco SD-WAN est une solution d'orchestration et de gestion de réseaux étendus. Cette technologie permet de créer un overlay network (un réseau virtuel construit par-dessus un réseau physique existant, comme une autoroute privée construite au-dessus des routes publiques.) sur l'infrastructure WAN existante, offrant une flexibilité et une agilité accrues dans la gestion du réseau étendu.

Composants principaux de la solution Cisco SD-WAN

- **vManage :** contrôleur centralisé de gestion et d'orchestration du réseau SD-WAN via une interface graphique intuitive
- **vSmart :** contrôleur distribuant les politiques de routage et de sécurité aux équipements edge
- **vBond :** orchestrateur d'authentification et de découverte des équipements, facilitant l'établissement des tunnels sécurisés
- **Cisco Catalyst 8300 (Edge routers) :** routeurs de périphérie installés sur chaque site, assurant le chiffrement du trafic, l'application des politiques et l'optimisation du trafic

Fonctionnalités clés

- **Routage intelligent :** sélection dynamique du meilleur chemin réseau basée sur la performance en temps réel (latence, gigue, perte de paquets) et les exigences applicatives
- **Topologie Regional-Mesh :** les sites au sein d'un même organisme établissent des tunnels directs entre eux et communiquent sans passer par le hub central, optimisant ainsi la latence et réduisant la charge sur les CSH
- **Sécurité intégrée :** chiffrement de bout en bout via IPsec, pare-feu de nouvelle génération, IPS intégré et segmentation du réseau
- **Optimisation applicative :** compression du trafic, mise en cache et QoS granulaire remplaçant les fonctionnalités IPANEMA
- **Visibilité et analytique :** monitoring en temps réel des performances réseau et applicatives avec tableaux de bord détaillés

OSPF (Open Shortest Path First) : OSPF est un **protocole de routage interne** (IGP - Interior Gateway Protocol) utilisé **à l'intérieur d'un réseau d'entreprise**.

- Chaque routeur crée une carte complète du réseau
- Il calcule automatiquement le chemin le plus court vers chaque destination
- Si un lien tombe en panne, OSPF recalcule instantanément un nouveau chemin

BGP (Border Gateway Protocol) est un protocole de routage externe utilisé entre différents réseaux autonomes.

- BGP ne cherche pas le chemin le plus court
- Il négocie des accords entre réseaux pour échanger du trafic
- Il prend des décisions basées sur des politiques (pas seulement la distance)

Solution VMware SD-WAN

VMware SD-WAN est une solution de réseau étendu défini par logiciel, acquise par VMware en 2017. Elle est conçue pour simplifier la connectivité et optimiser les performances des applications cloud et SaaS.

Composants principaux de VMware SD-WAN

- VMware SD-WAN Orchestrator : console de gestion centralisée hébergée dans le cloud. Interface graphique web assurant la gestion de la configuration de tous les sites, le déploiement de politiques réseau, le monitoring en temps réel avec tableaux de bord.
- Avantage : pas besoin d'infrastructure locale pour le contrôleur, tout est dans le cloud.
- SD-WAN Edge : appliances déployées sur les sites (physiques ou virtuelles). Fonctions principales : établissement des tunnels sécurisés, application des politiques de routage, optimisation du trafic et connexion aux Gateways cloud.
- SD-WAN Gateway : points de présence (PoP) stratégiquement déployés dans le monde entier. Ils optimisent l'accès aux applications SaaS (Office 365, Salesforce, etc.), offrent une sortie Internet optimisée et peuvent être gérés par VMware ou le client. Avantage clé : rapproche le trafic des applications cloud pour de meilleures performances.

