Dossier d'architecture

H4413

11 mai 2011

Table des matières

1 Architecture de la solution

L'AIPRAO dispose de 3 site à interconnecter :

Le **site central**,

Le **site GE**,

Le **site de Roanne**.

1.1 Interconnexion

Les sites du réseau de la Doua sont interconnectés via le réseau de campus ROCAD géré par les DSI des établissements du campus et le CISR.

L'interconnexion avec le site de Roanne est réalisée via le réseau du campus géré par la DSI de l'université de St Étienne.

Chacun des réseaux de campus est relié à RENATER.

Les différents sites communiqueront grâce à un VPN.

Les automates programmables, pour ne pas polluer le réseau avec leur broadcast, seront isolés dans un VLAN. La configuration de ce VLAN se fait en utilisant le système de *tags* des ports, permettant de faire passer toutes les informations concernant les VLAn d'unswitch à l'autre en utilisant qu'un seul câble de connexion entre chaque switch, et non pas un câble par réseau.

1.2 Site central (cf. figure 1)

Le **site central** est situé bâtiment Jaquard sur le campus de la Doua à Villeurbanne. Il peut intégrer plusieurs plateformes industrielles (jusqu'à 12 plateformes (ou «plaques») de 5 équipements).

1.3 Site GE (cf. figure 2)

Le **site GE**, situé lui aussi sur le campus de la Doua, bâtiment Ferrié, dispose d'un serveur vidéo et de 4 automates programmables.

1.4 Site de Roanne (cf. figure 3)

Le **site de Roanne**, disposant d'una salle hébergeant des plateformes d'automates programmables et d'un serveur Windows.

Site central (bâtiment Jaquard)

