Mise en place de Secure Shell pour la sécurisation locale et distante des accès aux équipements réseaux.

Philippe JUNDT

BTS SIO option SISR

Table des matières

Mise en place de sécurisation d'équipement réseaux

Cahier des charges :

En raison du risque de comportements frauduleux l'entreprise entend sécuriser l'accès à son infrastructure réseaux. L'idée est de réduire le temps de SLA en autorisant les administrateurs à accéder à distance à des équipements. Mais aussi de se prémunir contre les risques d'intrusion ou de captation pour des utilisateurs externes à l'entreprise.

I. Mise en place d'un mot de passe

Cette technique est un préalable nécessaire pour réduire le risque lié à une modification en interne des configurations des équipements.

Avec la procédure qui suit, le mot de passe sera nécessaire pour un accès local depuis la console.

II. Méthodes de sécurisation d'infrastructure avec SSH:

Présentation du protocole SSH

Secure Shell (ci-après SSH) est un protocole qui permet de sécuriser des accès distants à un périphérique réseau, ici des routeurs[1]. La communication entre le client et le serveur sera encrypté avec une version de SSH 1 ou SSH 2. L'implémentation et la mise en œuvre de SSH version 2 est plus sécurisant lorsque cela est possible puisque ce protocole offre une protection renforcée du chiffrement algorithmique.
Les documentations CISCO ont notamment vocation à présenter comment configurer ou débugger SHH sur les routeurs et switch CISCO qui utilisent une version de CISCO IOS[2].

Les équipements CISCO sont des équipements compatibles avec des protocoles propriétaires et libres de droits. Le software CISCO IOS est compatible avec les versions 1 et 2 de SSH.
SSH est un protocole qui permet de sécurité des accès distants à un périphérique réseau, ici des routeurs[3].

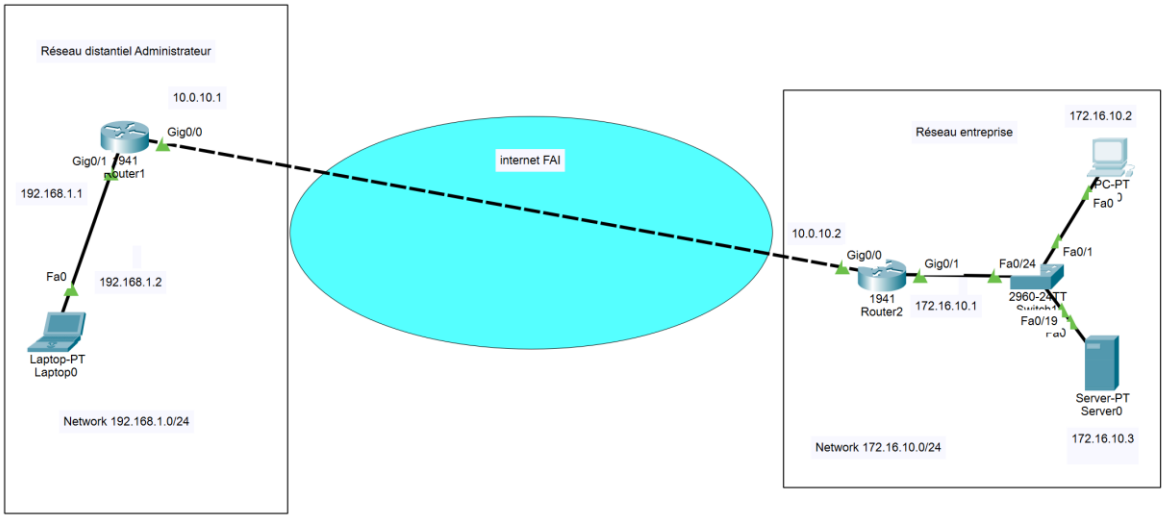
Prérequis

S'assurer de la gamme d'équipement utilisée :
CISCO IOS image repose sur une version k9(crypto), c3750e-universalk9-tar.122-35.SE5.tar est une image k9 (crypto).
Attention certaines gammes d'équipements CISCO, notamment les équipements Catalyst ont des spécificités qu'il faut prendre en compte.

Les équipements CISCO récent prennent en charge SSH 1 et SSH2.

[1] Présentation du protocole SSH pour les équipements CISCO p2, url : https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html, dernière consultation le 12 mars 2021
[2] Présentation du protocole SSH pour les équipements CISCO, url : https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html, dernière consultation le 12 mars 2021
[3] Présentation du protocole SSH pour les équipements CISCO, url : https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html, dernière consultation le 12 mars 2021

III. Méthodes de sécurisation d'infrastructure via SSH:



Installation fonctionnelle sous CISCO Packet Tracert, les différents éléments sont sur trois réseaux différents :

- Réseau de l'entreprise : 172.16.10.0/24
- Réseau du Fournisseur d'accès à l'Internet : 10.0.10.0/24
- Réseau distant de l'administrateur : 192.168.1.0/24

Un équipement de type Switch prend en charge les différents équipements installés dans l'infrastructure de l'entreprise.

L'intérêt de cet exercice est de permettre à un utilisateur distant, un administrateur systèmes et réseaux de l'entreprise d'accéder au router2 pour le configurer sans que les informations transitant par le FAI soient exploitables par des tiers.

