

BTS SIO2 LM ECOLE IRIS

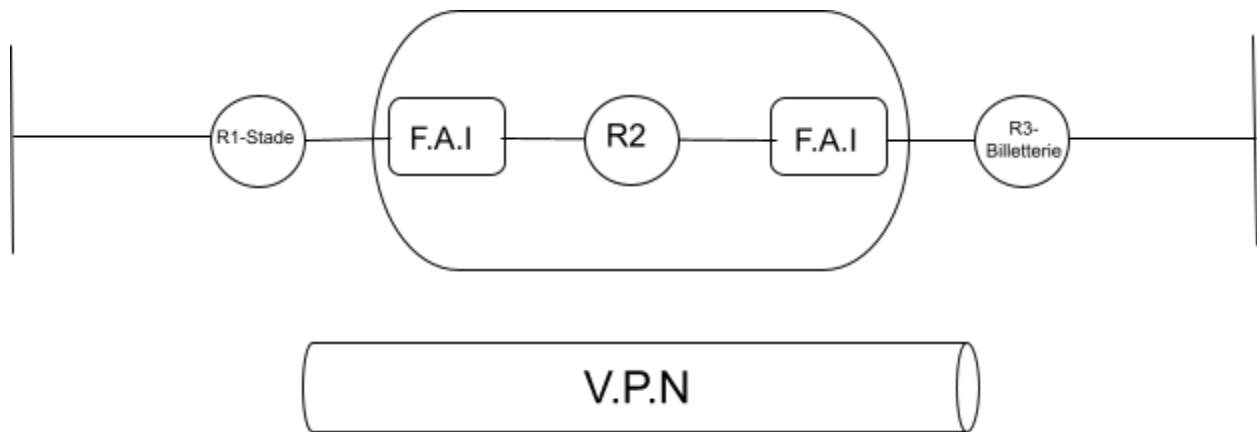
**Mise en place d'une solution pour
l'administration à distance sécurisée et la
sécurisation des interconnexions (Protocole
SSH, VTY, EIGRP, cryptographie)**

Table des matières

I) Contexte.....	2
L'objectif de la mission.....	2
II) Solutions mises en place.....	3
Sécurisation des accès routeur.....	3
Configurer le mot de passe de la Console.....	3
Configurer le mot de passe du Terminal Virtuel (VTY).....	3
Configurer le mot de passe pour les mode Enable et Enable Secret.....	4
Protocole SSH.....	5
Définir un compte utilisateur (Login et Mot de passe).....	5
Définir un hostname pour le routeur.....	5
Définir un nom de domaine pour le routeur.....	5
Explication approfondie des deux dernières étapes.....	5
Générer une clé de chiffrement RSA.....	6
Activer SSH sur les lignes virtuelles.....	6
Vérifier l'existence de la clé RSA.....	7
Configuration des routeurs.....	7
Restauration par défaut du routeur R1-Stade.....	8
Configuration des interfaces du routeur R1-Stade.....	8
Configuration du routage EIGRP du R1-Stade.....	9
Restauration par défaut du routeur R2-FAI.....	10
Configuration des interfaces du R2-FAI.....	10
Configuration du routage EIGRP du R2-FAI.....	10
Restauration par défaut du routeur R3.....	11
Configuration des interfaces du routeur R3-Billetterie.....	11
Configuration du routage EIGRP du routeur R3-Billetterie.....	11
Restauration par défaut des switches.....	12
Test de communication avec un PING.....	12
Configuration du PC0.....	12
Configuration du PC1.....	13
Configuration du VPN.....	15
Configuration de base du routeur R1.....	15
Activations des fonctions crypto du routeur de R1.....	16
Configurer la police de R1.....	16
Configuration de la clef de R1.....	16
Configuration des options de transformations des données de R1.....	17
Création d'ACL de R1.....	17
Configuration de la crypto map de R1.....	17
Application de la crypto map sur l'interface de sortie de R1.....	18
Configuration de base du routeur R3.....	18
Activations des fonctions crypto du routeur de R3.....	18

Configurer la police de R3.....	18
Configuration de la clef de R3.....	19
Configuration des options de transformations des données de R3.....	19
Création d'ACL de R3.....	19
Configuration de la crypto map de R3.....	19
Test du VPN.....	20
III) Conclusion.....	21

I) Contexte



L'objectif de la mission

L'objectif de cette mission est de consolider l'infrastructure de Stadium mise en place, grâce à une administration à distance sécurisée, avec des liaisons réseaux entre les sites protégées.

Le site du stade est connecté au site de la billetterie (et inversement), en passant par un fournisseur d'accès, puis par Internet, en tant que réseau public. Afin de sécuriser les échanges, nous utiliserons un **VPN**, ainsi que des protocoles d'authentification et de connexion renforcés, notamment **SSH**. La mise en place et la gestion des certificats numériques nous permettra également de garantir l'authenticité des connexions SSH.