Fonctionnalités principales

- Routage intelligent cloud-native : la solution mesure la qualité de tous les liens en temps réel (Dynamic Multipath Optimization - DMPO), bascule instantanément si un lien se dégrade et peut dupliquer les paquets sur plusieurs liens pour la fiabilité. Le routage s'adapte automatiquement selon le type d'application : SaaS vers Gateway cloud le plus proche, Datacenter interne via tunnel direct MPLS, Internet général via sortie locale.
- Optimisation WAN (Application QoE) : déduplication pour réduire les données redondantes, compression pour économiser la bande passante, correction d'erreur (FEC) pour compenser la perte de paquets et QoS granulaire pour prioriser les applications critiques.
- Sécurité de base : pare-feu avec état (stateful firewall), segmentation réseau, chiffrement IPsec des tunnels et NAT avec filtrage basique. Limitation importante : sécurité avancée limitée comparée à Cisco ou Fortinet. Nécessite souvent des équipements tiers pour IPS, NGFW avancé, filtrage URL et protection anti-malware, généralement via intégration avec des partenaires sécurité (Zscaler, Palo Alto).
- Topologie flexible : supporte Hub-and-Spoke, Mesh dynamique (tunnels directs entre branches si nécessaire) et via Gateway cloud (branch vers Gateway VMware puis Internet/SaaS).

Limitations : sécurité limitée en natif nécessitant souvent des partenaires tiers, augmentant la complexité. Dépendance au cloud avec Orchestrator uniquement dans le cloud, pouvant

poser des problèmes de souveraineté. Capacités de routage avancées moins étendues que Cisco pour les environnements complexes.

Comparaison des solutions :

Critères	Cisco SD-WAN	VMware SD-WAN
Routage intelligent	Très performant avec politiques avancées basées sur les applications et temps réel	Performant avec optimisation cloud-native
Sécurité intégrée	Chiffrement IPsec, IPS, pare-feu. Micro-segmentation avancée	Sécurité de base, nécessite souvent équipements complémentaires
Topologie mesh	Supporte Regional-Mesh et Full-Mesh avec tunnel dynamique	Supporte mesh via gateway cloud
Optimisation WAN	Compression, déduplication, mise en cache. Remplace efficacement IPANEMA	Bonne optimisation avec techniques de déduplication
Gestion centralisée	vManage : console complète et mature	Orchestrator : interface intuitive et moderne
Analytique et reporting	Tableaux de bord détaillés avec métriques en temps réel	Analytics cloud intégrés
Coût	Investissement initial élevé, ROI sur le long terme	Modèle par abonnement, coûts prévisibles
Écosystème	Leader du marché, vaste écosystème partenaires	Intégration forte VMware

Choix d'une solution

Après analyse comparative des deux solutions, le choix s'est porté sur la solution Cisco Catalyst SD-WAN pour plusieurs raisons stratégiques et techniques.

Justification du choix

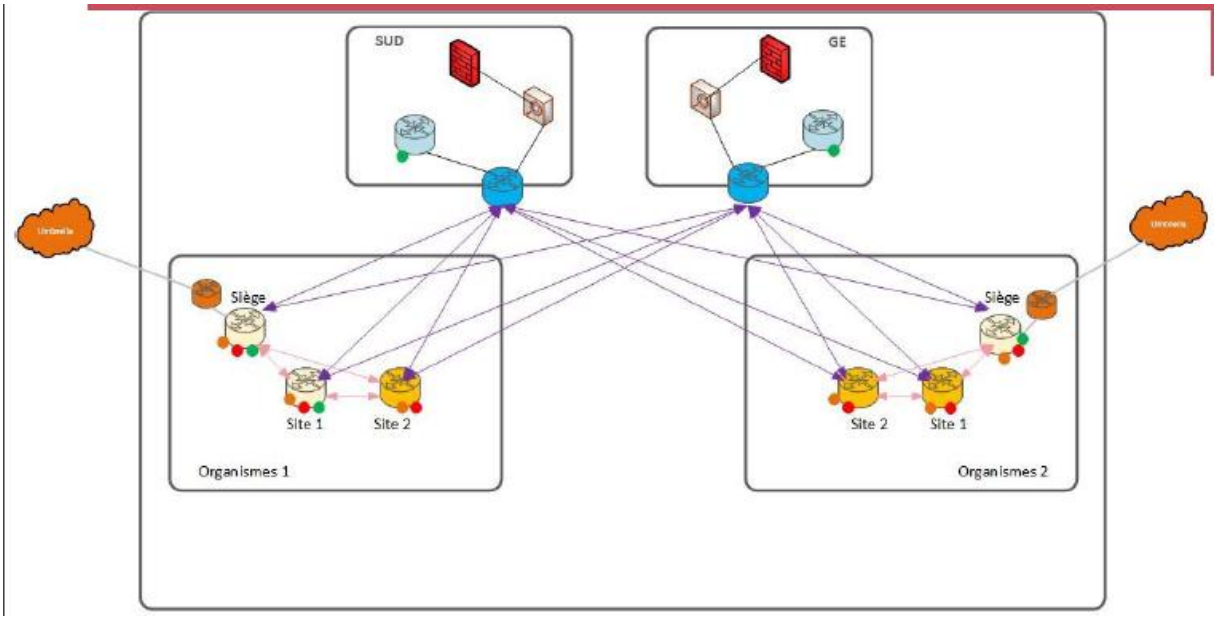
- **Maturité et fiabilité :** La solution bénéficie d'une base installée importante et d'un retour d'expérience conséquent
- **Réponse exhaustive aux besoins :** la solution répond intégralement aux trois axes majeurs identifiés (routage, performance applicative, sécurité). Elle remplace efficacement les sondes IPANEMA grâce aux fonctionnalités d'optimisation WAN intégrées dans les Catalyst 8300
- **Topologie Regional-Mesh :** permet l'établissement de tunnels directs entre sites d'un même organisme, réduisant la latence et optimisant l'utilisation de la bande passante. Les sites n'appartenant pas au même organisme passent par les CSH, préservant ainsi la gouvernance et la sécurité
- **Sécurité distribuée :** déploiement d'IPS sur chaque routeur SD-WAN permettant l'analyse exhaustive du trafic au niveau local, répondant à l'exigence de distribution des fonctionnalités de sécurité dans le réseau capillaire

