Mission 3 : Administration à Distance Sécurisée et Sécurisation des Interconnexions

StadiumCompany - Protocole SSH, VPN IPSec et Access Control Lists

Haidara Ibrahim

CONTEXTE DE LA MISSION 3 : La sécurisation des interconnexions et de l'administration à distance constitue un enjeu majeur pour StadiumCompany, dont les trois sites (Stade, Billetterie, Magasin) doivent communiquer de manière sécurisée tout en permettant une gestion centralisée de l'infrastructure réseau. Les équipements CISCO (routeurs et commutateurs) déployés lors de la Mission 1 nécessitent désormais une protection renforcée contre les accès non autorisés et les interceptions de données.

Le protocole SSH (Secure Shell) remplace Telnet pour l'administration à distance, offrant un chiffrement des communications et une authentification robuste via des clés RSA. Les liaisons inter-sites entre le Stade et les sites distants sont sécurisées par des tunnels VPN site-à-site utilisant IPSec, garantissant la confidentialité et l'intégrité des données transitant sur Internet. Le protocole IPSec, avec chiffrement 3DES et authentification MD5-HMAC, établit des associations de sécurité (SA) dynamiques entre les passerelles VPN situées sur les routeurs d'extrémité.

Les Access Control Lists (ACL) complètent le dispositif de sécurité en filtrant le trafic réseau selon des règles précises. Les ACL standard (numérotées 1-99) contrôlent l'accès par adresse IP source, tandis que les ACL étendues (100-199) permettent un filtrage granulaire par protocole, port source/destination et adresses IP. Ces ACL sécurisent notamment l'accès aux lignes VTY des équipements CISCO, limitant les connexions SSH aux seules adresses IP autorisées.

PARTIE 1 : CONFIGURATION SSH SUR LES ÉQUIPEMENTS CISCO

1.1. Sécurisation Préalable : Mots de Passe sur le Routeur

Avant d'activer SSH, il faut sécuriser les accès de base au routeur avec des mots de passe. Trois types de mots de passe sont nécessaires : console (accès physique), VTY (accès distant) et enable (mode privilégié).

Mot de passe de console

```
! Sécurisation de l'accès physique console Router(config)# line console 0
Router(config-line)# login Router(config-line)# password Bts2026$ Router(config-
line)# exit
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1-stade
R1-stade(config)#line console 0
R1-stade(config-line)#login
% Login disabled on line 0, until 'password' is set
R1-stade(config-line)#password Bts2026$
R1-stade(config-line)#
```

Mot de passe VTY (Telnet/SSH)

```
! Sécurisation des lignes de terminal virtuel Router(config)# line vty 0 4
Router(config-line)# login Router(config-line)# password Bts2026$ Router(config-
line)# exit
```

```
Password:
R1-stade>en
R1-stade#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-stade(config)#line console 0
R1-stade(config-line)#line vty 0 4
R1-stade(config-line)#login
% Login disabled on line 514, until 'password' is set
% Login disabled on line 515, until 'password' is set
% Login disabled on line 516, until 'password' is set
% Login disabled on line 517, until 'password' is set
% Login disabled on line 518, until 'password' is set
R1-stade(config-line)#password Bts2026$
```

Mots de passe enable

```
! Mot de passe enable (en clair - non recommandé seul) Router(config)# enable
password Bts2026$ ! Mot de passe enable secret (chiffré MD5 - recommandé)
Router(config)# enable secret Bts2026$
```

```
% Login disabled on line 515, until 'password' is set
% Login disabled on line 516, until 'password' is set
% Login disabled on line 517, until 'password' is set
% Login disabled on line 518, until 'password' is set
R1-stade(config-line)#password Bts2026$
R1-stade(config-line)#enable password Bts2026$
R1-stade(config)#enable secret Bts2026$$
```

⚠ **Important** Si les deux mots de passe (enable password et enable secret) sont configurés, seul l'enable secret sera utilisé. L'enable secret est chiffré avec MD5, tandis que l'enable password est en clair dans la configuration.

1.2. Configuration SSH Complète sur R1-Stade

La configuration SSH nécessite 5 étapes obligatoires : créer un utilisateur local, définir un hostname, configurer un nom de domaine, générer la clé RSA, et activer SSH sur les lignes VTY.

