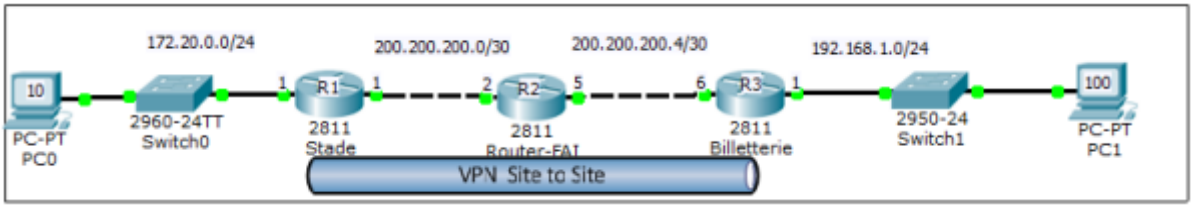
MISSION 3 : Mise en place d'une Solution pour l'Administration à Distance Sécurisée et la Sécurisation des Interconnexions

Représentation de l'infrastructure :



Plan :

- *Partie 1 : Mise en place du VPN.*
- *Partie 2 : Mise en place des Vlans et du NAT.*
- *Partie 3 : Mise en place du SSH.*

Partie 1 : Mise en place du VPN

Configuration du VPN sur le Routeur 1

Etape 1 :

1. La commande : crypto isakmp enable permet d'activer les fonctions crypto du routeur.
Cette fonction peut déjà être activée par défaut sur les IOS avec les options cryptographiques.

```
R1#crypto isakmp enable
```

Etape 2 :

1. Maintenant, il faut commencer par configurer différentes choses comme la police avec la commande : crypto isakmp policy 10.

```
R1(config)#crypto isakmp policy 10
```

2. Après cela, il faut déterminer quel type d'authentification qu'on va utiliser. Pour cela, on peut utiliser la commande : authentification pre-share.

```
R1(config-isakmp)#authentication pre-share
```

3. De plus, déterminer l'encryption qu'on va utiliser en s'aidant de la commande : encryption 3des.

```
R1(config-isakmp)#encryption 3des
```

4. Aussi, quel hash il va falloir mettre en place concernant la vérification de l'intégrité des données échangées. La commande : hash md5 nous permet de le mettre en place.

```
R1(config-isakmp)#hash md5
```

5. Il faut choisir le groupe pour l'échange des clés qu'on va utiliser avec cette commande : group 5. Cela spécifie l'identifiant Diffie-Hellman.

```
R1(config-isakmp)#group 5
```

6. Il faut mettre en place un temps de validité de la connexion avant une nouvelle négociation des clés. Cette commande permet de le spécifier : lifetime 3600.

```
R1(config-isakmp)#lifetime 3600
```

7. Une fois toutes les commandes tapées, la configuration de tous ces éléments est maintenant terminée, il ne reste plus qu'à quitter l'interface en utilisant : exit.

```
R1(config-isakmp)#exit
```

Etape 3 :

1. Il faut configurer la clé que nous allons utiliser en s'aidant de la commande : crypto isakmp key iris123 address 200.200.200.6.
(200.200.200.6 correspond à l'ip du routeur 3)

```
R1(config)#crypto isakmp key iris123 address 200.200.200.6
```

Etape 4 :

1. Pour que les données puissent s'envoyées sans problème, il faut configurer les options de leurs transformations : crypto ipsec transform-set 50 esp-3des-md5-hmac.

```
R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
```

Chose importante à prendre en compte : Il faut utiliser les mêmes protocoles d'encryptions et de hash
Pour notre cas :

- Encryption : 3des.
- Hash : md5.

2. Il faut une nouvelle fois fixer une valeur lifetime mais cette fois-ci concernant les données avec la commande : crypto ipsec security-association lifetime seconds 1800. Au bout de cette durée, il y aura un renouvellement des clés.

```
R1(config)#crypto ipsec security-association lifetime seconds 1800
```

Etape 5 :

1. Cette fois-ci, il faut créer une ACL (liste de contrôle d'accès) qui va permettre de déterminer le trafic autorisé. Il faut pour cela utiliser cette commande : access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255

```
R1(config)#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Etape 6 :

1. Maintenant, il faut pouvoir affilier toutes les configurations qui ont été faites, c'est-à-dire l'access-list, le trafic et la destination. Tout d'abord, il faut nommer la crypto map stade et ensuite on crée une règle de configuration IPsec, entrée n°10 qui nous servira à définir les paramètres du tunnel VPN.

Tout cela se retrouve dans cette commande : crypto map stade 10 ipsec-isakmp.

