République Algérienne démocratique et populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université de Abbas Laghrour Khenchela
Faculté Science et Technologie – Département Math et Informatique

SSH et Tunneling

Étudiants:
TAOUS MOHAMED
MEBARKIA Abdenour
SABEG Hichem
TRAD TEJEDDINE
DJELLAL SALAHEDDINE

Enseignant:
DJELLAB ISSAM

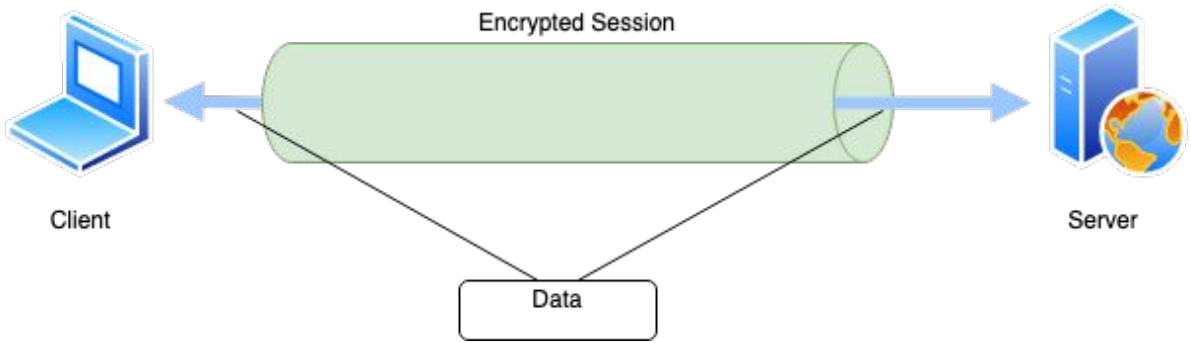
3éme Année SI - 2021/2022

Sommaire

La définition et Architecture :

Définition:

Le tunneling SSH, ou redirection de port SSH, est une méthode de transport de données via une connexion cryptée. Les tunnels SSH permettent aux connexions établies à un port local (c'est-à-dire à un port sur votre propre bureau) d'être transmises à une machine distante via un canal sécurisé.



Architecture et fonctionnement de base :

1

La couche de transport SSH:

authentification du serveur, négociation des algorithmes, mise en place d'une clef de session, intégrité et confidentialité des données, compression, identification de session

2

La couche d'authentification SSH:

authentification du client (clé publique, mot de passe, clé d'hôte), chargement de mot de passe.

3

La couche de connexion SSH:

-transfert de port TCP et transfert X, transfert d'agent d'authentification

-gestion des sessions interactives, exécution de programmes distants

-contrôle de flux, gestion des terminaux (modes et tailles des fenêtres)

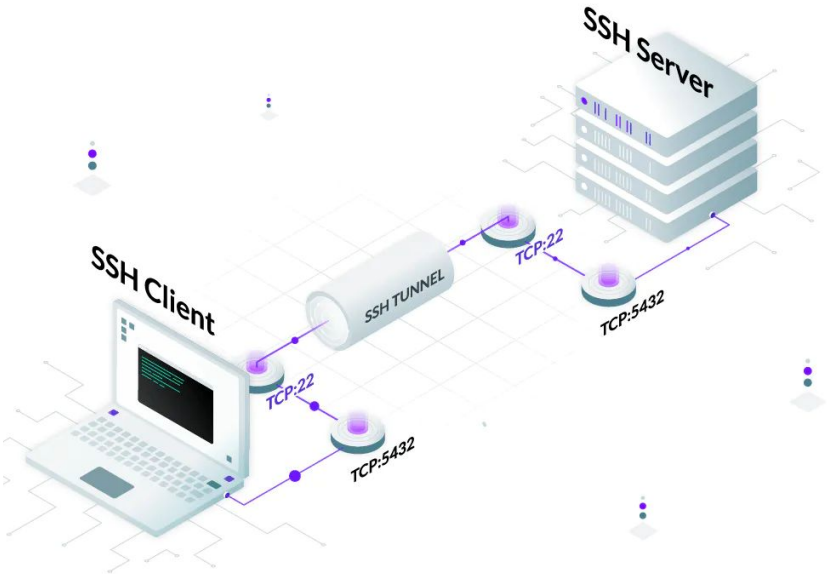
-compression des données

Les fonctionnalités offertes par SSH:

Les méthodes d'authentification avec SSH

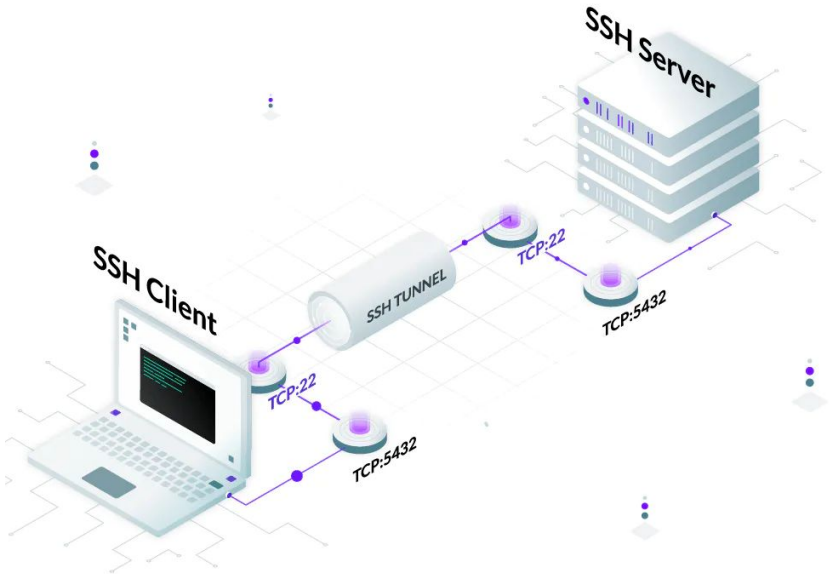
Authentification avec mot de passe :
La méthode la plus connue est le traditionnel mot de passe (login) .

Authentification par clés:
L'utilisateur place sa clé publique sur les serveurs SSH sur lesquels il souhaite se connecter et garde sa clé privée sur sa station de travail.



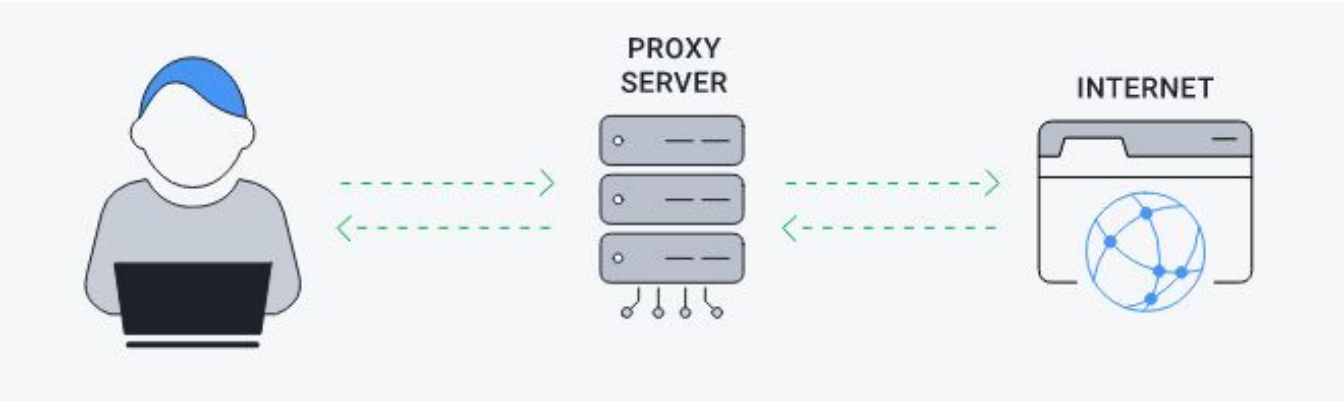
L'authentification par hôte (host based) :

Il s'agit d'une authentification similaire à celle utilisée par les commandes et les fichiers tels que /etc/rhosts et /.rhosts, qui certifient les sites client en ayant préalablement enregistré leur adresse dans le serveur. En effet, avec cette méthode d'authentification, quand le client demande une connexion à un serveur SSH, ce dernier va chercher dans le fichier rhosts un nom d'hôte qui correspond à l'adresse source de la connexion réseau du client.



