Communications Sécurisées : Protocoles et Architectures

Sécurité Informatique (Licence 3)

Abdelmalik Bachir

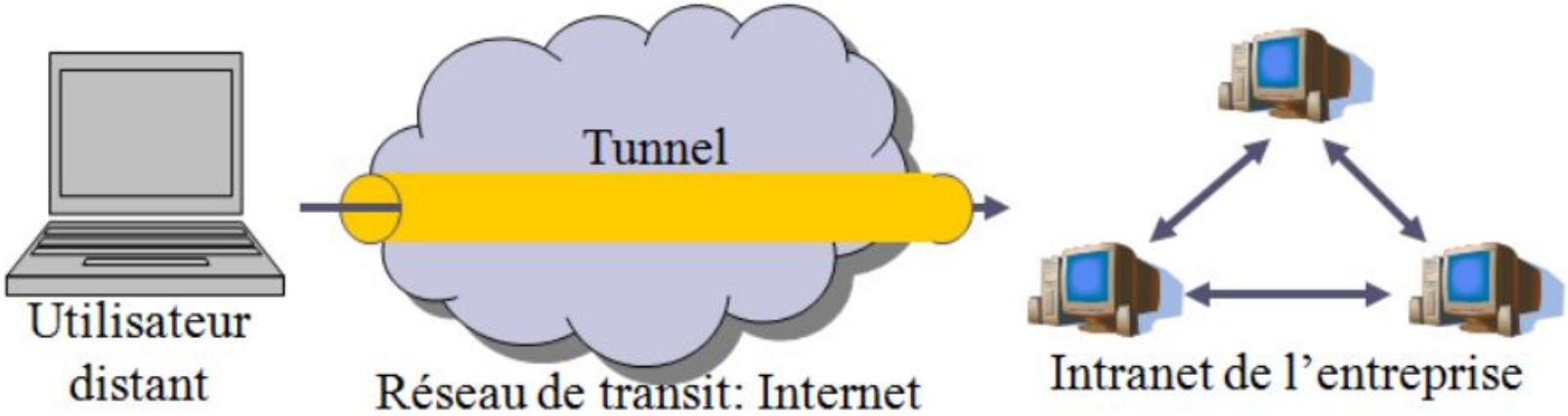
Réseaux Privés Virtuels (VPN)

Problématique : Comment assurer l'accès sécurisé à des applications distribuées sur des sites géographiquement distants. Les VPN ont été mis en place pour répondre à ce type de problématique.

Méthode : Un VPN repose sur un protocole de « tunneling ». Ce protocole permet de transporter les données de l'entreprise chiffrées d'un bout à l'autre du tunnel. Il construit un chemin virtuel d'une source à une destination après leur identification. La source chiffre les données qui empruntent ce chemin virtuel, et la destination déchiffre. Le protocole encapsule les données dans une entête. Le tunneling est le processus d'encapsulation, transmission puis décapsulation. Les usagers auront l'impression de se connecter au réseau local de l'entreprise.

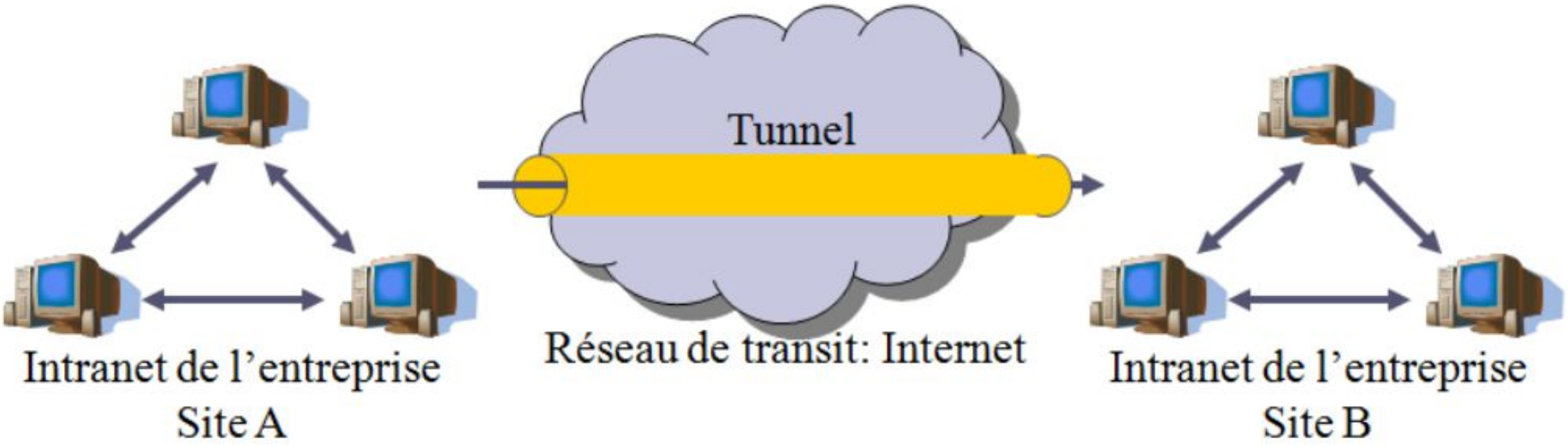
Types de VPN

VPN d'accès : Clients itinérants accèdent au réseau local de l'entreprise.