```
R1(config)#crypto map stade 10 ipsec-isakmp
```

2. Ensuite, on indique le destinataire du tunnel VPN qui est dans notre cas le routeur 3 : set peer 200.200.200.6.

```
R1(config-crypto-map)#set peer 200.200.200.6
```

3. On définit le mode de protection concernant les données, c'est-à-dire un mode de chiffrement mais aussi d'authentification. On utilise cette commande : set transform-set 50.

```
R1(config-crypto-map)#set transform-set 50
```

4. Ici, on définit la durée de vie concernant l'association de sécurité IPsec. Ainsi, les clés se renouvelleront toutes les 15 minutes à l'aide de cette commande : set security-association lifetime seconds 900.

```
R1(config-crypto-map)#set security-association lifetime seconds 900
```

5. De plus, le 101 est relié aux adresses utilisées pour le trafic des données, cela a été configuré plus haut. Donc, on définit quelles seront les données envoyées entre elles avec : match address 101.

```
R1(config-crypto-map)#match address 101
```

6. Enfin, la configuration est terminée, il faut quitter l'interface crypto.

```
R1(config-crypto-map)#exit
```

Etape 7 :

1. Enfin, pour que la crypto map fonctionne, il faut l'appliquer sur l'interface de sortie. Dans notre cas, ce sera l'interface FastEthernet 0/1 du routeur stade donc crypto map stade.

```
R1(config)#interface FastEthernet 0/1
```

```
R1(config-if)#crypto map stade
```

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Ce message apparaît et nous indique que la configuration IPsec/ISAKMP est bien fonctionnelle et active

Configuration du VPN sur le routeur 3

Etape 1 :

1. La commande : crypto isakmp enable permet d'activer les fonctions crypto du routeur.

Cette fonction peut déjà être activée par défaut sur les IOS avec les options cryptographiques.

```
R3(config)#crypto isa
R3(config)#crypto isakmp enable
```

Etape 2 :

1. Maintenant, il faut commencer par configurer différentes choses comme la police qui est une politique ISAKMP avec la commande : crypto isakmp policy 10.

```
R3(config)#crypto isakmp policy 10
```

2. Après cela, il faut déterminer quel type d'authentification qu'on va utiliser. Pour cela, on peut utiliser la commande : authentification pre-share.

```
R3(config)#authentication pre-share
```

3. De plus, déterminer l'encryption qu'on va utiliser en utilisant de la commande : encryption 3des.

```
R3(config)#encryption 3des
```

4. Aussi, quel hash il va falloir mettre en place concernant la vérification de l'intégrité des données échangées. La commande : hash md5 nous permet de le mettre en place.

```
R3(config-isakmp)#hash md5
```

5. Il faut choisir le groupe pour l'échange des clés qu'on va utiliser avec cette commande : group 5. Cela spécifie l'identifiant Diffie-Hellman.

```
R3(config-isakmp)#group 5
```

6. Il faut mettre en place un temps de validité de la connexion avant une nouvelle négociation des clés. Cette commande permet de le spécifier : lifetime 3600.

```
R3(config-isakmp)#lifetime 3600
```

7. Une fois toutes les commandes tapées, la configuration de tous ces éléments est maintenant terminée, il ne reste plus qu'à quitter l'interface en utilisant : exit.

```
R3(config-isakmp)#exit
```

Etape 3 :

1. Il faut configurer la clé pré-partagée que nous allons utiliser pour l'authentification en s'aidant de la commande : crypto isakmp key iris123 address 200.200.200.1.
(200.200.200.1 correspond à l'ip du routeur 1)

```
R3(config)#crypto isakmp key iris123 address 200.200.200.1
```

Etape 4 :

1. Pour que les données puissent s'envoyées sans problème, il faut configurer les options de leurs transformations : crypto ipsec transform-set 50 esp-3des-md5-hmac.

```
R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
```

2. Il faut une nouvelle fois fixer une valeur lifetime mais cette fois-ci concernant les données avec la commande : crypto ipsec security-association lifetime seconds 1800. Au bout de cette durée, il y aura un renouvellement des clés.