Par ailleurs, Stadium bénéficiera d'un système de surveillance en continue, qui analysera le trafic pour détecter en temps réel toute tentative d'intrusion ou d'attaque sur le système d'information. Enfin, il sera primordial de former le personnel de l'entreprise à l'utilisation sécurisée des connexions à distance, tout en les sensibilisant à la sûreté informatique au sein de l'entreprise.

Cette approche systémique du système d'information nous permettra d'obtenir une protection globale robuste, en sécurité et en sûreté informatique.

II) Solutions mises en place

Sécurisation des accès routeur

On souhaite configurer le protocole **Secure Shell (SSH)** sur le routeur **R1-Stade**, afin que d'autres équipements et utilisateurs puissent s'y connecter à distance, de manière sécurisée.

Étant donné que le routeur sert de support pour les divers équipements et utilisateurs qui vont s'y connecter, il est primordial de correctement sécuriser l'accès aux différentes interfaces et modes du routeur.

Configurer le mot de passe de la Console

Nous allons d'abord créer un **mot de passe console** afin de sécuriser directement l'accès physique, lors d'une connexion directe via un câble console. Cela est important puisque tout accès non autorisé ne doit pas être permis. Ici, même si une personne a un accès **physique** au routeur et s'y branche, elle devra malgré tout entrer un mot de passe pour pouvoir interagir avec le routeur. Avec cette sécurité, les risques de modifications locales sont fortement réduites :

#line console 0 → Sélectionne la ligne de console 0 (la ligne de console représente également l'interface physique du routeur)

#Router(config-line)# login → Active la demande de mot de passe

#Router(config-line)# password Bts2025\$ → Définit le mot de passe pour interagir avec la console du routeur.

```
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 Bts2025$
```

Configurer le mot de passe du Terminal Virtuel (VTY)

De la même manière, le mot de passe de terminal virtuel permet la protection de l'accès au routeur **via des connexions distantes** (comme **Telnet** ou **SSH**). Ce sont les lignes VTY qui permettent cet accès distant. Il est donc important de les sécuriser afin d'empêcher les tentatives de connexions non autorisées. En fixant un mot de passe, on s'assure que seules les personnes autorisées peuvent y accéder :

line vty 0 4 → Sélectionne les 5 premières lignes VTY (de 0 à 4) sur le routeur pour définir jusqu'à 5 connexions en simultané à distance

login → Active la demande de mot de passe

password Bts2025\$ → Définis le mot de passe requis pour interagir avec le Terminal Virtuel du routeur

```
R1-Stade(config)#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 Bts2025$
```

Configurer le mot de passe pour les mode **Enable** et **Enable Secret**

Ces mots de passes protègent l'accès au mode privilégié du routeur, là où se trouvent les commandes sensibles :

#enable password Bts2025\$ → protège l'accès aux configurations avancées en définissant le mot de passe

#enable secret Bts2025\$ → permet de crypter le mot de passe dans le fichier de configuration

Avec le cryptage **enable secret**, même si le fichier de configuration est visualisé, ce mot de passe ne sera pas lisible en clair.

Avec ces ajouts, la confidentialité des configurations critiques du routeur est renforcée.

Il est également possible de crypter l'ensemble des mots de passe afin d'ajouter une couche de sécurité supplémentaire :

service password encryption → Crypte tous les mots de passe du fichier de configuration du routeur

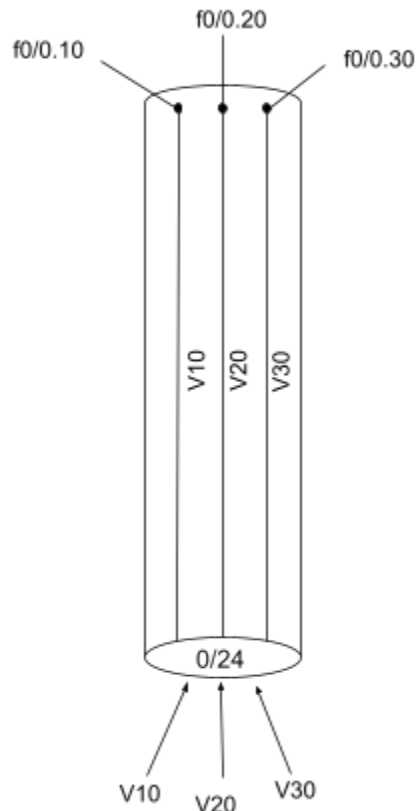
Ici, il n'est pas utile d'utiliser cette ligne de commande, car nous préférons pouvoir localiser facilement les mots de passe, et ainsi différencier le mot de passe **enable secret** des autres.

show running-config → Affiche le fichier de configuration du routeur

Protocole SSH

Les différents accès possibles du routeur sont désormais sécurisés. Nous allons maintenant configurer le protocole SSH sur le routeur.

SSH est un protocole réseau utilisé pour accéder à distance à un système de manière sécurisée. Il permet une communication cryptée entre deux machines, garantissant la confidentialité et l'intégrité des données transmises.