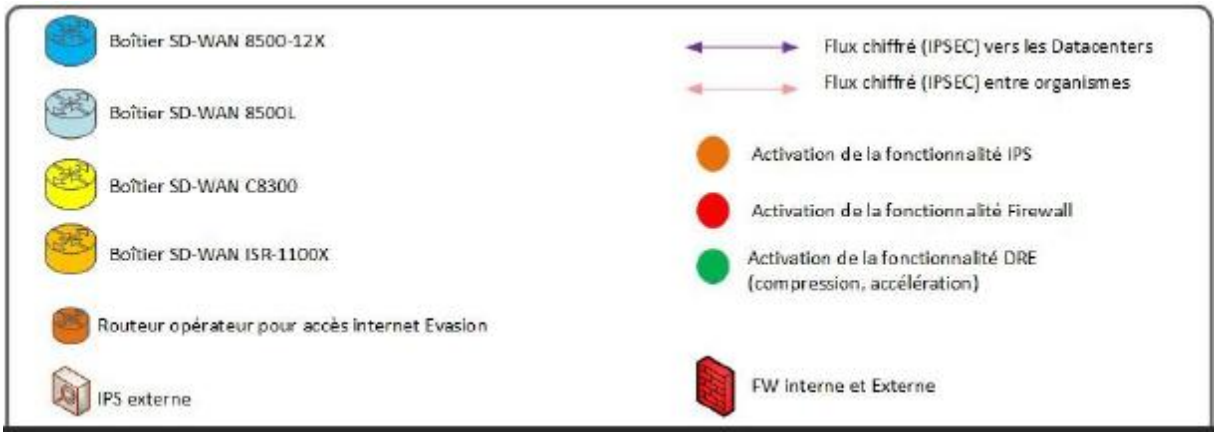
Plan d’adressage et schéma

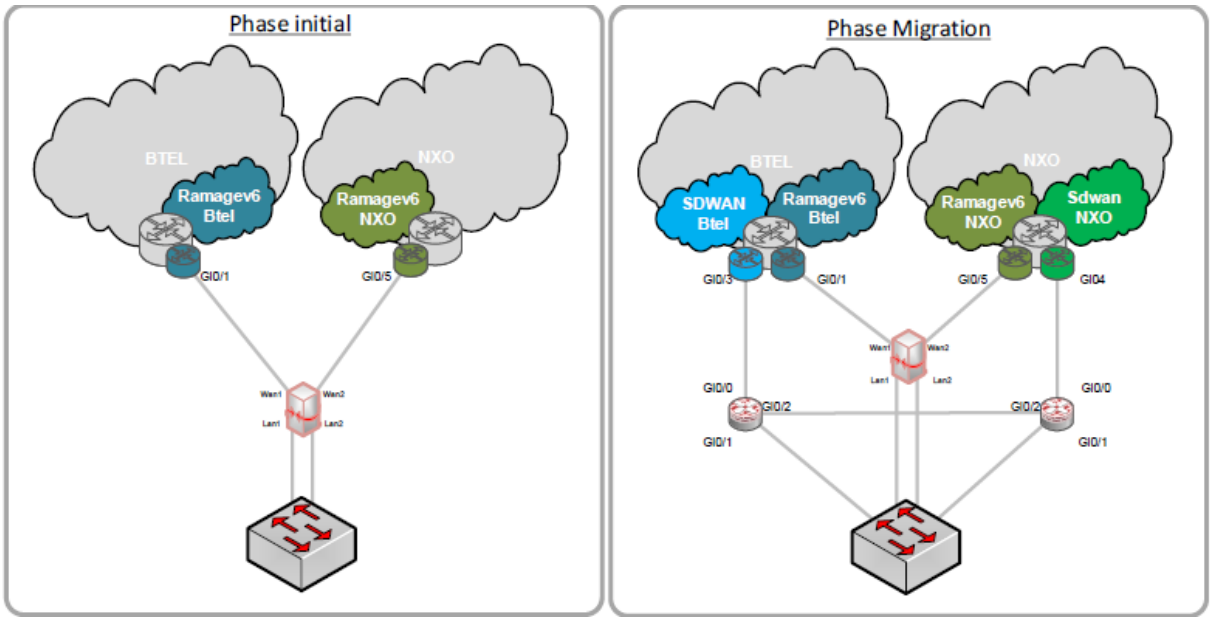
L'architecture SD-WAN repose sur une topologie Regional-Mesh permettant aux sites d'un même organisme de communiquer directement entre eux via des tunnels sécurisés. Les sites appartenant à des organismes différents transitent par les CSH (Centres de Services Hébergés).

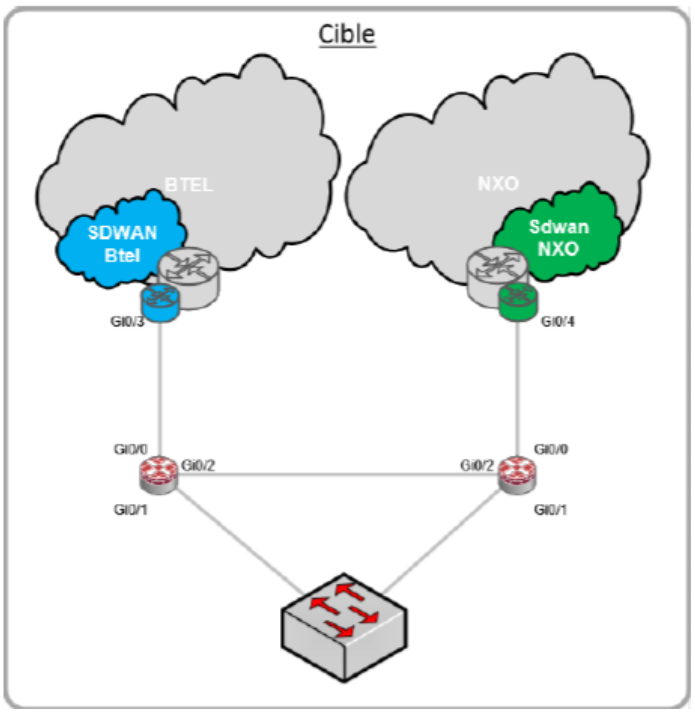
Architecture réseau

- Topologie : Regional-Mesh avec tunnels IPsec dynamiques
- Protocole de routage : OSPF (Open Shortest Path First) en remplacement de BGP
- Équipements edge : Cisco Catalyst 8300 en configuration redondante (Master/Slave)
- Liens WAN : double connexion vers opérateurs distincts pour garantir la haute disponibilité
- Sécurité : IPS déployé sur chaque routeur SD-WAN pour l'analyse du trafic









Etude de l'impact sur le SI existant

Le déploiement de la solution SD-WAN génère plusieurs impacts sur le système d'information existant, identifiés lors de la phase pilote.

