Mission 3

Présenté par :

Chahine Zitouni

Mathieu Barthez

Massila Camara

Zoe Lasm

Wisdom Tamakloe



Sécurisation des accès distants & entre sites

Table des matières

* Contexte professionnel........
* Besoins ................................
* Environnement ...................
* Utilisateurs concernés.........
* Taches à réaliser .................
* Description détaillée de la mission................................
* NAT/PAT.............................
* TELNET................
* SSH..............................
* VPN ..................................
* Conclusion.............................

**CONTEXTE PROFESSIONNEL**

StadiumCompany est une société qui gère un grand stade. IL souhaite améliorer la satisfaction des clients en ajoutant des fonctions de haute technologie et ajouter à son réseau de nouveaux services, tels que la vidéo. La société envisage également de remplacer le PABX vocal numérique existant. Elle souhaiterait un meilleur accès à son réseau existant de caméras de sécurité. Vu son réseau existant ne le permet pas faute à des multiples changement liés aux ajouts d'équipement et à l'augmentation de connexions sans tenir compte des objectifs commerciaux généraux. Elle décide de faire appel à NetworkingCompany qui est un prestataire spécialisé dans la conception des réseaux et le conseil de la phase 1, la conception de haut niveau.

**BESOINS**

Solution permettant l’administration à distance sécurisées et la sécurisation des

Interconnexions

- La sécurité du système d’information devra être renforcée entre les différents sites

- Sécurisation des interconnexions entre le site du stade et les sites distants Billetterie et

Le Magasin.

- La solution retenue devra être administrable à distance via un accès sécurisé par SSH

**ENVIRONNEMENT**

L’administration et gestion des accès est celui du service informatique du centre administratif qui se trouve dans le stade. Dans son sein, s’effectue toutes les opérations concernant la gestion du personnel et l'administration du stade.

**UTILISATEURS CONCERNÉS**

L’administration et gestion des accès concerne les utilisateurs de plusieurs services notamment :

-Service Administration.

- Service Équipes.

- Service Wi-Fi.

- Service Caméra IP.

- Service VIP-Presse.

- Service Fournisseurs.

- Service Restaurant.

**TÂCHES À RÉALISER**

-Mise en place du NAT/PAT

-Mise en place de Telnet sur le switch

- Mise en place de SSH sur Routeur

- Mise en place du VPN

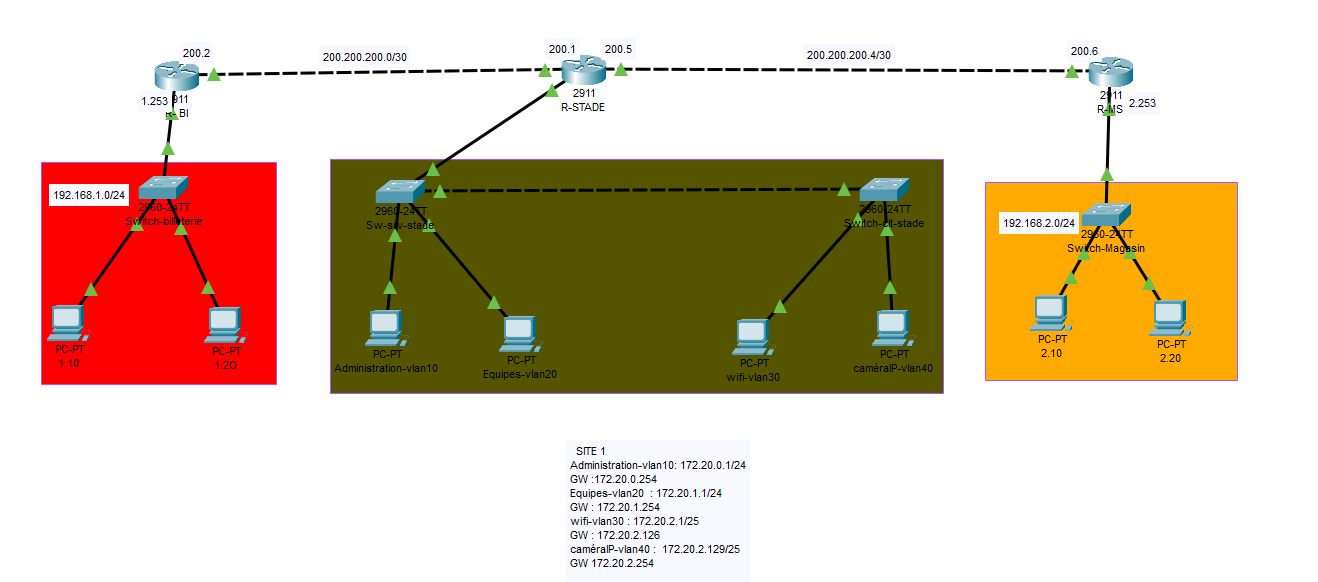
**DESCRIPTION DETAILLEE DE LA MISSION**

**Infrastructure**

Pour la mise en place de la plateforme, nous avons retenus certains prerogative à savoir :

