**VPN :**

Le protocole de chiffrement IPSec offre un cryptage des données pour les liaisons intersites fonctionnant avec un échange de clés entre les sites connectés, grâce à cette technologie les données échangées seront chiffrées et protégées

**Harmonisation des adresses :**

Les réseaux seront facilement identifiables grâce au numéro du site (respectivement 1 pour le site A, 2 pour le site B, 3 pour le site C et 4 pour la DMZ du site C) qui sera représenté par le 3e octet de l’adresse IP.

**Redondance – Haute disponibilité**

Les serveurs seront doublés et synchronisés avec le site B afin de pallier à tout incident matériel.

Les cartes réseaux fonctionneront en IP Bonding pour assurer la haute disponibilité des données

**Le partage réseau**

Le partage réseau se fera en DFS, cette technologie

* Bonjour à tous,
* OpenVPN existe depuis 18ans, on pense qu'il est fortement sécurisé, sauf que pour l'être, il faut bien choisir une suite cryptographique et modifier quelques paramètres par défaut.
* Il est surtout beaucoup utilisé car plutôt simple à mettre en oeuvre et du fait de son antériorité, bien connu dans le métier.
* Même si IPsec est plutôt recommandé pour des connexions site à site, il est également capable de faire du Road Warrior, il faudra préféré IKEv2 (protocole plus récent) et une suite cryptographique correcte (voir recommandations de l'ANSSI en fin de mail).
* L'autre raison de préférer IPsec est qu'il agit sur la couche 3 du modèle OSI alors qu'OpenVPN agit à partir de la couche 4. Ainsi la surface d'attaque est moindre avec IPsec
* **Afin d'approfondir les aspects sécuritaires liés à OpenVPN, voici quelques liens :**
* <http://www.dsih.fr/article/3158/chiffrement-compression-revisons-nos-configurations-openvpn.html>
* <https://lafibre.info/cryptographie/tls-1-0/>
* En effet, le chiffrement utilisé par défaut SHA1 est a éviter, par ailleurs, TLS en version 1.0 (très dangereux) est utilisé.
* Enfin, nous pourrions évoquer la compression LZO activé par défaut, ce qu'il faut éviter.
* Il faut donc forcer à la main les configurations.
* **Voici un exemple de configuration d'un fichier .opvpn côté client.**
* dev tun
* persist-tun
* persist-key
* **cipher AES-256-CBC**
* **auth SHA384**
* tls-client
* client
* resolv-retry infinite
* remote "votre reseau" "port" tcp-client
* verify-x509-name "nom certificat" name
* auth-user-pass
* pkcs12 pfSense-TCP-1194-xxxx.p12
* tls-auth pfSense-TCP-1194-xxxx-tls.key 1
* remote-cert-tls server
* **comp-lzo no**
* **tls-version-min 1.2**
* **auth-nocache**
* **2 guides de l'ANSSI :**
* <https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/>
* <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-ipsec-pour-la-protection-des-flux-reseau/>