Impacts techniques

- **Coupure brève de service :** une interruption d'environ 30 secondes est constatée lors de l'activation des modules de sécurité sur les boîtiers SD-WAN. Cette coupure doit être planifiée en dehors des heures ouvrées
- **Reconnexion applicative :** les applications métier utilisant un navigateur web remontent automatiquement leur connexion sans intervention utilisateur

- **Clients lourds :** certaines applications en mode client lourd (exemple : Progres) nécessitent d'être relancées manuellement. Communication préventive aux utilisateurs requise

Impacts sur les performances

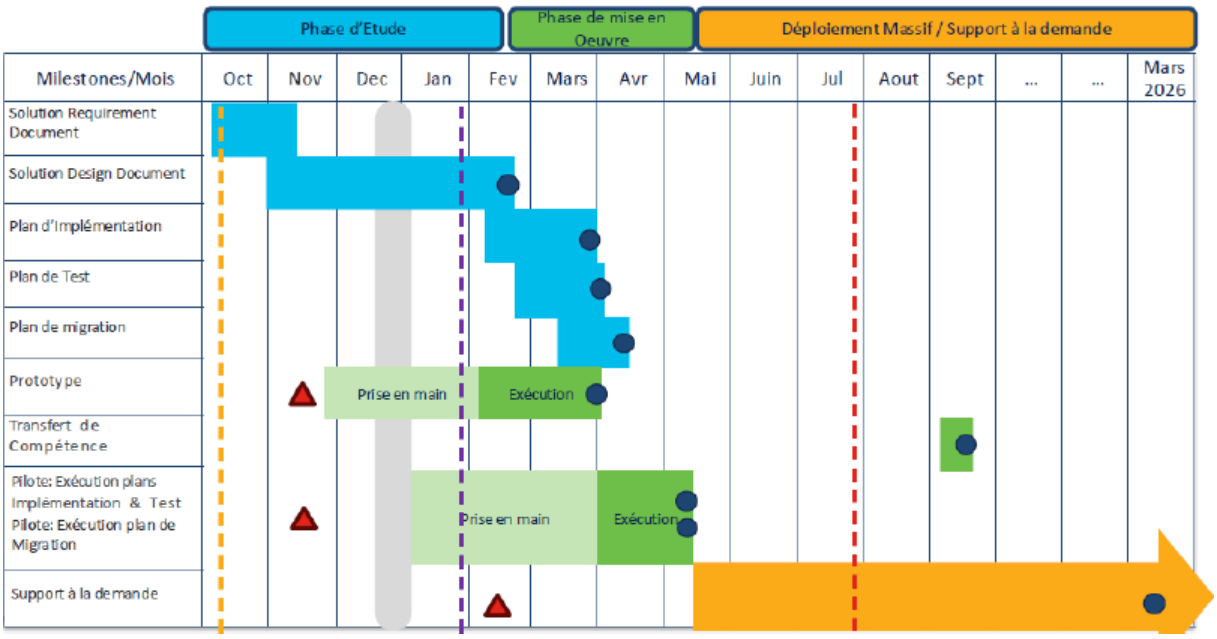
Le ressenti des utilisateurs varie selon le profil des sites :

- **Sites de profil 1 (sièges, PFS) :** ressenti utilisateur inchangé. L'équilibrage du trafic sur les liens opérateurs est resté stable. Sur certains sites, le passage en SD-WAN provoque une inversion de l'accès le plus utilisé, résultant en une meilleure répartition des flux en fonction de la qualité réelle des liens
- **Sites de profil 2 (sites moyens) :** amélioration notable. La migration SD-WAN a provoqué une diminution de la charge sur les accès Direction Générale. La suppression des contraintes liées aux applications délestées s'avère bénéfique
- **Sites de profil 3 (petits sites) :** améliorations lors des fortes sollicitations réseau, notamment pendant les mises à jour WSUS. La priorisation intelligente du trafic maintient les applications critiques accessibles

Phasage et Prévision des tests :

1) Vérifications entrée DNS
2) Câblage physique
3) Configuration port switch N3
4) Vérification SWITCH N3
   a. Vlan
   b. Interface
5) Vérification routeurs
6) Test accès sites distants
   a. Accès site distants organisme CPAM Ardèche
   b. Accès site distants autres

Déploiement



Voici le planning prévisionnel initiale qui a été décalé sur l'année 2026, le deadline de déploiement des SDWAN au niveau national est donc fixé avant juillet 2026 où va s'arrêter le support IPANEMA.

