DESCRIPTION D'UNE MISSION | BTS SIO			
Prénom – Nom	Tymothé-Sainte	**N° mission**	3
Option	**SISR** ☒	**SLAM** ☐	
Situation	**Formation** X ☒	**Entreprise** ☐	

Lieu de réalisation	Ecole IRIS Paris 17ème	
Période de réalisation	Du :	Au :
Modalité de réalisation	VÉCUE ☒	OBSERVÉE ☐

Intitulé de la mission	Sécurisation de l'administration réseau et mise en place d'un VPN IPsec intersites pour StadiumCompany
Description du contexte de la mission	StadiumCompany dispose de plusieurs sites (Stade et Billetterie) qui communiquent entre eux. Cependant, les échanges intersites n'étaient pas sécurisés, et l'administration réseau se faisait via Telnet, un protocole non chiffré. Pour assurer la confidentialité des données et protéger l'infrastructure, il a été décidé de : - Sécuriser l'administration des équipements réseau via SSH - Mettre en place un tunnel VPN IPsec afin de chiffrer les communications entre les sites Configurer le routage dynamique EIGRP pour assurer la résilience réseau

Ressources et outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels) • Cisco Packet Tracer • Routeur Cisco ISR 2811 (×3 : R1-Stade, R2-Internet, R3-Billetterie) • Switchs Cisco Catalyst 2960-24TT (×2) • Postes clients (PC-PT ×2) • Documentation du cahier des charges StadiumCompany
Résultat attendu	Résultat attendu avec la réalisation de cette mission • Administration sécurisée via SSH au lieu de Telnet • Mise en place d'un tunnel VPN IPsec site-à-site entre R1 (Stade) et R3 (Billetterie) • Chiffrement des données circulant entre les sites • Routage dynamique entre les 3 routeurs via EIGRP • Vérification : ping intersites, tracert, commandes show crypto
Contraintes	Contraintes : techniques | budgétaires | temps | O.S. ou outils imposés… • L'administration réseau devait être sécurisée : interdiction d'utiliser Telnet. • Le tunnel VPN devait garantir la confidentialité et l'intégrité des données entre les sites.

Compétences associées	Liste des intitulés du tableau de compétences (avec les références)
	• A1.1.1 : Analyse du cahier des charges d'un service à produire • A1.2.3 : Élaboration de solutions pour la sécurisation du SI • A2.3.1 : Installation et configuration d'éléments d'interconnexion • A4.1.1 : Rédaction d'une documentation technique • A5.2.1 : Exploitation des services pour garantir la continuité

Description simplifiée des différentes étapes de réalisation de la mission

en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées

- Analyse du cahier des charges et identification des risques liés à l'utilisation de Telnet et au manque de chiffrement intersite.
- Activation et configuration de l'administration sécurisée via SSH sur les routeurs R1 et R3.
- Génération et gestion des clés RSA pour la sécurisation des accès administrateur.
- Configuration d'un tunnel VPN IPsec site-à-site entre le Stade (R1) et la Billetterie (R3).
- Paramétrage de la phase 1 (ISAKMP) : négociation et authentification.
- Paramétrage de la phase 2 (IPsec) : chiffrement et intégrité des données.
- Création de listes de contrôle d'accès (ACL) pour définir les réseaux autorisés dans le tunnel.
- Application du crypto map sur les interfaces WAN pour activer le VPN.
- Réalisation de tests de connectivité (ping intersites).
- Vérification du chiffrement et de l'établissement du tunnel via les commandes show crypto.
- Sauvegarde des configurations et documentation de l'architecture finale.

Conclusion	Que pouvez-vous dire de cette mission : apport personnel, expérience, etc
	Cette mission m'a permis de comprendre et de mettre en œuvre des mécanismes concrets de Sécurisation du système d'information. La mise en place du protocole SSH m'a montré comment Remplacer un accès non sécurisé par une administration chiffrée. Le tunnel VPN IPsec a permis De garantir la confidentialité des échanges intersites. Cette mission a été très formatrice car elle M'a fait manipuler des concepts de sécurité réseau utilisés en entreprise.