L'objectif ici est que les VLANs 10, 20 et 30 puissent emprunter directement le tunnel VPN depuis le routeur R1-Stade jusqu'au R3-Billetterie :

Définir un hostname pour le routeur

Dans notre contexte, le routeur a déjà été renommé lors de l'exécution de la Mission 1 avec le nom définitif **R1-Stade**.

Toutefois, si le routeur doit changer de nom, il est pertinent de le faire à cette étape avec la ligne de commande suivante : **#hostname+nommachine**

Définir un compte utilisateur (Login et Mot de passe)

Tout d'abord, nous devons créer un utilisateur directement sur le routeur :

#en → Passer en mode privilégié

#conf t → Passer en mode de configuration du routeur

#username user1 password Bts2025\$ → Définit le nom de l'utilisateur et son mot de passe

```
R1-Stade(config)#username user1 password Bts2025$
```

Définir un nom de domaine pour le routeur

#ip domain-name Stadium.local → Définit un nom de domaine qui sera utilisé pour compléter le nom d'hôte du routeur.

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

Après cette commande, le nom complet du routeur sera : **R1-Stade.Stadium.local**

Explication approfondie des deux dernières étapes

Le nom de domaine est nécessaire pour créer une clé de cryptage RSA sur le routeur afin de sécuriser les connexions SSH. En effet, le routeur utilise ce nom de domaine pour créer la clé cryptée liée au nom complet.

Le renommage du routeur permet également de l'identifier de manière unique dans le réseau configuré avec un DNS interne, en facilitant la gestion de plusieurs routeurs (ou autres équipements). Comment ? En utilisant des **noms explicites** plutôt que des **adresses IP**.

Générer une clé de chiffrement RSA

RSA est l'acronyme de **Rivest-Shamir-Adleman** du nom des trois chercheurs qui ont développé cet algorithme de chiffrement en 1977. C'est un système de **chiffrement asymétrique** qui utilise une clé publique pour chiffrer les données, et une clé secrète gardée par le propriétaire pour déchiffrer les données.

Une **clé RSA** est utile pour le chiffrement SSH sur un routeur Cisco. Elle permet de sécuriser les connexions SSH en chiffrant les données échangées entre le routeur et les appareils qui s'y connectent.

#crypto key generate rsa modulus 1024 → Indique au routeur de générer une clé RSA, en définissant la taille de la clé sur 1024 bits.

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

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

R1-Stade(config)#
*Oct 29 12:35:59.807: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Activer SSH sur les lignes virtuelles

Nous allons configurer les protocoles d'entrée de sorte à ce que le routeur utilise obligatoirement une authentification basée sur les comptes d'utilisateurs configurés localement.

#line vty 0 4 → Accède à nouveau aux lignes VTY du routeur

#transport input ssh → Précise que seul le protocole ssh est autorisé pour les connexions entrantes sur les lignes VTY.

#login local → Précise que l'authentification des utilisateurs ne peut se faire que via des comptes configurés localement sur le routeur. Cela oblige le routeur à comparer les identifiants fournis par l'utilisateur avec ceux définis dans la configuration locale.

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

Vérifier l'existence de la clé RSA

#show crypto key mypubkey rsa → Affiche les détails de la clé publique RSA générée pour le chiffrement


```

R1-Stade#show crypto key mypubkey rsa
% Key pair was generated at: 12:48:56 UTC Oct 29 2024
Key name: R1-Stade.stadium.local
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 009A
2E9F
 97955375 C5CC8EC8 96C24661 33AF6C73 FF6E9958 69C5724D B1203C68 18AC
9D75
 05221C13 F7D96408 025CA42F 2659F02C FC6C7A7F 780E4A13 721478BF 1028
1E6E
 FF92D63C 476C0824 AC1C6D8A 4F8536B2 B9E8DAD7 5B70B737 F8E872A8 F244
3167
 C98083B7 D8174E9E FDC0A057 9549703D 32E933C3 AD95A78A 3A699316 4B02
0301 0001

```

Configuration des routeurs

VPN est l'acronyme de **Virtual Private Network**. Il est utilisé pour établir des connexions sécurisées entre un hôte et un réseau distant via un tunnel chiffré. Il garantit la confidentialité et la sécurité des données, tout en masquant l'adresse IP qui est remplacée par celle du serveur VPN.

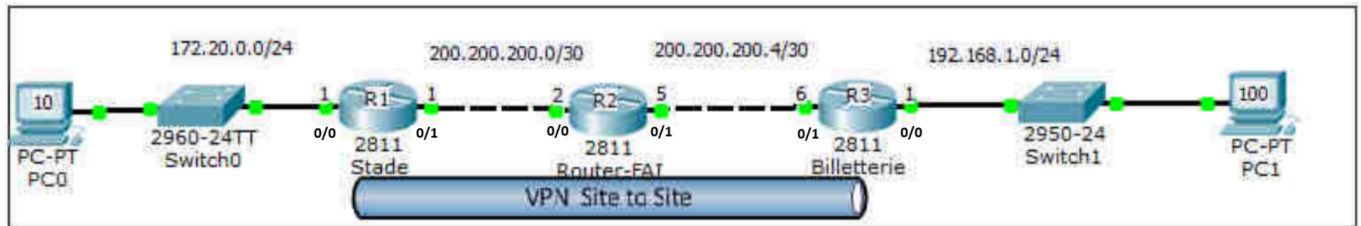
On peut considérer qu'une connexion VPN reviendrait à se connecter en réseau local mais en utilisant Internet. En effet, l'on peut ainsi communiquer avec les machines de ce réseau en prenant comme adresse de destination, l'adresse IP locale de la machine que l'on veut atteindre.