```
R3(config)#crypto ipsec security-association lifetime seconds 1800
```

Etape 5 :

1. Cette fois-ci, il faut créer une ACL (liste de contrôle d'accès) qui va permettre de déterminer le trafic autorisé et donc celui qui sera chiffré. Il faut pour cela utiliser cette commande : access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

```
R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
```

Etape 6 :

1. Maintenant, il faut pouvoir affilier toutes les configurations qui ont été faites, c'est-à-dire l'access-list, le traffic et la destination. Tout d'abord, il faut nommer la crypto map billetterie et ensuite on crée une règle de configuration IPsec, entrée n°10 qui nous servira à définir les paramètres du tunnel VPN.
   Tout cela se retrouve dans cette commande : crypto map billetterie 10 ipsec-isakmp.

```
R3(config)#crypto map billetterie 10 ipsec-isakmp
```

2. Ensuite, on indique le destinataire du tunnel VPN qui est dans notre cas le routeur 1 : set peer 200.200.200.1.

```
R3(config-crypto-map)#set peer 200.200.200.1
```

3. On définit le mode de protection concernant les données, c'est-à-dire un mode de chiffrement mais aussi d'authentification. On utilise cette commande : set transform-set 50.

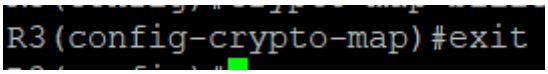
```
R3(config-crypto-map)#set transform-set 50
```

4. Ici, on définit la durée de vie concernant l'association de sécurité IPsec. Ainsi, les clés se renouvelleront toutes les 15 minutes à l'aide de cette commande : set security-association lifetime seconds 900.

```
R3(config-crypto-map)#set security association lifetime seconds 900
```

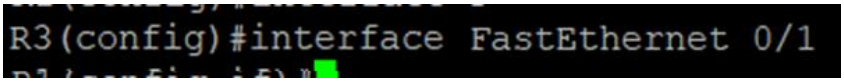
5. De plus, le 101 est relié aux adresses utilisées pour le trafic des données, cela a été configuré plus haut. Donc, on définit quelles seront les données envoyées entre elles avec : match address 101.

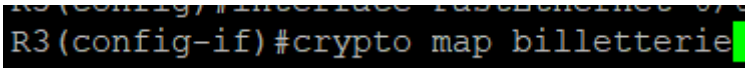
6. Enfin, la configuration est terminée, il faut quitter l'interface crypto.



Etape 7 :

1. Enfin, pour que la crypto map fonctionne, il faut l'appliquer sur l'interface de sortie. Dans notre cas, ce sera l'interface FastEthernet 0/1 du routeur billetterie donc crypto map billetterie.





*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Ce message apparaît et nous indique que la configuration IPsec/ISAKMP est bien fonctionnelle et active.

Vérification de la configuration sur chaque routeur

Pour pouvoir le vérifier, il faut taper cette commande sur chaque routeur et regarder d'abord si c'est la bonne interface tout comme la bonne adresse.

Show Running

La commande "show running" permet d'afficher toute la configuration en cours d'exécution, et permet de constater si la configuration entre R1 et R3 est identique.

```
R1#show running
Building configuration...