Nous avons quant à nous réaliser l'installation et paramétrage switch en 1h le vendredi 23.01.2026. Après branchement et paramétrage des switch, nous envoyons un mail au CSH qui valide et met en route le SDWAN. Puis, nous décommissionnons les anciens liens WAN.

Mise en place

1) Vérifications entrée DNS

Nous vérifions la présence des entrées DNS des deux routeurs C8300 sur l'interface web de gestion du DNS :

De plus je m'assure aussi via cmd la bonne résolution nom de domaine en adresse IP en cmd :

```
Nslookup <nom_sdwan_master>
```

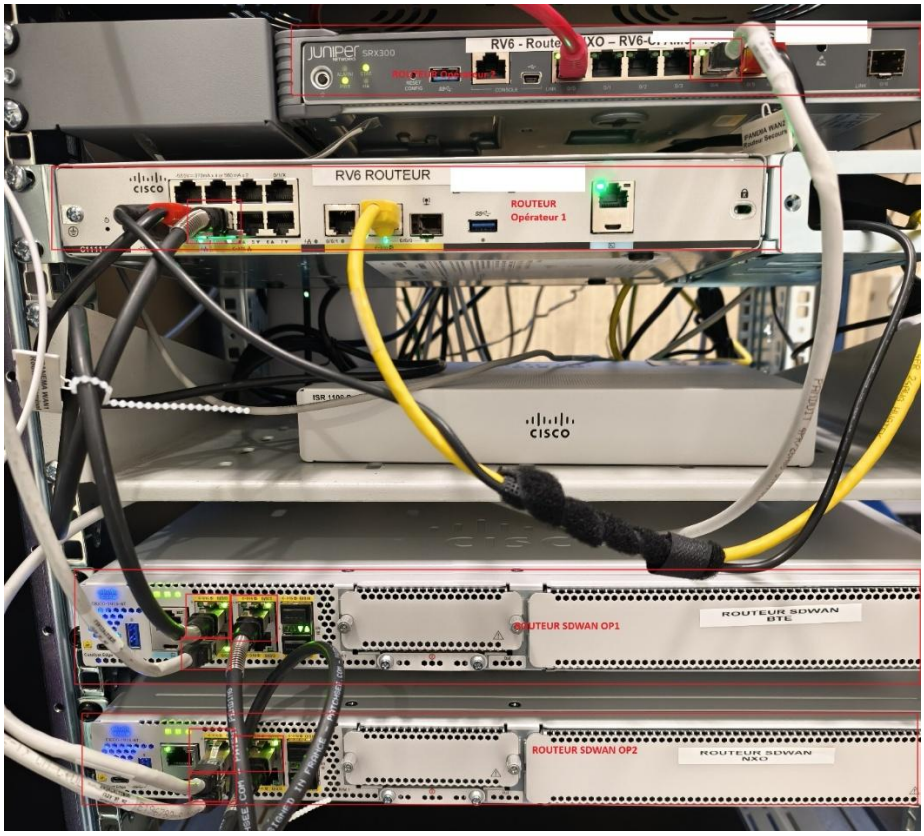
```
Nslookup <nom_sdwan_slave
```

```
C:\Users\collet>nslookup
Serveur :
Address:

Nom :
Address:

C:\Users\collet>nslookup
Serveur :
Address:

Nom :     -privas-master-8300
Address:
```

2) Câblage physique

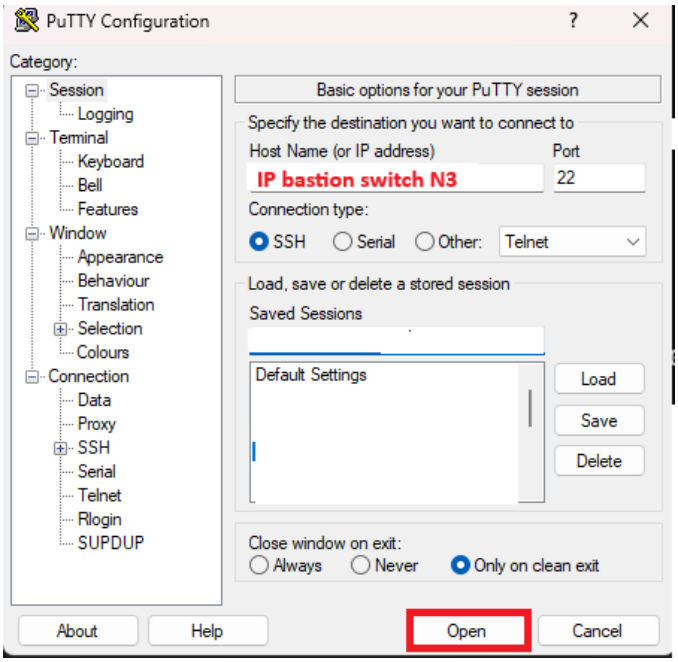
Avec des câbles croisés catégories 6a pour le lien slave master et des routeurs vers les liens NXO / BTE :