La principale différence entre SSH et VPN :

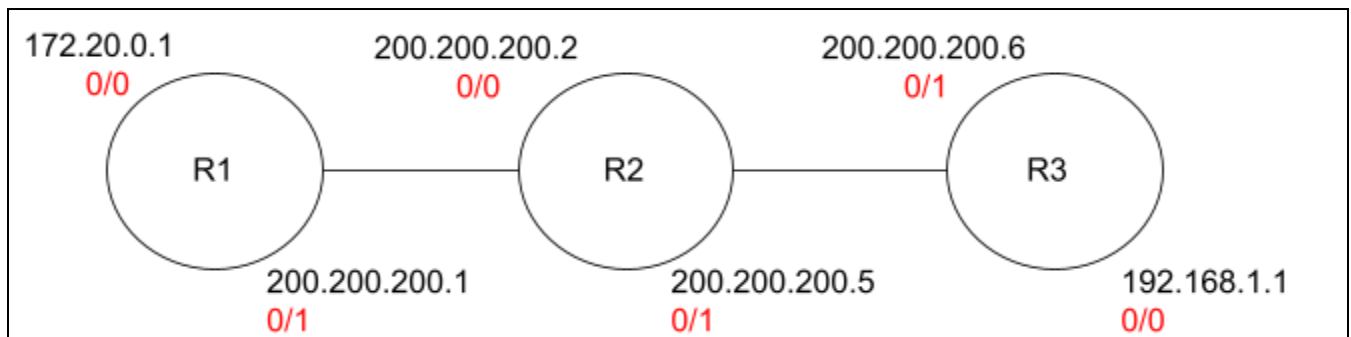
- **SSH** : Conçu principalement pour l'administration à distance ou le transfert de fichiers avec une sécurité renforcée. C'est un outil de gestion spécialisé.
- **VPN** : Conçu pour sécuriser **tout le trafic réseau entre l'hôte et le serveur distant**, pas seulement des sessions spécifiques comme le fait SSH.

Ici, nous allons utiliser **OpenVPN** pour sa souplesse d'utilisation. Nous devons au préalable configurer les différentes interfaces des routeurs, avant de configurer le VPN.

Voici le schéma de notre infrastructure, avec le Routeur R2 en tant que fournisseur d'accès, qui relie le routeur R1-Stade et le routeur R3 de la billetterie :



Pour plus de clarté, voici un schéma supplémentaire détaillant les adresses IP des interfaces de chaque routeur que nous allons configurer :



Configuration des interfaces du routeur R1-Stade

On définit les adresses IP des interfaces et leur masque à partir des adresses réseau du schéma, puis on les active :

```
#interface FastEthernet 0/0
#ip address 172.20.0.1 255.255.255.0
#no shutdown
#exit
#interface FastEthernet 0/1
#ip address 200.200.200.1 255.255.255.252
#no shutdown
#exit
```

Précision : Le VPN est mis en place pour relier les routeurs d'extrémité R1 et R3 sans exposer le R2. Ici, le routeur R2, en tant que routeur de de périphérie, ne fait pas partie du tunnel VPN car il est caché dans l'infrastructure, même si son rôle reste de fournir la connectivité internet pour permettre les connexions entre R1 et R3 dans le tunnel VPN.