Étape 1 : Créer un utilisateur local

```
Router> enable Router# configure terminal Router(config)# username user1 password Bts2026$
```

```
R1-stade(config)#enable
% Incomplete command.

R1-stade(config)#username user1 password Bts2026$
R1-stade(config)#
```

Étape 2 : Définir le nom de domaine

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

```
R1-stade(config)#username user1 password Bts2026$
R1-stade(config)#ip domain-name stadiumcompany.local
R1-stade(config)#
```

Configuration du nom de domaine stadiumcompany.local

Étape 3 : Générer la clé RSA

```
R1-Stade(config)# crypto key generate rsa modulus 1024 ! Le routeur affiche : The name for the keys will be: R1-Stade.stadiumcompany.local % Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
```

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

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

R1-stade(config)#
*Jan  1 03:04:00.483: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Génération de la clé RSA 1024 bits

Étape 4 : Activer SSH sur les lignes VTY

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

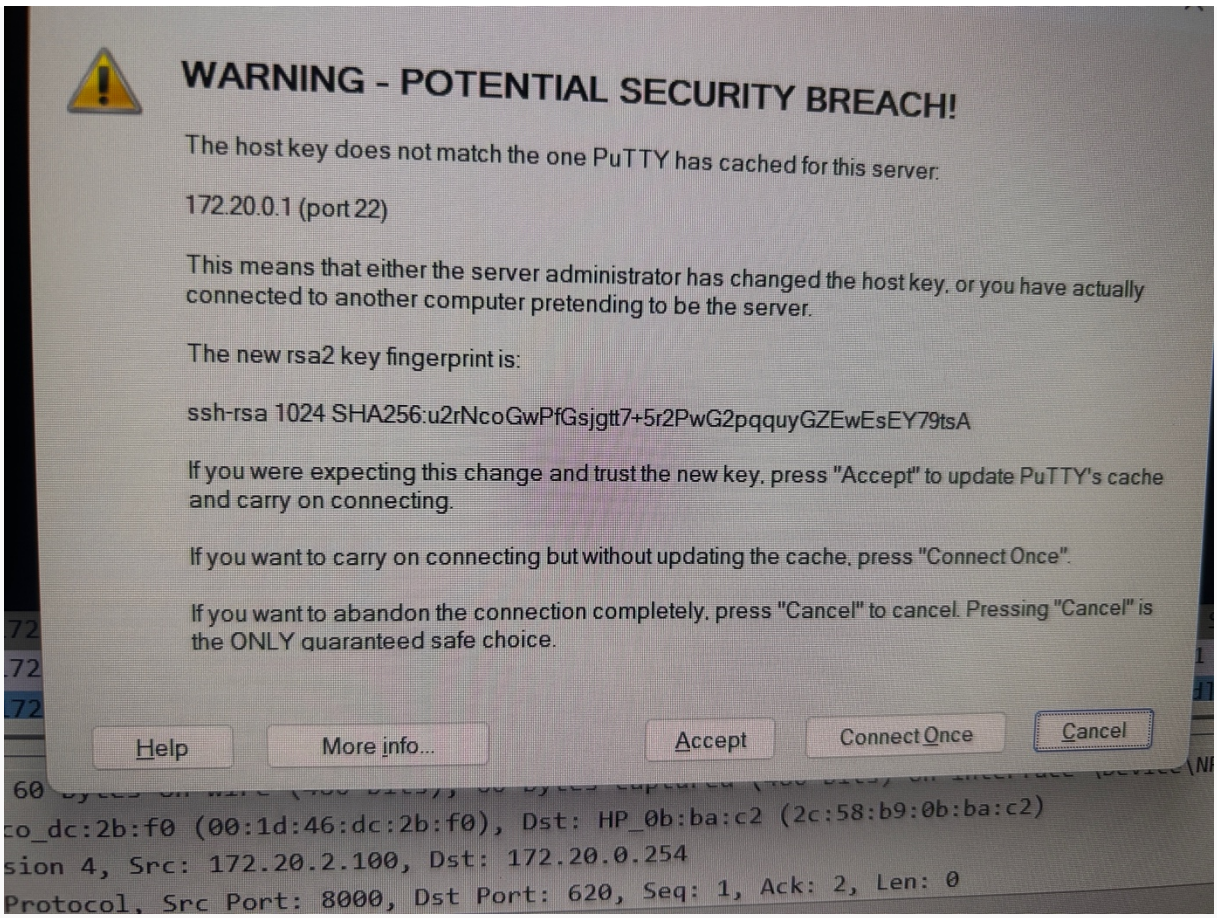
```
R1-stade(config)#
R1-stade(config)#line vty 0 4
R1-stade(config-line)#transport input ssh
R1-stade(config-line)#login local
R1-stade(config-line)#exit
R1-stade(config)#
```

