Sécurité informatique

Pare-feu

IDS

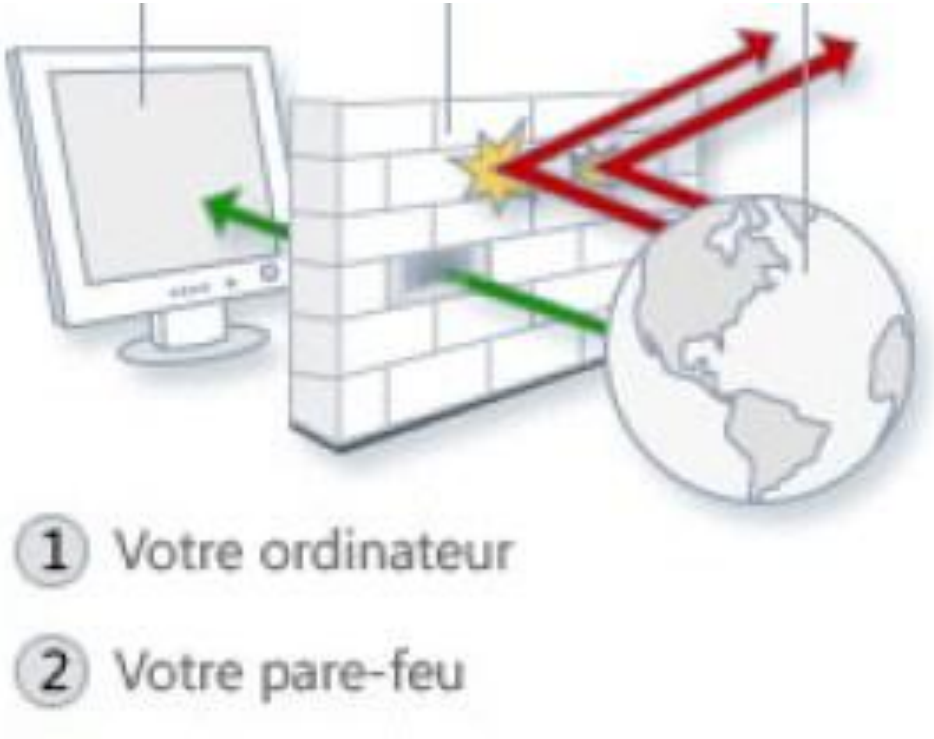
VPN

Architecture de sécurité (Firewalls)

Un pare-feu ou firewall est un système permettant de protéger l'ordinateur des intrusions extérieures via le réseau Internet ou local.

Il agit comme un **filtre** de données entre **les Réseaux et votre Ordinateur**.

Le terme **pare-feu** est métaphorique : il évoque une porte empêchant les flammes de l'Internet d'entrer chez soi et/ou de contaminer un réseau.



Il en existe deux types:

1. Le pare-feu matériel
2. Le pare-feu logiciel

Le **pare-feu matériel** c'est votre Modem, Routeur ou votre Box, c'est le plus ancien dispositif de filtrage, il y a peu de réglages à faire. Ils sont limités, en tous les cas pour l'abonné, et la modification de certains paramètres pourrait entraîner des dysfonctionnement pouvant aller jusqu'à la perte de synchronisation et donc la perte de votre accès internet…C'est donc votre opérateur qui le gère.

Le **pare-feu logiciel** est tout simplement un logiciel de sécurité que vous installez sur chaque ordinateur. C'est donc un pare-feu personnel. Il y a quelques années on le trouvait la plupart du temps en tant que programme seul.

Fonctionnement du pare feu logiciel

Il est paramétré selon des règles bien précises permettant :

- D'autoriser une connexion
- De bloquer une connexion
- De rejeter une demande de connexion

Il permet d'empêcher des utilisateurs et / ou des logiciels malveillants d'accéder à votre ordinateur.

Il peut aussi empêcher votre ordinateur d'envoyer des logiciels nuisibles à d'autres ordinateurs.

Système de détection d’intrusions
IDS

Definition

Un système de détection d'intrusion (ou IDS : Intrusion Détection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une action de prévention sur les risques d'intrusion.

Les différents types d'IDS

À cause de la diversité des attaques que mettent en œuvre les pirates, la détection d'instrusion doit se faire à plusieurs niveaux.

