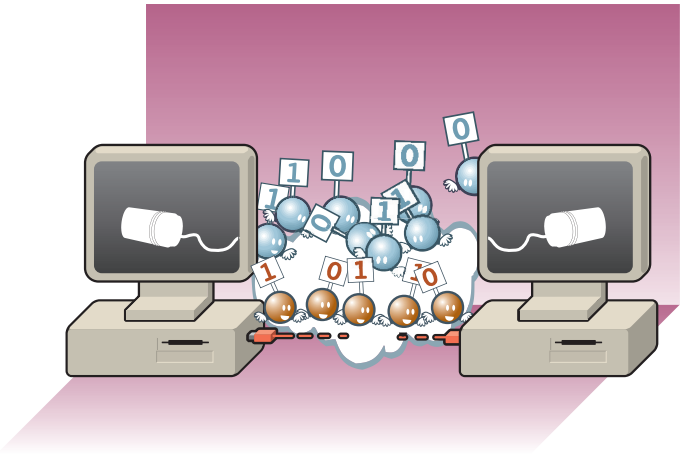
VPN

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

La croissance de l'utilisation d'Internet donne lieu à de nouveaux modes de travail tel que le télétravail, l'échange d'informations privilégiées entre différentes filiales d'une entreprise, ou encore la consultation de sites web et des systèmes informatiques de ses fournisseurs ou clients. En conséquence, une réelle problématique de sécurité liée à ces nouveaux modes de travail est en train d'émerger. Les « Virtual Private Networks » (VPN) peuvent répondre à certains de ces problèmes et sont de plus en plus utilisés. L'objet de cette fiche est de présenter les différents types de VPN existant, mais aussi d'en proposer quelques scénarios d'utilisation.

Table des matières



1 Qu'est-ce qu'un VPN ?

Un Réseau Privé Virtuel (anglais : Virtual Private Network, VPN) est un moyen de communication assurant la sécurité des transferts de données sur des réseaux publics ou partagés (comme la télédistribution ou encore l'ADSL). Un VPN est, en fait, un réseau de communication avec les mêmes paramètres de sécurité qu'un réseau privé. Ses principales caractéristiques sont :

- **Confidentialité des données :** le chiffrement assure que le contenu des données transmises n'est connu que des parties qui échangent l'information. De ce fait, un tiers interceptant le trafic du VPN n'aura pas la possibilité d'en déterminer la teneur.
- **Intégrité des données :** le chiffrement et le hachage assurent que les données reçues au travers du VPN par le destinataire sont identiques à celles envoyées par l'expéditeur : il n'y aura ainsi aucune possibilité, pour une tierce partie, de changer les données en transit dans le VPN.
- **Authentification des utilisateurs du VPN :** pour certains VPN, (dans le cas du télétravail par exemple), il est important de savoir quels sont ceux qui participent au processus afin d'éviter les problèmes de sécurité liés à l'usurpation d'identité et par la même à l'accès illicite aux réseaux privés.

Il existe 3 grands catégories de VPN :

1 VPN pour l'accès à distance :
Ce type de VPN peut être utilisé pour accéder à certaines ressources prédéfinies d'une entreprise sans y être physiquement présent. Cette oportunité peut ainsi être très utile au commercial ou au cadre qui souhaite se connecter au réseau de son entreprise lors d'un déplacement. En général, l'utilisateur de ce type de VPN possède un accès Internet chez un fournisseur d'accès standard (ISP).

2 VPN Intranet :
Ce type de VPN lie plusieurs réseaux internes d'une même entreprise (par exemple les réseaux de plusieurs filiales). Sans VPN, les entreprises seraient forcées d'utiliser des lignes dédiées (« lignes louées ») entre leurs filiales ; procédé très onéreux, surtout lorsqu'il s'agit de lignes internationales. Avec les VPN, ces mêmes communications peuvent passer par l'Internet sans souci de confidentialité ou d'intégrité des transferts, et ce, pour un coût bien moindre.

3 VPN Extranet :
Cette catégorie de VPN est utilisée pour permettre aux clients, fournisseurs, partenaires ou autres interlocuteurs d'accéder à certaines données d'une entreprise. Presque tous les sites « e-commerce » ainsi que les banques offrent ce type de connexion sécurisée à leurs clients.