A. Sécurisation de l'équipement préalable en local

1. Installation du protocole SSH sur l'équipement

a. Pour l'équipement : Router2

Relier l'ordinateur qui servira de terminal à l'équipement cisco. Nous procèderons avec une connexion copper straight-through classique, en langage technique un câble droit cuivre.

La procédure CISCO préconise un processus à 4 étapes[4] :

Step 1: Configure the hostname if you have not previously done so.
Step 2: Configure the DNS domain of the router.
Step 3: Generate an SSH key to be used with SSH.
Step 4: By default the vtys' transport is Telnet. In this case --- Telnet

Instead of **aaa new-model**, you can use the **login local** command.

[4] Configuration Secure Schell on Routers and Switches Running Ciso IOS: https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html, dernière consultation le 12 mars 2021

Ici le PC1 est connecté au Routeur2 via des équipements intermédiaires préprogrammés, le réseau est déjà opérationnel. Il est préférable de se connecter via la console pour procéder à cette opération, il faut se rendre dans le CLI de l'équipement.

Step 1: Configure the hostname if you have not previously done so.

Router>conf t
Router>hostname Router2

Step 2: Configure the DNS domain of the router.

Router2>en
Router2>conf t
Router2>int g0/0
Router2>ip add 10.0.10.2 255.255.255.0
Router2>no sh

Step 3: Generate an SSH key to be used with SSH.

Router2>int g0/0
Router2> ip domain-name ssh.com
Router2> crypto key generate rsa

```
Router2(config)#crypto key generate rsa
% You already have RSA keys defined named Router2.ssh.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: Router2.ssh.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

Ici le routeur avait été sécurisé lors de son installation, il est demandé à changer de clé.

Le routeur propose un range de sécurisation, une clé à 2048 bits est la norme actuelle

```
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
```

Pour des raisons de sécurité cette clé n'est pas exportable.

Step 4: By default the vtys' transport is Telnet. In this case --- Telnet

Router2>conf t
Router2>line vty 0 4

```
Router2(config)#line vty 0 4
*Mar 1 2:2:22.450: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Router2(config-line)>transport input ssh
Router2(config-line)>login local
Router2(config-line)>exit
*Router2(config)>username ICIadmin privilege password *PSWcisco**
*Router2(config)>enable secret *PSWcisco**

```
[OK]

Router2(config)#
```

Attention à bien sauvegarder les données, autrement toutes les étapes réalisées ici seront retirée de la mémoire si le routeur est débranché ou éteint, il s'allumera alors avec les derniers éléments sauvegardé (ici avec l'intervention du dernier administrateur, ce qui est une faille de sécurité).

Contrôle du versioning : en fonction des types de connexion et des équipements CISCO vous préconisera d'utiliser soit SSH V1, soit SSH V2 ou les 2, dans les 2 cas penser quitter une session pour désactiver correctement SSH, par défaut une temporisation est configurée sur les équipements pour désactiver une session inactive pendant un certain temps :

Variations on banner Command Output

The **banner** command output varies between the Telnet and different versions of SSH connections. This table illustrates how different **banner** command options work with various types of connections.

Banner Command Option	Telnet	SSH v1 only	SSH v1 and v2	SSH v2 only
banner login	Displayed **before** logging into the device.	Not displayed.	Displayed **before** logging into the device.	Displayed **before** logging into the device.
banner motd	Displayed **before** logging into the device.	Displayed **after** logging into the device.	Displayed **after** logging into the device.	Displayed **after** logging into the device.
banner exec	Displayed **after** logging into the device.	Displayed **after** logging into the device.	Displayed **after** logging into the device.	Displayed **after** logging into the device.