Current configuration : 1577 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key iris123 address 200.200.200.6
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
!
crypto map stade 10 ipsec-isakmp
 set peer 200.200.200.6
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
!
!
!
!
interface FastEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.200.200.1 255.255.255.252
 duplex auto
 speed auto
 crypto map stade
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 1
 network 172.20.0.0 0.0.0.255
 network 200.200.200.0 0.0.0.3
 auto-summary
```

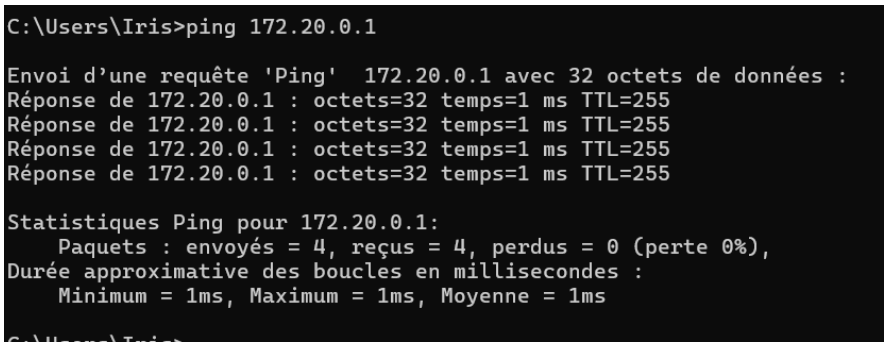
La partie la plus importante se situe au niveau du crypto isakmp ainsi que la suite de la configuration crypto.

Il faut que le type encryptage et le hash soient identiques sur le R1 et le R3.
Vérification du R3 ci-dessous.

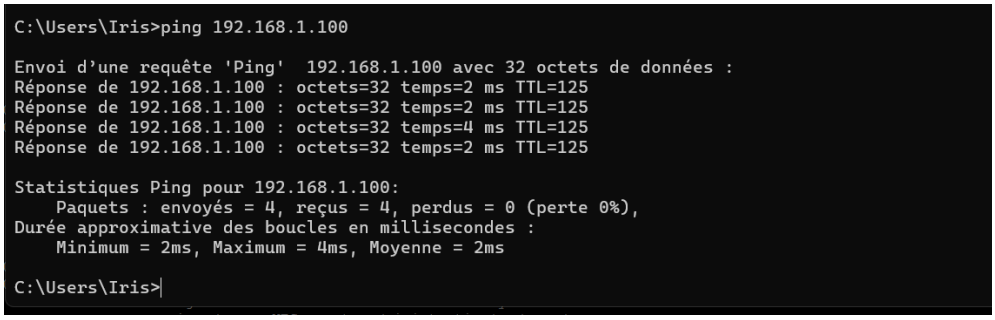
```
hostname R3
!
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
```

Vérification ping entre les deux routeurs :

R1 vers R3 : Le ping fonctionne correctement !



R3 vers R1 : Le ping fonctionne correctement !



Les pings entre les routeurs, d'un côté comme de l'autre fonctionne, cela montre que la configuration a bien été faite. Ils peuvent donc communiquer entre eux et le chiffrement fonctionne aussi dans les deux sens.

Partie 2 : Mise en place du NAT

Configuration du NAT sur le routeur

Préparation du matériel pour les configurations :

Etape 1 :

1. Avant de commencer toute configuration, il faut réinitialiser le matériel.

Pour cela, sur le switch, il faut taper 3 commandes à la suite qui sont les suivantes :
Erase startup-config : qui sert à supprimer le fichier de configuration se trouvant dans le NVRAM.

```
Switch#erase startup-config
```

Delete flash :vlan.dat : Supprime le fichier vlan.dat qui comporte les configurations des VLANs.

```
Switch#delete flash:vlan.dat
```

Reload : Redémarre le switch pour que tout soit remis à 0.

```
Switch#reload
```

Etape 2 :

1. On refait la même chose du côté du routeur sauf la commande delete flash :vlan.dat

Erase startup-config : qui sert à supprimer le fichier de configuration se trouvant dans le NVRAM.

```
Router#erase startup-config
```

Reload : Redémarre le switch pour que tout soit remis à 0.

```
Router#reload
```

Etape 3 :

1. Après cela, il faut renommer le switch ainsi que le routeur.

La commande suivante permet de le faire : hostname en étant en conf t.
Pour le switch :

```
Switch(config)#hostname SW1-SRV
```

Pour le routeur :

```
Router(config)#hostname R1
R1(config)#
```

Etape 4 :

1. Pour commencer la configuration du NAT, il faut créer un lien entre le routeur et internet. Tout d'abord, c'est l'interface FastEthernet 0/1 qui obtiendra automatiquement une IP avec DHCP et qui servira au routeur d'accéder à internet. Il faut utiliser les commandes suivantes :
Interface fastEthernet 0/1 puis ip address dhcp.
De plus, on utilise la commande no shutdown qui permet d'activer l'interface.
Puis, désigner un port de sorti avec la commande : ip nat outside.

```
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
R1(config-if)#ip nat outside
R1(config-if)#
*Jan  1 00:37:21.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
```

Etape 5 :

1. Maintenant, pour chaque VLAN, on utilise la commande ip nat inside qui indique que le trafic venant de tel VLAN est considéré comme interne pour la traduction NAT.
Pour se faire, on choisit l'interface de chaque VLAN avec cette commande :
Interface fastEthernet 0/0.10 par exemple.

2. On configure le côté LAN du NAT de l'interface sous réseau du VLAN 10.

