DESCRIPTION D'UNE MISSION | BTS SIO			
Prénom – Nom	Ajay Muthu Kumar	**N° mission**	3
Option	**SISR** ☒	**SLAM** ☐	
Situation	**Formation** ☒	**Entreprise** ☐	

Lieu de réalisation	Ecole IRIS Paris 17ème	
Période de réalisation	Du : 14/10/2025	Au : 27/10/2025
Modalité de réalisation	VÉCUE ☒	OBSERVÉE ☒

Intitulé de la mission	**Mise en Place d'une Solution pour l'Administration à Distance Sécurisée et la Sécurisation des Interconnexions**
Description du contexte de la mission	Description en 2 à 3 lignes maxi Dans le contexte de la mission du projet StadiumCompany, l'objectif de cette tâche est d'établir une solution sécurisée d'administration à distance via SSH et un VPN IPsec entre divers lieux (stade, billetterie, boutique), dans le but de garantir la confidentialité des communications et la protection des interconnexions du système d'information.

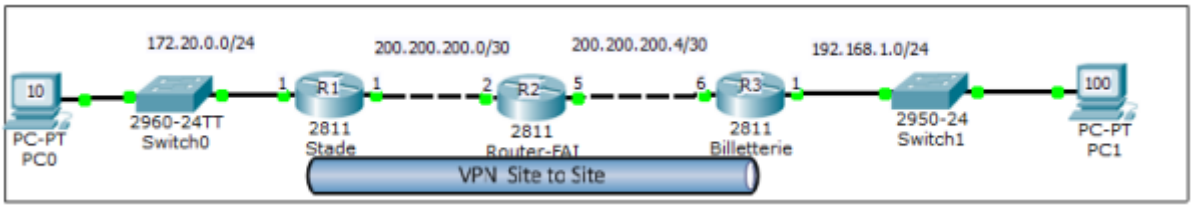
Ressources et outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels) Routeur Cisco – Windows 11 – Switch Cisco - PuTTY
Résultat attendu	Résultat attendu avec la réalisation de cette mission Avec la réalisation de cette mission, le résultat attendu est l'accès à distance de la sécurité aux équipements, sécurisation des interconnexions inter-sites, les applications de politiques d'authentification renforcées en gestion des certificats numériques et de journalisation des connexions administratives pour la traçabilité et la sécurité
Contraintes	Contraintes : techniques | budgétaires | temps | O.S. ou outils imposés… Pour la technique : On fait la compatibilité entre les routeurs Cisco, la configuration cohérente des politiques IPsec Pour le temps : La réalisation pendant une journée en classe puis rédigé proprement dans le délai imparti (Une semaine) Pour le logiciel et O.S : L'environnement Cisco IOS, outils d'administration réseau et PuTTY

Compétences associées	Liste des intitulés du tableau de compétences (avec les références)

Description simplifiée des différentes étapes de réalisation de la mission
en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées

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

Représentation de l'infrastructure :



Configuration du VPN sur le Routeur 1

Etape 1 :

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

```
R1#crypto isakmp enable
```

Etape 2 :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Etape 3 :

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

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

Etape 4 :

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

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

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

- Encryption : 3des.
- Hash : md5.

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

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

Etape 5 :

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

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

Etape 6 :

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

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

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

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

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

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

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

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

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

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

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

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

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

Etape 7 :

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

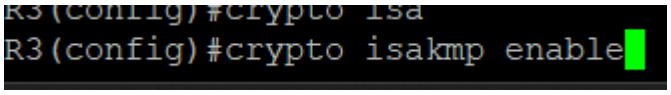
```
R1(config)#interface FastEthernet 0/1
R1(config-if)#crypto map stade
```

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

Configuration du VPN sur le routeur 3

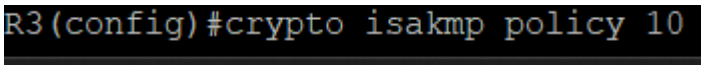
Etape 1 :

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

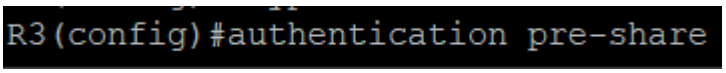


Etape 2 :

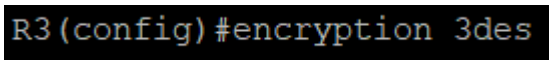
1. Maintenant, il faut commencer par configurer différentes choses comme la police qui est une politique ISAKMP avec la commande : crypto isakmp policy 10.



