PRINCE TOGBLE

REALISATION 2

ADMINISTRATION À DISTANCE SÉCURISÉE ET SÉCURISATION DES INTERCONNEXIONS

SOMMAIRE

CONTEXTE

Dans le cadre de cette Mission, il est essentiel de mettre en place une solution robuste permettant une administration à distance sécurisée tout en renforçant la sécurité du système d'information entre les différents sites de StadiumCompany. De plus, il est impératif de sécuriser les communications, notamment entre le site du stade et les sites distants de la billetterie et du magasin.

La solution sélectionnée doit permettre une administration à distance via un accès sécurisé basé sur le protocole SSH (Secure Shell). Pour atteindre ces objectifs, voici les principales actions à entreprendre :

1. **Sécurisation du Système d'Information entre les Sites**
   Mise en place de mesures de sécurité pour protéger les données sensibles et les communications entre les sites : pare-feux, authentification renforcée, surveillance du trafic réseau.
2. **Sécurisation des Interconnexions**
   Les liaisons réseau entre le stade et les sites distants doivent être sécurisées via des technologies telles que les VPN ou des connexions chiffrées.
3. **Administration à Distance Sécurisée**
   Mise en place d'un accès distant sécurisé via SSH, avec chiffrement et authentification robuste. L'usage du 2FA est recommandé lorsque possible.
4. **Gestion des Certificats et des Identités**
   Gestion efficace des certificats numériques et des identités pour garantir l'authenticité des connexions SSH.
5. **Surveillance de la Sécurité**
   Mise en place d'un système de surveillance pour détecter les intrusions et analyser les journaux SSH.
6. **Formation du Personnel**
   Sensibilisation et formation à l'utilisation sécurisée des connexions SSH et à la gestion des accès distants.

En appliquant ces mesures, StadiumCompany bénéficiera d'une infrastructure réseau sécurisée, d'interconnexions protégées et d'une administration à distance fiable.

I – Mise en Place d'une Solution pour l'Administration à Distance Sécurisée

1 - Configuration des mots de passe sur un routeur Cisco

a) Mot de passe de la console

Le mot de passe de la console est utilisé pour sécuriser l'accès physique au routeur via la console. Toute personne connectée directement au routeur devra fournir ce mot de passe.

Procédure :

- Accéder au mode de configuration : `configure terminal`
- Accéder à la ligne console : `line console 0`
- Activer l'authentification : `login`
- Définir le mot de passe : `password Bts20245`

Configuration :

```
R1>enable
R1#conf t
R1(config)#line con 0
R1(config-line)#login
% Login disabled on line 0, until 'password' is set
R1(config-line)#password Bts20245
R1(config-line)#exit
```

```
R1-stade>en
R1-stade>enable
R1-stade#conf t
R1-stade#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-stade(config)#lin
R1-stade(config)#line cons
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 Bts2024$
R1-stade(config-line)#exit
```

Ainsi, toute personne accédant physiquement à la console devra fournir le mot de passe.

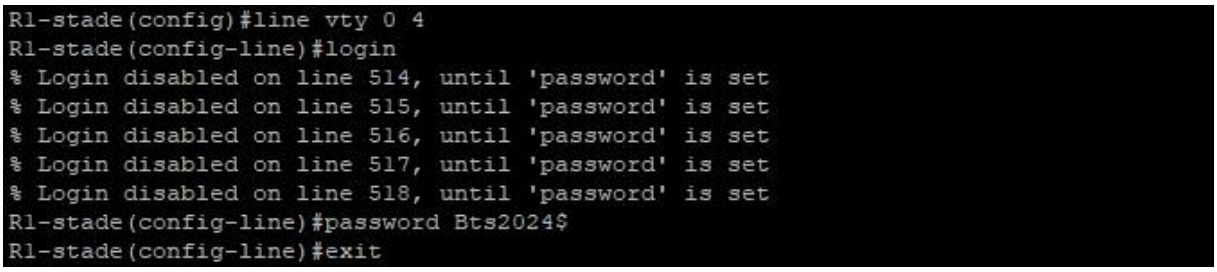
b) Mot de passe de terminal virtuel (VTY)

Les lignes VTY permettent l'accès distant via Telnet ou SSH.
Pour sécuriser cet accès, on configure un mot de passe.