* Telnet sera mise sur les switch
* SSH sera mise sur les routeur

**Schéma Réseau de l’infrascturture**

****

NAT/PAT

Les adresses IP ne sont pas routables sur internet, Lorsqu'un réseau qui utilise des adresses privées veut se connecter à Internet, il faudra, alors faire, une translation des adresses privées en adresses publiques.

Ce processus, qui transforme les adresses privées en public, pour pouvoir aller sur internet, s'appelle le NAT.

Et le périphérique réseau qui s’occupe du NAT, c’est le routeur !

Configuration du NAT/PAT

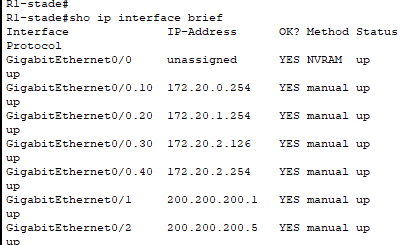
Pour la configuration du PAT, et comme toute sorte de nat, il faut taguer les interfaces en entrée et sortie !

Ensuite, comme pour le nat dynamique, il faut créer une acess-list pour définir les adresses locales qui pourront être translater.

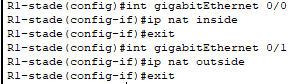
Et pour finir, il faut indiquer au routeur de translater notre access-list, à travers notre interface sortie, la Fast Ethernet 0/1, avec la commande « ip nat inside ».

Ne pas oublier le petit mot « overload » à la fin de la commande.

Dans le réseau du stade, sur le routeur nous créons des sous-interfaces pour faire passer les flux propres au VLANs.



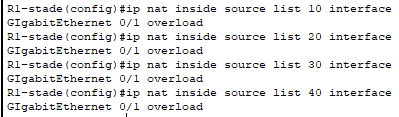
Creation des interfaces en entrée et en sortie « inside » et « outside »



Creation des access-list pour autoriser les adresses qui doivent etre natter .



Indication au routeur de faire natter notre access-list à travers notre interfaces de sortie.



TELNET

Telnet est un protocole qui permet de se connecter, depuis un ordinateur, à un équipement en utilisant une connexion réseau. Une fois connecté en Telnet, vous disposez d’un accès à la Command Line Interface (CLI), et êtes en mesure de réaliser toutes les configurations possibles de la même manière que par une connexion en console.

**Configuration de telnet sur les Switch.**

Tout d’abord création d’un username associé à un mot de passe en entrant simplement

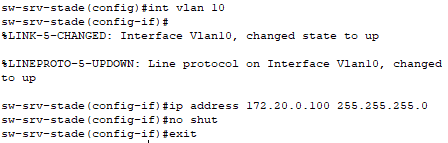
Pour que ce compte utilisateur soit utilisé pour la connexion Telnet, il faut entrer en mode configuration de ligne VTY en entrant “line vty 0 4” et préciser que le compte utilisateur est celui enregistré localement grâce à “login local”. Nous le configurons ici de manière à ce que 5 sessions Telnet puissent se faire simultanément.

Ensuite choisir l’interface qui va permettre de se connecter en Telnet.

Switch stade.



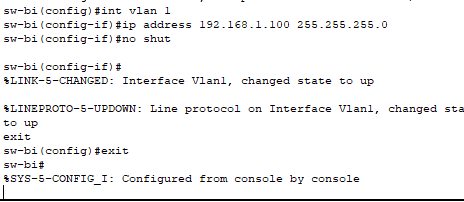
L’interface qui va permettre de se connecter en Telnet.



Switch billetterie



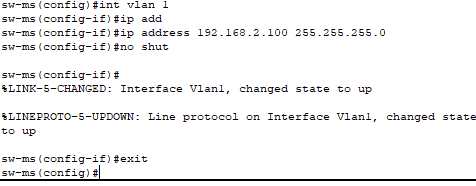
L’interface qui va permettre de se connecter en Telnet.