```
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#ip nat inside
R1(config-subif)#exit
```

3. On configure le côté LAN du NAT de l'interface sous réseau du VLAN 20.

```
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#ip nat inside
R1(config-subif)#exit
```

4. On configure le côté LAN du NAT de l'interface sous réseau du VLAN 30.

```
R1(config)#interface fastEthernet 0/0.30
R1(config-subif)#ip nat inside
R1(config-subif)#exit
```

Etape 6 :

1. Il faut définir les listes d'accès standard, pour identifier quelles adresses IP internes sont autorisées à être traduites lorsqu'elles sortent vers internet. Utiliser la commande suivante :

   Access-list 10 (correspond au VLAN) permit 172.20.0.0 0.0.0.255.

   Et reproduire la même chose pour les autres VLANs.

```
R1(config)#access-list 10 permit 172.20.0.0 0.0.0.255
R1(config)#access-list 20 permit 172.20.1.0 0.0.0.255
R1(config)#access-list 30 permit 172.20.2.0 0.0.0.127
```

2. Indiquer vers où est le NAT aux différents VLANs, et overload signifie que plusieurs adresses internes partagent une seule adresse IP publique.

   La commande suivante permet de le mettre en place :

   Ip nat inside source list 10 interface fastEthernet 0/1 overload.

   Encore une fois, reproduire la même chose pour les autres VLANs.

```
R1(config)#ip nat inside source list 10 interface fastEthernet 0/1 overload
R1(config)#ip nat inside source list 20 interface fastEthernet 0/1 overload
R1(config)#ip nat inside source list 30 interface fastEthernet 0/1 overload
```

Etape 7 :

1. Maintenant il faut définir une route par défaut spécifique à notre réseau pour aller vers internet.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.228.1
```

Vérification de la configuration sur le routeur

Sur le routeur, on utilise la commande : show ip interface brief.

Il faut vérifier si l'interface 0/1 à bien récupérer une IP dynamique grâce au DHCP.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  up                    up
FastEthernet0/0.10         172.20.0.1      YES manual up                    up
FastEthernet0/0.20         172.20.1.1      YES manual up                    up
FastEthernet0/0.30         172.20.2.1      YES manual up                    up
FastEthernet0/1            10.0.228.28     YES DHCP   up                    up
Serial0/1/0                unassigned      YES unset  administratively down down
Serial0/1/1                unassigned      YES unset  administratively down down
NVI0                       unassigned      NO  unset  up                    up
```

De plus, il faut vérifier que l'interaction entre chaque VLANs soit fonctionnelle.

Depuis un PC externe, on ping un PC depuis le VLAN 20 vers le VLAN 10.

```
PS C:\Users\Users> ping 172.20.0.10

Envoi d'une requête 'Ping'  172.20.0.10 avec 32 octets de données :
Réponse de 172.20.0.10 : octets=32 temps=4 ms TTL=127
Réponse de 172.20.0.10 : octets=32 temps=5 ms TTL=127
Réponse de 172.20.0.10 : octets=32 temps=4 ms TTL=127
Réponse de 172.20.0.10 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 172.20.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 5ms, Moyenne = 4ms
```

Ici, on ping un PC se trouvant sur le VLAN 20 vers le VLAN 30.

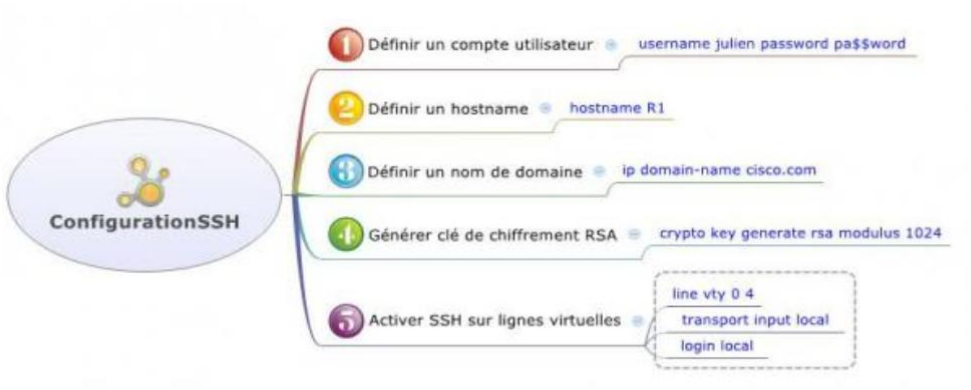
```
PS C:\Users\Users> ping 172.20.2.10