Procédure :

- Accéder au mode de configuration : `configure terminal`
- Accéder aux lignes VTY : `line vty 0 4`
- Activer l'authentification : `login`
- Définir le mot de passe : `password Bts2024$`

```
R1-state(config)# line vty 0 4
R1-state(config-line)# login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
R1-state(config-line)# password Bts2024$
R1-state(config-line)# exit
```



Toute connexion distante devra fournir ce mot de passe.

c) Mot de passe enable

Le mot de passe *enable* protège l'accès au mode privilégié (`enable`), qui donne accès aux commandes sensibles.

Deux méthodes existent :

- `enable password` (non chiffré)
- `enable secret` (chiffré — recommandé)

```
R1-state(config)# enable password Bts2024$
R1-state(config)# enable secret Bts2024$
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.

R1-state(config)# enable secret Bts2024@
The enable secret you have chosen is the same as your enable password.
```

```
This is not recommended. Re-enter the enable secret.
```

```
R1-stade(config)#enable password Bts2024$
R1-stade(config)#en
R1-stade(config)#enable secret  Bts2024$
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.

R1-stade(config)#enable secret Bts2024$
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
```

Le routeur refuse un `enable secret` identique au `enable password` pour des raisons de sécurité.

2 - Activation du SSH

a) Création d'un compte utilisateur

On crée un utilisateur qui servira pour l'authentification SSH.

```
R1(config)#username user1 password Bo2014#
R1(config)#ip domain-name stadiumcompany.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.stadiumcompany.com
The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#ip ssh version 2
Sep 28 13:51:01.391: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Le nom d'hôte est utilisé pour générer la clé RSA.
- Le nom de domaine complète le FQDN.
- Une clé RSA de 1024 bits est générée.
- SSH version 2 est activé.

```
R1-stade(config)#
R1-stade(config)#
R1-stade(config)#username user1 password Bts2024$
R1-stade(config)#ip domain-name stadiumcompany.com
R1-stade(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1-stade.stadiumcompany.com
```

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

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

R1-stade(config)#
*Sep 29 16:15:21.591: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

b) Activation du service SSH

On configure les lignes VTY pour accepter uniquement SSH et utiliser l'authentification locale.

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