Configuration du routage EIGRP du R1-Stade

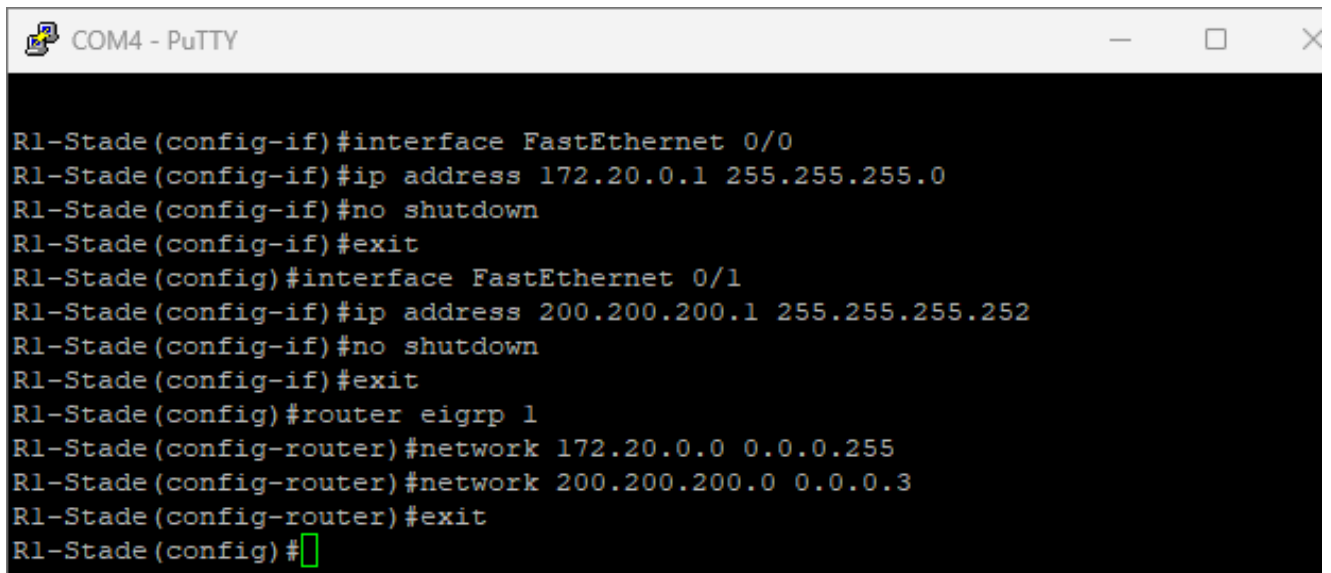
Les interfaces définies, nous pouvons maintenant configurer le routage avec **EIGRP** (Enhanced Interior Gateway Routing Protocol)

#router eigrp 1 > Active le protocole EIGRP avec une instance autonome. Le "1" est le numéro du processus qui identifie l'instance EIGRP

#network 172.20.0.0 0.0.0.255 > Ajoute le sous-réseau 172.20.0.0/24 au processus EIGRP

#network 200.200.200.0 0.0.0.3 > Ajoute le sous-réseau 200.200.200.0/30 au processus EIGRP (utilisé ici pour des connexions de point à point avec 2 hôtes possibles)

#exit



```
COM4 - PuTTY
R1-Stade(config-if)#interface FastEthernet 0/0
R1-Stade(config-if)#ip address 172.20.0.1 255.255.255.0
R1-Stade(config-if)#no shutdown
R1-Stade(config-if)#exit
R1-Stade(config)#interface FastEthernet 0/1
R1-Stade(config-if)#ip address 200.200.200.1 255.255.255.252
R1-Stade(config-if)#no shutdown
R1-Stade(config-if)#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)#
```

Le choix du routage EIGRP est avant tout une préférence personnelle, mais également basé sur les caractéristiques de notre réseau :

- **Un routage statique** induit une configuration manuelle des routes sur les routeurs (sans communication dynamique), chaque routeur doit forcément savoir à l'avance quel chemin emprunter pour atteindre un autre réseau. Bien que simple, ce choix se complexifie si des changements fréquents de topologie se produisent (en particulier dans des grands réseaux).
- **OSPF**, en tant que protocole de routage dynamique, est plutôt basé sur **l'état de lien**. C'est-à-dire que chaque routeur connaît l'intégralité de la topologie du réseau et calcule le meilleur chemin à l'aide de l'algorithme **SPF (Shortest Path First)**. OSPF est un protocole standardisé et open source, qui s'adapte parfaitement dans des réseaux hétérogènes avec différents fabricants, et qui pourrait être utilisé dans notre réseau également.
- **EIGRP** est également un protocole de routage dynamique, développé par **Cisco**. Il se distingue par sa **conception hybride** : également basé sur **l'état de lien**, il

combine aussi les avantages du **routing par distance vectorielle** (utilisation de métriques comme la bande passante, le délai, etc). Il se révèle particulièrement efficace dans des environnements Cisco, par **sa rapidité à converger** (le temps nécessaire pour qu'un réseau s'adapte aux changements, comme la perte d'un lien) et **son évolutivité** pour les réseaux de grande taille.

Afin de **fiabiliser l'automatisation** de ces processus et par **préférence de compatibilité Cisco**, c'est donc **EIGRP** qui a été favorisé dans notre contexte.

Restauration par défaut du routeur R2-FAI

#erase startup-config > on efface la configuration de démarrage actuelle

#reload > redémarrage du routeur

#conf t

#hostname R2-FAI

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2-FAI
R2-FAI(config)#
```

Configuration des interfaces du R2-FAI

L'interface FastEthernet 0/0 est l'interface côté R1 :

```
R2-FAI(config)#interface FastEthernet 0/0
R2-FAI(config-if)#ip address 200.200.200.2 255.255.255.252
R2-FAI(config-if)#no shutdown
R2-FAI(config-if)#exit
```

L'interface FastEthernet 0/1 est l'interface côté R3 :