Figure 1. Documentation CISCO

b. Accès depuis un poste distant

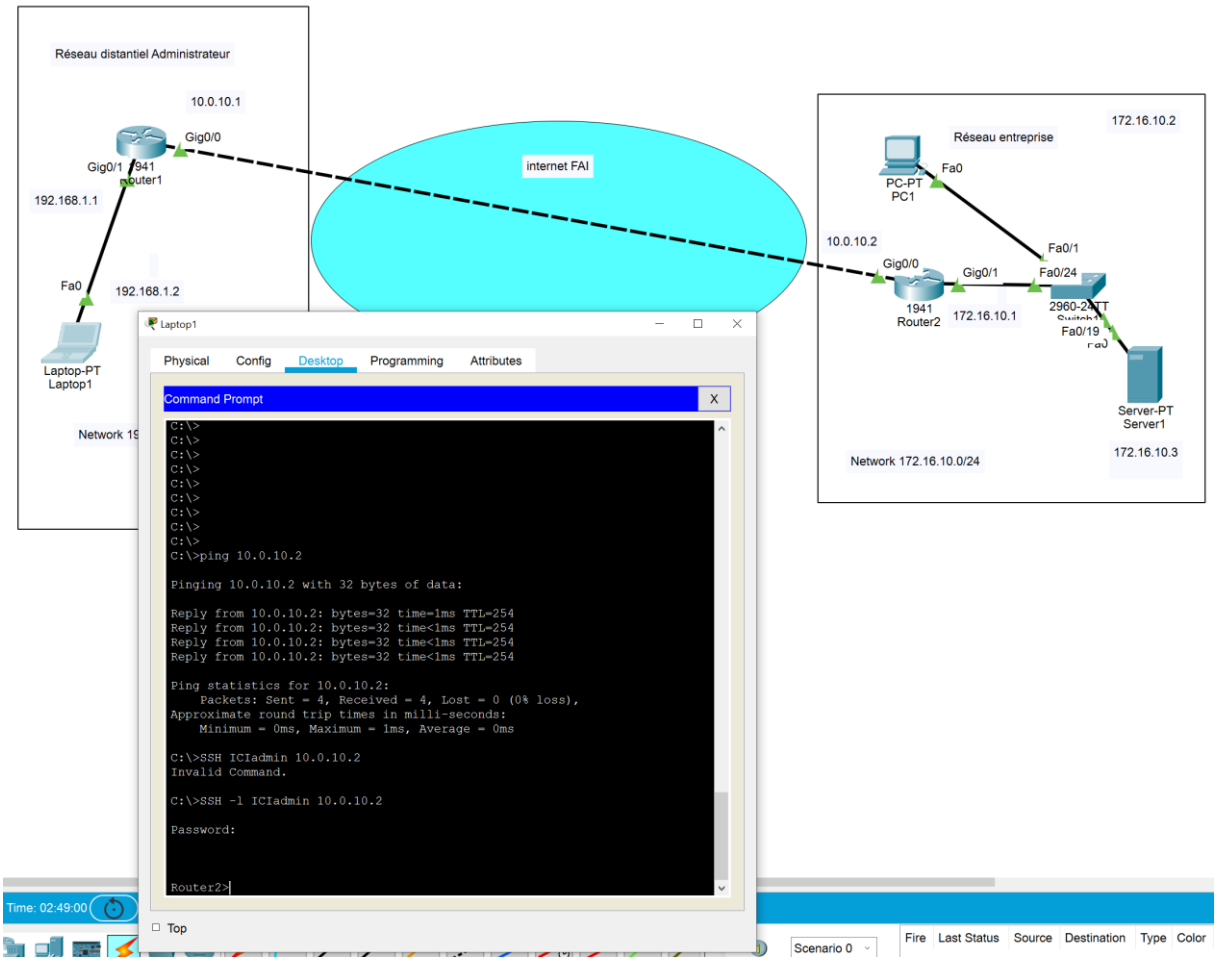
Ici Laptop1 pourra accéder à la console de Router2
Il est possible de réaliser un contrôle de connectivité avec ICMP
Depuis Laptop1 utilisateur distant, via internet

```
C:\>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:

Reply from 10.0.10.2: bytes=32 time=1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



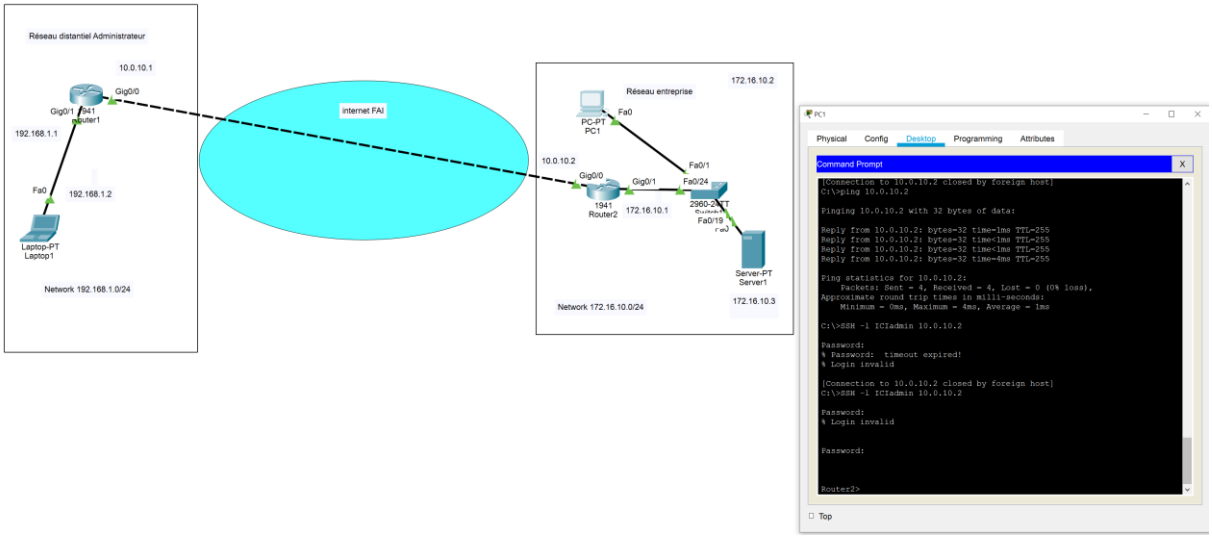
Depuis PC1 utilisateur distant sur l'intranet

```
C:\>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:

Reply from 10.0.10.2: bytes=32 time=1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254
Reply from 10.0.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



2. Définir des accès utilisateurs avec ACLs

ACLs ou Access Control list permet de gérer des accès à des équipements réseaux ou serveurs.

