DESCRIPTION D'UNE MISSION | BTS SIO			
Prénom – Nom	Tino Franic Nathan Jox Jeremy Nsamu Latufa Riama	**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	Restructuration de l'infrastructure réseau du site principal de 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. L'objectif était donc de renforcer la sécurité du système d'information tout en garantissant la continuité des services.

Ressources et outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels) • Cisco Packet Tracer • Routeur Cisco ISR 4331 • Switchs Cisco Catalyst 2960 • Postes clients (PC-PT) • 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 • Vérification du bon fonctionnement via des tests : • Ping intersites
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
	• Mise en place d'un système d'authentification centralisé (RADIUS / TACACS+). • Ajout d'une authentification renforcée (MFA / clés SSH). • 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.

Sécurisation de l'administration via SSH

-Configuration SSH sur R1

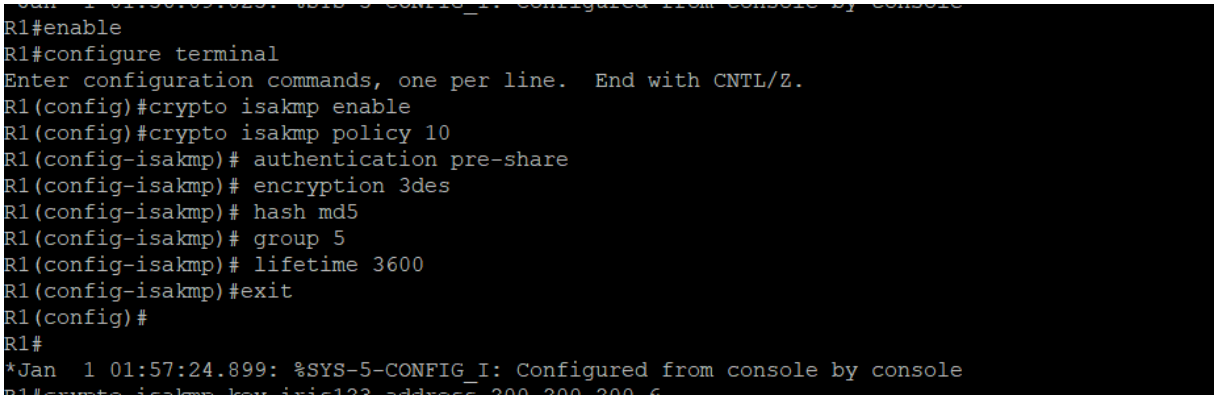
```
enable
configure terminal
hostname R1
ip domain-name stadiumcompany.local
username admin privilege 15 secret Admin@2025!
crypto key generate rsa modulus 2048
ip ssh version 2
line vty 0 4
 transport input ssh
 login local
 exec-timeout 10 0
end
wr
```

