MISE EN PLACE DE POLITIQUE DE SECURITE

Merci de trouver ci-dessous l'architecture globale ains que les flux qui y transitent. Cette architecture est divisée en deux groupes :

- Le **Réseau Internet** (LAN) ;
- Et **Reseau avec l'Extérieur** (partenaire télécoms, interco avec nos filiales, accès nomade et accès à la connexion Internet).

Nous sollicitons votre expertise afin de nous accompagner à mettre les bons équipements qu'il faut pour assurer tant la sécurité des ressources reseau ainsi que le dimensionnement (fluidité de la bande passante).

1- Réseau Interne

Le réseau Interne est subdivisé en VLAN en fonction des différents départements. Les serveurs aussi se trouvent dans un VLAN. Ce sont ces ressources à qui nous souhaitons apporter une haute sécurité et ne laisser accéder que les profiles ou plage d'adresse souhaitée.

2- Réseau Externe :

a- Partenaire télécoms

Les partenaires télécoms sont nos clients donneurs d'ordre. Dans le cadre de notre prestation de services, ils nous ouvrent l'accès à une partie de leur réseau afin d'accéder à certaines applications. L'accès se fait via **http** et **https**. Les adresse IP de ces applications sont connus. Les règles de politique non exhaustives que nous souhaitons :

- Permettre uniquement certaines adresses ou plage d'adresse à accéder à sur notre LAN ;
- Possibilité d'autoriser spécifiquement un ou des protocoles d'accéder à notre LAN ;
- Interdire l'accès à notre LAN aux adresses ou autres protocoles en dehors de ceux qu'on a autoriser ;
- Historique de toutes les transactions (qui et à quoi) ;

- Monitoring du taux d'utilisation des liaisons ainsi que la QoS
- Etc…

b- Interconnexion avec nos différentes filiales :

Nous avons plusieurs filiales et nous souhaitons les interconnecter par VPN site à site. Le but est de nous permettre d'accéder à des ressources et vice versa. Le BENIN étant le siège, il y a certaines applications dont les utilisateurs se trouvant dans ces filiales doivent accéder. Pour cela, nous souhaitons :

- Possibilité d'autoriser uniquement certaines adresses vers des serveurs spécifiques (tout ne monde ne doit pas accéder à tout).
- Mettre en place des serveurs en DMZ ;
- Avoir l'historique de toutes les transactions (qui, quand et à quoi) ;

c- Accès Nomade :

L'accès nomade concerne nos utilisateurs en déplacement mais qui doivent accéder aux ressources de l'entreprise.

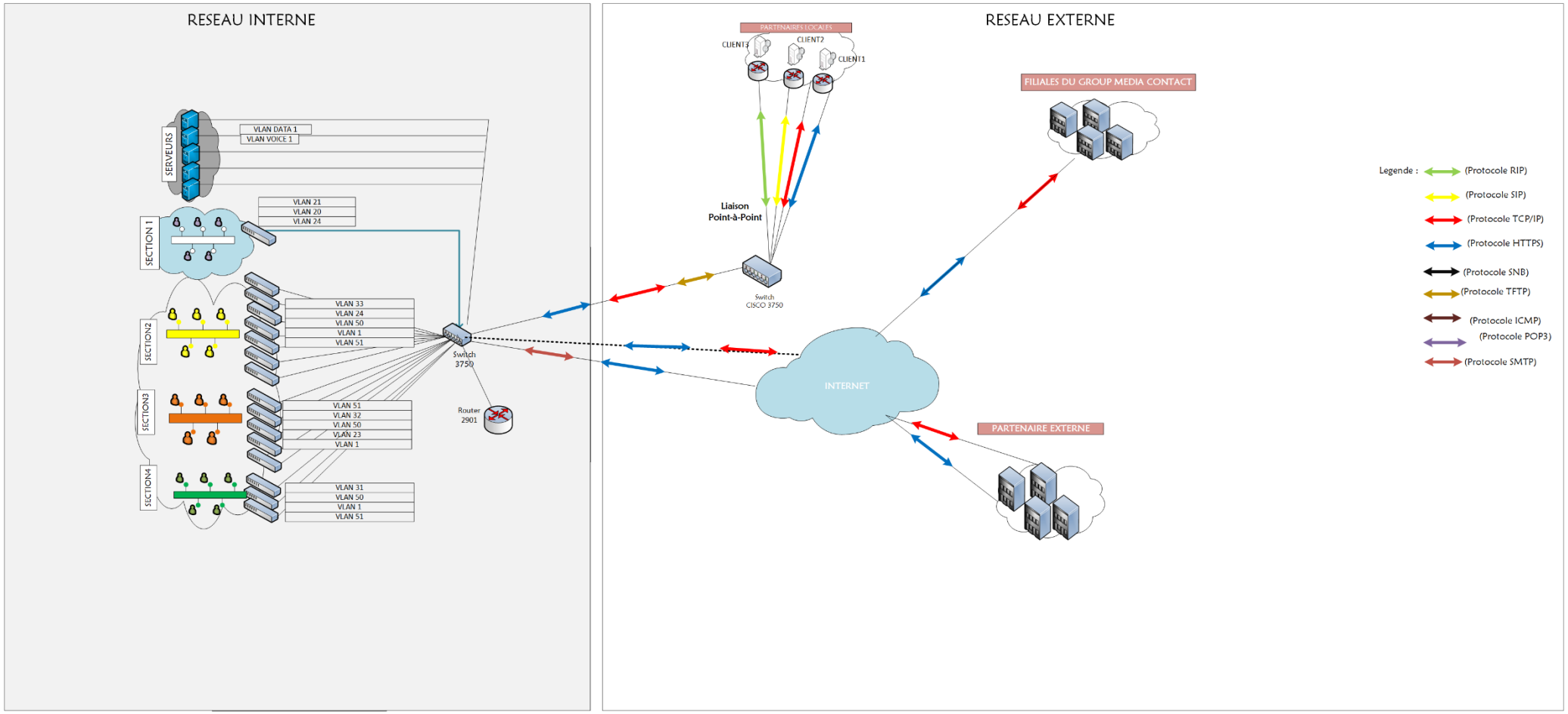
- Nous souhaitons avoir des différents profils en fonction des droits d'accès à donner aux utilisateurs (Agents – Superviseurs – Administration – Support) ;
- En fonction de chaque profil définir aux ressources réseaux à accéder ;
- Permettre une double authentification (user local à ASA + user LDAP) ;
- Possibilité d'accéder aux applications de nos partenaires ;
- Définir différents niveaux d'accès à l'équipement ASA pour l'equipe IT (Observateur - Admin – et SuperAdmin) ;
- Mise en place de certains serveurs dans une DMZ ;
- Historique de toutes les transactions (qui, quand et à quoi) ;
- Monitoring en temps réel ;
- Etc...