Mise en place d’un canal sécurisé :

Utiliser un proxy :
est un serveur informatique dont le rôle est de servir de relais entre un client et un serveur,Quand vous vous connectez à internet à partir du poste de travail, il se peut qu'une boite de dialogue s'ouvre et vous demande un identifiant et un mot de passe pour surfer sur internet : c'est le proxy qui demande cette authentification pour vous autorisez ou non l'accès au site désiré



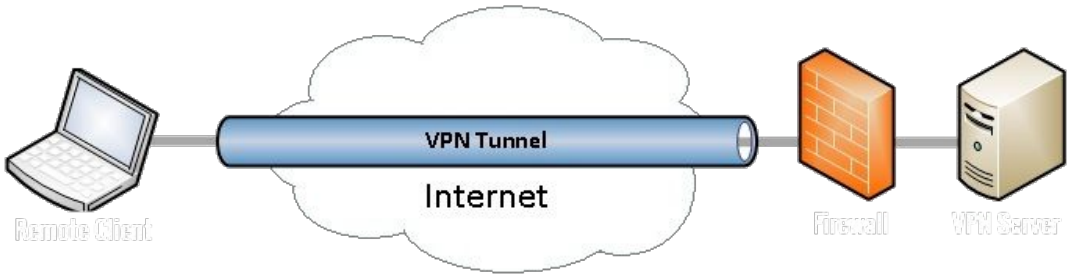
Utiliser un tunnel SSH:

La mise en œuvre d'un tunnel est un peu plus complexe que l'utilisation standard d'une application. Un tunnel représente une connexion traversant plusieurs interfaces de manière transparente pour le client et le serveur. L'utilisation de tunnel SSH peut servir à différents buts tels que la sécurisation d'un protocole non crypté.

SSH combine cryptage asymétrique et cryptage symétrique. SSH utilise les deux cryptages : asymétrique et symétrique. Cela fonctionne dans cet ordre :

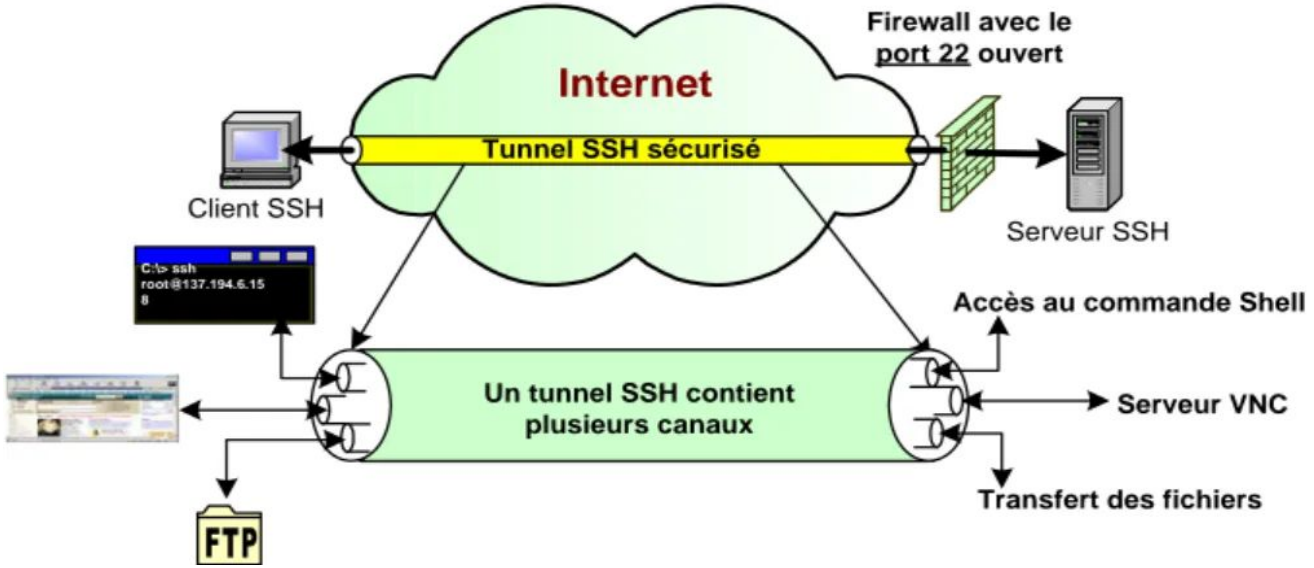
• On utilise d'abord le cryptage asymétrique pour s'échanger discrètement une clé secrète de cryptage symétrique.

• Puis ensuite on utilise tout le temps la clé de cryptage symétrique pour crypter les échanges. Le cryptage asymétrique demande beaucoup trop de ressources au processeur.il est 100 à 1000 fois plus lent que le cryptage symétrique. Les ordinateurs s'échangent donc la clé de cryptage symétrique de manière sécurisée (grâce au cryptage asymétrique) et ils peuvent ensuite communiquer plus rapidement en utilisant tout le temps du cryptage symétrique.