```
R2-FAI(config)#interface FastEthernet 0/1
R2-FAI(config-if)#ip address 200.200.200.5 255.255.255.252
R2-FAI(config-if)#no shutdown
R2-FAI(config-if)#exit
```

Configuration du routage EIGRP du R2-FAI

#router eigrp 1

#network 200.200.200.0 0.0.0.3 > Définit l'adresse réseau du 1er sous-réseau pour la connection de point à point, entre R1 et R2

#network 200.200.200.4 0.0.0.3 > Définit l'adresse réseau du 2ème sous-réseau pour la connection de point à point, entre R2 et R3

#exit

```

R2-FAI(config)#router eigrp 1
R2-FAI(config-router)#network 200.200.200.0 0.0.0.3
R2-FAI(config-router)#
*Jan 1 00:48:25.715: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 200.200.200.1 (FastEthernet0/0) is up: new adjacency
R2-FAI(config-router)#network 200.200.200.4 0.0.0.3
R2-FAI(config-router)#exit
*Jan 1 00:49:03.343: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 200.200.200.6 (FastEthernet0/1) is up: new adjacency

```

Restauration par défaut du routeur R3

#erase startup-config > on efface la configuration de démarrage actuelle

#reload > redémarrage du routeur

#conf t

#hostname R3-Billetterie

Configuration des interfaces du routeur R3-Billetterie

#hostname R3

#interface FastEthernet 0/0

#ip address 192.168.1.1 255.255.255.0

#no shutdown

#exit

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3-Billetterie
R3-Billetterie(config)#interface FastEthernet 0/0
R3-Billetterie(config-if)#ip address 192.168.1.1 255.255.255.0
R3-Billetterie(config-if)#no shutdown
R3-Billetterie(config-if)#exit
*Nov 19 10:17:32.899: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Nov 19 10:17:33.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3-Billetterie(config)#exit
R3-Billetterie#

```

Configuration du routage EIGRP du routeur R3-Billetterie

#interface FastEthernet 0/1

#ip address 200.200.200.6 255.255.255.252

#no shutdown

#exit

#router eigrp 1

#network 192.168.1.0 0.0.0.255

#network 200.200.200.4 0.0.0.3

#exit

```
R3-Billetterie#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3-Billetterie(config)#interface FastEthernet 0/1
R3-Billetterie(config-if)#ip address 200.200.200.6 255.255.255.252
R3-Billetterie(config-if)#no shutdown
R3-Billetterie(config-if)#exit
R3-Billetterie(config)#
*Nov 19 10:20:05.087: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
R3-Billetterie(config)#router eigrp 1
R3-Billetterie(config-router)#
*Nov 19 10:20:18.203: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3-Billetterie(config-router)#network 192.168.1.0 0.0.0.255
R3-Billetterie(config-router)#network 200.200.200.4 0.0.0.3
R3-Billetterie(config-router)#exit
R3-Billetterie(config)#
```

Restauration par défaut des switches

Si ce TP est réalisé à part, sans suivre la mission de restructuration de l'architecture de Stadium, alors il est plus simple de réinitialiser les switches. Si ce TP est effectué dans la continuité de la restructuration de l'infrastructure de Stadium, alors il ne faut pas réinitialiser les switches.

#erase startup-config > Efface la configuration actuelle enregistrée dans le fichier de démarrage. Cela réinitialise donc le commutateur

#delete flash :vlan.dat > Supprime le fichier VLAN, pour effacer toutes les configurations VLAN précédentes.

#reload > Redémarre le commutateur pour appliquer les changements

Configuration du VPN

Le VPN se configure uniquement au niveau des routeurs, plus précisément sur les routeurs d'extrémités (ici R1 et R3 dans notre infrastructure).

Il n'y aura donc aucune modification à effectuer sur le routeur R2.

Configuration de base du routeur R1

Il faut vérifier si le système d'exploitation (IOS) du routeur R1 supporte le VPN :

#show version

```
R1-Stade#show version
Cisco IOS Software, 2801 Software (C2801-ADVENTERPRISEK9-M), Version 12.4(16), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 20-Jun-07 08:10 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

R1-Stade uptime is 16 minutes
System returned to ROM by reload at 03:54:50 UTC Thu Jan 1 1970
System image file is "flash:c2801-adventerprisek9-mz.124-16.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2801 (revision 7.0) with 97280K/33792K bytes of memory.
Processor board ID FCZ131711ZJ
 2 FastEthernet interfaces
 2 Serial(sync/async) interfaces
 1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

R1-Stade#
```

La ligne "1 Virtual Private Network (VPN) module" en fin d'image indique bien que notre routeur Cisco 2801 possède un module VPN intégré.