Switch réseau Magasin



L’interface qui va permettre de se connecter en Telnet.



SSH

Tout comme Telnet, Secure Shell (SSH) est un protocole qui permet de se connecter à un switch ou un routeur distant, mais de manière bien plus sécurisée. En effet, ce protocole chiffre les données, ce que Telnet ne fait pas.

Création des noms d'hôte et de domaine, et d'un mot de passe pour le mode privilégié

La création d’un nom d’hôte et d’un nom de domaine est indispensable à la configuration d’une connexion SSH. Commande : hostname <nom\_hôte>  
ip domain-name <nom\_domaine>

Pour créer un mot de passe pour le mode privilégié, il faut se placer dans le mode configuration et entrer la commande : enable password <mot\_de\_passe>

 Génération de la paire de clés asymétriques RSA

RSA est une méthode de chiffrement dite asymétrique. Elle est composée de deux clés, une privée et une publique, chiffrées sur 1024 bits minimum pour le SSH v2, et permet d’assurer une sécurité optimale. Commande : crypto key generate rsa

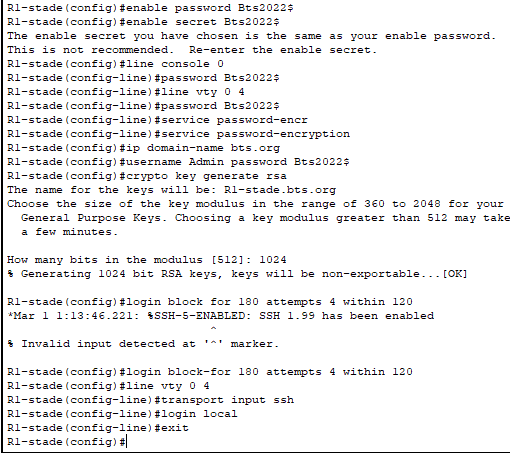
Activation du protocole SSH sur le routeur Cisco

Il faut entrer en mode configuration de ligne VTY dans le but de :

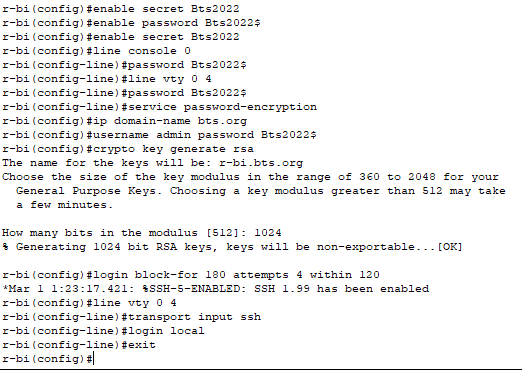
N’accepter que les connexions SSH au routeur ou au switch, au moyen de la commande “transport input ssh” ;

Enregistrer le compte utilisateur existant comme compte permettant de mettre en place la connexion en entrant “login local”.

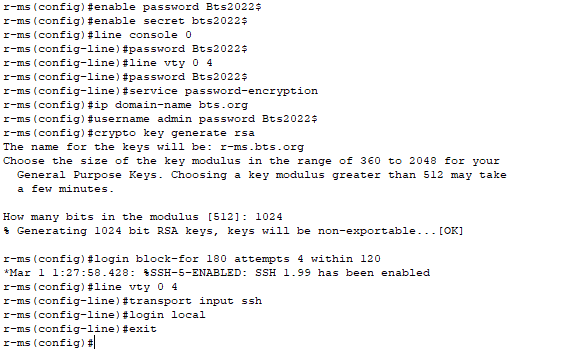
R1-STADE



R-Bi



R-MS



VPN

**VPN site to site (IPsec)**

* **Explications**

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau comme Internet. Il permet de faire transiter des informations, entre les différents membres de ce VPN, le tout de manière sécurisée.