Ce listing permet de limiter l'accès à des équipements ou des réseaux. Si une personne malveillante a été identifié par les administrateurs de l'entreprise. Un spammeur qui souhaite utiliser les service mail de l'entreprise par exemple, une personne qui compte exploiter les failles système pour encrypter des bases de données pour exiger une contrepartie.

Si les moyens de sécurité style honeypot ont pu identifier une adresse publique de la personne malveillante il est alors possible de l'ajouter dans la liste.

- Création d'une ACL : autorise ou interdit l'accès à un réseau
- L'associer à une interface du routeur, en entrée (vers le routeur) ou en sortie (vers l'extérieur)
- Listes CISCO :
    - Standard : 1 à 99 bloque ou autorise une adresse source
      Le plus prêt possible de la destination
    - Etendue 100 à 199 : bloque ou autorise l'adresse source, adresse de destination ou un port ou service (notamment SSH).
      Le plus prêt possible de la source

L'intérêt de ce type de démarche est de rendre progressivement un réseau de plus en plus sur, les éléments recueillis qui ont service à de précédentes intrusion permettrons de réduire .

B. Ouvrir un tunnel SSH, accès client :

Certains contenus, comme des sites ou des équipements peuvent être sécurisés par SSH. Ce protocole à vocation à sécuriser tant les contenus, que les liaisons distantes en chiffrant les transferts d'information dans les 2 sens.
Ce protocole implique certaines contraintes, il faut notamment une autorisation. Une sécurisation préalable est nécessaire et une authentification est nécessaire à chaque connexion. Le principe du tunnel permet de faciliter la procédure d'accès pour un utilisateur identifié sécurisé.

1. Les clients Linux, Mac OS et tous les dérivé d'UNIX (comme BSD) ont une procédure simple :

Depuis le terminal
user@ordinateur $: ss -ND 22* monlogin@serveur** (ou adresse IP de l'équipement)
*il est préférable d'avoir changé le numéro du port SSH à 22 par défaut)
Il convient de taper le mot de passe définit préalablement ou communiqué par l'administrateur
** A ce niveau il faut contrôler l'adresse IP du serveur ou de l'équipement pour s'assurer de communiquer avec le bon destinataire.

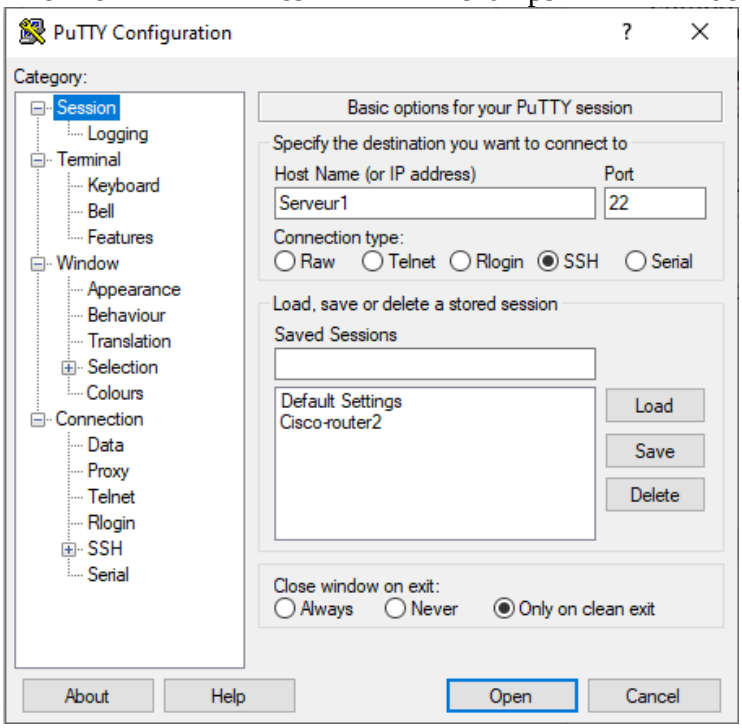
Avant de confirmer la connexion, le client reçoit une information de l'équipement :
Il est alors possible de confirmer « vérification du fingerprint » qui permet d'entrer l'information en mémoire.

2. Client Administrateur Windows, vers un serveur Unix-Linux

Par la suite la simple ligne : ssh -D 22* monlogin@adresse** permet de se connecter
Pour Windows :

Putty est un bon logiciel pour ouvrir des connexions SSH depuis Windows :
Ouvrez le programme putty.exe :