Evolution possible	Evolution du service concerné par cette mission qui pourrait être envisagée
	• Extension du VPN IPsec au troisième site (magasin) • Mise en place d'un système d'authentification centralisé (RADIUS / TACACS+) • Ajout d'une authentification renforcée (MFA / clés SSH par utilisateur) • Surveillance proactive du VPN via un outil de supervision (PRTG / Zabbix) • Mise en place d'un firewall dédié pour un contrôle plus avancé des flux réseau

Étapes de réalisation

• Analyse du cahier des charges et identification des risques liés à l'utilisation de Telnet et au manque de chiffrement intersite.
• Activation et configuration de l'administration sécurisée via SSH sur les routeurs R1 et R3.
• Génération et gestion des clés RSA pour la sécurisation des accès administrateur.
• Configuration du routage dynamique EIGRP sur les trois routeurs.
• Configuration d'un tunnel VPN IPsec site-à-site entre le Stade (R1) et la Billetterie (R3).
• Paramétrage de la phase 1 (ISAKMP) : négociation et authentification.
• Paramétrage de la phase 2 (IPsec) : chiffrement et intégrité des données.
• Création de listes de contrôle d'accès (ACL) pour définir les réseaux autorisés dans le tunnel.
• Application du crypto map sur les interfaces WAN pour activer le VPN.
• Réalisation de tests de connectivité (ping intersites, tracert).
• Vérification du chiffrement et de l'établissement du tunnel via les commandes show crypto.
• Sauvegarde des configurations et documentation de l'architecture finale.

Schéma réseau

La topologie mise en place comprend trois routeurs Cisco 2811 interconnectés, deux switchs Catalyst 2960 et deux postes clients. Le routeur R2 joue le rôle de routeur Internet (FAI) entre les deux sites.

Topologie – Plan d'adressage IP

PC0 ── Switch0 (2960-24TT) ── R1-Stade (2811) ── R2-FAI (2811) ── R3-Billetterie (2811) ── Switch1 (2950-24) ── PC1

Interface	Équipement	Adresse IP	Masque
Fa0/0	R1 (Stade)	172.20.0.1	/24 (LAN Stade)
Fa0/1	R1 (Stade)	200.200.200.1	/30 (lien R1-R2)
Fa0/0	R2 (FAI)	200.200.200.2	/30 (lien R1-R2)
Fa0/1	R2 (FAI)	200.200.200.5	/30 (lien R2-R3)
Fa0/0	R3 (Billetterie)	192.168.1.1	/24 (LAN Billetterie)
Fa0/1	R3 (Billetterie)	200.200.200.6	/30 (lien R2-R3)

Sécurisation de l'administration via SSH

L'administration du routeur était auparavant accessible via Telnet, un protocole non chiffré. Dans un objectif de sécurisation du SI, Telnet a été désactivé et remplacé par SSH, permettant un accès distant chiffré et authentifié.

Un utilisateur administrateur a été créé et les clés RSA en 2048 bits ont été générées pour garantir la confidentialité des connexions.

Configuration SSH sur R1

```
enable
configure terminal
hostname R1
ip domain-name stadiumcompany.local
username admin privilege 15 secret Admin@2025!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 transport input ssh
 login local
 exec-timeout 10 0
end
wr
```

Configuration SSH sur R3

```
enable
configure terminal
hostname R3
ip domain-name stadiumcompany.local
username admin privilege 15 secret Admin@2025!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 transport input ssh
 login local
 exec-timeout 10 0
end
wr
```

Configuration du tunnel VPN IPsec

Un tunnel VPN IPsec a été configuré entre le site du Stade (R1) et le site Billetterie (R3) afin de chiffrer les communications intersites. La configuration a été réalisée en deux phases : négociation ISAKMP (phase 1) et chiffrement IPsec (phase 2), puis application du crypto map sur l'interface WAN.

Configuration Phase 1 (ISAKMP) – R1

Cette étape définit les paramètres de négociation du tunnel : méthode d'authentification, algorithme de chiffrement, fonction de hachage et durée de validité.

```
R1# conf t
R1(config)# crypto isakmp enable
R1(config)# crypto isakmp policy 10
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
```

Configuration Phase 2 (IPsec) + ACL + Crypto Map – R1

```
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)# access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)# crypto map stade 10 ipsec-isakmp
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)# end
  --> *Nov 19 14:36:46: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Configuration complète VPN – R3

La configuration sur R3 comprend les mêmes phases avec les adresses symétriques.

```
R3(config)# crypto isakmp enable
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash md5
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 3600
R3(config-isakmp)# exit
R3(config)# crypto isakmp key iris123 address 200.200.200.1
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 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3(config)# crypto map billetterie 10 ipsec-isakmp
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 0/1
R3(config-if)# crypto map billetterie
R3(config-if)# end
  --> *Jan  1 04:20:31: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Configuration EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) a été configuré sur les trois routeurs afin d'assurer un routage dynamique et une reconvergence rapide en cas de panne. Il calcule les meilleurs chemins pour les données entre les sites.