Activation SSH sur les lignes VTY

1.3. Test de Connexion SSH

Une fois SSH configuré, tester la connexion depuis un poste client pour valider le bon fonctionnement.

```
# Depuis un client Linux ou Windows PowerShell ssh user1@172.20.0.1 # Accepter l'empreinte à la première connexion Are you sure you want to continue connecting (yes/no)? yes # Entrer le mot de passe Password: Bts2026$ # Connexion réussie R1-Stade>
```



Connexion SSH réussie au routeur R1-Stade

```
! Vérifications sur le routeur R1-Stade# show ip ssh SSH Enabled - version 2.0 R1-Stade# show ssh Connection Version Mode Encryption State Username 0 2.0 IN aes256-cbc Session started user1
```

PARTIE 2 : CONFIGURATION VPN SITE-À-SITE IPSEC

2.1. Topologie et Architecture VPN

Le VPN site-à-site connecte le site du Stade avec les sites distants (Billetterie et Magasin) via des tunnels IPSec sécurisés traversant Internet. Le VPN se configure uniquement sur les routeurs d'extrémité.

Site	Routeur	Réseau Local	IP Publique

Stade	R1-Stade	172.20.0.0/22	200.200.200.1
Billetterie	R3-Billetterie	192.168.1.0/24	200.200.200.6

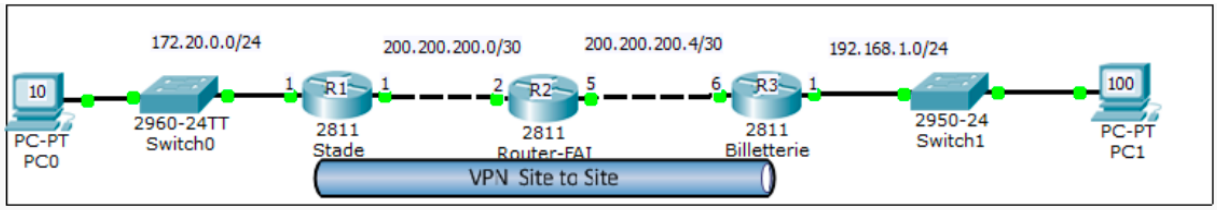


Schéma de la topologie VPN (Stade ↔ Internet ↔ Billetterie)

2.2. Configuration VPN sur R1-Stade (6 étapes)

Étape 1 : Activer ISAKMP

```
R1-Stade(config)# crypto isakmp enable
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentification pre-share
                  ^
% Invalid input detected at '^' marker.

R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key iris123 address 200.200.200.6
R1(config)#crypto isakmp key 6  iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R1(config)#$ 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#crypto map stade 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
R1(config-if)#
*Oct 17 10:14:00.111: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
R3>en
R3#cong t
     ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#crypto isakmp key iris123 address 200.200.200.1
R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1
A pre-shared key for address mask 200.200.200.1 255.255.255.255 already exists!

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192
% Incomplete command.

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0
% Incomplete command.

R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)#crypto map billeterie 10 ispec-isakmp
                                 ^
```

Activation d'ISAKMP

Étape 2 : Configurer la politique ISAKMP

```
R1-Stade(config)# crypto isakmp policy 10 R1-Stade(config-isakmp)# authentication
pre-share R1-Stade(config-isakmp)# encryption 3des R1-Stade(config-isakmp)# hash
md5 R1-Stade(config-isakmp)# group 5 R1-Stade(config-isakmp)# lifetime 3600 R1-
Stade(config-isakmp)# exit
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentification pre-share
                  ^
% Invalid input detected at '^' marker.

R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key iris123 address 200.200.200.6
R1(config)#crypto isakmp key 6  iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R1(config)#$ 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#crypto map stade 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
R1(config-if)#
*Oct 17 10:14:00.111: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
R3>en
R3#cong t
     ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#crypto isakmp key iris123 address 200.200.200.1
R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1
A pre-shared key for address mask 200.200.200.1 255.255.255.255 already exists!

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192
% Incomplete command.

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0
% Incomplete command.

R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)#crypto map billeterie 10 ispec-isakmp
                                 ^
```

Configuration politique ISAKMP (3DES, MD5, groupe 5)

Étape 3 : Configurer la clé pré-partagée

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

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentification pre-share
                  ^
% Invalid input detected at '^' marker.

R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key iris123 address 200.200.200.6
R1(config)#crypto isakmp key 6  iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R1(config)#$ 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#crypto map stade 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
R1(config-if)#
*Oct 17 10:14:00.111: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
R3>en
R3#cong t
     ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#crypto isakmp key iris123 address 200.200.200.1
R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1
A pre-shared key for address mask 200.200.200.1 255.255.255.255 already exists!