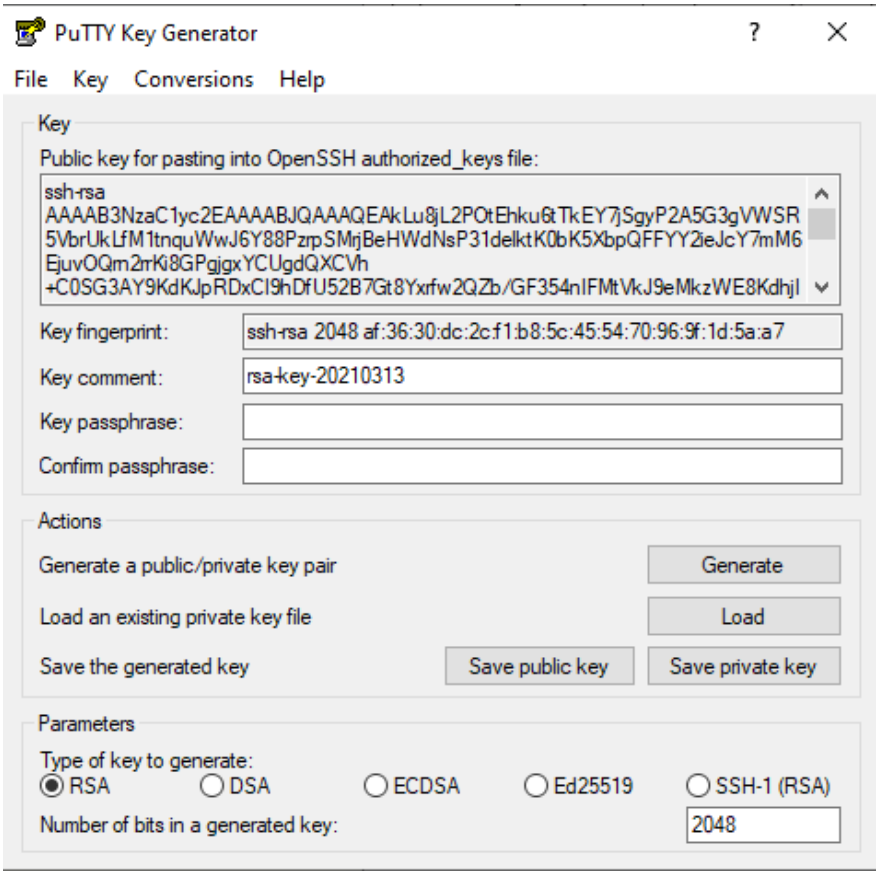
Informer les champs de façon adaptée



SSH-1 est suffisant à ce niveau, il est alors possible de créer des clés publiques et privés pour identifier un utilisateur.

Si vous êtes l'administrateur, il convient alors de générer des clés publiques et privées pour accéder à l'équipement.

Il convient d'utiliser puttygen pour générer une clé RSA d'un minimum de 2048 (ou SSH-2).



Il est possible d'aller plus loin avec les équipements qui prennent en charge SSH-2, mais l'équipement doit avoir été configuré au préalable.

Une clé publique et privée est une paire de fichier compatibles qui permet une authentification de l'utilisateur. Seule la clé publique a vocation à être communiquée, la clé privé elle doit être connue du seul utilisateur ou administrateur.

A ce niveau il est possible de verrouiller cette paire par un mot de passe, c'est une option qui nécessite de se souvenir d'un mot de passe pour déverrouiller l'usage des clés.

Sauvegarder la clé privée dans un lieu sur
Copier coller la clé publique sur l'équipement.

Pour un serveur linux standard :

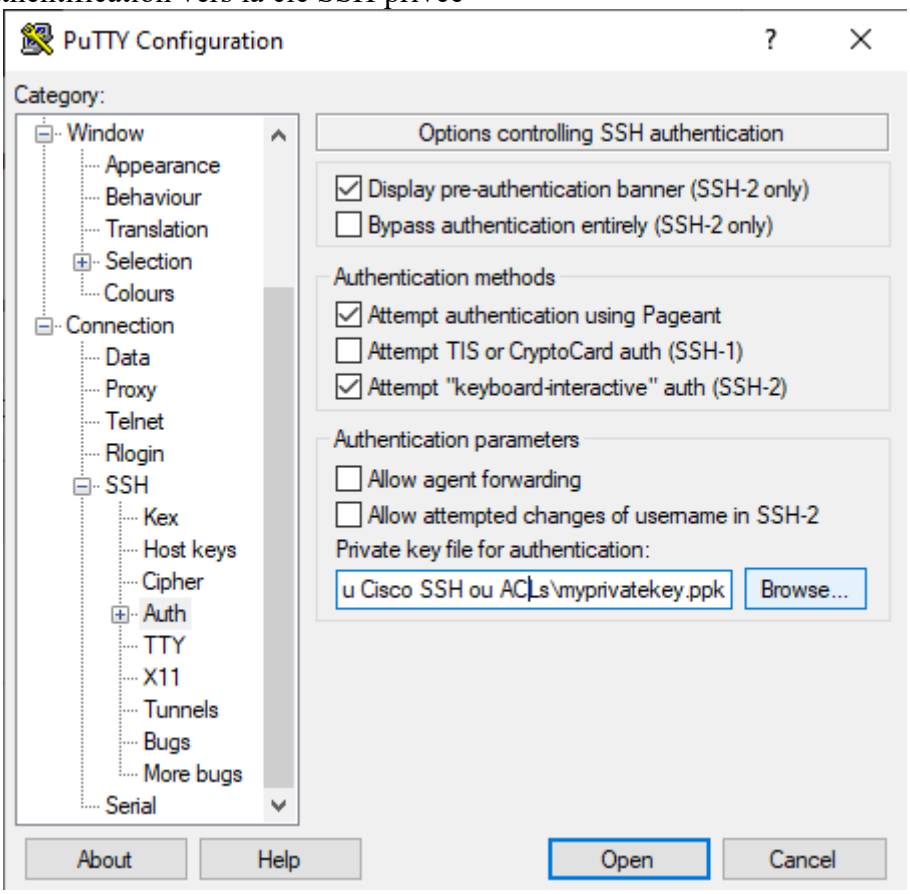
mkdir .ssh
chmod 700 .ssh
cd .ssh
vi authorized_keys
coller la clé publique

il est préférable de rendre intangible cette clé publique avec :
chmod 600 authorized_keys

Cette méthode permet de sécuriser l'accès.