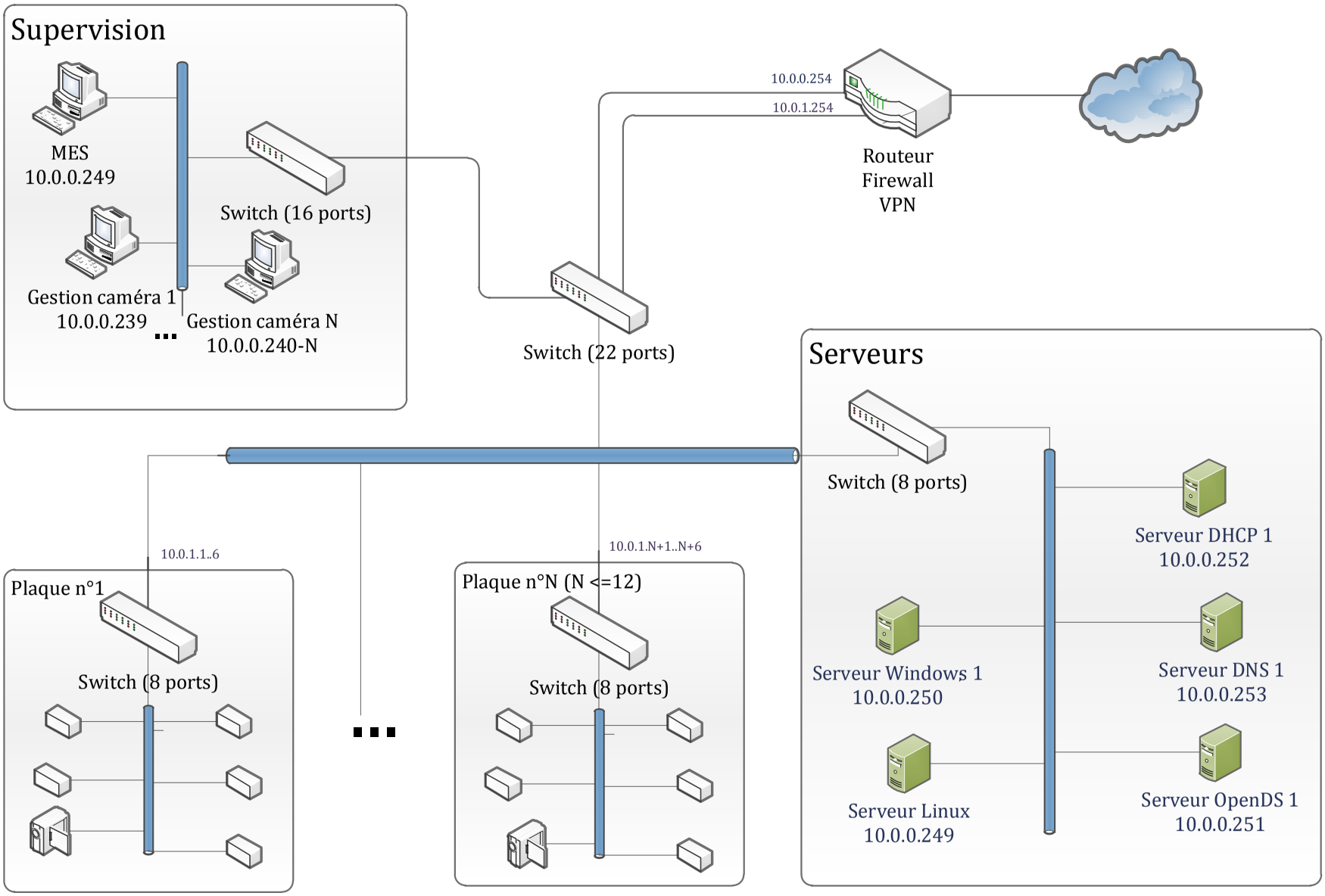

FIGURE 1: Architecture du site central

Site GE (bâtiment Ferrié)