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192
% Incomplete command.

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0
% Incomplete command.

R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)#crypto map billeterie 10 ispec-isakmp
                                 ^
```

Configuration clé pré-partagée vers Billetterie

Étape 4 : Configurer le transform-set

```
R1-Stade(config)# crypto ipsec transform-set 50 esp-3des esp-md5-hmac R1-
Stade(config)# crypto ipsec security-association lifetime seconds 1800
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentification pre-share
                  ^
% Invalid input detected at '^' marker.

R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key iris123 address 200.200.200.6
R1(config)#crypto isakmp key 6  iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R1(config)#$ 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#crypto map stade 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
R1(config-if)#
*Oct 17 10:14:00.111: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
R3>en
R3#cong t
     ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#crypto isakmp key iris123 address 200.200.200.1
R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1
A pre-shared key for address mask 200.200.200.1 255.255.255.255 already exists!

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192
% Incomplete command.

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0
% Incomplete command.

R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)#crypto map billeterie 10 ispec-isakmp
                                 ^
```

Configuration transform-set IPSec

Étape 5 : Créer l'ACL pour le trafic VPN

```
R1-Stade(config)# access-list 101 permit ip 172.20.0.0 0.0.3.255 192.168.1.0
0.0.0.255
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentification pre-share
                  ^
% Invalid input detected at '^' marker.

R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key iris123 address 200.200.200.6
R1(config)#crypto isakmp key 6  iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R1(config)#$ 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#crypto map stade 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 200.200.200.6
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
R1(config-if)#
*Oct 17 10:14:00.111: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#
R3>en
R3#cong t
     ^
% Invalid input detected at '^' marker.

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#crypto isakmp key iris123 address 200.200.200.1
R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1
A pre-shared key for address mask 200.200.200.1 255.255.255.255 already exists!

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
R3(config)#access-list 101 permit ip 192
% Incomplete command.

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0
% Incomplete command.

R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)#crypto map billeterie 10 ispec-isakmp
                                 ^
```

Création ACL définissant le trafic à chiffrer

Étape 6 : Créer et appliquer la crypto map

```
R1-Stade(config)# crypto map stade 10 ipsec-isakmp R1-Stade(config-crypto-map)# set
peer 200.200.200.6 R1-Stade(config-crypto-map)# set transform-set 50 R1-
Stade(config-crypto-map)# set security-association lifetime seconds 900 R1-
Stade(config-crypto-map)# match address 101 R1-Stade(config-crypto-map)# exit R1-
Stade(config)# interface FastEthernet 0/1 R1-Stade(config-if)# crypto map stade
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
R1>en
R1#show crypto map
Crypto Map "stade" 10 ipsec-isakmp
        Peer = 200.200.200.6
        Extended IP access list 101
            access-list 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 200.200.200.6
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                50:  { esp-3des esp-md5-hmac  } ,
        }
        Interfaces using crypto map stade:
                FastEthernet0/1
```

Crypto map créée et appliquée sur Fa0/1

2.3. Configuration VPN sur R3-Billetterie

Configuration identique sur R3, avec inversion des réseaux dans l'ACL et changement des IPs.

```
! Configuration complète R3-Billetterie R3-Billetterie(config)# crypto isakmp
enable R3-Billetterie(config)# crypto isakmp policy 10 R3-Billetterie(config-
isakmp)# authentication pre-share R3-Billetterie(config-isakmp)# encryption 3des
R3-Billetterie(config-isakmp)# hash md5 R3-Billetterie(config-isakmp)# group 5 R3-
Billetterie(config-isakmp)# lifetime 3600 R3-Billetterie(config-isakmp)# exit R3-
Billetterie(config)# crypto isakmp key iris123 address 200.200.200.1 R3-
Billetterie(config)# crypto ipsec transform-set 50 esp-3des esp-md5-hmac R3-
Billetterie(config)# crypto ipsec security-association lifetime seconds 1800 R3-
Billetterie(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0
0.0.3.255 R3-Billetterie(config)# crypto map billetterie 10 ipsec-isakmp R3-
Billetterie(config-crypto-map)# set peer 200.200.200.1 R3-Billetterie(config-
crypto-map)# set transform-set 50 R3-Billetterie(config-crypto-map)# set security-
association lifetime seconds 900 R3-Billetterie(config-crypto-map)# match address
101 R3-Billetterie(config-crypto-map)# exit R3-Billetterie(config)# interface
FastEthernet 0/1 R3-Billetterie(config-if)# crypto map billetterie
```

```
R3(config)#crypto map billeterie 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 200.200.200.1
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit
R3(config)#interface fastethernet 0/0
R3(config-if)#crypto map billeterie
R3(config-if)#
*Jan  1 02:42:22.835: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
R1>show crypto ipsec transform-set
                    ^
% Invalid input detected at '^' marker.