Contrôle de conformité des droits et des fichiers :
pwd
ls -ald .ssh .ssh/authorized_keys

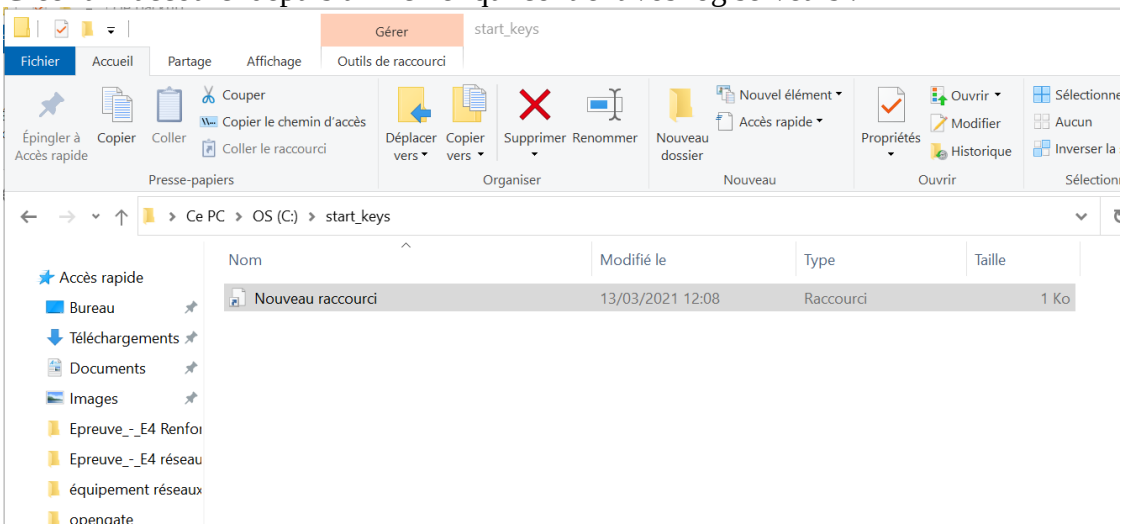
Faciliter l'exécution de la clé privée :
Pointer l'authentification vers la clé SSH privée



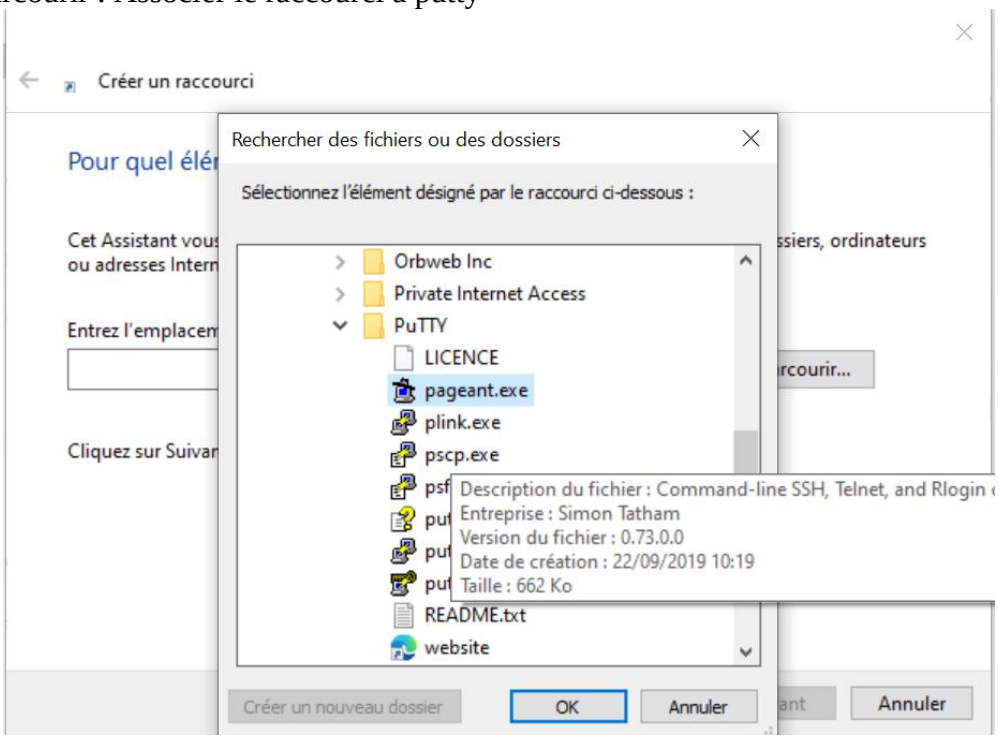
Lancer la connexion au serveur comme vu plus haut : le serveur vous demandera la passphrase ou mot de passe vu plus haut, s'il n'y en a pas, la connexion aboutira directement dans la session utilisateur.