d- Accès Internet :

Nous disposons de deux liaisons Internet (FAI). Le but est de permettre aux utilisateurs du réseau LAN d'accéder à Internet à partir d'un FAI précise (soit FAI 1)

- Possibilité de créer des profits et définir la bande passante à octroyer ;
- Permettre ou refuser le streaming en fonction du profil ;
- Permettre ou refuser l'accès à un site spécifique à un profil ;
- Historique de toutes les transactions (qui, quand et à quoi) ;
- Monitoring en temps réel ;

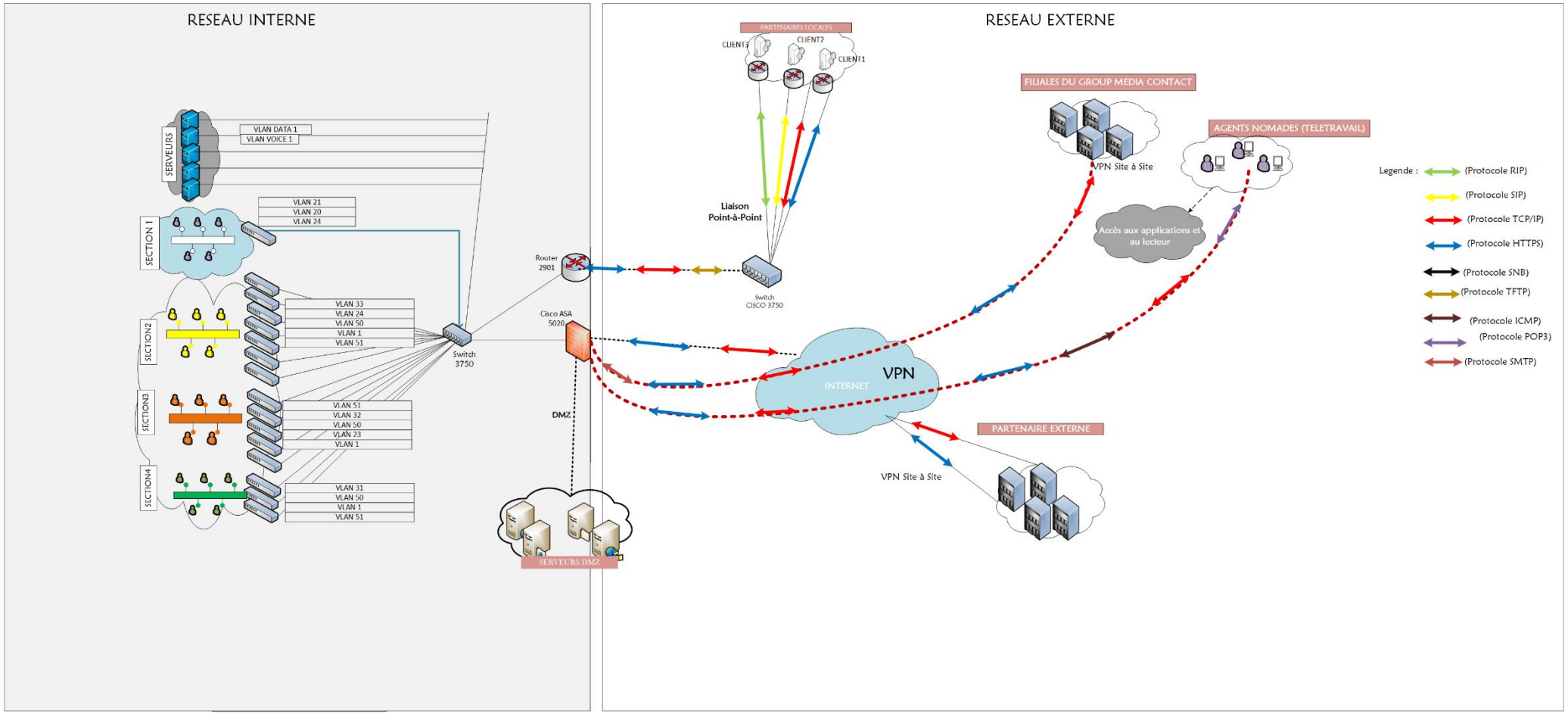
ARCHITECTURE RESEAU EXISTANT



ARCHITECTURE RESEAU EXISTANT

MEDIA CONTACT Bénin

ARCHITECTURE RESEAU CIBLE



ARCHITECTURE RESEAU CIBLE