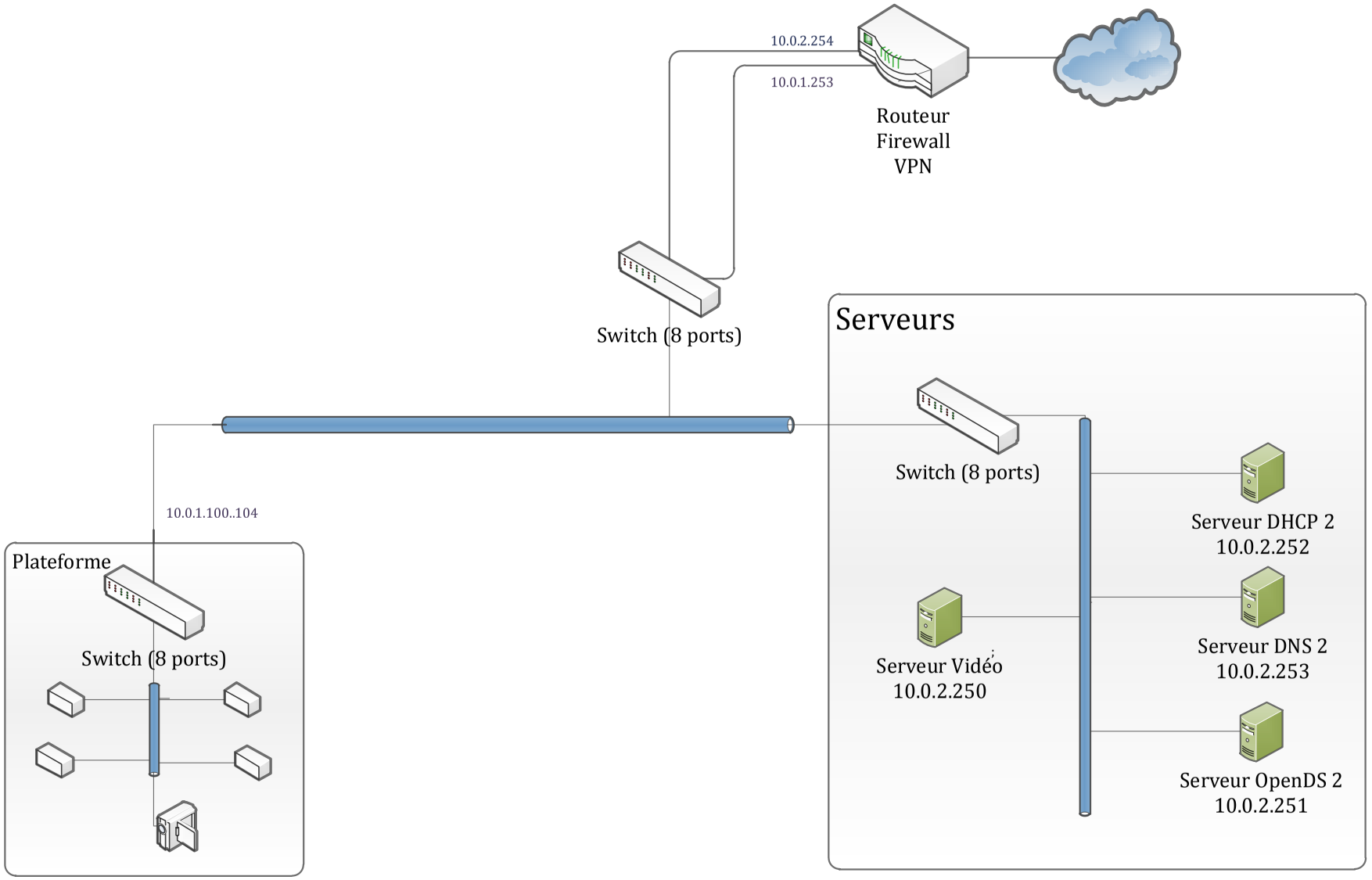

FIGURE 2: Architecture du site GE

Site de Roanne

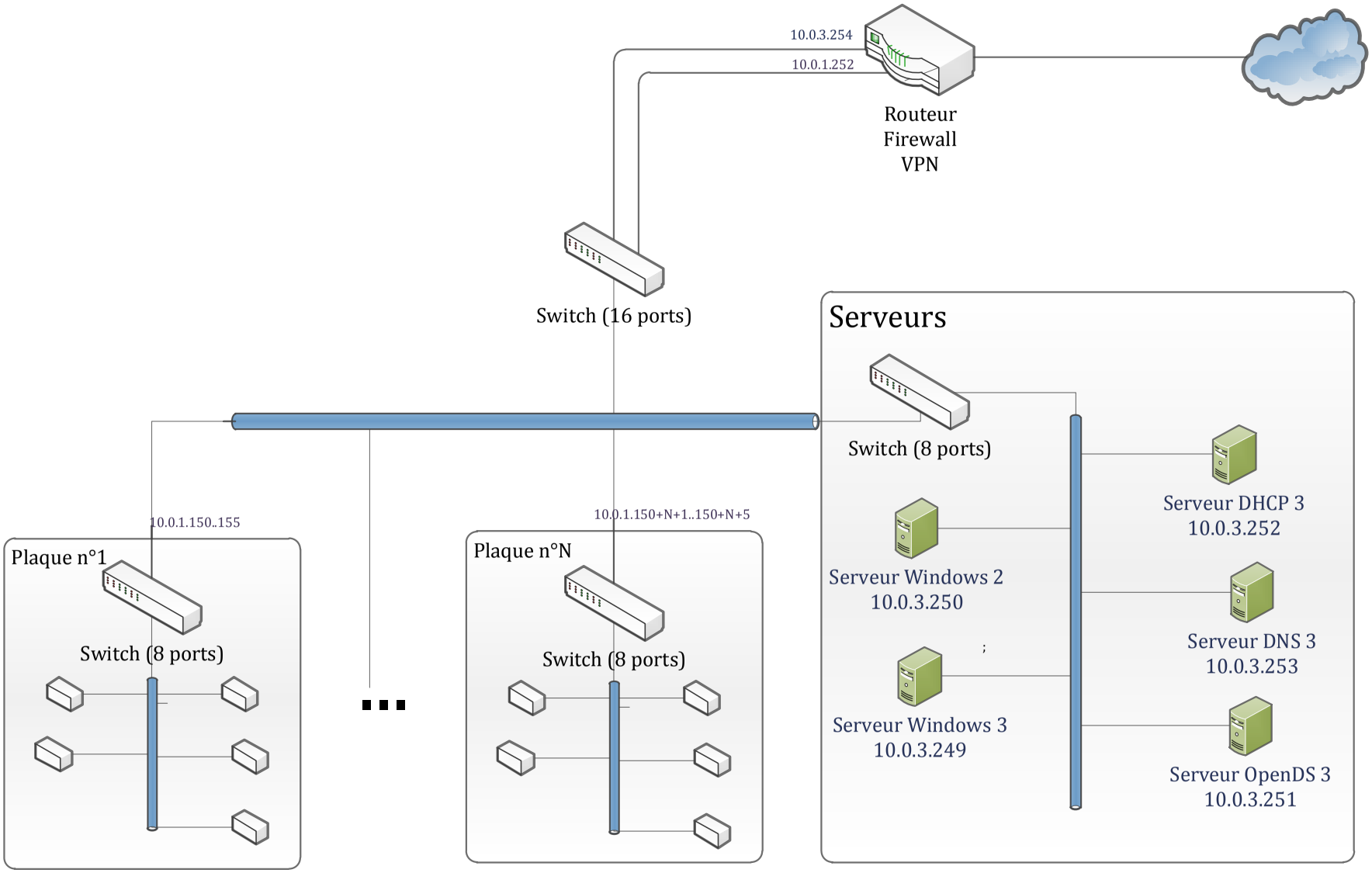

FIGURE 3: Architecture du site de Roanne

2 Solution

La problématique consiste à restructurer l'architecture d'un réseau inter-établissement (réseau industriel et réseau de gestion) afin de permettre de déplacer facilement des équipements d'un établissement à un autre et de pouvoir limiter la pollution du réseau lors du broadcast des variables globales des différents équipements industriels.