Il est possible de créer un pageant pour faciliter le travail de l'utilisateur :

Créer un raccourci depuis un fichier qui contient vos log serveurs :

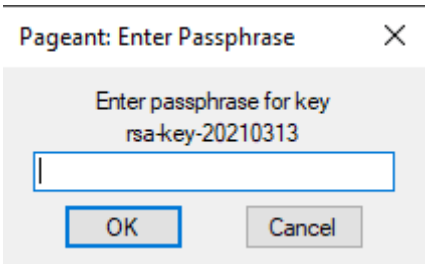


Avec Parcourir : Associer le raccourci à putty

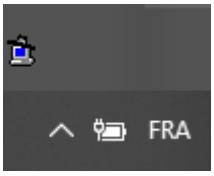


Ajouter au raccourci le chemin vers la clé privée :

Si l'opération s'est bien passée un simple double clique permettra de lancer le pageant :



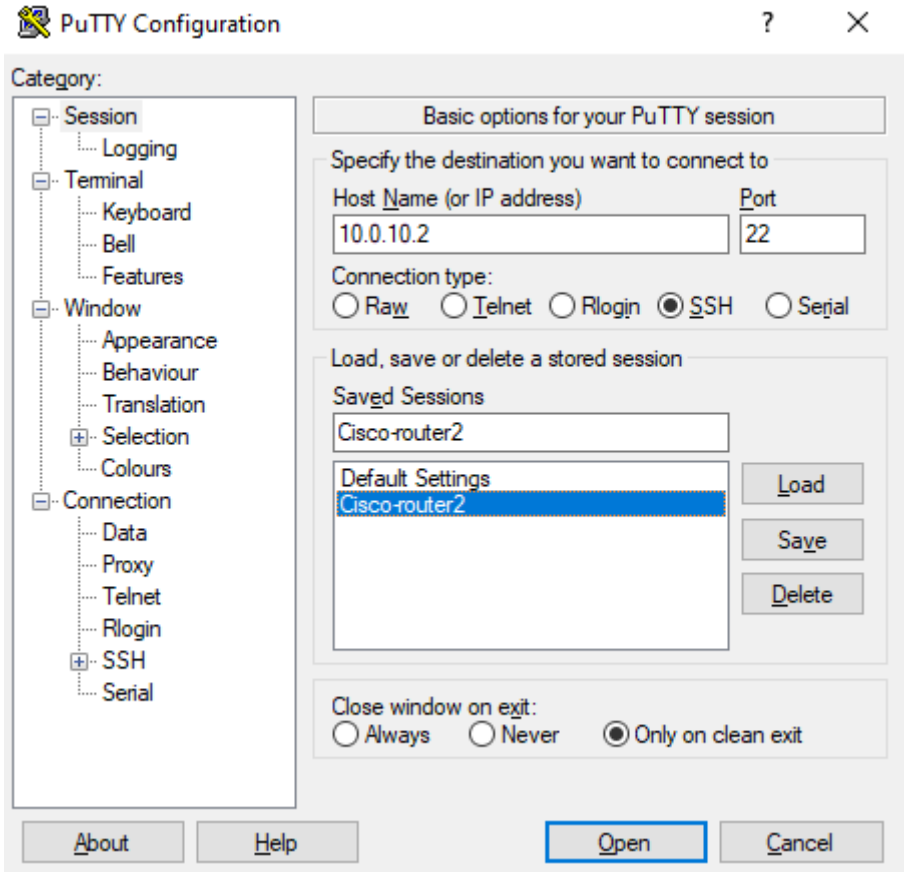
Une icône s'affiche alors dans les éléments en cours d'exécution



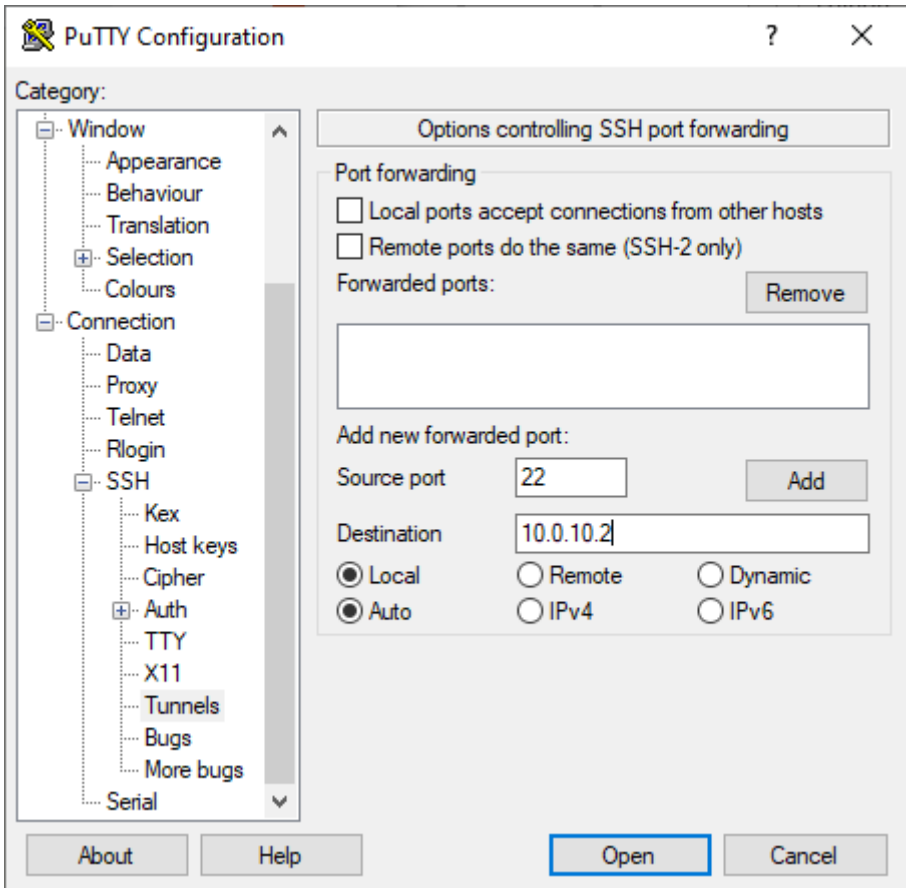
Vos équipements sont alors accessibles en 1 clics de façon sécurisée.