```
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)#
```

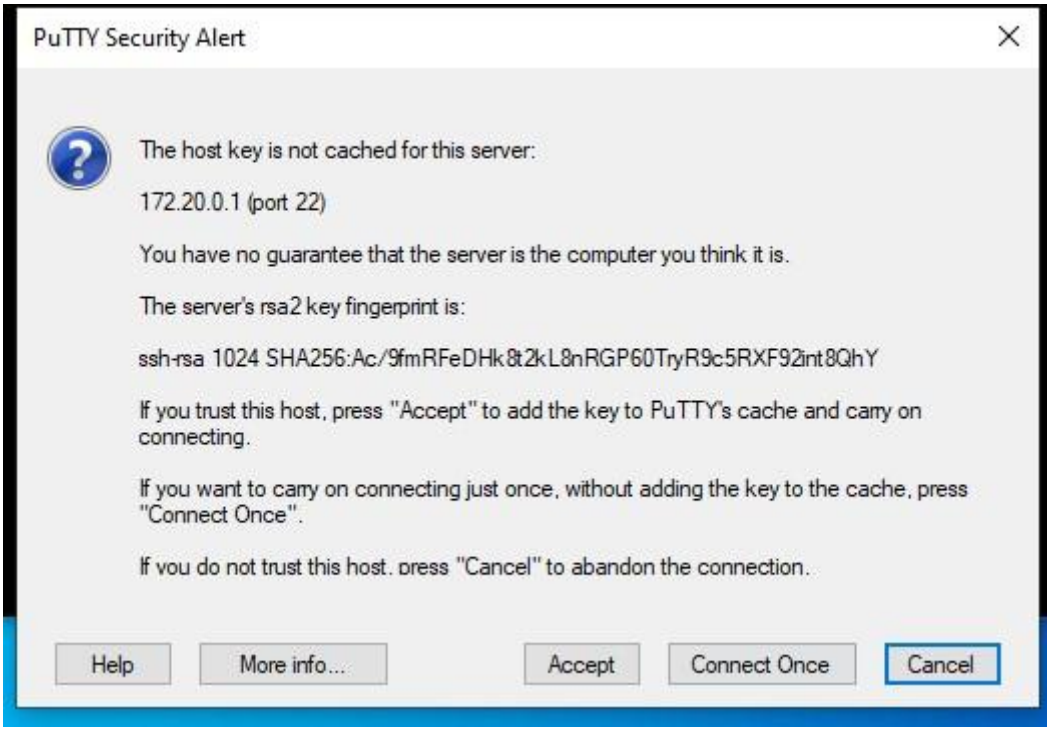
Le routeur accepte désormais les connexions SSH sécurisées.

c) Vérification

On utilise **PuTTY** :

1. Saisir l'adresse IP du routeur
2. Choisir SSH (port 22)
3. Cliquer sur *Connect*

Lors de la première connexion, une alerte apparaît :



On clique sur **Accept**, puis on saisit :

- le nom d'utilisateur : `user1`
- le mot de passe : `Bo2014#`

L'accès SSH sécurisé est alors établi.

II - Sécurisation des Interconnexions

1 - Introduction au VPN Site-to-Site

Le VPN site-to-site est une technologie permettant de relier **deux réseaux locaux distants** de manière sécurisée en utilisant Internet comme support.
Les données circulant entre les sites sont **chiffrées**, garantissant :

- la **confidentialité**,
- l'**intégrité**,
- la **protection contre les interceptions**.

Ce type de VPN est idéal pour relier le **stade**, la **billetterie** et le **magasin**.

2 - Choix du protocole

Plusieurs protocoles VPN existent : PPTP, IPsec, OpenVPN…

Le protocole choisi est :

➞ IPsec

Parce qu'il offre :

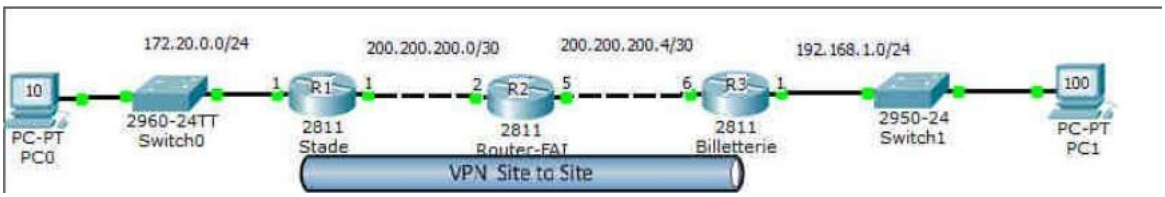
- une sécurité robuste,
- un chiffrement fort,
- une compatibilité avec les routeurs Cisco,
- une performance adaptée aux interconnexions professionnelles.

Il demande plus de configuration, mais garantit un niveau de sécurité supérieur.

3 - Schéma Réseau

Le document présente un schéma du réseau reliant :

- R1 (Stade)
- R2 (Routeur intermédiaire)
- R3 (Billetterie)
- Les PC locaux
- Les adresses IP des interfaces



4 – Configuration de R1 (Routeur 1)

Après avoir changé le nom du routeur, on configure les adresses IP des interfaces.