-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
```

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.

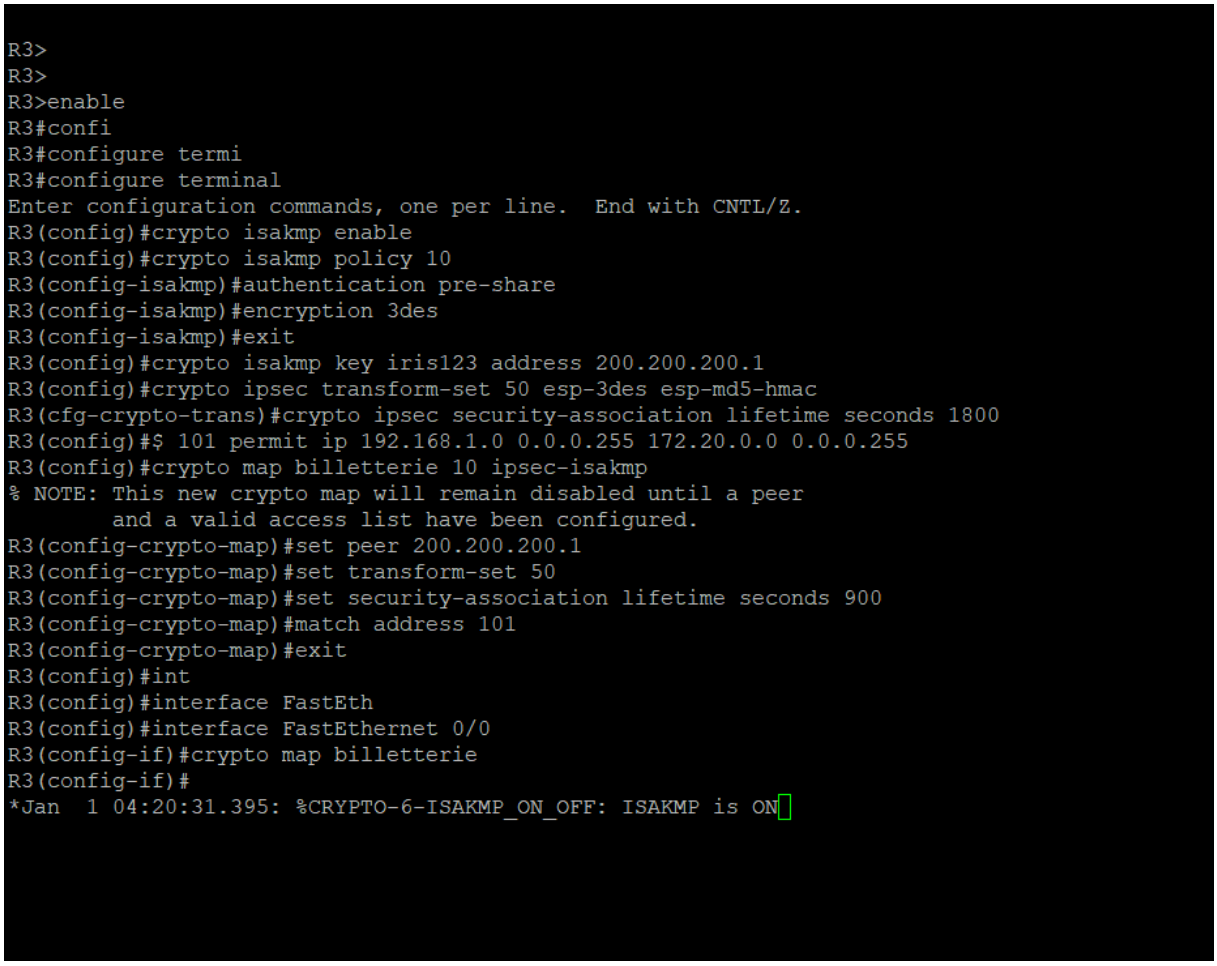
Un tunnel VPN IPsec a été configuré entre le site du Stade (R1) et le site Billetterie (R3) afin de chiffrer les communications intersites.
La configuration a été réalisée en deux phases : négociation ISAKMP (phase 1) et chiffrement IPsec (phase 2), puis application du crypto map sur l'interface WAN.



Configuration de la phase 1 du VPN sur le routeur R1.
Cette étape définit les paramètres de négociation du tunnel : méthode d'authentification, algorithme de chiffrement, fonction de hachage et durée de validité.
Ces paramètres permettent d'établir une connexion sécurisée entre les deux routeurs.

```
R1#end
Translating "end"...domain server (255.255.255.255)
 (255.255.255.255)
Translating "end"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
R1#
R1#
R1#
R1#
R1#
R1#enable
R1#con
R1#confi
R1#configure term
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp
% Incomplete command.

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)#crytpo isakmp key iris123 address 200.200.200.6
             ^
% Invalid input detected at '^' marker.

R1(config)#crytpo isakmp key 6 iris123 address 200.200.200.6
             ^
% Invalid input detected at '^' marker.

R1(config)#crypto isakmp key iris123 address 200.200.200.6
A pre-shared key for address mask 200.200.200.6 255.255.255.255 already exists!

R1(config)#
```

Définition de la clé pré-partagée utilisée pour authentifier les deux extrémités du tunnel VPN.
Cette clé doit être identique sur les deux routeurs afin de permettre l'établissement de la connexion sécurisée.



Configuration complète du VPN sur le routeur R3.
Elle comprend :
- la phase 1 (ISAKMP) pour la négociation sécurisée,
- la phase 2 (IPsec) pour le chiffrement des données,
- l'ACL permettant de sélectionner les réseaux à chiffrer,
- l'application du crypto map sur l'interface WAN pour activer le tunnel VPN.
Cette configuration permet d'assurer la confidentialité des communications entre les deux sites.

```
R3#show run | include crypto isakmp key
crypto isakmp key iris123 address 200.200.200.1
R3#show run | section crypto isakmp
crypto isakmp policy 10
 encr 3des
 authentication pre-share
crypto isakmp key iris123 address 200.200.200.1
R3#show run | include transform-set
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
 set transform-set 50
R3#show run | section crypto map
crypto map billetterie 10 ipsec-isakmp
 set peer 200.200.200.1
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
 crypto map billetterie
R3#show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
R3#show run interface faste
R3#show run interface fastethernet 0/1
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/1
 ip address 200.200.200.6 255.255.255.252
 duplex auto
 speed auto
 crypto map billetterie
end

R3#
```

Vérification de la prise en compte de la configuration VPN sur le routeur R3.
La commande show run permet de confirmer que le crypto map est bien appliqué à l'interface WAN,
ce qui signifie que le tunnel IPsec est opérationnel.

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.
J'ai ainsi appris à configurer les phases ISAKMP et IPsec, à utiliser des ACL pour définir les réseaux autorisés dans le tunnel, 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, en particulier sur les bonnes pratiques d'administration et de protection des flux.