VPN

2 Comment fonctionne un VPN ?

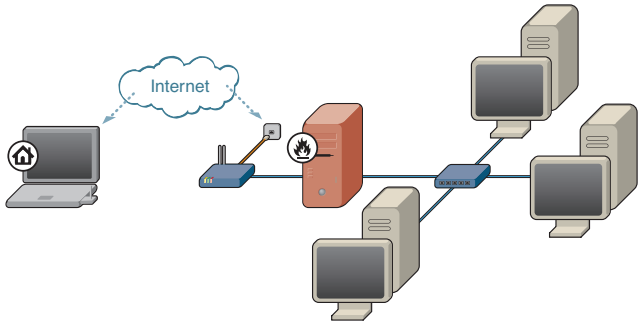
Un VPN utilise la cryptographie pour assurer la confidentialité, l'intégrité et l'authentification des données, même si celles-ci sont envoyées sur l'Internet.

Il existe à ce jour plusieurs standards et implémentations dans les VPN. Afin de mieux appréhender le système dans sa globalité, il est nécessaire d'en présenter les paramètres les plus caractéristiques :

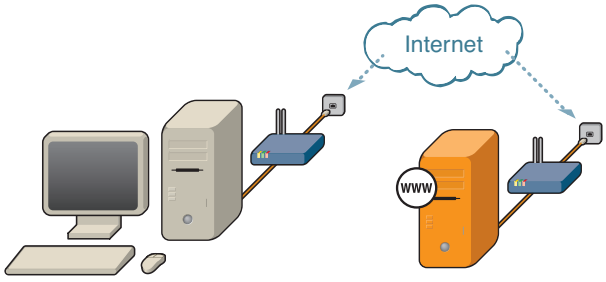
2.1 Tunnel / transport

Le premier critère qui peut être utilisé pour différencier des VPN est la distinction tunnel / transport. De quoi s'agit-il exactement ?

Un VPN tunnel est défini par deux points fixes (« endpoints »), bien que le VPN puisse gérer le trafic entre bien plus d'utilisateurs. Un exemple concret de ce type de VPN serait un télétravailleur devant pouvoir accéder aux ressources d'un réseau interne d'une entreprise ; alors qu'un observateur externe au VPN ne pourrait voir qu'un échange d'informations chiffrées entre les deux endpoints.



Un VPN transport est un tunnel ou les deux « endpoints » sont toujours les 2 mêmes machines. Un observateur pourra donc dans le cas présent, deviner qui communique avec qui.



2.2 Cryptographie

Les VPN utilisent la cryptographie pour garantir leur sécurité dans un environnement pouvant se révéler hostile. La cryptographie est utilisé dans 3 buts précis :

1 **Confidentialité.**
Le chiffrement fort garantit la confidentialité des données. Il existe une panoplie d'algorithmes de chiffrement qui peuvent être utilisés dans les VPN. En général, seuls les algorithmes de chiffrement symétriques sont utilisés pour la protection des données. Les algorithmes les plus connus comme 3DES (« Triple DES ») ou encore AES (le remplaçant du DES) utilisent une clé de 128 bits ou plus (ce qui est considéré comme « secure »).

2 **Intégrité.**
Pour garantir la non-modification des données lors de la transmission par le réseau public, les algorithmes de hachage sont utilisés. Ces algorithmes constituent une signature du contenu de la transmission très difficile à falsifier quand elle est protégée par un des algorithmes de chiffrement mentionnés ci-dessus.

3 **Authentification.**
Envoyer des données avec l'assurance qu'elles resteront confidentielles et qu'elles ne pourront être modifiées est essentiel, tout comme il est primordial de s'assurer de l'identité du correspondant. L'authentification est donc une étape très importante dans l'établissement d'un lien VPN entre deux entités. Il existe bien évidemment plusieurs approches pour établir l'authentification, la plus simple (mais la moins sûre) étant l'utilisation d'un mot de passe (« password »). D'autres alternatives peuvent être l'utilisation d'un « token » qui donne des codes d'accès valables pour une seule et unique connexion, ou encore l'utilisation d'une PKI (« Public Key Infrastructure ») qui utilise des certificats (comparables à une carte d'identité électronique).

2.3 Différents types : SSL-VPN, PPTP, IPsec

Il existe plusieurs standards pour créer des VPN. Ces standards représentent des choix de tunnel ou transport ainsi que des choix de chiffrement et d'authentification.