```
R1-Sada(config)#int fa 0/0
R1-Sada(config-if)#ip add 172.20.0.1 255.255.255.0
R1-Sada(config-if)#no shut

R1-Sada(config)#int fa 0/1
R1-Sada(config-if)#ip add 200.200.200.1 255.255.255.252
R1-Sada(config-if)#no shut
```

```
R1-Stade(config)#int fa 0/0
R1-Stade(config-if)#ip add 172.20.0.1 255.255.255.0
R1-Stade(config-if)#no shut
R1-Stade(config-if)#exit
R1-Stade(config)#
*Jan  1 06:47:07.519: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
R1-Stade(config)#int fa 0/1
R1-Stade(config-if)#ip add 200.200.200.1 255.255.255.252
R1-Stade(config-if)#no shut
R1-Stade(config-if)#exit
R1-Stade(config)#
*Jan  1 06:48:27.295: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
```

Choix du protocole de routage

Le choix dépend des besoins du réseau :

- **EIGRP** : simple, rapide, efficace, idéal pour environnements Cisco.
- **Routage statique** : simple mais non évolutif.
- **OSPF** : très scalable, adapté aux réseaux complexes et hétérogènes.

```
R1-Scada(config)#router eigrp 1
R1-Scada(config-router)#network 172.200.0.0 0.0.0.255
R1-Scada(config-router)#network 200.200.200.0 0.0.0.3
R1-Scada(config-router)#exit
```

```
R1-Stade(config)#router eigrp 1
R1-Stade(config-router)#network 172.20.0.0 0.0.0.255
R1-Stade(config-router)#network 200.200.200.0 0.0.0.3
R1-Stade(config-router)#exit
R1-Stade(config)#
```

La configuration de base de R1 est terminée.

5 - Configuration de R2 (Routeur 2)

Même procédure que pour R1.

```
Router(config)#hostname R2-FIA

R2-FIA(config)#int fa 0/0
R2-FIA(config-if)#ip add 200.200.200.2 255.255.255.252
R2-FIA(config-if)#no shut

R2-FIA(config)#int fa 0/1
R2-FIA(config-if)#ip add 200.200.200.5 255.255.255.252
R2-FIA(config-if)#no shut

R2-FIA(config)#router eigrp 1
R2-FIA(config-router)#network 200.200.200.0 0.0.0.3
R2-FIA(config-router)#network 200.200.200.4 0.0.0.3
R2-FIA(config-router)#exit
```

```
Router(config)#hostname R2-FIA
R2-FIA(config)#
R2-FIA(config)#int fa 0/0
R2-FIA(config-if)#ip add 200.200.200.2 255.255.255.252
R2-FIA(config-if)#no shut
R2-FIA(config-if)#exit
R2-FIA(config)#
*Jan  1 02:02:48.651: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jan  1 02:02:49.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R2-FIA(config)#
R2-FIA(config)#int fa 0/1
R2-FIA(config-if)#ip add 200.200.200.5 255.255.255.252
R2-FIA(config-if)#no shut
R2-FIA(config-if)#exit
R2-FIA(config)#
R2-FIA(config)#
*Jan  1 02:03:20.267: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
R2-FIA(config)#router eigrp 1
R2-FIA(config-router)#network 200.200.200.0 0.0.0.3
R2-FIA(config-router)#
*Jan  1 02:03:53.971: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 200.200.200.1 (
FastEthernet0/0) is up: new adjacency
R2-FIA(config-router)#network 200.200.200.4 0.0.0.3
R2-FIA(config-router)#exit
R2-FIA(config)#
```

6 - Configuration de R3 (Routeur 3)

Même procédure que pour R1 et R2.

```
Router>en
Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host
Router(config)#hostname R3-Bill
R3-Bill(config)#
R3-Bill(config)#inter
R3-Bill(config)#interface fast
R3-Bill(config)#interface fastEthernet 0/0
R3-Bill(config-if)#ip address 192.168.1.1 255.255.255.0
R3-Bill(config-if)#no sh
R3-Bill(config-if)#no shutdown
R3-Bill(config-if)#
*Oct 13 14:17:33.659: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Oct 13 14:17:34.659: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R3-Bill(config-if)#
R3-Bill(config-if)#exit
R3-Bill(config)#inter
R3-Bill(config)#interface fas
R3-Bill(config)#interface fastEthernet 0/1
R3-Bill(config-if)#ip
*Oct 13 14:18:11.827: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
% Incomplete command.