Dans une première ébauche de l'architecture, nous avions opté pour un VLAN(Réseau Local Virtuel, regroupant un ensemble de machines de façon logique et non physique) de niveau 3 afin de pouvoir broadcaster les variables globales sur les différents VLAN des établissements. Cependant, compte tenu des contraintes matérielles imposées par le cahier des charges, nous avons dû modifier l'architecture étant donné que les équipements réseau imposés par le client ne supportent pas le VLAN de niveau 3, mais seulement celui de niveau 2 (également appelé VLAN MAC, ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station).

Les avantages d'utiliser un VLAN : plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées Réduction de la diffusion du trafic sur le réseau

Ces contraintes vont avoir un impact important sur l'organisation du réseau puisque chaque VLAN sera alors isolé, le broadcast des variables globales vers le réseau d'un autre établissement ne sera alors plus possible. Les utilisateurs pourront accéder à distance aux réseaux des établissements en utilisant la fonction RAS (Remote Access Service) des routeurs qui permettent d'établir une connexion sécurisée à distance via le réseau téléphonique, en fonction des droits attribués par le firewall.

3 Nouvelle architecture matérielle

Matériel à acquérir :
Afin de répondre à la problématique, les équipements réseaux suivant ont été retenus :

Routeur S@n 2000 Rôle : interconnexion de tous les équipements locaux et liaison VPN pour les équipements distants, pare-feu.
Lieu : un par site
L'achat d'un routeur est discutable. En effet, les fonctionnalités de routeur n'étaient pas indispensables à la mise en place d'un réseau VPN (on aurait pu opter pour une solution de serveur VPN logiciel, sur serveur dédié ou sur un serveur préexistant). Cependant, la matérialisation du réseau de l'AIPRAO est plus élégante. En outre, la majorité des équipements sont situés au même emplacement que ce routeur, et le fait que ces connexions ne soient pas cryptées et encapsulées dans un tunnel VPN ne peut qu'améliorer les performances de l'ensemble. A fortiori, ce routeur représente un excellent compromis entre sécurité et simplicité d'administration, étant données les conditions d'utilisation et de maintenance du réseau de l'AIPRAO : faible criticité des données véhiculées, exigeances de disponibilité modérées, compétences informatiques modérées de l'administrateur habituel.

Switch administrable 8 ports TCS ESM 083F23F0 Rôle : Relier tous les équipements d'une même plateforme
Débit : 10 Base-T / 100 Base-TX

Switch administrable 16 ports TCS ESM 163F23F0 Rôle : Relier plusieurs équipements à l'intérieur d'une des trois salle de l'AIPRAO
Débit : 10 Base-T / 100 Base-TX
Fonctionnalité : Client FDR, SMTP V3, SNTP, filtrage multicast d'optimisation du protocole Global Data, configuration par accès Web VLAN, IGMP Snooping, RSTP (Rapide Scanning Tree Protocol), port prioritaire, controle des flux, port sécurisé.

Switch administrables 22 ports TCS ESM 243F2CU0 Rôle : Relier tous les équipements du site central
Débit : 10 Base-T / 100 Base-TX

Eventuellement, il faudra également acquérir des cartes réseaux supplémentaires pour les PC des plateformes, puisque chaque PC de plateforme devra être muni de deux cartes réseau.

4 Mise en place du VPN

Côté serveur , le la gestion du VPN est déléguée au routeur du site central. La documentation de cette fonctionnalité du S@n2000 étant indisponible sur internet, il convra de se renseigner auprès de Schneider lors de l'achat afin de prendre connaissances des modalités de configuration.

Côté client , le script de démarrage sera modifié afin de se connecter automatiquement au serveur VPN. Le client VPN devra être également fourni par Schneider, puisqu'il n'existe pas de client VPN libre. L'appel au client VPN se fera après l'établissement d'une connexion réseau sur le réseau local.

Rappelons que les ordinateurs localisés dans le site principal se connecterons directement au réseau de l'AIPRAO, et ne devront donc pas lancer ce client au démarrage. Si les administrateurs système souhaitent déployer un unique script pour tout le parc, on pourra par exemple leur conseiller de tester l'adresse IP de l'interface réseau dans leur script. Si cette IP appartient à la plage réservée aux équipements de l'AIPRAO, cela signifie que l'ordinateur est sur le site principal, et qu'il n'y a pas besoin de lancer le client VPN. Dans le cas contraire, il faut lancer le client VPN afin de se connecter au réseau à distance.

La mise en place d'un serveur d'authentification pour accéder aux service de l'AIP est également indispensable. Sa mise en oeuvre sort toutefois du cadre de cette étude, comme spécifié dans le cahier des charges fonctionnel.