1 **Le SSL-VPN** est probablement le plus simple, et c'est sans doute le plus utilisé. Il s'agit simplement de sites type « e-commerce » ou « web-banking » offrant à leur clientèle des accès à des données personnelles par navigateur web, protégé par SSL ou TLS (voir la fiche technique HTTPS). Ce type de VPN a l'avantage d'être très convivial à l'utilisation et peut être utilisé par un maximum de personnes puisqu'il ne nécessite pas l'installation de logiciels ou de hardware spécifiques. Les SSL-VPN sont des VPN transport. Il existe des machines dédiées à la tâche de gestion d'accès des utilisateurs par SSL et qui prennent la responsabilité de l'authentification des utilisateurs ;

VPN

ceci afin d'éviter que des utilisateurs non autorisés se connectent directement aux systèmes qui pourraient contenir des informations sensibles (comme par exemple tous les mails, documents ou calendriers internes d'une organisation). SSL-VPN est flexible dans le choix du chiffrement et de l'authentification qui peut être basée sur des mots de passe fixes, des «tokens» ou encore des certificats X.509.

2 **PPTP (Point-to-Point Tunneling Protocol)** est un protocole crée par Microsoft qui permet de créer des tunnels entre différents réseaux ou machines. La plus grande différence entre PPTP et SSL-VPN est qu'avec le premier, un utilisateur peut se connecter à tout un réseau distant en utilisant juste un tunnel, tandis qu'avec le second, une nouvelle connexion doit être créée pour chaque serveur contacté. PPTP est disponible dans tous les systèmes d'exploitation Windows, MacOS et Linux ainsi que sur de nombreux firewalls et routeurs embarqués. Sa plus grande faiblesse est la qualité inférieure de la protection des données.

3 **IPsec** est un standard pour la sécurisation des données sur Internet . IC'est une collection de protocoles pour la sécurisation des trames ainsi qu'un protocole pour l'échange de clés.

- Pour la sécurisation des trames, IPsec offre deux mécanismes:
  - ➜l'Encapsulating Security Payload (ESP), assurant l'authentification, la confidentialité et l'intégrité des données et utilisant un mode «tunnel», et
  - ➜l'Authentication Header (AH), assurant l'authentification et l'intégrité, (mais pas la confidentialité) et utilisant un mode «transport».
- Pour l'échange de clés, le IKE (Internet Key Exchange) est le seul protocole actuellement utilisé, même si sa flexibilité rend parfois difficile l'interopérabilité entre ses différentes implémentations.

Pour plus d'information sur la compatibilité de différents produits, la source la plus complète et la plus neutre est le «VPN Consortium» (http://www.vpnc.org/).

Exemple:

EXTENSION RÉSEAU: REMOTE OFFICE / BRANCH OFFICE

Les filiales d'une entreprise veulent avoir accès aux serveurs de fichiers et aux serveurs pour la gestion de la clientèle qui se trouvent dans le réseau de la maison mère. La solution optimale sera l'utilisation d'un VPN en mode «tunnel» car avec ce modèle, la totalité du trafic entre deux filiales est géré dans la même connexion. Un observateur sur l'Internet pourra voir qu'il y a une connexion entre les différentes filiales mais ne pourra pas déterminer le contenu des échanges ni le modifier. Les filiales et la maison mère doivent s'identifier avant que la connexion VPN puisse être activée: dans le cas contraire, un cracker pourrait usurper l'identité d'une filiale (ou même de la maison mère) et forcer les autres parties à se connecter à lui.

3 Menaces contrées

L'Internet ne donne aucune garantie sur la confidentialité ni l'intégrité des données qui y circulent. Par exemple, si vous envoyez un email, il est tout à fait possible qu'une tierce personne l'intercepte, le regarde et change même son contenu. Ceci n'est en aucun cas acceptable et encore moins en ce qui concerne les connexions d'ordre sensible comme des transactions avec des clients ou partenaires ou dans le cas d'accès à distance aux informations internes d'une entreprise (sur un serveur de fichiers par exemple).

À l'heure actuelle, le meilleur moyen pour contrer ces menaces est bien l'utilisation d'un VPN.

4 Recommandations

Les cas d'utilisation des VPN étant très variés, nous nous limiterons ici à quelques remarques générales.

Les SSL-VPN représentent la solution la plus simple si la seule application devant être accessible à partir d'un réseau externe (Internet) est une application «web» car dans ce cas, il n'y a pas de configuration ni d'installation à réaliser sur les postes des utilisateurs.

Pour avoir un accès plus complet au réseau d'une entreprise (et pouvoir ainsi travailler de chez vous comme si vous étiez au bureau), il est préférable de s'orienter vers des VPN IPsec en mode tunnel. Attention, il existe de nombreux logiciels et machines sur le marché, il est donc vital de toujours en vérifier la compatibilité (http://www.vpnc.org).

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie et du Commerce extérieur