



Mettre en œuvre un VPN (réseau privé virtuel)

Un VPN (réseau privé virtuel) a pour fonction de faire abstraction des distances et de relier de façon sécurisée à travers Internet les différentes entités d'une entreprise. Ces entités peuvent être des établissements (siège social, agence, dépôts, usines...), des collaborateurs itinérants (nomades) ou travaillant à domicile (télé-travailleurs). Elles peuvent être également des utilisateurs ne faisant pas partie de l'entreprise (partenaires, fournisseurs, clients etc...), étant autorisés à accéder à certaines ressources.

Concrètement, grâce au VPN, les utilisateurs peuvent utiliser, à distance et dans un environnement sécurisé, les logiciels métiers ou les documents, qui sont installés sur le serveur de l'entreprise.

La sécurité des VPN repose sur la mise en place de 2 systèmes :

- l'authentification, qui autorise les 2 entités à communiquer entre elles après avoir été identifiées ;
- et le cryptage, qui rend indéchiffrable les informations échangées à travers Internet, afin qu'elles ne puissent être ni récupérées, ni lues par une personne étrangère à l'entreprise.

Les architectures VPN sont de 3 types :

- le VPN intranet qui permet de connecter de façon permanente les différents établissements de l'entreprise ou les télétravailleurs avec le site principal.
- le VPN nomade qui est une extension du VPN Intranet. Il permet de connecter les utilisateurs nomades aux bureaux de l'entreprise. Ce cas est traité dans la fiche « Sécuriser le nomadisme ».
- et le VPN extranet qui est aussi une extension du VPN intranet. Il permet de connecter les utilisateurs ne faisant pas partie de l'entreprise (partenaires, fournisseurs, clients...). Ce cas est traité dans la fiche « Sécuriser les échanges avec les partenaires ».

Les technologies VPN les plus utilisées sont de 3 types :

- Le VPN IPSEC repose sur la création de tunnels de communication cryptés et étanches construits à travers Internet.
- Le VPN MPLS repose sur la création de tunnels de communication étanches construits à travers le réseau privé du fournisseur d'accès à Internet. Ce dernier maîtrise, gère et sécurise entièrement son réseau privé, qui est physiquement séparé de l'Internet.
- Le VPN SSL permet l'accès sécurisé, à travers Internet, aux logiciels métier sans accéder au reste du réseau interne de l'entreprise. Cette technologie implique que les applications métiers soient webisées c.à.d. accessibles par les navigateurs Internet comme Internet Explorer, Firefox ou Opéra.

Nous allons traiter dans cette fiche 2 cas de VPN intranet. Les VPN nomades et extranet sont quant à eux traités dans les fiches « Sécuriser le nomadisme » et « Sécuriser les échanges avec les partenaires ».

Cas 1 : L'entreprise Encélade désire relier de façon permanente et transparente son siège social à son usine et à ses 2 télétravailleurs, qui sont répartis sur le territoire français. Tous les



utilisateurs doivent travailler dans les mêmes conditions, quelque soit le lieu. De plus l'entreprise n'a ni le temps ni les compétences en interne pour assurer le suivi, le dépannage et le contrôle du VPN.

Cas 2 : L'entreprise Rhéa Services, quant à elle, veut relier ses 2 sites. Elle veut également que ses commerciaux sédentaires, qui travaillent à leur domicile puissent saisir des devis, commandes pour leur clients, visualiser l'état des stocks et imprimer. La solution VPN mise en place est gérée par l'entreprise.

Cas 1 : L'entreprise Encélade

L'entreprise Encélade désire relier de façon permanente et transparente son siège social à son usine et à ses 2 télétravailleurs, qui sont répartis sur le territoire français. Tous les utilisateurs doivent travailler dans les mêmes conditions, quelque soit le lieux. De plus l'entreprise n'a pas le temps ni les compétences en interne pour assurer le suivi, le dépannage et le contrôle du VPN.

Facilité de mise en œuvre : moyenne
Facilité d'exploitation : simple
Hauteur de l'investissement humain : moyenne

La solution technique adoptée par l'entreprise :

- Il a été décidé de déployer un VPN MPLS, fourni par un fournisseur d'accès à Internet. Cela implique l'installation sur chaque site d'un routeur, qui va permettre le trafic VPN inter – sites mais aussi l'accès sécurisé à Internet.
- Installer en complément un pare-feu derrière le routeur d'accès à Internet même s'il est dit que le VPN opérateur protège l'entreprise de toutes les menaces. On se protège ainsi des attaques en provenance de l'intérieur. Ces attaques peuvent en fait être lancées à partir de clés usb ou CD, consultés sur les postes de travail.
- Un serveur Terminal Server Edition (TSE) est installé au siège social. Il a pour fonction de réaliser les opérations à la place des utilisateurs distants, qui utilisent le client TSE intégré par défaut au système Windows 2000, XP et VISTA. Ce système permet le travail à distance sur les logiciels métiers ou les documents, qui sont installés sur le serveur de l'entreprise situé lui aussi au siège social.

Les règles que l'entreprise doit suivre pour mettre en œuvre un VPN.