Activations des fonctions crypto du routeur de R1

(Même si cette fonction est activée par défaut sur les IOS avec les options cryptographiques, ce qui est le cas ici, voici la ligne de commande utile) :

#crypto isakmp enable

Configurer la politique ISAKMP de R1

Ces lignes de commande mettent en place une politique **ISAKMP** pour établir notre **tunnel VPN IPSec** en définissant : l'authentification par clé pré-partagée, le chiffrement **3DES**, le hachage **MD5**, un groupe Diffie-Hellman **5** pour l'échange de clés sécurisé, et une durée de vie de la session de **3600 secondes** avant une nouvelle négociation des clés :

#crypto isakmp policy 10 > configure une politique de sécurité pour établir un canal sécurisé entre les 2 routeurs (en utilisant le protocole ISAKMP)

#authentication pre-share > précise que l'authentification se fait avec PSK (Pre-Shared Keys)

#encryption 3des > Choisi un algorithme, ici 3des qui est un algorithme de chiffrement symétrique appliqué 3 fois

#hash md5 > Définit un algorithme de hachage, ici md5, pour l'intégrité des données

#group 5 > spécifie le groupe Diffie-Hellman utilisé pour l'échange des clefs

#lifetime 3600 > à la fin de durée, la session VPN est renégociée en arrière-plan. Cela veut dire que tous les paramètres négociés au début du tunnel doivent l'être à nouveau.

#exit

```
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
```

Précision : le processus VPN IPsec comporte 2 phases :

Phase 1 - Etablissement du tunnel IKE sécurisé :

Sécurise les communications initiales en établissant un tunnel IKE sécurisé entre les 2 routeurs avec la clé pré-partagée PSK. Ensuite, la négociation des paramètres de sécurité se fait grâce au protocole ISAKMP (cryptographie, hachage, groupe Diffie-Hellman...). Les routeurs peuvent ainsi communiquer entre eux en sécurité car ils se sont authentifiés mutuellement.

Phase 2 - Création du tunnel de données IPsec :

Se concentre sur le chiffrement des flux pour l'échange des informations (selon les paramètres négociés en phase 1), en créant le tunnel IPsec pour transiter les données réelles. C'est aussi à ce moment-là que les clés symétriques sont échangées.

Configuration de la clef de R1

#crypto isakmp key iris123 address 200.200.200.6

Sur certains routeurs avec certains IOS, il se peut que cette ligne de commande ne fonctionne pas, car le routeur demande si le mot de passe doit être chiffré ou pas.

Dans cette situation, il faut indiquer cette commande :

#crypto isakmp key 6 iris123 address 200.200.200.6

```
R1-Stade(config)#crypto isakmp key iris123 address 200.200.200.6
R1-Stade(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R1-Stade(cfg-crypto-trans)#$c security-association lifetime seconds 1800
R1-Stade(config)#
```

Configuration des options de transformations des données de R1

Pour sécuriser les données dans le tunnel VPN, il faut paramétrer un ensemble de paramètres de transformation.

Ici notre ensemble se nomme 50 avec les paramètres suivants :

Utilisation du chiffrement 3DES et authentification par hachage **MD5 avec HMAC** :

#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

Il faut faire attention à utiliser les mêmes algorithmes de chiffrement (**3DES**) et de hachage (**MD5**) que ceux configurés précédemment dans la politique **ISAKMP** (#crypto isakmp policy 10) définie juste avant.

Cela garantit la compatibilité et la cohérence entre les différentes étapes de configuration du tunnel VPN.

On fixe ensuite une valeur de Lifetime :

#crypto ipsec security-association lifetime seconds 1800

Création d'ACL de R1

Le but est ici de déterminer le trafic des autorisations.

L'access-list 101 permet au réseau 172.20.0.0 à communiquer avec le réseau 192.168.1.0 :

#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255

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

Configuration de la crypto map de R1

Le but d'une crypto map est d'associer différentes configurations et d'orienter le trafic vers une destination sécurisée. l'ACL :

#crypto map stade 10 ipsec-isakmp > nomme la cryptomap "stade" en appliquant également la politique ISAKMP dessus

#set peer 200.200.200.6 > Désigne le pair distant, qui est l'adresse IP du routeur distant avec lequel il faut établir un tunnel de sécurité

#set transform-set 50 > définit l'ensemble d'algorithmes prédéfinis pour le chiffrement et le hachage des données dans le tunnel IPsec

#set security-association lifetime seconds 900 > Définit la durée de vie d'une SA à la suite de laquelle les clés symétriques seront renégociées

#match address 101 > Applique les règles de l'ACL créée pour déterminer quel trafic doit être inclus dans la politique de chiffrement

#exit

```
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 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
```

Application de la crypto map sur l'interface de sortie de R1

Dans notre cas, il s'agit de l'interface fastEthernet 0/1 :

R1(config)#interface fastEthernet 0/1

R1(config-if)#crypto map stade

```
R1-Stade(config)#interface FastEthernet 0/1
R1-Stade(config-if)#crypto map stade
R1-Stade(config-if)#
*Jan  1 04:27:03.115: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1-Stade(config-if)#
```

Configuration de base du routeur R3

Le système d'exploitation (IOS) du routeur R3 supporte également le VPN :

#show version

Activations des fonctions crypto du routeur de R3

(Optionnel car activé par défaut sur notre IOS) :