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

Il existe plusieurs types de VPN fonctionnant sur différentes couches réseau, voici les VPN que nous pouvons mettre en place sur un serveur dédié ou à la maison :

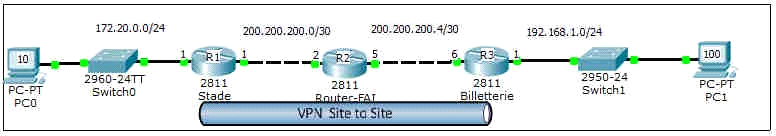
PPTP : Facile à mettre en place, mais beaucoup d'inconvénients liés à la lourdeur du protocole de transport GRE, le matériel réseau (routeur ADSL, wifi, doit être compatible avec le PPTP)

**Ipsec :** Plus efficace que le PPTP en termes de performance, mais aussi très contraignant au niveau de la mise en place

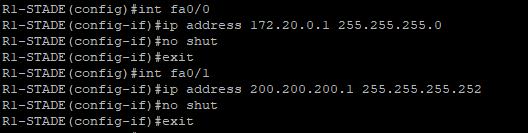
**OpenVPN :** La Rolls des VPN, il suffit de se prendre un peu la tête sur la mise en place, mais son utilisation est très souple.

**Dans notre cas nous allons utiliser IPsec**

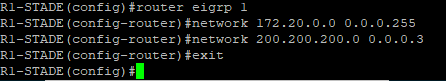
* **Schéma réseau**



* **Routeur R1**



Nos interfaces sont maintenant configurées, il nous reste à configurer le routage. J'ai choisi de faire du routage EIGRP, c'est un choix qui n'engage que moi et qui ne vous empêche pas de faire un routage OSPF ou routage statique si vous préférez.

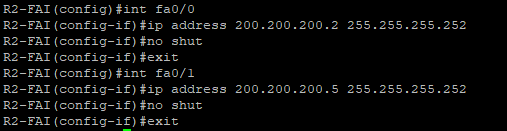


La configuration de base de notre routeur R1 est terminée.

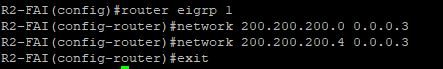
* **Routeur R2**

Même procédure pour notre routeur R2 :

On commence par le Hostname :



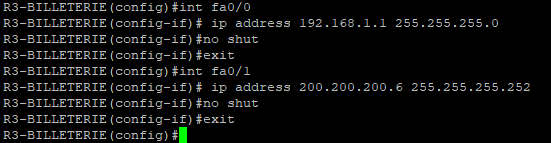
Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.



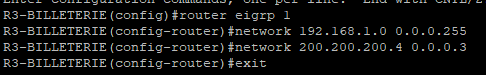
La configuration de base de notre routeur R2 est terminée.

* **Routeur R3**

Même procédure pour notre



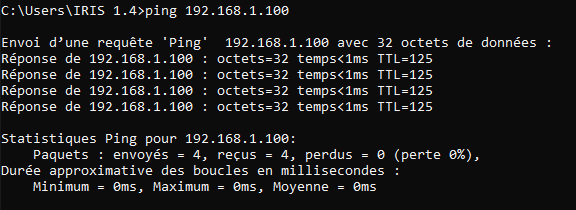
Nos interfaces sont maintenant configurées, il nous reste à configurer le routage



La configuration de base de notre routeur R3 est terminée.

* **Test de fonctionnement**

Nous essayons de pinger depuis le PC du réseau local du Stade vers le PC du réseau local de la billetterie.



**IV) Configuration du VPN**

Il faut savoir que le VPN se configure juste sur les Routeurs d'extrémités dans notre cas R1 et R3 on n'aura aucune modification à faire sur R2.

**Configurations de base**

Nous commencerons par configurer notre PC et notre serveur en leur attribuant la bonne configuration réseau. Nous attaquerons ensuite la configuration du routeur R1 :

**Première étape :**

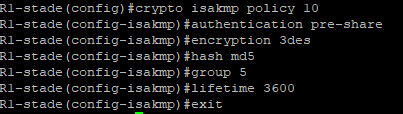
Commençons par notre routeur R1, vous devez vérifier que l'IOS de vos routeurs supporte le VPN. On active ensuite les fonctions crypto du routeur :



Cette fonction est activée par défaut sur les IOS avec les options cryptographiques.

**Deuxième étape :**

Nous allons configurer la police qui détermine quelle encryptions on utilise, quelle Hash quelle type d'authentification, etc.



group 5 : Spécifie l'identifiant Diffie-Hellman

lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

**Troisième étape :**

Ensuite nous devons configurer la clef :



Sur certains routeur avec certains IOS la commande ne fonctionne pas car le routeur demande si le mot de passe doit être chiffré ou pas, tapez cette commande :

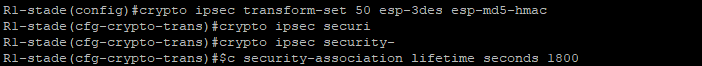
R1(config)#crypto isakmp key 6 iris123 address 200.200.200.6