R3-Bill(config-if)#
R3-Bill(config-if)#
*Oct 13 14:18:13.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R3-Bill(config-if)#
R3-Bill(config-if)#
R3-Bill(config-if)#ip add
R3-Bill(config-if)#ip address 200.200.200.6 255.255.255.252
R3-Bill(config-if)#no sh
R3-Bill(config-if)#no shutdown
R3-Bill(config-if)#exit
```

```
R3-Bill(config)#router eigrp 1
R3-Bill(config-router)#netw
R3-Bill(config-router)#network 192.168.1.0 0.0.0.255
R3-Bill(config-router)#net
R3-Bill(config-router)#network 200.200.200.4 0.0.0.3
R3-Bill(config-router)#
*Oct 13 14:21:07.207: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 200.200.200.5 (
FastEthernet0/1) is up: new adjacencye
% Ambiguous command:  "e"
R3-Bill(config-router)#
R3-Bill(config-router)#exit
```

```
:\Users\IRIS>ping 192.168.1.100

nvoi d'une requête 'Ping'  192.168.1.100 avec 32 octets de données :
éponse de 192.168.1.100 : octets=32 temps=2 ms TTL=126
éponse de 192.168.1.100 : octets=32 temps=1 ms TTL=126
éponse de 192.168.1.100 : octets=32 temps=2 ms TTL=126
éponse de 192.168.1.100 : octets=32 temps=1 ms TTL=126

tatistiques Ping pour 192.168.1.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
urée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

7 - Configuration du VPN sur R1 (Routeur 1)

NB : Le VPN se configure uniquement sur les **routeurs d'extrémité**, donc **R1** et **R3**. Aucune modification n'est nécessaire sur **R2**.

---

a) Activation d'ISAKMP et configuration de la politique ISAKMP

ISAKMP est indispensable pour établir une communication sécurisée entre les routeurs.

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

Cette étape définit :

- la méthode d'authentification,
- le chiffrement,
- le hachage,
- le groupe Diffie-Hellman,
- la durée de vie de la SA.

b) Configuration de la clé ISAKMP

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

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

c) Configuration du transform-set IPsec

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

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

NB : `esp` signifie *Encapsulation Security Protocol*.

d) Création de l'ACL et de la crypto map

L'ACL définit le trafic à chiffrer.

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

Création de la crypto map :

```
R1-Stade(config)#crypto map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
    and a valid access list have been configured.
R1-Stade(config-crypto-map)#set peer 200.200.0.6
R1-Stade(config-crypto-map)#set transform-set trans
R1-Stade(config-crypto-map)#match address 101
R1-Stade(config-crypto-map)#set security-association lifetime seconds 900
R1-Stade(config-crypto-map)#exit
```

e) Application de la crypto map sur l'interface de sortie

```
R1-Stade(config)#int fa 0/1
R1-Stade(config-if)#crypto map 10
*Jan  6 00:03:15.591: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Un message confirme que la crypto map fonctionne.

```
R1-Stade(config)#$ 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1-Stade(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-Stade(config-crypto-map)#set peer 200.200.200.6
R1-Stade(config-crypto-map)#set trans
R1-Stade(config-crypto-map)#set transform-set 50
R1-Stade(config-crypto-map)#set sec
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)#
R1-Stade(config)#
R1-Stade(config)#int fa 0/1
R1-Stade(config-if)#crypto map stade
R1-Stade(config-if)#
*Jan  1 08:03:15.931: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1-Stade(config-if)#
```

8 - Configuration du VPN sur R3 (Routeur 3)

La configuration est similaire à celle de R1, avec les adresses adaptées.

a) Configuration ISAKMP

```
R3-Bill(config)#crypto isakmp enable
R3-Bill(config)#crypto isakmp policy 10
R3-Bill(config-isakmp)#authentication pre-share
R3-Bill(config-isakmp)#encryption 3des
R3-Bill(config-isakmp)#hash md5
R3-Bill(config-isakmp)#group 2
R3-Bill(config-isakmp)#lifetime 3600
R3-Bill(config-isakmp)#exit
```

b) Clé ISAKMP