Envoi d'une requête 'Ping'  172.20.2.10 avec 32 octets de données :
Réponse de 172.20.2.10 : octets=32 temps=4 ms TTL=127
Réponse de 172.20.2.10 : octets=32 temps=4 ms TTL=127
Réponse de 172.20.2.10 : octets=32 temps=2 ms TTL=127
Réponse de 172.20.2.10 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 172.20.2.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 4ms, Moyenne = 3ms
```

Ainsi, la connexion inter-vlan est bien fonctionnelle entre tous les VLANs.

Partie 3 : Mise en place du SSH



Configuration des mots de passe sur le routeur

Etape 1 :

1. Il est possible de définir un mot de passe facultatif pour la console, et cela est recommandé de le faire. Les commandes suivantes permettant de le faire :

Line console 0

Login

Password Bts2026$

```
R1(config)#line console 0
R1(config-line)#login
% Login disabled on line 0, until 'password' is set
R1(config-line)#password Bts2026$
R1(config-line)#login
R1(config-line)#password Bts2026$
R1(config-line)#exit
```

2. De plus, il faut aussi configurer un mot de passe sur le terminal virtuel car cela permettrait à un utilisateur d'accéder à distance au routeur via telnet. Les commandes suivantes permettent de définir un mot de passe sur les lignes VTY :

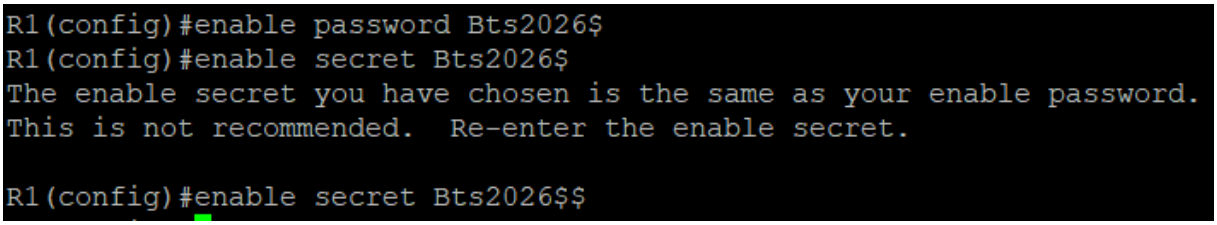
Line vty 0 4

Login

Password Bts2026$

```
R1(config)#line vty 0 4
R1(config-line)#login
% Login disabled on line 194, until 'password' is set
% Login disabled on line 195, until 'password' is set
% Login disabled on line 196, until 'password' is set
% Login disabled on line 197, until 'password' is set
% Login disabled on line 198, until 'password' is set
R1(config-line)#password Bts2026$
R1(config-line)#exit
```

3. Concernant la configuration des mots de passe enable et enable secret qui sont utilisés pour empêcher l'accès au mode privilège. Il est recommandé de mettre en place el mot de passe enable secret car il est crypté.
Pour cela, il faut utiliser les commandes suivantes :
Enable password Bts2026$
Enable secret Bts2026$$
Il y a un message d'erreur recommandant de ne pas mettre le même mot de passe entre enable et enable secret.



Configuration du SSH sur le routeur

Etape 1 :

1. Définir un compte utilisateur en choisissant un login et un mot de passe. Ici le login sera user1 et le mot de passe Bts2026$.
   Cette commande permet de le faire : username user1 password Bts2026$.

```
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username user1 password Bts2026$
```

Etape 2 :

1. Pour que le routeur génère des clés RSA, il faut obligatoirement indiquer un nom de domaine à l'aide de la commande suivante : ip domain-name stadiumcompany.local.

```
R1(config)#ip domain-name stadiumcompany.local
```

2. Après cela, générer les clés cryptographiques RSA qui seront utilisées par le SSH avec la commande : crypto key generate rsa general-keys modulus 1024.