- Liaison Back To Back (Port gi0/0/2 Rtr Sdwan Master <-> Port gi0/0/2 Rtr Sdwan Slave)
- Liaison Wan depuis le Routeur SDWAN Master port gi0/0/0 vers le Routeur Opérateur 1 Port Gi0/3
- Liaison Wan depuis le Routeur SDWAN Slave port gi0/0/0 vers le Routeur Opérateur 2 Juniper Port Gi0/4
- Liaison Lan depuis le Routeur SDWAN Master port Gi0/0/1 vers le switch N3 du site Port à définir libre
- Liaison Lan depuis le Routeur SDWAN Backup port Gi0/0/1 vers le switch N3 du site Port à définir libre soit le deuxième si existant soit un deuxième port libre



3) Configuration port switch N3

Pour ceci, j'accède via PuTTY en SSH au bastion du switch N3 de la CPAM de Privas :




```
System-view

Interface GigabiteEthernet1/0/x
port link-mode bridge
description SDWAN-OP1 NXO
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan x
undo stp enable
no shutdown

Interface GigabiteEthernet2/0/x
port link-mode bridge
description SDWAN-OP2 BTE
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan x
undo stp enable
no shutdown
```

Nous communiquons maintenant la configuration des switches et le branchement des routeurs au CSH.

4) Vérification SWITCH N3

Puis :

Show interface vlan

```
Vlan-interface3:
Current state: UP
Line protocol state: UP
Description: INT-VLAN-SDWAN
Bandwidth: 10000000 kbps
Maximum transmission unit: 1500
Internet address:                    (primary)
IP packet frame type: Ethernet II, hardware address:
IPv6 packet frame type: Ethernet II, hardware address:
Last clearing of counters: Never
```

L'interface VLAN est bien créée et opérationnelle

Show vlan brief

```
ID vlan     SDWAN                                GE1/0/[redacted]  GE2/0/[redacted]
```

Le Vlan est bien configuré pour les ports correspondant aux routeurs C8300.

Show interface brief

```
GE1/0/1                  UP    1G(a)    F(a)    T    1    SDWAN-OP1
GE2/0/1                  UP    1G(a)    F(a)    T    1    SDWAN-OP2
```

5) Vérification routeurs

Le ping va me permettre de vérifier d'une part la bonne connexion réseau des routeurs.

Ping <ip SDWAN master>

```
C:\Users\collet[redacted]>ping [redacted]

Envoi d'une requête 'Ping'  [redacted] avec 32 octets de données :
Réponse de [redacted] : octets=32 temps=21 ms TTL=254
Réponse de [redacted] : octets=32 temps=21 ms TTL=254
Réponse de [redacted] : octets=32 temps=21 ms TTL=254
Réponse de [redacted] : octets=32 temps=21 ms TTL=254

Statistiques Ping pour [redacted]:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 21ms, Maximum = 21ms, Moyenne = 21ms
```