**Quatrième étape :**

Configurons les options de transformations des données : R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

On fixe ensuite une valeur de Lifetime :

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



esp : Signifie Encapsulation Security Protocol

N'oubliez pas d'utiliser les mêmes protocoles d'encryptions et de Hash utilisés dans la première étape. Dans notre cas :

**Encryption : 3des hash : md5**

**Cinquième étape :**

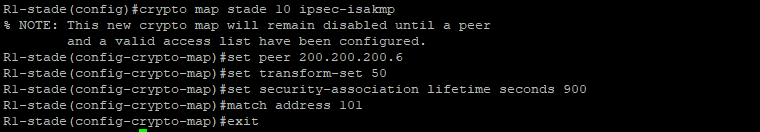
La 5éme étape consiste à créer une ACL qui va déterminer le trafic autoris

R1(config)#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0255

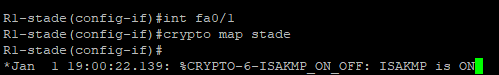


Dernière étape de la configuration :

Dans cette dernière étape nous configurons la crypto map qui va associé l'access-list, le traffic, et la destination



La configuration de R1 est presque terminée nous devons appliquer la crypto map sur l'interface de sortie : Dans notre cas FastEthernet 0/1.



Un message vous indique que la crypto map fonctionne.

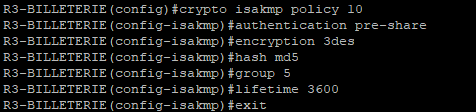
* **Configuration VPN sur R3**

On refait la même configuration que sur R1 :

**Première étape** :



**Deuxième étape :**



**Troisième étape :**



**ou**

R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1

**Quatrième étape :**



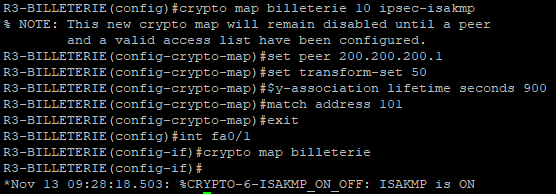
**Cinquième étape** :

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

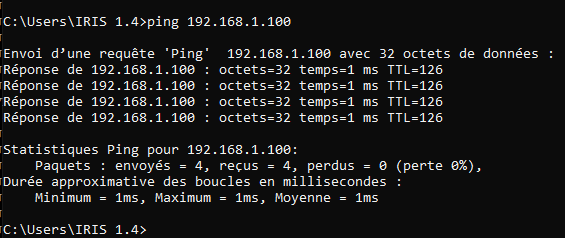
172.20.0.0. 0.0.0.255



Dernière étape de la configuration :

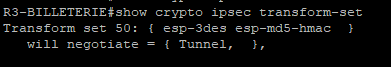


* **Vérifications PC>ping 192.168.1.1**



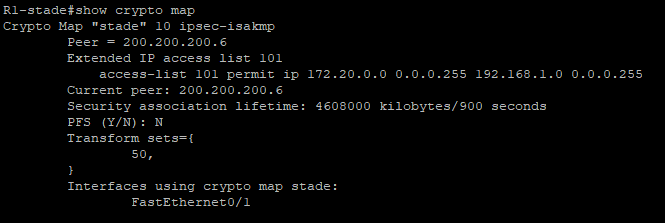
Nous vérifions les informations retournées par le VPN sur R1 et R3 : show crypto ipsec transform-set



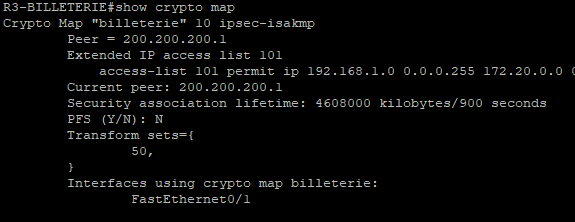


Nous vérifions la map vpn :