#crypto isakmp enable

Configurer la police de R3

#crypto isakmp policy 10

#authentication pre-share

#encryption 3des

#hash md5

```
#group 5
#lifetime 3600
#exit
```

Configuration de la clef de R3

```
#crypto isakmp key iris123 address 200.200.200.1
ou
#crypto isakmp key 6 iris123 address 200.200.200.1
```

Configuration des options de transformations des données de R3

```
#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
#crypto ipsec security-association lifetime seconds 1800
```

Création d'ACL de R3

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

Configuration de la crypto map de R3

```
#crypto map billetterie 10 ipsec-isakmp
#set peer 200.200.200.1
#set transform-set 50
#set security-association lifetime seconds 900
#match address 101
#exit
#interface FastEthernet 0/1
#crypto map billetterie
```

```

R3-Billetterie>enable
R3-Billetterie#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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(cfg-crypto-trans)#$-association lifetime seconds 1800
R3-Billetterie(config)#$t ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3-Billetterie(config)#crypto map billetterie 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.
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)#$y-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-Billetterie(config-if)#
*Nov 19 13:56:55.947: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON

```

Test de communication avec un PING

La configuration des routeurs (et éventuellement la réinitialisation des switches) est faite.

Nous allons tenter un PING entre le PC0 et le PC1.

Pour cela, nous branchons chaque PC sur un Switch, puis nous leur attribuons une adresse IP à chacun

Configuration du PC0

Branché sur le **switch0** avec un câble Ethernet, nous naviguons via le GUI pour lui attribuer l'adresse IP **172.20.0.10** :

Paramètres > Réseau et Internet > Wifi ou Ethernet > Attribution d'adresse IP :
Modifier > Sélectionner Manuel > Activer IPV4

Modifier les paramètres IP du réseau

Manuel

IPv4

☒ Activé

Adresse IP

172.20.0.10

Masque de sous-réseau

255.255.255.0

Passerelle

172.20.0.1

DNS préféré

1.1.1.1

DNS sur HTTPS

Désactivé

Configuration du PC1

Branché sur le **switch1** avec un câble Ethernet, pour lui attribuer l'adresse IP **192.168.1.100** :

**Paramètres > Réseau et Internet > Wifi ou Ethernet > Attribution d'adresse IP :
Modifier > Sélectionner Manuel > Activer IPV4 :**

Modifier les paramètres IP du réseau

Manuel

IPv4

☒ Activé

Adresse IP

192.168.1.100

Masque de sous-réseau

255.255.255.0

Passerelle

192.168.1.1

DNS préféré

1.1.1.1

DNS sur HTTPS

Désactivé

Le PC0 parvient à envoyer un PING au PC1 :

```
C:\Users\iris>ping 192.168.1.100
```

```
Envoi d'une requête 'Ping' 192.168.1.100 avec 32 octets de données :  
Réponse de 192.168.1.100 : octets=32 temps=1 ms TTL=125  
Réponse de 192.168.1.100 : octets=32 temps=1 ms TTL=125  
Réponse de 192.168.1.100 : octets=32 temps=2 ms TTL=125  
Réponse de 192.168.1.100 : octets=32 temps=1 ms TTL=125
```

```
Statistiques Ping pour 192.168.1.100:
```

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

Test du VPN

Le Ping fonctionne et la commande tracert permet de regarder le chemin complet emprunté par le paquet.

L'itinéraire utilisé confirme que le paquet est directement passé du routeur R1-Stade (via l'interface interne 172.20.0.1) pour arriver au PC 192.168.1.100 du routeur R3-Billetterie, en passant par l'interface externe 200.200.200.6

Le VPN fait le transfert via le tunnel VPN et cache l le routeur R2-FAI

```
C:\Users\iris>ping 192.168.1.100

Envoi d'une requête 'Ping' 192.168.1.100 avec 32 octets de données :
Réponse de 192.168.1.100 : octets=32 temps=2 ms TTL=126
Réponse de 192.168.1.100 : octets=32 temps=3 ms TTL=126
Réponse de 192.168.1.100 : octets=32 temps=3 ms TTL=126
Réponse de 192.168.1.100 : octets=32 temps=3 ms TTL=126

Statistiques Ping pour 192.168.1.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\iris>tracert 192.168.1.100

Détermination de l'itinéraire vers 192.168.1.100 avec un maximum de 30 sauts.

  1      1 ms    <1 ms    <1 ms    172.20.0.1
  2      2 ms     1 ms     2 ms    200.200.200.6
  3      3 ms     2 ms     2 ms    192.168.1.100

Itinéraire déterminé.
```

III) Conclusion

La sécurisation des routeurs est une étape essentielle pour protéger nos réseaux et garantir la confidentialité des données échangées.

En configurant correctement les mots de passe, en paramétrant les protocoles SSH et le VPN et en surveillant les connexions en continue, on met en place une protection solide contre les menaces extérieures. Mais au-delà de la technologie, il est crucial d'assurer une formation sur la durée, ainsi qu'une vigilance permanente du SI pour que la sécurité reste optimale sur le long terme.

Chaque détail compte, et la combinaison de bonnes pratiques et de vigilance fait toute la différence.