```
R3-Bill(config)#crypto isakmp key iris123 address 200.200.0.1
```

c) Transform-set IPsec

```
R3-Bill(config)#crypto ipsec transform-set ts esp-3des esp-md5-hmac
R3-Bill(cfg-crypto-trans)#exit
```

d) Crypto map

```
R3-Bill(config)#crypto map 10 ipsec-isakmp
R3-Bill(config-crypto-map)#set peer 200.200.0.1
R3-Bill(config-crypto-map)#set transform-set ts
```

```
R3-Bill(config-crypto-map)#match address 101
R3-Bill(config-crypto-map)#set security-association lifetime seconds 1800
R3-Bill(config-crypto-map)#exit
```

ACL correspondante :

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

e) Application de la crypto map

```
R3-Bill(config)#int fa 0/1
R3-Bill(config-if)#crypto map billetterie
*Oct 13 15:28:04.955: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
R3-Bill(config)#crypto isakmp enable
R3-Bill(config)#
```

```
R3-Bill(config)#crypto isakmp policy 10
R3-Bill(config-isakmp)#authen
R3-Bill(config-isakmp)#authentication pre-sh
R3-Bill(config-isakmp)#authentication pre-share
R3-Bill(config-isakmp)#encry
R3-Bill(config-isakmp)#encryption 3des
R3-Bill(config-isakmp)#hash md5
R3-Bill(config-isakmp)#group 5
R3-Bill(config-isakmp)#life
R3-Bill(config-isakmp)#lifetime 3600
R3-Bill(config-isakmp)#exit
```

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

```
R3-Bill(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3-Bill(cfg-crypto-trans)#
R3-Bill(cfg-crypto-trans)#exit
R3-Bill(config)#crypto ipsec sec
R3-Bill(config)#crypto ipsec security-association lifetime seconds 1800
```

```
R3-Bill(config)#
R3-Bill(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0$
```

9 - Vérifications et tests du VPN

a) Vérification des transform-sets

```
R1-Stade#show crypto ipsec transform-set
Transform set s0: { esp-3des esp-md5-hmac }
  will negotiate = { Tunnel, }

R3-Bill#show crypto ipsec transform-set
Transform set s0: { esp-3des esp-md5-hmac }
  will negotiate = { Tunnel, }
```

```
R1-Stade#sh 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-Bill#sh 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-Bill#
```

b) Vérification des crypto maps

```
R3-Bill#sh 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
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                50:  { esp-3des esp-md5-hmac  } ,
        }
        Interfaces using crypto map billeterie:
                FastEthernet0/1


R3-Bill#
```

```
R1-Stade#sh crypto map
Crypto Map "stade" 10 ipsec-isakmp
        Peer = 200.200.200.6
        Extended IP access list 101
            access-list 101 permit ip 172.20.0.0 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


R1-Stade#
```

c) Vérification des Security Associations (IPsec SA)

```
R1-Stade#sh crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: stade, local addr 200.200.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.20.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 200.200.200.6 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 200.200.200.1, remote crypto endpt.: 200.200.200.6
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xDD9BD0B2(3717976242)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xADA1F1BD(2913071549)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: stade
        sa timing: remaining key lifetime (k/sec): (4391782/672)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xDD9BD0B2(3717976242)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: stade
        sa timing: remaining key lifetime (k/sec): (4391781/672)
        IV size: 8 bytes
        replay detection support: Y
```

```
    inbound esp sas:
     spi: 0xADA1F1BD(2913071549)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: stade
       sa timing: remaining key lifetime (k/sec): (4391782/672)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xDD9BD0B2(3717976242)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: stade
       sa timing: remaining key lifetime (k/sec): (4391781/672)
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
R1-Stade#
R1-Stade#
```

```
R3-Bill#sh crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: billeterie, local addr 200.200.200.6