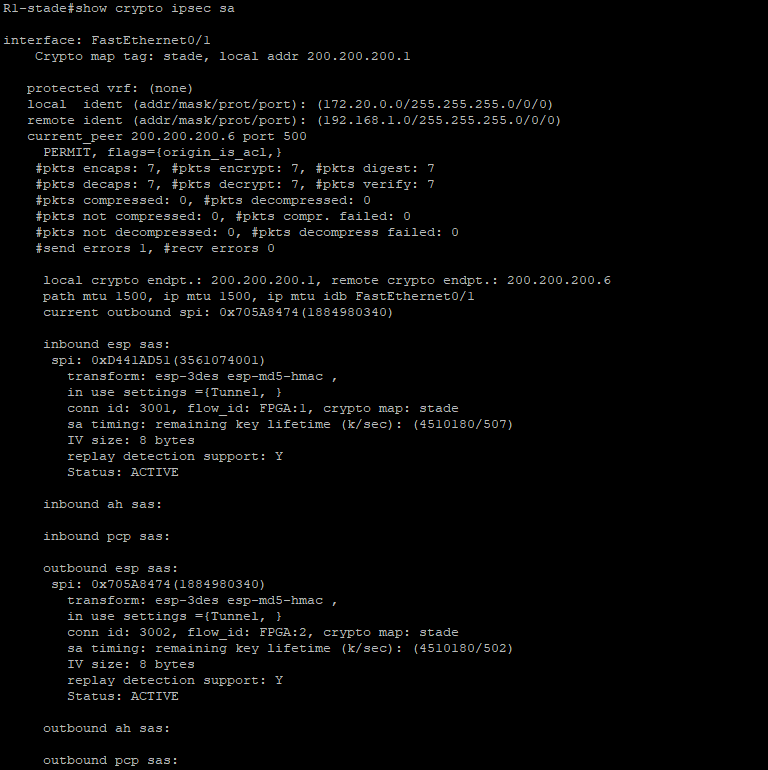
Pour information j'ai nommé ma map "stade". R1#show crypto map