Il existe donc différents types d'IDS :

Les différents types d’IDS

- Les systèmes de détection d’intrusions (IDS)
- Les systèmes de détection d’intrusions "réseaux" (NIDS)
- Les systèmes de détection d’intrusions de type hôte (HIDS)
- Les systèmes de détection d’intrusions hybrides
- Les systèmes de prévention d’intrusions (IPS)
- Les systèmes de prévention d’intrusions "noyau" (KIDS/KIPS)
- Les pare-feux

Les systèmes de détection d'intrusions (IDS)

ensemble de composants logiciels et matériels dont la fonction principale est de détecter et d'analyser toute tentative d'effraction (volontaire ou non).

Fonctions de détection :

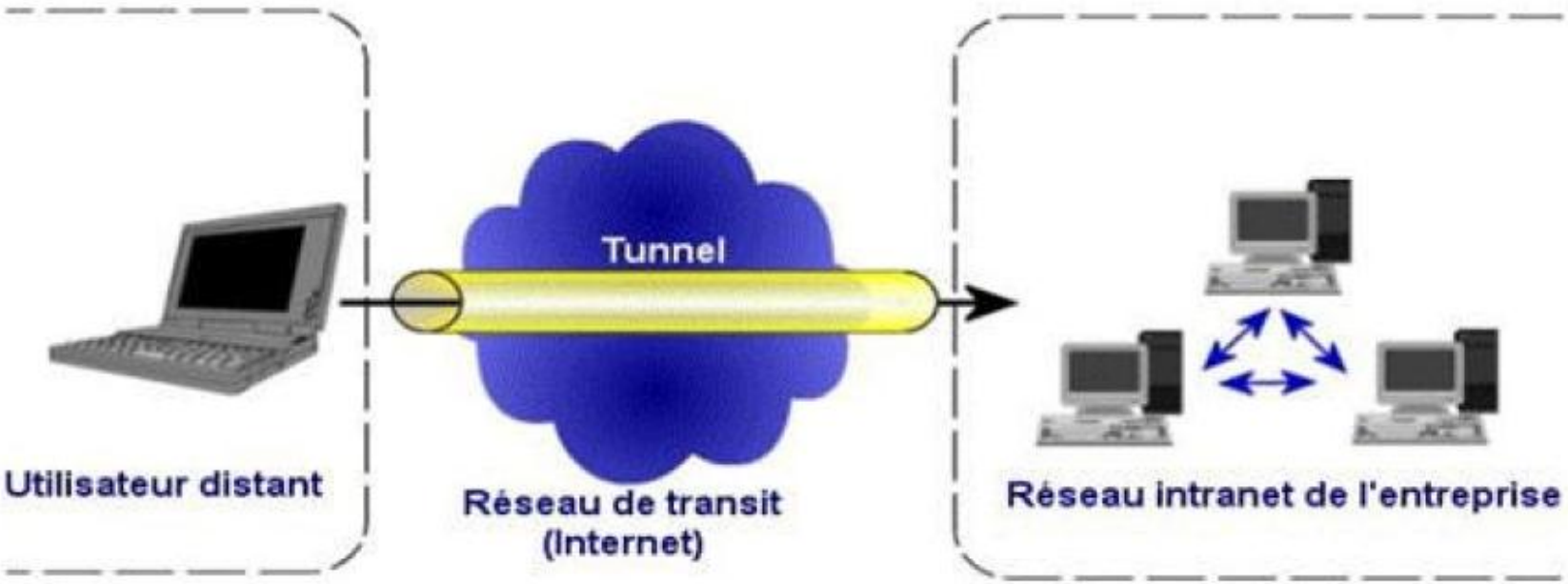
- des techniques de sondage (balayage de ports, fingerprinting),
- des tentatives de compromission de systèmes,
- d'activités suspectes internes,
- des activités virales,
- ou encore des audits de fichiers journaux (logs).

Deux notions fondamentales :

- Faux positifs : une alerte provenant d'un IDS qui ne correspond pas à une attaque réelle.
- Faux négatifs : une intrusion réelle qui n'a pas été détectée.

Virtual Private Network
VPN

VPN est une technique permettant a un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant des infrastructures publiques , ce type de liaison est apparu suite a un besoin croissant des entreprises de relier les différents sites


Tunnel
Utilisateur distant
Réseau de transit
(Internet)
Réseau intranet de l'entreprise

Principe de fonctionnement d’un VPN

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Les principaux avantages d'un VPN :

- **Sécurité :** assure des communications sécurisées et chiffrées.
- **Simplicité :** utilise les circuits de télécommunication classiques.
- **Économie :** utilise Internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée.

