

V P N

Offre Topnet

Répartition géographique de votre entreprise et importance du travail collaboratif

Au terme de l'évolution de son activité, votre entreprise se trouve structurée en plusieurs filiales. Vous avez aussi réussi à conclure des partenariats avec des compagnies étrangères. Outre les agents résidents au niveau de vos différents locaux, vous avez déployé sur terrain plusieurs représentants commerciaux et techniciens de support et de maintenance. Du fait de cette grande répartition géographique caractérisant les différentes structures impliquées dans votre commerce, que l'on conjugue à la mobilité accrue de certains de vos agents, vous ressentez le besoin de fédérer le tout en un grand réseau de données qui rendrait possible la mise en oeuvre d'une solution de travail collaboratif, l'accès à des applicatifs ou bases de données centralisés ou l'instauration d'une politique de sauvegarde centralisée ou de disaster recovery entre autres. Mais ce réseau devrait être aussi sécurisé que possible pour ne pas compromettre l'intégrité ou la confidentialité des flux échangés à travers ce grand réseau.

inadéquation des solutions de connexion par liaisons physiques dédiées

Vous pensez alors à des connexions spécialisées entre toutes les filiales. Vous vous rendez tout de suite compte de la complexité d'une telle solution, vu que ces raccordements coûtent cher, dépendent du nombre de filiales que vous allez connecter, ne sont pas pratiques pour les utilisateurs itinérants et sont tout simplement inconcevables pour les partenaires étrangers.

inadéquation des solutions de connexion par liaisons physiques dédiées

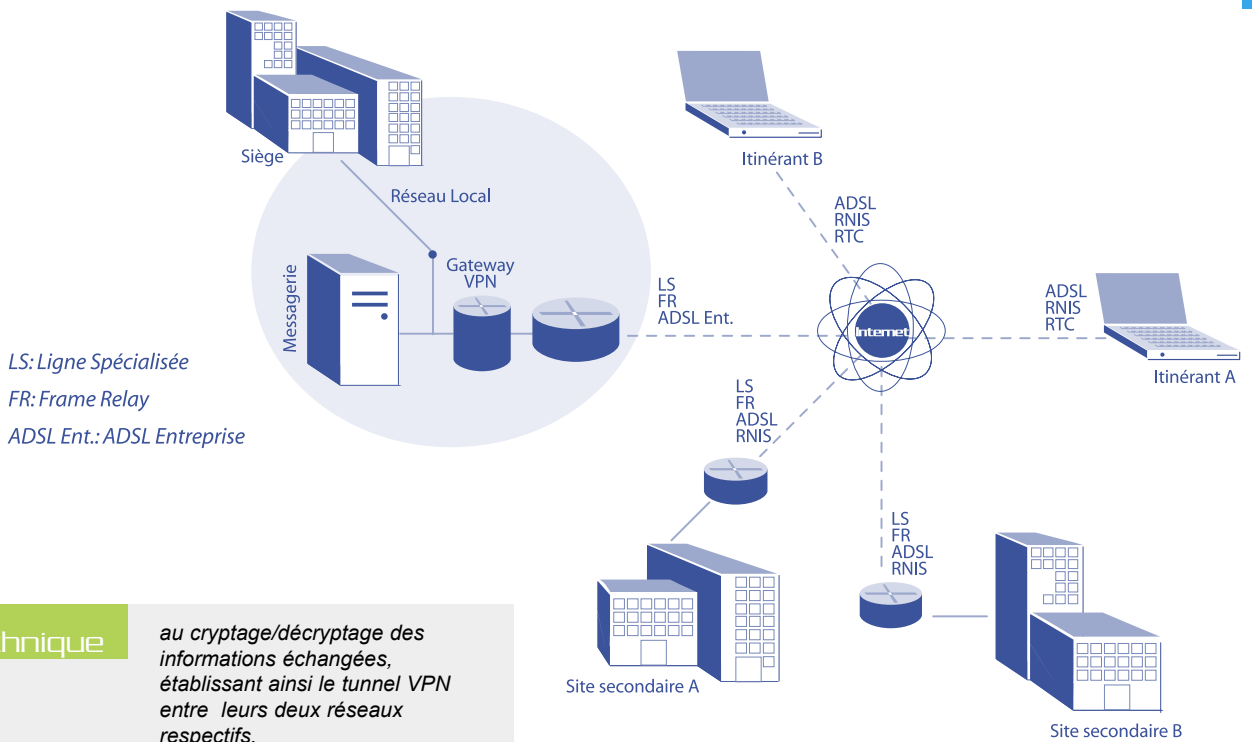
Vous pensez alors à des connexions spécialisées entre toutes les filiales. Vous vous rendez tout de suite compte de la complexité d'une telle solution, vu que ces raccordements coûtent cher, dépendent du nombre de filiales que vous allez connecter, ne sont pas pratiques pour les utilisateurs itinérants et sont tout simplement inconcevables pour les partenaires étrangers.

Solution de Connexion sécurisée sur le réseau public internet : les VPNs

Vous vous tournez alors vers l'alternative d'utiliser le réseau public internet pour connecter les locaux et les utilisateurs nomades, mais vous vous préoccupez pour la sécurité des échanges qui vont avoir lieu sur un tel réseau. Les VPNs (Virtual Private Network) ou réseaux privés virtuels se présentent alors comme solution à ce dilemme.

Le VPN consiste en une plateforme offrant différents mécanismes de cryptage et d'authentification pour pouvoir relier vos différents locaux et télé-travailleurs en un seul réseau "virtuellement" privé en utilisant l'infrastructure de connexion publique internet, ce qui présente des avantages financiers et fonctionnels majeurs par rapport au raccordement point à point des différentes filiales par liaisons privées.