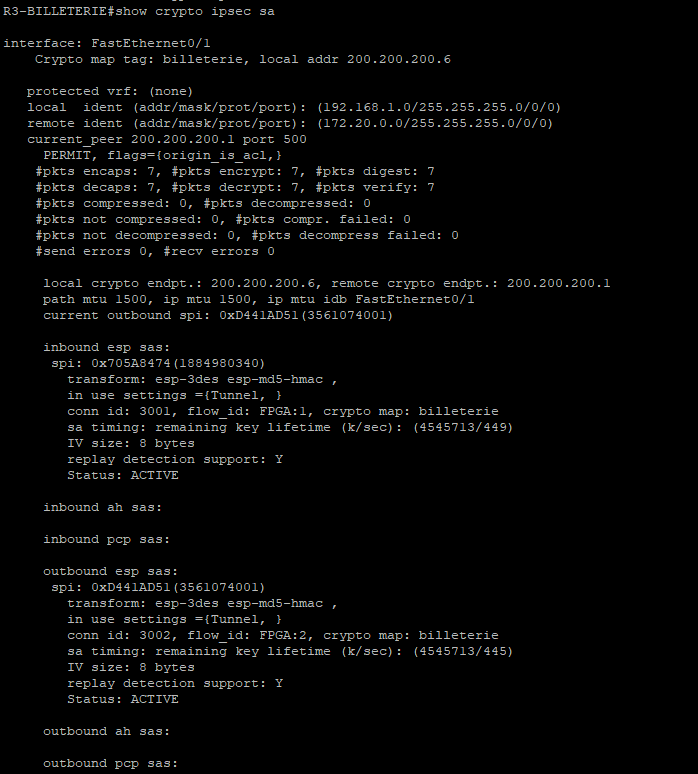
R3#show crypto map



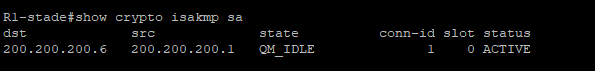
R1#show crypto ipsec sa



R3#show crypto ipsec sa



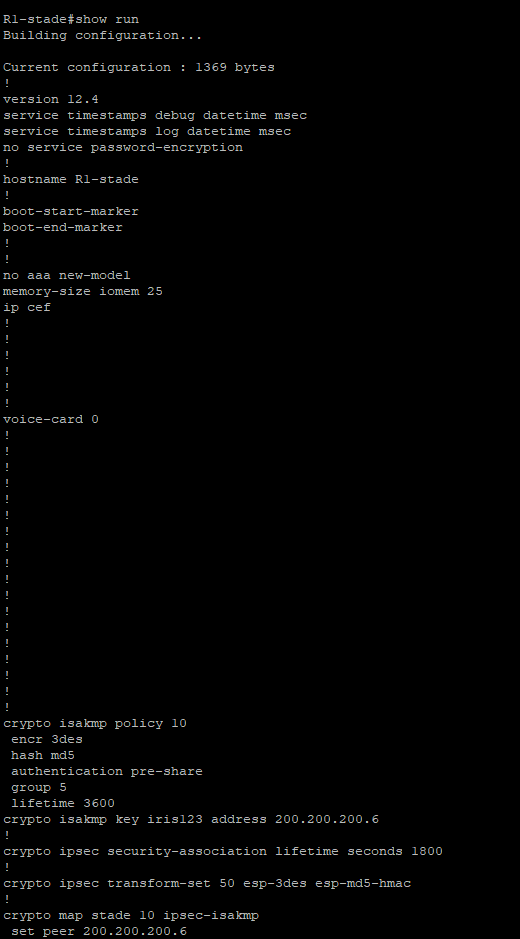
R1#show crypto isakmp sa

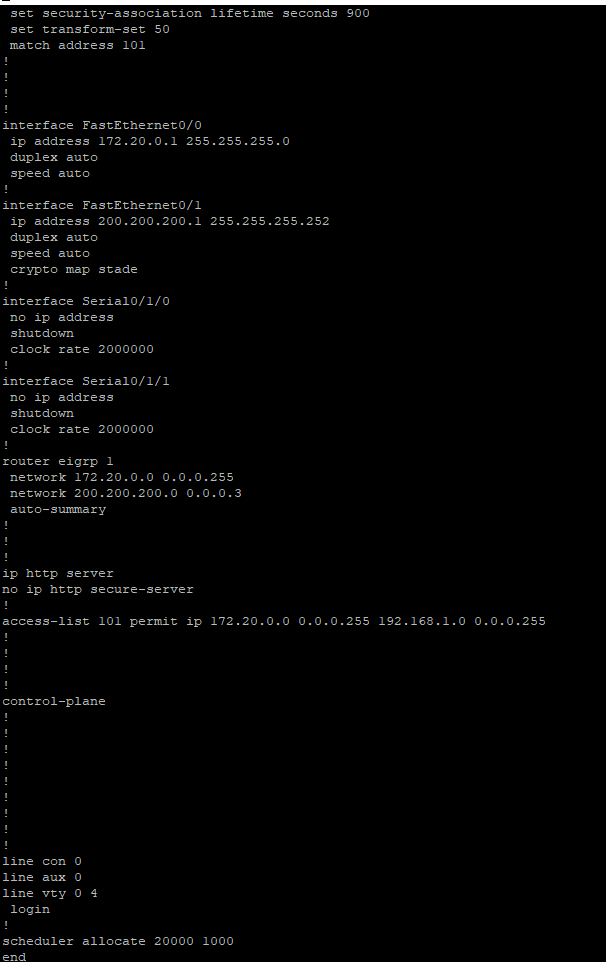


R3#show crypto isakmp sa

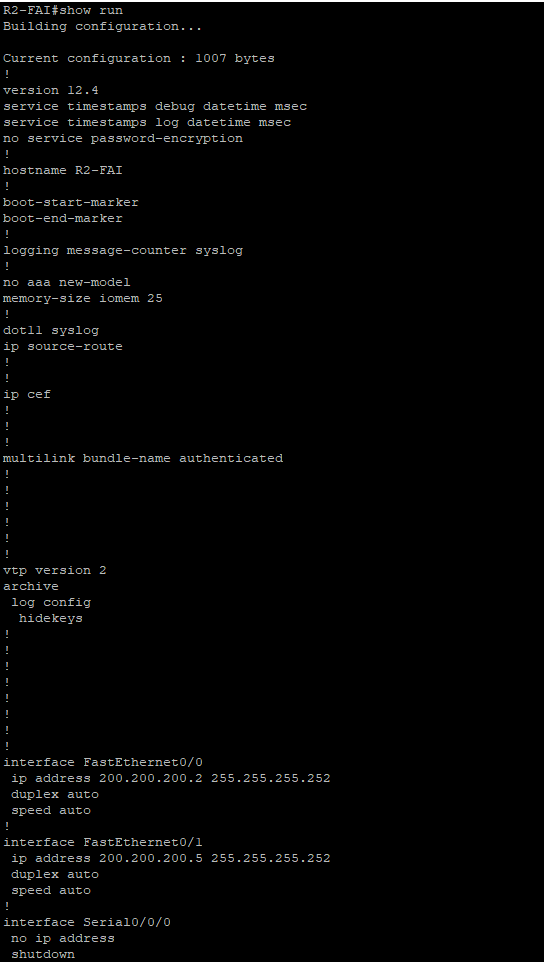


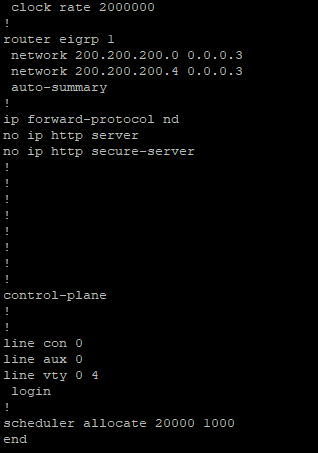