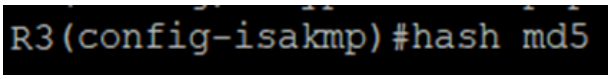
2. Après cela, il faut déterminer quel type d'authentification qu'on va utiliser. Pour cela, on peut utiliser la commande : authentification pre-share.



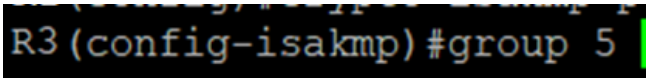
3. De plus, déterminer l'encryption qu'on va utiliser en utilisant de la commande : encryption 3des.



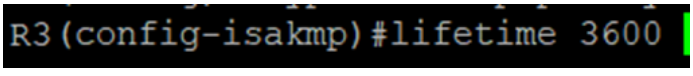
4. Aussi, quel hash il va falloir mettre en place concernant la vérification de l'intégrité des données échangées. La commande : hash md5 nous permet de le mettre en place.



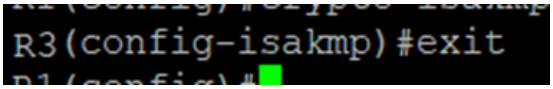
5. Il faut choisir le groupe pour l'échange des clés qu'on va utiliser avec cette commande : group 5. Cela spécifie l'identifiant Diffie-Hellman.



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



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



Etape 3 :

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

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

Etape 4 :

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

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

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

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

Etape 5 :

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

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

Etape 6 :

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

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

2. Ensuite, on indique le destinataire du tunnel VPN qui est dans notre cas le routeur 3 : set peer 200.200.200.1.

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

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

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

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

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

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

```
R3(config-crypto-map)#match address 101
```

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

```
R3(config-crypto-map)#exit
```

Etape 7 :

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

```
R3(config)#interface FastEthernet 0/1
```

```
R3(config-if)#crypto map billetterie
```

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

Vérification de la configuration sur chaque routeur

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

Show Running

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

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

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

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

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

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

Vérification ping entre les deux routeurs :

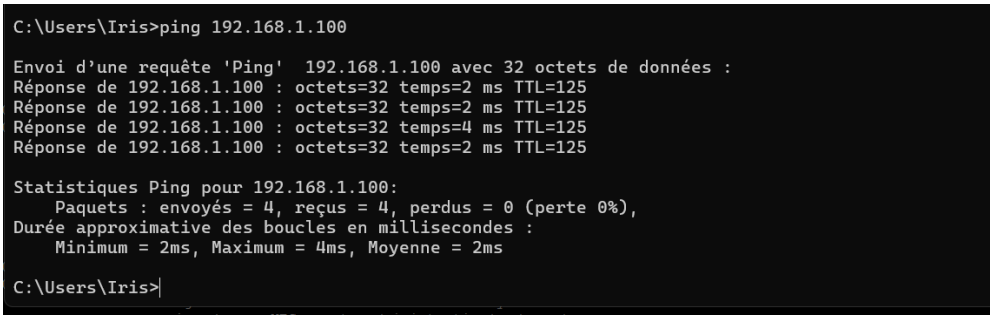
R1 vers R3 : Le ping fonctionne correctement !

```
C:\Users\Iris>ping 172.20.0.1

Envoi d'une requête 'Ping'  172.20.0.1 avec 32 octets de données :
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 172.20.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

R3 vers R1 : Le ping fonctionne correctement !



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

Conclusion	Que pouvez-vous dire de cette mission : apport personnel, expérience, etc
	Cette mission m'a permis de mettre en œuvre concrètement une solution VPN IPsec et d'assurer une administration à distance sécurisée. On a pu renforcer les compétences en configuration des vrais routeurs Cisco, en sécurisation réseau et en gestion des accès. Cette expérience nous a bien aidé à mieux comprendre dans les enjeux de la sécurité des communications inter-sites et la traçabilité dans l'administration réseau

Evolution possible	Evolution du service concerné par cette mission qui pourrait être envisagée
	Cette mission qui pourrait être envisagée sont l'automatisation des sauvegardes et la supervision comme Nagios, on pourrait mettre une authentification à deux facteurs pour les connexions SSH.

Productions associées	Liste des documents produits et description
	- Fichier de configuration des routeurs R1, R2 et R3 - Rapport de test de connectivité et journalisation des accès - La connexion SSH et le VPN qui sont actif