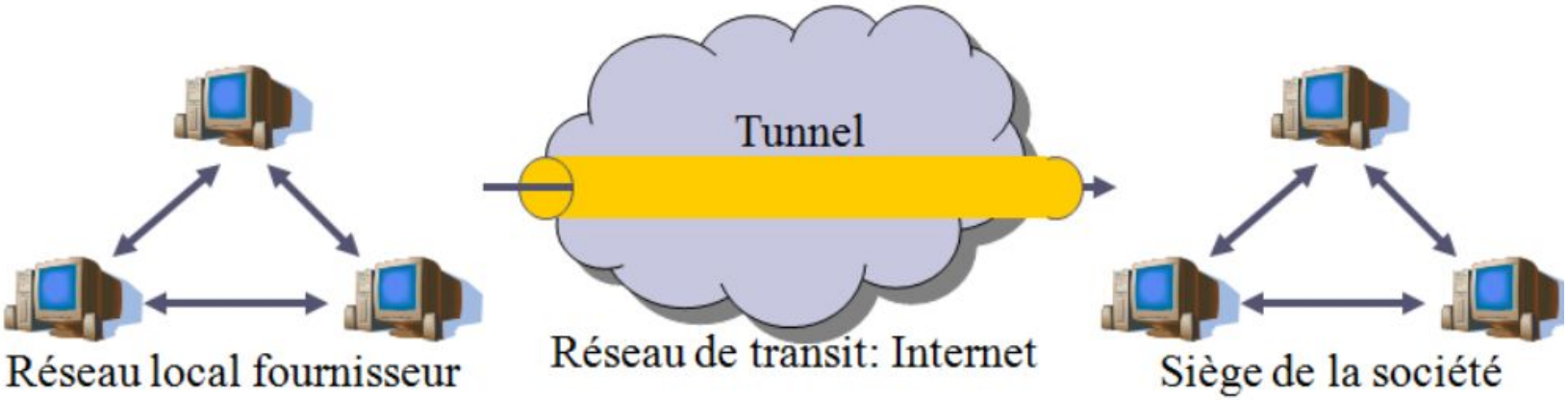
Types de VPN

Intranet VPN : L'entreprise possède plusieurs sites distants



Types de VPN

Extranet VPN : L'entreprise ouvre son réseau local à ses partenaire. Il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits d'accès de chacun sur le réseau.



Mise en oeuvre des VPNs

Un système VPN doit pouvoir assurer les fonctionnalités suivantes:

- Authentification d'utilisateur: seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le VPN. Un historique des connexions et actions effectuées doit être conservé.
- Gestion d'adresses: chaque client sur le réseau doit avoir une adresse privée confidentielle.
- Chiffrement des données: lors de leurs transports sur le réseau publique, les données doivent être protégées par un chiffrement efficace.
- Gestion de clés: les clés de chiffrement pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multiprotocole: la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publiques en particulier IP.

Implémentations des VPNs

Le VPN est un principe: il ne décrit pas l'implémentation effective, c'est pourquoi il existe plusieurs produits différents dont certains sont devenus standards.

Exemple : Cisco VPN, OpenVPN, …

Parfois ces implémentations ne sont pas compatibles entre elles.

Email sécurisé : Pretty Good Privacy (PGP)

Principe de fonctionnement : PGP choisit une clef symétrique aléatoire: clef de session. Chiffre le courrier avec la clé de session. Puis, chiffre la clé de session avec la (les) clef(s) publique(s) du (des) destinataire(s). Ces derniers pourront alors déchiffrer la clé de session avec leur clé privée puis déchiffre le message avec la clé de session.

Protection des clés privées : Les clefs privées sont chiffrées sur le disque de l'utilisateur de PGP en utilisant un algorithme de dérivation de clef à partir d'un mot de passe. Quand la clef privée est nécessaire (pour signer ou déchiffrer un message), l'utilisateur saisit le mot de passe pour déchiffrer sa clé privée

Email sécurisé : Pretty Good Privacy (PGP)

Distribution des clés publiques : Le moyen le plus simple et efficace est de rencontrer la personne, de l'authentifier et lui demander sa clé publique. Cette rencontre physique n'est pas toujours commode. On récupère les clefs publiques des annuaires (dit serveurs) PGP. Une clef PGP obtenue sur un serveur PGP ne devrait pas être considérée de confiance sans vérification supplémentaire. Un intrus peut enregistrer une clef PGP sous un faux nom car il n y a pas de vérification. Quelqu'un peut être victime d'une usurpation de DNS et être redirigé vers un faux serveur PGP. Pour faire cette vérification, Alice récupère de l'annuaire une clé publique de Bob signée par Charlie à qui elle fait confiance (elle connaît la clef publique de Charlie).