```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.stadiumcompany.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Jan  1 02:29:24.651: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

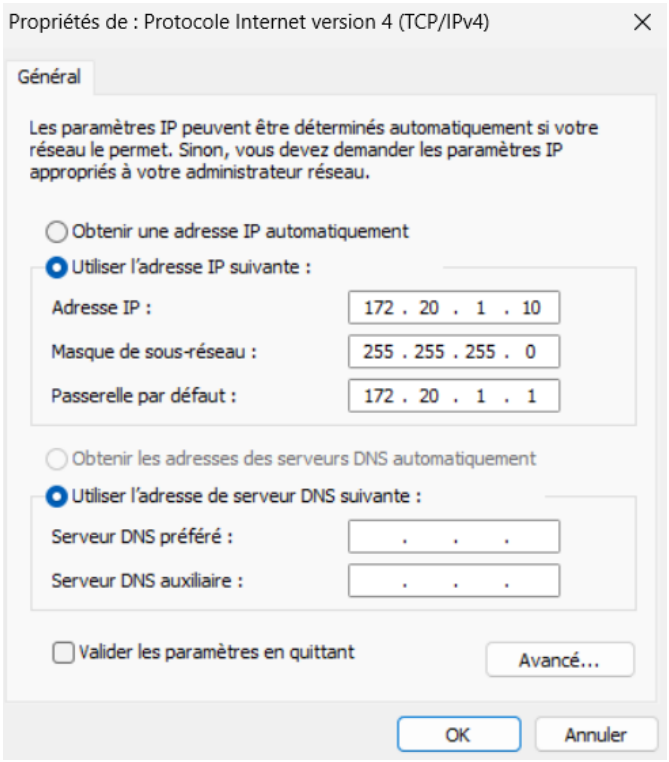
Etape 3 :

1. Pour activer le SSH, il faut utiliser la commande : line vty 0 4 qui permet de configurer des lignes de connexions à distance.
   La commande transport input ssh indique qu'on utilisera le protocole SSH.
   Enfin, la commande login local indique que la connexion doit utiliser les comptes locaux créés sur le routeur.

```
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
```

Vérification de la configuration

1. Pour procéder à la vérification, il faut brancher un poste (PC) sur le vlan 20, et régler l'IP du poste en 172.20.1.10.

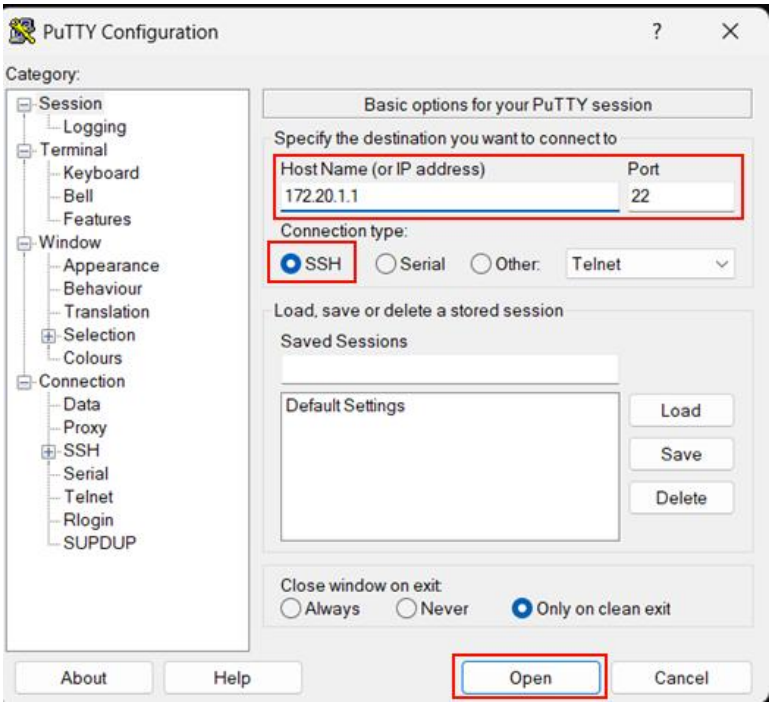


2. Ensuite, procéder à un Ipconfig / all sur l'invité de commande du poste et vérifier que l'IP a bien été prise en compte.