Ping <ip SDWAN slave>

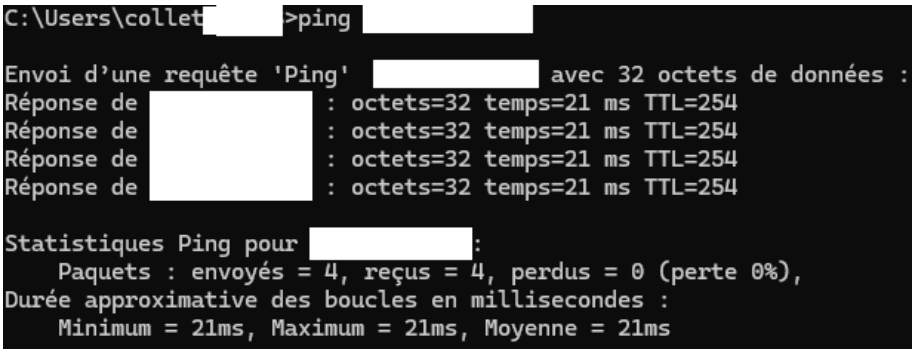
```
C:\Users\collet[redacted]>ping [redacted]

Envoi d'une requête 'Ping'  [redacted] avec 32 octets de données
Réponse de [redacted] : octets=32 temps=17 ms TTL=254
Réponse de [redacted] : octets=32 temps=14 ms TTL=254
Réponse de [redacted] : octets=32 temps=15 ms TTL=254
Réponse de [redacted] : octets=32 temps=15 ms TTL=254

Statistiques Ping pour [redacted]
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 14ms, Maximum = 17ms, Moyenne = 15ms
```

Les deux routeurs sont joignables.

6) Après contact CSH

Vérification de l'accessibilité des autres sites de la CPAM Ardèche (et donc des tunnels) :

Ping <ip_serveur_bureautique_annonay>



Tentative d'accès aux fichiers de bureautiques partagés aux sites distants de l'organismes CPAM Ardèche : OK.

De même pour les accès distant aux serveurs de la CPAM Loire (donc site distant autre organisme).

Rapport de tests

Les tests sont effectués de manière systématique sur chaque site déployé, selon la procédure de test définie et sont inclus dans la mise en place.

Rapport de déploiement

Le déploiement de la solution SD-WAN sur le site s'est déroulé conformément à la procédure établie.

Déroulement de l'intervention

L'intervention a été planifiée un vendredi soir à 19h00, après la fermeture des bureaux, pour minimiser l'impact sur les utilisateurs. Deux techniciens étaient présents pour effectuer le rackage et le câblage des équipements.

Validation post-déploiement

Suite au déploiement, l'ensemble des tests de validation a été effectué avec succès :

- Connectivité réseau validée vers tous les sites distants
- Applications métier accessibles et fonctionnelles

Bilan

Conclusion

Le projet de déploiement de la solution Cisco SD-WAN au sein de la CPAM Ardèche constitue une transformation majeure de l'infrastructure réseau. Cette migration s'inscrit dans une démarche de modernisation globale visant à améliorer la performance, la sécurité et la simplicité de gestion du réseau étendu.

Les objectifs fixés en début de projet ont été atteints avec succès. La solution SD-WAN a permis de remplacer efficacement l'infrastructure IPANEMA arrivée en fin de support, tout en apportant des fonctionnalités supplémentaires significatives. Le routage intelligent basé sur les performances en temps réel optimise l'utilisation des liens WAN et garantit la qualité de service pour les applications critiques.

Ce projet représente une avancée stratégique pour la CPAM, positionnant l'organisme sur une infrastructure réseau moderne.

Auto-évaluation

Ce projet m'a permis d'approfondir mes compétences techniques dans le domaine des réseaux étendus et des technologies SD-WAN. La complexité du projet, impliquant la coordination entre multiples acteurs (Direction Régionale, CSH, sites locaux), m'a confronté aux réalités du travail en environnement professionnel.

Points positifs

- **Compréhension approfondie des architectures SD-WAN :** j'ai développé une maîtrise des concepts fondamentaux (overlay/underlay, routage dynamique) et de leur application concrète dans un environnement de production
- **Rigueur méthodologique :** la réalisation d'une analyse comparative structurée des solutions disponibles, suivie d'un déploiement méthodique par phases, a renforcé mon approche professionnelle des projets d'infrastructure

Compétences développées

Au-delà des aspects techniques, ce projet a renforcé ma capacité à travailler en équipe, à communiquer efficacement avec différents niveaux d'interlocuteurs (techniciens, direction, utilisateurs) et à gérer des situations nécessitant adaptation et réactivité.

Cette expérience constitue un atout majeur pour ma future carrière dans le domaine de l'administration des systèmes et réseaux, en me dotant d'une compréhension concrète des enjeux et des technologies qui transforment actuellement les infrastructures réseau d'entreprise.