R1#show run



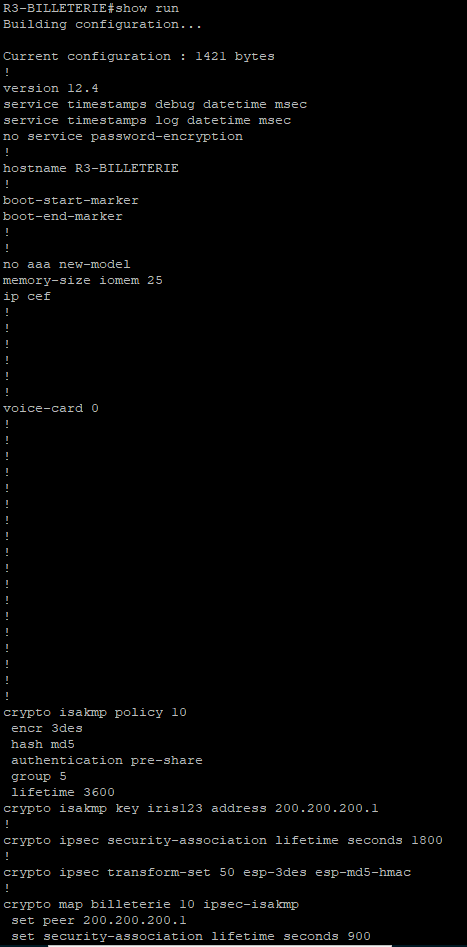


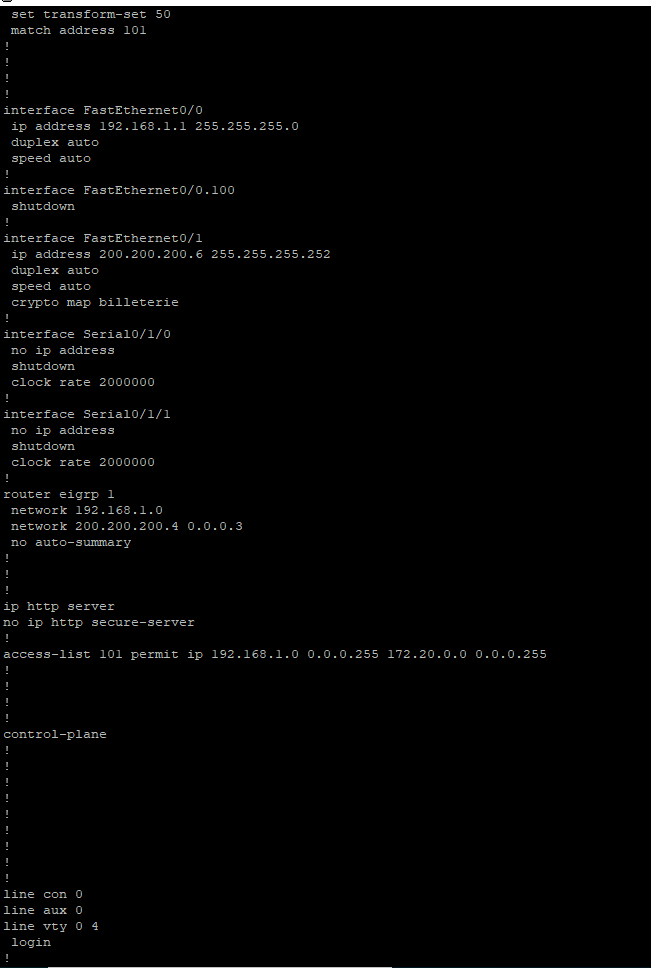
R2#show run





R3#show run





Conclusion

La mise en place de NAT/PAT jumelé a telnet sur le switch ainsi que ssh sur les routeurs sans oublier le vpn entre sites permet sans l’ombre d’aucun doute la sécurisation des accès distants et entre sites .