Accès sécurisé à distance Secure Shell (SSH)

Définition : SSH est un protocole qui permet de faire des connexions sécurisées (i.e. chiffrées) entre un serveur et un client SSH.

Etablissement d'une connexion SSH

Un serveur SSH dispose d'un couple de clefs RSA stocké dans le répertoire `/etc/ssh/` et généré lors de l'installation du serveur. Le fichier `ssh_host_rsa_key` contient la clef privée et a les permissions `600`. Le fichier `ssh_host_rsa_key.pub` contient la clef publique et a les permissions `644`. Le serveur envoie sa clef publique au client. Celui-ci vérifie qu'il s'agit bien de la clef du serveur, s'il l'a déjà reçue lors d'une connexion précédente, ou comparaison à un hash ou certificat.

Etablissement d'une connexion SSH

Le client génère une clef secrète (symétrique) et l'envoie au serveur, en chiffrant l'échange avec la clef publique du serveur. Le serveur déchiffre cette clef secrète en utilisant sa clé privée. Pour le prouver au client, il chiffre un message standard avec la clef secrète et l'envoie au client. Si le client retrouve le message standard en utilisant la clef secrète, il a la preuve que le serveur est bien le vrai serveur. le client et le serveur peuvent alors établir un canal sécurisé grâce à la clef secrète commune (chiffrement symétrique).

Une fois que le canal sécurisé est en place, le client va pouvoir envoyer au serveur le login et le mot de passe de l'utilisateur pour vérification.

Etablissement d'une connexion SSH

Remarque : Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clefs privée/publique, comme le fait le serveur SSH auprès du client SSH. La clé privée de l'utilisateur est protégée (chiffrée) par un mot de passe, qui lui sera demandé à chaque utilisation de cette clé.

Exemple :

Générer les clés publiques / privées

```
bachir@bachir-ThinkPad-T430:~$ ssh-key
ssh-keygen   ssh-keyscan
bachir@bachir-ThinkPad-T430:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bachir/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bachir/.ssh/id_rsa
Your public key has been saved in /home/bachir/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:6cJ8vI7pjDkdrJJQljMFMYkRsD4Q2y/DN/CSq6tmoxU bachir@bachir-ThinkPad-T430
The key's randomart image is:
+---[RSA 3072]----+
|*+++             |
|.=...            |
|+ oo             |
|o.*=     .       |
| =Eo=.  S        |
|. .B +oo         |
| .o. o+.+        |
| *o o+.= .       |
|X...oo=.o        |
+----[SHA256]-----+
```