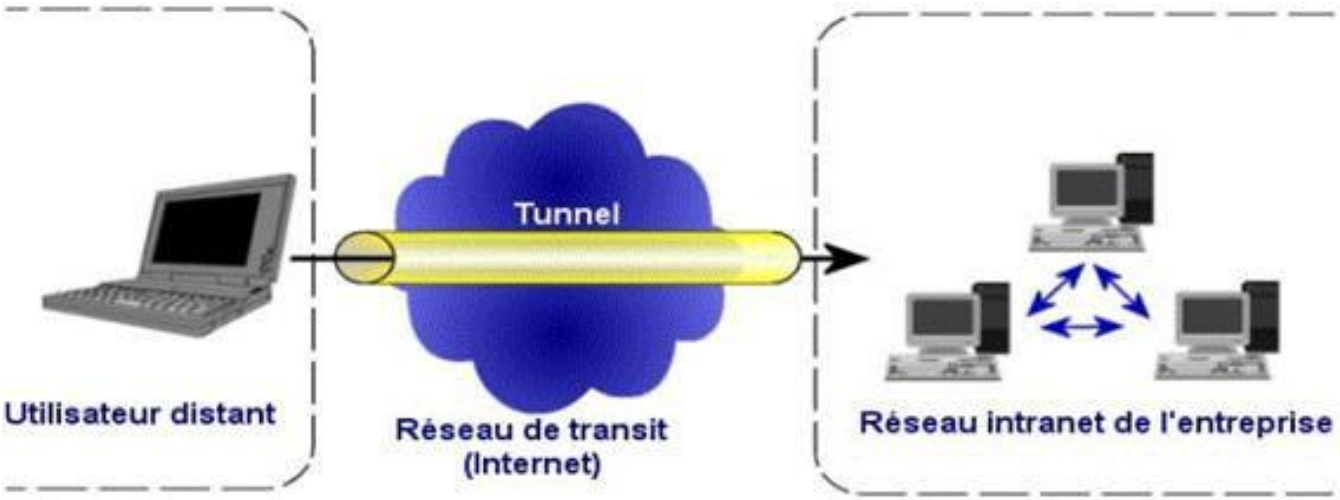
Les contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accés. Il doit être capable de mettre en oeuvre les fonctionnalités suivantes :

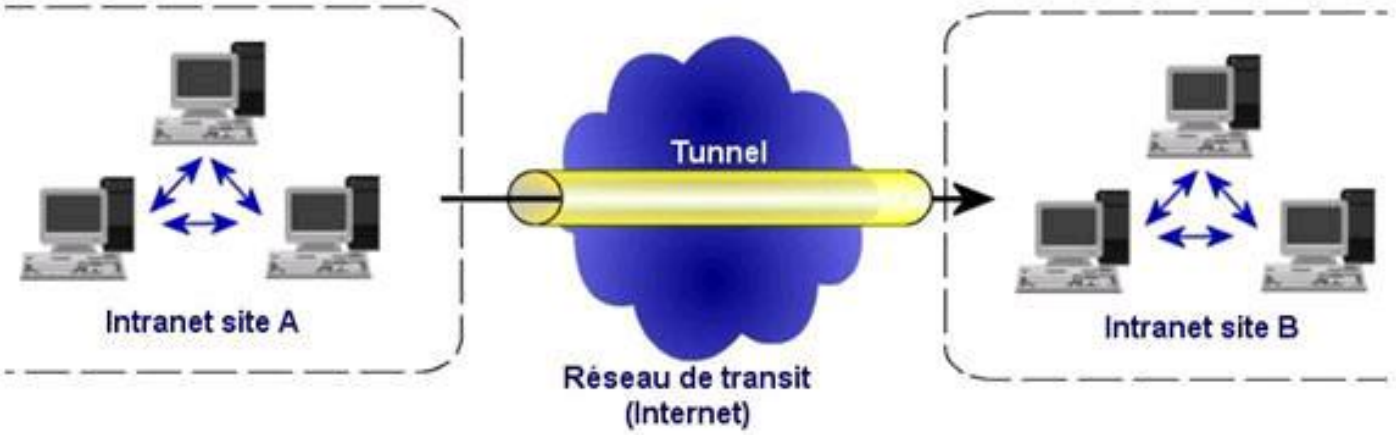
- Authentification d'utilisateur : seuls les utilisateurs autorisés doivent avoir accés au canal VPN.
- Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Les différents types d’un VPN

Le VPN d’accès : il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.



L'intranet VPN : il est utilisé pour relier deux ou plusieurs intranets d'uen même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants …



L'extranet VPN : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accés. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.