   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: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
    #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.: 200.200.200.6, remote crypto endpt.: 200.200.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0xADA1F1BD(2913071549)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xDD9BD0B2(3717976242)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: NETGX:1, sibling_flags 80000046, crypto map: billeterie
        sa timing: remaining key lifetime (k/sec): (4464371/646)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xADA1F1BD(2913071549)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: billeterie
        sa timing: remaining key lifetime (k/sec): (4464372/646)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xADA1F1BD(2913071549)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: NETGX:2, sibling_flags 80000046, crypto map: billeterie
        sa timing: remaining key lifetime (k/sec): (4464372/646)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
R3-Bill#
```

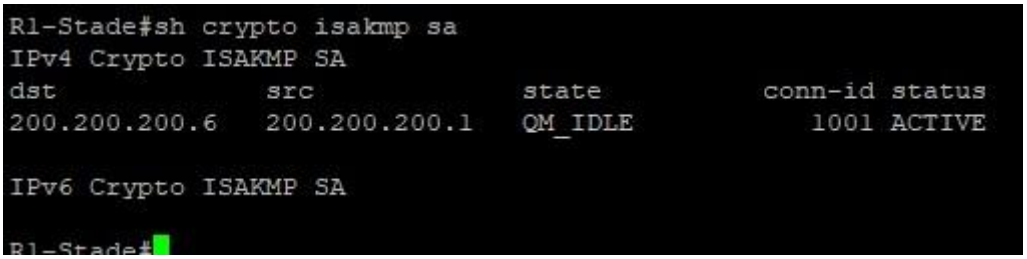
Les SAs montrent :

- les paquets chiffrés,
- les paquets déchiffrés,
- les SPI,
- l'état : **ACTIVE**.

d) Vérification ISAKMP SA

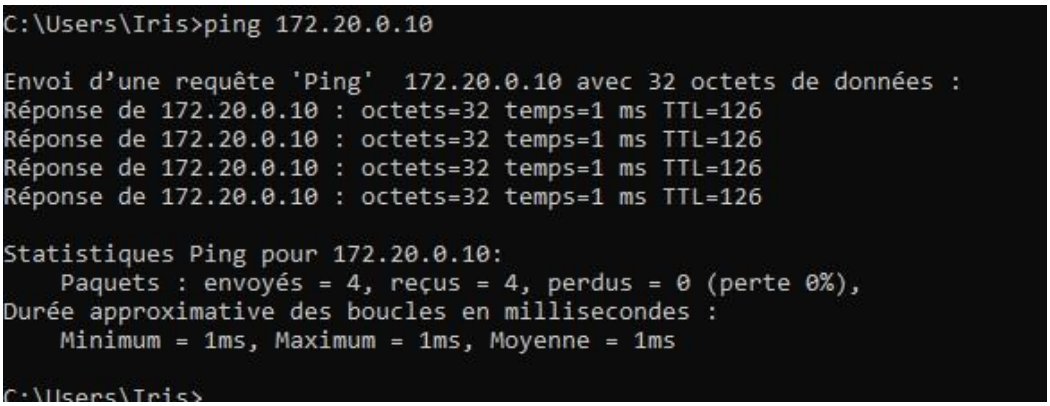
```
R1-Stade#show crypto isakmp sa
dst             src             state          conn-id status
200.200.200.2   200.200.200.1   QM_IDLE        1001 ACTIVE

R3-Bill#show crypto isakmp sa
dst             src             state          conn-id status
200.200.200.1   200.200.200.2   QM_IDLE        1001 ACTIVE
```



e) Test de communication (ping)

Depuis un PC du réseau de la billetterie vers le réseau du stade :



Le VPN fonctionne correctement.

f) Affichage de la configuration complète

```
R1-Stade#show run
```

```
R1-Stade#sh run
Building configuration...

Current configuration : 1596 bytes
!
! Last configuration change at 08:06:18 UTC Sat Jan 1 2000
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1-Stade
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
memory-size iomem 25
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
!
!
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
!
!
license udi pid CISCO2811 sn FHK1332F1KW
!
redundancy
!
```

```
redundancy
!
!
!
!
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 Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
```

```
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 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
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end

R1-Stade#
R1-Stade#
R1-Stade#
```