Générer les clés publiques / privées

Générer les clés publiques / privées

```
bachir@bachir-ThinkPad-T430:~$ cat .ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx5MGOzPlbRlkSrxLKFIX02Ddb4MVF9pcDwK5bL3QwWmOCHwy/b3K
bUXalHWvWRvxVny5SiVYzTHRFWt2SQfGDMWCjmsBYS9mpDnCT59JGpJLJ3QJcU2Lc10SxV
PizQiy+HWfUtVE6kgwDpEYG1qxAcBBasVONXaYYovKkCBF+NeRXxAnFFp18qdd4KHZLKR5
r8v2Aa4Y6TOMSWiH9XmfUNXhZleeKcjz6bP07CiJOH+mNvejom05sm17X61UQLLhe21b5e
m21FAjf4PGImZVbD1r1cFrOolC5mgwDqIFy+jIiTzFZ01RFdONA+bs5zU4SwhLTcRF1x0O
yOURbtlkGwN2OmGzivNqO6zl6mBvVFQv6/x+vSdN11FqIaSMpg3/ZkUXiVmRbRBfuHnpLu
iLTdwkRp9/kp0jH8kbFhCWRgkZCxuyzKnQ5weZvwEQe4o+Xa9+DYkbW0PJ0qg8Ac9X9edo
ozlGbhEsTU43Rf6g7VmqkZxb8JrQzffvWnntEH/LAAAFmCBDc84gQ3POAAAAB3NzaC1yc2
EAAAGBAMeTBjsz5W0ZZEq8SyhSF9Ng3W+DFRfaXA8CuWy90MFpjgh8Mv29ym1F2pR1r1kb
8VZ8uUolWM0x0RVrdkkHxgzFgo5rAWEvZqQ5wk+fSRqSSyd0CXFNi3NdEsVT4s0Isvh1n1
LVROpIMA6RGBtasQHAQWrFTjV2mGKLypAgRfjXkV8QJxRadfKnXeCh2Sykea/L9gGuGOkz
jEloh/V5n1DV4WZXninI8+mz9OwoiTh/pjb3o6JtObJte1+tVECy4XttW+XpttRQI3+Dxi
JmVWw9a9XBazqJQuZoMA6iBcvoyIk8xWdNURXTjQPm7Oc1OEsIS03ERdcdDsjlEW7ZZBsD
djphs4rzajus5epgb1RUL+v8fr0nTddRaiGkjKYN/2ZFF4lZkW0QX7h56S7oi03cJEaff5
KdIx/JGxYQlkYJGQsbssyp0OcHmb8BEHuKPl2vfg2JG1tDydKoPAHPV/XnaKM5Rm4RLE1O
N0X+oO1ZqpGcW/Ca0M3371p57RB/ywAAAAMBAAEAAAGBAKPQeNLrnCxbJUl7GS31hH0LC3
fW3t9/awUfNViezdWUcPNiDvDccmYTaoFlwBKirwxQwD6uPR/g/kBYvvTfHp+pF6sTBkTh
hZzTlD2K/5SB9JJj2sRX5FlDUn8KhiXKOC1dTvPM/w5XRqsOSf1aCeToDEo5viKAQEDTge
eftg+10it3tLwuLJaK7rHN59ePAhtcjYd/gg8ZMtOmq8LAnBbcGHHLBZZCzoNMJYQbGdd4
X9TKnFRc13kwCI7WVUvuB1f8lCnxJCbPRzff9FHOUUhmHY4YlqNAz3UeRudzfaTFbbNHL+
ogNnJzX4G9HF0AUl5kBUX8C3Ar3EfrlAE4sTcJCiRMcIk4phovmFlgG9U56GDcd7FYdN56
C1233Lbfg5gCeHxVOwspCS1UVJzOluXwPeAJHgSZ2RE08v+iJCHMGiIuGmLyNTHxjuchT7
sXyM50wAF5CFGgh9fVgsScVp1pHkRZ/OPOLMbZcWSP19DstJknrKgMb6oeRhgyrX3h4QAA
AMA0krkMAgXNpfr7fTzORrLzUevvJnL57taZJZOLQrMcWteV0hAkSlEa6xaRWLAPCGbO+B
ryRUgFunLpbjn+FwuedfiREu88GQY9IxmjpOe7v9oBWjwE2tPMtI0UsbCh6jO++ys+dbeD
/9jYtM+45yGK0xoP3WsSzP4rXdxxF5hhyG6jIMPIKdMCe+CvrXM+5gsYvS+CCvW9SZTv+s
9B6rIrFMHupX8IgPHosyqk16QzobgHiGTN/dvPi3Tzu7pR6xQAAADBAOebNClNtYrmPBcw
2DdrrAlJEd0drb1rC7zmpvLzO8hvoyogpGPpIittKZPCUT9LEL6es69j9sakO7Fl5Ut8A0
AvdrrBOHPCY2Da/xBWGIP+yRId5D4L4vrjAXtJWgOn3ce1mEy1tOpmx2jhrEVE1m5hXeUy
r+eQLqRv8P7iAxINGaNwA3hsAEspeyNhrnPa6Z6npu3wOHGJ1YXj7CFk2zbUsbi5s475Hf
xBlp1Sa/Nt8m9adEFmryeObiDoo6IWeQAAAMEA3JgkwVVh8K6abBGAzpz0LvYwSEY3Azxf
vJ+tpfIhvN/qtcPf1ESl6dRqDqFbcsh5Wbp3bfGD1ub2WMLL8pLAhPeIKHquhE6ti51EDg
itYZrYbsV24b+vFvOrCZyGnahy9e78lRSrT6MhesUMR+XgKEkGvREu5R6JM6kEh9Q+JwKw
Yw2q9wV6eN395siXQtcbOqPpLXgeHEpVCXXJkgz8+xMT5dfJx9PR8yygDyn0RUooNNqZjd
38vzc9hchFyIdjAAAAG2JhY2hpckBiYWNoaXItVGhpbmtQYWQtVDQzMAECAwQFBgc=
-----END OPENSSH PRIVATE KEY-----
```

Se connecter à un serveur distant

Références bibliographiques

Yacine Challal, *Ingénierie des protocoles et logiciels sécurisés*
http://y_challal.esi.dz/index.php/2016/04/30/ingenierie-des-protocoles-et-logiciels-securises-ipls/

James F. Kurose, Keith W. Ross Computer Networking: A Top-Down Approach, 6th Edition (2013)

https://www.pearson.com/us/higher-education/product/Kurose-Computer-Networking-A-Top-Down-Approach-6th-Edition/9780132856201.html