3. Equipement Cisco compatible SSH-2

Les équipements CISCO fonctionnent sous des OS UNIX compatibles avec les procédures vu ci-avant. Les équipements les plus récents, dont les gammes Catalyst intègrent SSH-2 qui permet de configurer de façon sécuriser les équipements comme utilisateur distant.



SSH-2 est compatible avec la création de tunnel :



Putty retourne une information sur le forwarded port :

C. Générer des clés sur l'équipement directement

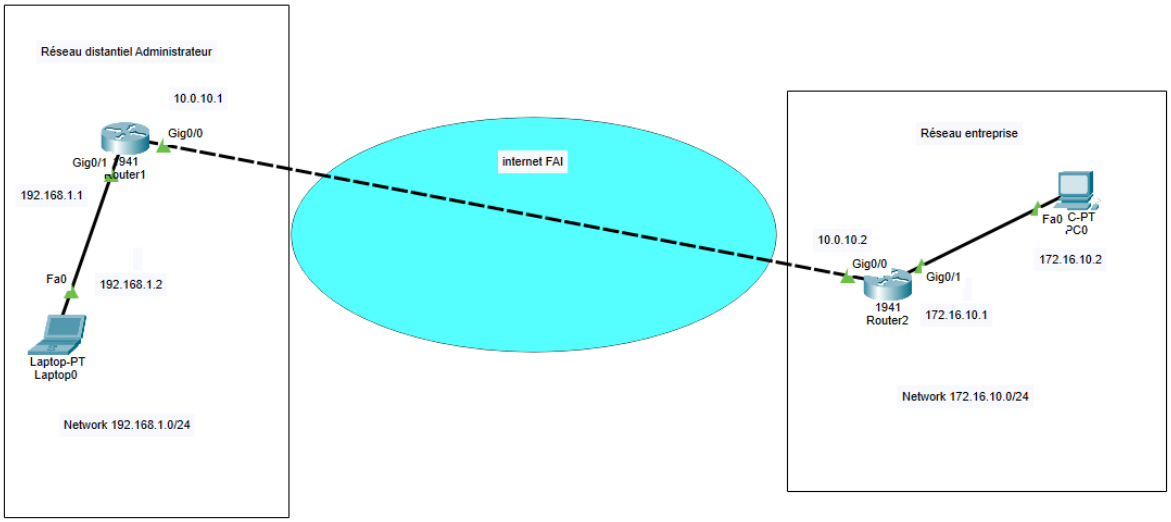
Redondance au niveau software :

Nous proposons d'implémenter un protocole de redondance de niveau 3 :
Mise en place d'équipements en standby pour pouvoir procéder au remplacement d'équipements défectueux sans coupure du réseau.
HSRP et OSPF pour assurer un fonctionnement efficace et la continuité de l'activité des routeurs.

L'infrastructure réseau de niveau 3 est relativement imposante pour le site, mais l'entreprise souhaite se regrouper avec d'autres acteurs du secteur et différentes filiales. Aussi la mise en

Avec définition des accès utilisateurs avec les ACLs (Access control list)

Présentation d'une maquette pour l'exercice, Cisco Packet Tracert



IV. Conclusion

Cette procédure a été présentée pour répondre à différents utilisateurs expérimentés administrateur dans l'optique de faciliter l'inter-compatibilité des différents équipements système sur le même réseau. Les utilisateur d'OS Microsoft, Apple ou Linux pourront tout aussi bien accéder au routeur CISCO configuré.

L'entreprise informatique a mis en place des moyens de défense actifs et passifs pour identifier les hackers ou les auteurs d'activités illicites. Elle assure un contrôle des identités sur son réseau interne avec un annuaires des utilisateurs, un ADDS pour les services Microsoft, un Honeypot. Elle a mise en place un VPN pour la sécurisation des collaborateurs externes. Ces moyens sont des éléments de défense passives autorisées, qui permettront de compléter une liste ACL et de garantir une intégrité accrue du réseau.

SSH est une façon de protéger les équipements réseaux de niveau 3, voir de niveau 2 pour éviter les attaques en provenance de l'extérieur.