Memento technique

VPNs IPSec

IPSec est un standard pour sécuriser des échanges IP en cryptant et/ou en authentifiant les paquets IP. IPSec offre la sécurité au niveau de la couche réseau du modèle OSI. Il englobe un ensemble de protocoles de cryptage pour la confidentialité des paquets et des mécanismes d'authentification au niveau de l'échange des clés de cryptage.

Architecture de déploiement des VPNs IPSec

Pour chaque réseau local afférent à une filiale de votre entreprise, il sera mis en place un dispositif IPSec. Quand il y a échange entre deux membres de deux filiales différentes, les deux unités IPSec responsables doivent tout d'abord s'authentifier mutuellement, par le moyen du protocole cryptographique ISAKMP (Internet Security Association and Key Management Protocol) servant de base pour l'authentification IKE (Internet Key exchange). A l'issue de cette phase, une SA (ou Security Association) sera établie pour chaque sens de communication. Une SA décrit un flux sécurisé des données entre deux passerelles VPN et inclut les différents clés et algorithmes de cryptage nécessaires pour s'assurer de l'identité des deux entités IPSec et pour pouvoir initier l'opération de cryptage/décryptage des différents flux de données entrant en jeu. Les deux passerelles VPN procéderont par la suite

au cryptage/décryptage des informations échangées, établissant ainsi le tunnel VPN entre leurs deux réseaux respectifs.

Avantages Fonctionnels des VPNs

Connectivité: Le fait d'avoir à disposition un réseau privé virtuel vous permet de travailler dans un réseau "virtuellement" local : en effet, visioconférence, téléphonie, ERPs, sauvegardes, sites de secours, ... Tout peut être désormais mis en place à l'échelle de l'entreprise à moindre coût et avec une sécurité et fiabilité accrues. De plus, la facilité pour un travailleur nomade de venir rejoindre ce réseau ouvre de nouveaux horizons : Les agents sur terrain pourront désormais accéder aux applicatifs de l'entreprise alors qu'ils sont en mission, les employés pourront avoir accès à leur documents à partir de chez eux ...

Facilité de mise en oeuvre: En reposant sur des connexions internet haut débit pour connecter vos locaux, les efforts et coût de mise en place sont minimes. Contrairement aux infrastructures de réseaux privés qui offrent un faible débit et sont en général assez chères, le VPN vous permet de tirer profit de vos connexions internet déjà établies pour connecter vos différents locaux. Ceci est d'autant plus vrai que maintenant il est très facile d'avoir, à l'entreprise comme chez soi, des connexions internet à haut débit et permanentes grâce à l'ADSL, notamment.

Cryptage des données

cryptage ?

Le cryptage est une fonction de brouillage de données destinée principalement à garder la confidentialité d'une correspondance qu'on veut secrète. On associe à une opération de cryptage spécifique une valeur particulière qu'on garde secrète et dont la connaissance permet de déchiffrer un message brouillé. Il s'agit de la clé de cryptage. Plusieurs algorithmes de cryptage plus ou moins robustes existent, mais la longueur de la clé (ensemble de valeurs possibles) permet pratiquement de déterminer la puissance d'un algorithme particulier, puisque pour déchiffrer un message codé on devra essayer toutes les valeurs. En général, le fait d'utiliser des clés de grande taille et de grande diversité, et le fait d'en changer souvent permet de garder la confidentialité d'un message.

Cryptage symétrique et cryptage asymétrique

On parle de cryptage symétrique ou asymétrique. Dans le premier cas, en symétrique, l'algorithme vient avec une seule clé pour crypter et décrypter un message, et son échange via un réseau public devient dangereux, puisque l'interception d'une clé permet de déchiffrer des messages. Dans le deuxième cas ou cryptage

asymétrique, la fonction de cryptage utilise deux valeurs ou clés complémentaires. Si l'on utilise l'une pour crypter on devra utiliser l'autre pour décrypter. On peut donc émettre l'une des clés sur internet pour que les correspondants puissent crypter des messages à l'intention du détenteur de l'autre valeur. On parle alors de clé publique. L'autre clé, gardée par le tier qui pourra lui seul décrypter des messages cryptés par la clé publique, est appelée privée et ne devra en aucun cas être communiquée par des moyens non sécurisés.

Authentification par cryptographie

Il est possible de s'assurer de l'identité de l'émetteur d'une clé publique en la signant par la clé privée de l'émetteur. si l'on arrive à déchiffrer un message crypté par une clé privée au moyen d'une clé publique, l'émetteur est bien le propriétaire de la clé publique qu'il nous envoie. On parle alors de signature électronique. Il reste maintenant à faire confiance à l'émetteur, même si l'on sait qu'il est bien celui qu'il prétend être. c'est en ce sens qu'interviennent les certificats et les autorités de certification, qui constituent des autorités légales dignes de foi et qui délivrent des certificats constitués par des couples de clé publique/clé privée. Ceci est géré par le protocole PKI ou (Public Key Infrastructure). Un des formats de certificats répandus sur internet est le format X.509

Pour plus d'informations, contactez-nous :

Tunis
75, Av. Kheireddine Pacha
Imm. Pacha Centre, Bloc B, 1^{er} étage - 1073 Tunis
Tél : 71 770 770 - Fax : 71 951 031

Sousse
5, av. Habib Bourguiba, Imm. Ghnima Centre
5^e étage, 4000 - Sousse
Tél : 73 201 000 - Fax : 73 215 35

commercial@topnet.tn

www.topnetpro.com

www.topnet.tn

TOPNET