R1>show crypto ipsec transform-set
                    ^
% Invalid input detected at '^' marker.

R1>en
R1#show crypto ipsec transform-set
Transform set 50: { esp-3des esp-md5-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

```
R3#show crypto ipsec transform-set
Transform set 50: { esp-3des esp-md5-hmac  }
   will negotiate = { Tunnel,  },


R3#show crypto map
Crypto Map "billeterie" 10 ipsec-isakmp
        Peer = 200.200.200.1
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
        Current peer: 200.200.200.1
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): N
        Transform sets={
                50,
        }
        Interfaces using crypto map billeterie:
                FastEthernet0/0
```

Configuration VPN complète sur R3-Billetterie

2.4. Vérifications du Tunnel VPN

```
# Test de ping depuis le Stade vers la Billetterie PC> ping 192.168.1.100 Reply
from 192.168.1.100: bytes=32 time=12ms TTL=126 Reply from 192.168.1.100: bytes=32
time=10ms TTL=126
```

```
R3#show ip rout
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     200.200.200.0/24 is variably subnetted, 3 subnets, 2 masks
D       200.200.200.0/30
           [90/30720] via 200.200.200.5, 01:50:39, FastEthernet0/1
D       200.200.200.0/24 is a summary, 01:51:34, Null0
C       200.200.200.4/30 is directly connected, FastEthernet0/1
D    172.20.0.0/16 [90/33280] via 200.200.200.5, 00:36:21, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R3#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: billeterie, local addr 192.168.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.20.0.0/255.255.255.0/0/0)
   current_peer 200.200.200.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.1.1, remote crypto endpt.: 200.200.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:
```

Test de ping réussi à travers le tunnel VPN

```
! Vérifier l'état ISAKMP R1-Stade# show crypto isakmp sa dst src state conn-id
status 200.200.200.6 200.200.200.1 QM_IDLE 1084 ACTIVE
```

```
R3#show crypto isakmp sa
dst             src             state          conn-id slot status

R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

IPv6 Crypto ISAKMP SA
```

État ISAKMP (QM_IDLE = tunnel actif)

```
! Vérifier les associations de sécurité IPSec R1-Stade# show crypto ipsec sa
interface: FastEthernet0/1 Crypto map tag: stade, local addr 200.200.200.1
protected vrf: (none) local ident: (172.20.0.0/255.255.252.0/0/0) remote ident:
(192.168.1.0/255.255.255.0/0/0) current_peer 200.200.200.6 port 500 #pkts encaps:
13, #pkts encrypt: 13 #pkts decaps: 13, #pkts decrypt: 13 Status: ACTIVE
```

```
R1>en
R1#show crypto map
Crypto Map "stade" 10 ipsec-isakmp
        Peer = 200.200.200.6
        Extended IP access list 101
            access-list 101 permit ip 170.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 200.200.200.6
        Security association lifetime: 4608000 kilobytes/900 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                50:  { esp-3des esp-md5-hmac  } ,
        }
        Interfaces using crypto map stade:
                FastEthernet0/1
```

Associations de sécurité IPSec (paquets chiffrés/déchiffrés)

PARTIE 3 : ACCESS CONTROL LISTS (ACL)

3.1. Principes des ACL

Les ACL sont des listes d'instructions permettant d'autoriser (permit) ou d'interdire (deny) le passage de paquets selon des critères. Elles filtrent le trafic réseau et contrôlent les accès aux équipements.

Type	Numérotation	Filtrage
ACL Standard	1-99	IP source uniquement
ACL Étendue	100-199	IP source/dest, protocole, ports

⚠ **Règles Importantes** • Une ACL se termine par un "deny any" implicite
• Les règles sont évaluées de haut en bas
• Une seule ACL par protocole, par interface, par sens

3.2. ACL Standard - Exemples

Interdire un hôte spécifique

```
Router(config)# access-list 1 deny host 192.168.10.120 Router(config)# access-list 1 permit any
```

Interdire un réseau

```
Router(config)# access-list 2 deny 192.168.10.0 0.0.0.255 Router(config)# access-list 2 permit any
```

3.3. ACL Étendue - Exemples

Bloquer les pings ICMP