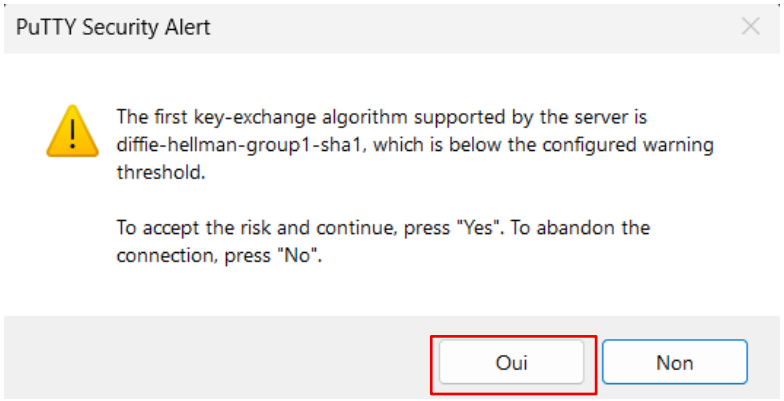
```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.1.10
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.20.1.1
```

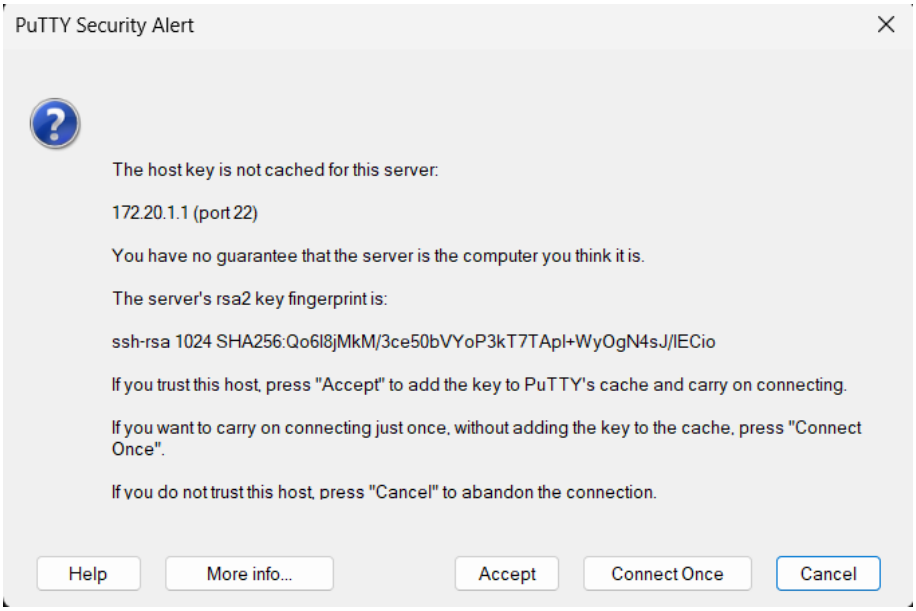
3. Sur l'application Putty, mettre l'IP du routeur, laisser cocher SSH, le port 22 par défaut, puis ouvrir la connexion.



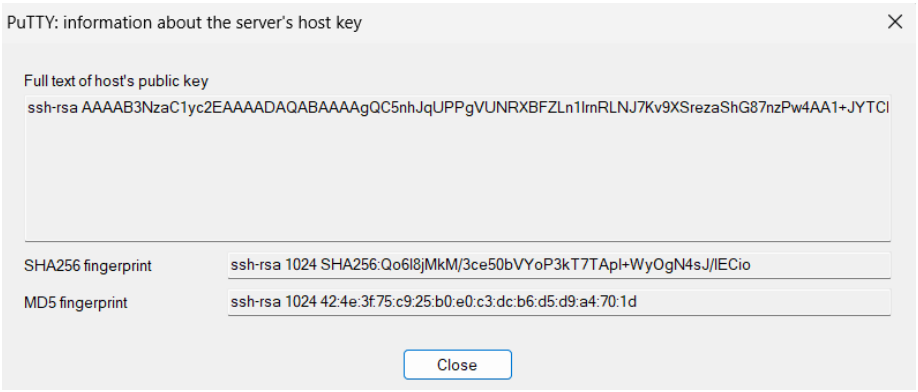
4. Une alerte apparaît ci-dessous expliquant que le serveur utilise un algorithme ancien, qui est considéré comme faible actuellement, donc il nous prévient que le niveau de sécurité est faible. Cliquer sur oui pour continuer malgré le risque.



5. Après cela, un message sous indique que le serveur a généré une empreinte (fingerprint) et nous laisse le choix entre accepter la connexion et conserver l'empreinte pour les futurs connexions, se connecter une seule fois ou annuler la connexion.



6. En cliquant sur more info..., cela nous permet d'avoir plus d'informations sur la clé.



7. Enfin, en cliquant sur Accept, on se connecte bien sur le routeur R1 avec le login choisi plus tôt.