Solution proposée

Les fonctionnalités offertes par SSH :


Internet
Firewall avec le
port 22 ouvert
Tunnel SSH sécurisé
Client SSH
Serveur SSH
C:\> ssh
root@137.194.6.15
8
Accès au commande Shell
Un tunnel SSH contient
plusieurs canaux
Serveur VNC
Transfert des fichiers
FTP

L’accès à distance par Shell SSH :

Le Shell SSH (la commande SSH) est une version sécurisé de rsh et rlogin. SSH veut dire Secure Shell à l’image de rsh qui veut dire remote Shell. Quand rsh permet d’obtenir un Shell distant aisément ; mais sans mécanisme d’authentification satisfaisant (du point de vue de la sécurité), SSH procure le même service de façon sécurisé. Ainsi, pour utiliser SSH, il suffit d’utiliser la commande SSH à la place des commandes Telnet, rsh et rlogin.

Le transfert de fichier par SFTP :

SFTP (Secure File Transfer Protocol) est un sous protocole séparé qui se situe au dessus du protocole SSH. Il est utilisé dans le transfert sécurisé des fichiers. SFTP a plusieurs avantages par rapport au protocole non sécurisé FTP. D’abord, SFTP chiffre le couple user-name/password ainsi que les données transférées en se basant sur des algorithmes cryptographiques. ce qui élimine la nécessité d’ouvrir un autre port sur le pare-feu. Ainsi l’utilisation de SFTP résout également le problème connu dans le protocole FTP.

Le tunneling :

Le transfert, ou tunneling, consiste à encapsuler un autre service TCP/IP comme Telnet, dans une session SSH afin de lui apporter les bénéfices de la sécurité de SSH (Confidentialité, intégrité, authentification, autorisation). En transférant Telnet par exemple, via SSH, toutes les données seront chiffrées et leur intégrité sera contrôlée.

SSH reconnaît trois types de transfert : le transfert de port TCP, le transfert des sessions interactives de type X-Windows et le transfert des agents SSH qui permet aussi d'utiliser des clés privées SSH sur des machines distantes.

la redirection de port (port forwarding) :

Le SSH permet de rediriger n'importe quel flux TCP dans le tunnel de la session SSH.

Cela veut dire que le flux de n'importe quelle application circulant entre les ports client et serveur habituels, pourra être encapsulé à l'intérieur du tunnel créer par la session SSH

la redirection de l'authentification (agent forwarding) :

L'agent SSH est un mécanisme d'authentification auprès de multiples serveur SSH qui reconnaisse la clé privée d'un client sans devoir retaper à chaque fois sur sa machine la pas phrase. En effet un agent SSH est un programme, qui s'appel SSH-agent, qui garde les clefs privées en mémoire et qui fournit les services d'authentification au client SSH. Cette méthode permet à un utilisateur d'introduire sa pas phrase lors de la première connexion à un serveur SSH. L'ouverture d'une session sécurisée avec un nouveau serveur SSH se fait de manière transparente pour l'utilisateur. Si l'utilisateur souhaite, par exemple, faire une copie de fichier (SCP) entre deux serveurs distants (figure-3-), SSH offre une fonctionnalité qui s'appel agent forwarding qui permet à des machines distantes d'accéder à l'agent local de l'utilisateur pour pouvoir récupérer ses droit d'accès et d'exécuter ces programmes distants (dans ce cas c'est le programme SCP).

Conclusion:

L’ SSH est un mécanisme d’authentification auprès de multiples serveur SSH qui reconnaisse la clé privée d’un client sans devoir retaper à chaque fois sur sa machine la pas phrase. En effet un agent SSH est un programme, qui s’appel SSH-agent, qui garde les clefs privées en mémoire et qui fournit les services d’authentification au client SSH. Cette méthode permet à un utilisateur d’introduire sa pas phrase lors de la première connexion à un serveur SSH. L’ouverture d’une session sécurisée avec un nouveau serveur SSH se fait de manière transparente pour l’utilisateur. Si l’utilisateur souhaite, par exemple, faire une copie de fichier (SCP) entre deux serveurs distants (figure-3-), SSH offre une fonctionnalité qui s’appel agent forwarding qui permet à des machines distantes d’accéder à l’agent local de l’utilisateur pour pouvoir récupérer ses droit d’accès et d’exécuter ces programmes distants (dans ce cas c’est le programme SCP).