R1 – Stade

```
R1(config)# router eigrp 1
R1(config-router)# network 172.20.0.0 0.0.0.255
R1(config-router)# network 200.200.200.0 0.0.0.3
R1(config-router)# exit
R1(config)# ip route 192.168.1.0 255.255.255.0 200.200.200.2
```

R2 – Routeur Internet (FAI)

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

R3 – Billetterie

```
R3(config)# router eigrp 1
R3(config-router)# network 192.168.1.0
R3(config-router)# network 200.200.200.4 0.0.0.3
R3(config-router)# exit
R3(config)# ip route 172.20.0.0 255.255.255.0 200.200.200.5
```

Vérification et tests

Vérification du tunnel – commandes show crypto

Ces commandes permettent de confirmer que le tunnel VPN est bien établi et que le chiffrement est actif :

show crypto isakmp sa – associations de sécurité phase 1

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state    conn-id  status
200.200.200.6  200.200.200.1  QM_IDLE  1001     ACTIVE

  --> statut QM_IDLE + ACTIVE : tunnel phase 1 opérationnel
```

show crypto ipsec transform-set – vérification du chiffrement

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

  --> chiffrement 3DES + HMAC-MD5 en mode Tunnel confirmé
```

show crypto map – crypto map appliqué sur l'interface WAN

```
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 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
  Transform sets={ 50: { esp-3des esp-md5-hmac } }
  Interfaces using crypto map stade: FastEthernet0/1
```

show crypto ipsec sa – tunnels IPsec actifs

```
R1# show crypto ipsec sa
interface: FastEthernet0/1
  Crypto map tag: stade, local addr 200.200.200.1
  local  ident: 172.20.0.0/255.255.255.0
  remote ident: 192.168.1.0/255.255.255.0
  current_peer 200.200.200.6 port 500
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  inbound esp sas:  Status: ACTIVE
  outbound esp sas: Status: ACTIVE
```

Test de connectivité – ping intersites

Un ping a été réalisé depuis PC1 (LAN Billetterie) vers PC0 (LAN Stade) pour valider la connectivité de bout en bout à travers le tunnel VPN :

Résultat ping – PC1 → 172.20.0.10
PS C:\Users\iris> ping 172.20.0.10
Envoi d'une requête Ping vers 172.20.0.10 avec 32 octets de données :
Réponse de 172.20.0.10 : octets=32 temps=2 ms TTL=126
Réponse de 172.20.0.10 : octets=32 temps=3 ms TTL=126
Réponse de 172.20.0.10 : octets=32 temps=2 ms TTL=126
Réponse de 172.20.0.10 : octets=32 temps=3 ms TTL=126
Statistiques : Paquets envoyés=4, reçus=4, perdus=0 (perte 0%)
Durée minimale=2ms, maximale=3ms, moyenne=2ms

Vérification du passage par le tunnel VPN – tracert

La commande tracert permet de confirmer que le trafic transite bien via le tunnel VPN et non en clair sur le réseau public :

Résultat tracert – PC1 → 172.20.0.10
PS C:\Users\iris> tracert 172.20.0.10
Détermination de l'itinéraire vers 172.20.0.10 (30 sauts max.) :
1 1 ms <1 ms <1 ms 192.168.1.1 (R3 – passerelle LAN Billetterie)
2 2 ms 2 ms 2 ms 200.200.200.1 (R1 – tunnel VPN, saut direct)
3 3 ms 2 ms 2 ms 172.20.0.10 (PC0 – destination atteinte)
--> Le saut 2 passe directement à R1 sans transiter par R2,
ce qui confirme le passage effectif par le tunnel VPN IPsec.

Conclusion

Cette mission m'a permis de mettre en œuvre des mécanismes concrets de sécurisation du système d'information. L'activation de l'administration sécurisée via SSH a remplacé l'accès non chiffré de type Telnet, ce qui garantit désormais la confidentialité des actions d'administration.

La mise en place d'un tunnel VPN IPsec entre les deux sites a permis de chiffrer les communications intersites afin d'éviter toute interception ou altération des données échangées. La configuration d'EIGRP assure quant à elle un routage dynamique et résilient entre les trois routeurs.

J'ai ainsi appris à configurer les phases ISAKMP et IPsec, à utiliser des ACL pour définir les réseaux autorisés dans le tunnel, à déployer EIGRP sur un réseau multi-sites, et à vérifier l'état du chiffrement via les commandes de diagnostic. Cette mission a été très formatrice et m'a permis de renforcer mes compétences en sécurité réseau.