- Bien dimensionner le débit Internet, c'est-à-dire le " tuyau " dans lequel vont transiter les trafics web et VPN.
- Toujours demander le mot de passe au client TSE, afin d'éviter qu'un pirate ayant pris le contrôle de l'ordinateur se connecte au serveur TSE distant, même s'il ignore le mot de passe de l'utilisateur.
 - Bridier l'environnement de travail des utilisateurs distants (TSE), afin de les empêcher de réaliser des opérations dangereuses sur le serveur TSE, comme l'arrêter ou provoquer des coupures. Cette restriction est possible sur un serveur Windows grâce aux objets de stratégie de groupe (GPO), qui permet d'appliquer des règles de sécurité centralisées.
 - Ces 3 règles doivent être complétées par les recommandations de bases, qui sont énoncées dans la fiche « Protection minimale de son environnement de travail » et qui doivent être appliquées sur tous les



sites de l'entreprise et les postes de travail des télétravailleurs

Cas 2 : l'entreprise Rhéa Services

L'entreprise Rhéa Services, quant à elle, veut relier ses 2 sites de façon permanente. Elle veut également que ses commerciaux sédentaires, qui travaillent à leur domicile puissent saisir des devis, commandes pour leur clients, visualiser l'état des stocks et imprimer. La solution VPN mise en place est gérée par l'entreprise.

Facilité de mise en œuvre : difficile
Facilité d'exploitation : difficile
Hauteur de l'investissement humain : difficile

La solution technique adoptée par l'entreprise :

- Il a été décidé d'installer un concentrateurs VPN sur chacun des 2 sites, derrière le routeur d'accès à Internet, afin de les relier de façon permanente par un tunnel de communication crypté à travers Internet.
 - Sur les postes de travail des télétravailleurs :
 - Un client VPN est installé. Ce client est en fait un logiciel, qui crée à la demande un tunnel de communication chiffré, afin d'assurer la confidentialité des échanges entre le télétravailleur et le réseau interne de l'entreprise. Ce tunnel n'est créé qu'après l'identification de l'utilisateur par la saisie d'un login et mot de passe dans ce client.
 - Le client TSE, intégré par défaut au système Windows 2000, XP et VISTA est également utilisé, afin de permettre le travail à distance sur les logiciels métiers et les documents de l'entreprise.
- Un serveur Terminal Server Edition (TSE) est installé au siège social. Il a pour fonction de réaliser les opérations à la place des utilisateurs distants et d'utiliser les logiciels métier et les documents qui sont installés sur le serveur de l'entreprise situé aussi dans le siège social.

Les règles que l'entreprise doit suivre pour mettre en œuvre un VPN.

- Bien dimensionner le débit Internet, c'est-à-dire le "tuyau" dans lequel vont transiter les trafics web et VPN.
- Toujours demander le mot de passe au client TSE, afin d'éviter qu'un pirate ayant pris le contrôle de l'ordinateur se connecte au serveur TSE distant, même s'il ignore le mot de passe de l'utilisateur.
 - Bridier l'environnement de travail des utilisateurs distants (TSE), afin de les empêcher de réaliser des opérations dangereuses sur le serveur TSE, comme l'arrêter ou provoquer des coupures. Cette restriction est possible sur un serveur Windows grâce aux objets de stratégie de groupe (GPO), qui permet d'appliquer des règles de sécurité centralisées.
- Déployer impérativement sur le site central des outils de surveillance et de contrôle comme des pare-feu réseaux et applicatifs, des détecteurs d'intrusion (IDS, IPS), des antivirus, antispyware, antirootkits, afin de protéger le VPN contre toutes les menaces d'intrusions, de vols ou de corruption.

Remarque : certaines appliances multifonction comme les boîtiers Arkoon ou Netasq embarquent les différentes fonctions de sécurité qui sont nécessaires à la protection d'un système informatique comme le pare-feu réseau et applicatif, la détection et prévention d'intrusion, le filtrage web, le concentrateur VPN, l'antivirus, l'antispyware et l'antispham.

- Superviser et contrôler régulièrement le VPN en utilisant les différents rapports qui peuvent être générés par le pare-feu et le détecteur d'intrusion.
- Toutes ces règles doivent être complétées par les recommandations de bases, qui sont énoncées dans la fiche « [Protection minimale de son environnement de travail](#) » et qui doivent être appliquées sur tous les sites et les postes de travail des télétravailleurs.

Les règles que l'entreprise doit suivre pour sécuriser l'utilisation du client VPN par les télétravailleurs.

- Bloquer les trafics non cryptés comme le trafic Internet et la messagerie, lorsque le tunnel VPN est créé. On empêche ainsi à un pirate d'attaquer par rebond c'est-à-dire de se faufiler à travers le tunnel chiffré et de s'introduire sur le réseau de l'entreprise, à partir d'Internet.
- Ne pas mémoriser le mot de passe de connexion de l'utilisateur et obliger sa saisie. On évite ainsi qu'un pirate qui vole le PC portable ou qui réussit à prendre son contrôle, ne puisse s'introduire dans le réseau interne de l'entreprise.
- Ces 2 règles doivent être complétées par les recommandations de bases énoncées dans la fiche « [Protection minimale de son environnement de travail](#) », qui doivent être appliquées sur les postes de travail des télétravailleurs.