Mission 3

I)Contexte

a) Présentation de l'entreprise :

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme. Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe. StadiumCompany fournit l'infrastructure réseau et les installations sur le stade.

StadiumCompany emploie 170 personnes à temps plein :

- 35 dirigeants et responsables
- 135 employés

De plus, environ 80 intérimaires sont embauchés en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.

À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide de faire appel à des consultants réseau pour prendre en charge la conception, la gestion du projet et sa mise en œuvre. Ce projet sera mis en œuvre suivant trois phases.

La première phase consiste à planifier le projet et préparer la conception réseau de haut niveau.

La deuxième phase consiste à développer la conception réseau détaillée.

La troisième phase consiste à mettre en œuvre la conception

b) Présentation du prestataire informatique

NetworkingCompany, une société locale spécialisée dans la conception de réseaux et le conseil, de la phase 1, la conception de haut niveau. NetworkingCompany est une société partenaire Cisco Premier Partner. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d'une grande

expérience dans ce secteur. Pour créer la conception de haut niveau, NetworkingCompany a tout d'abord interrogé le personnel du stade et décrit un profil de l'organisation et des installations.

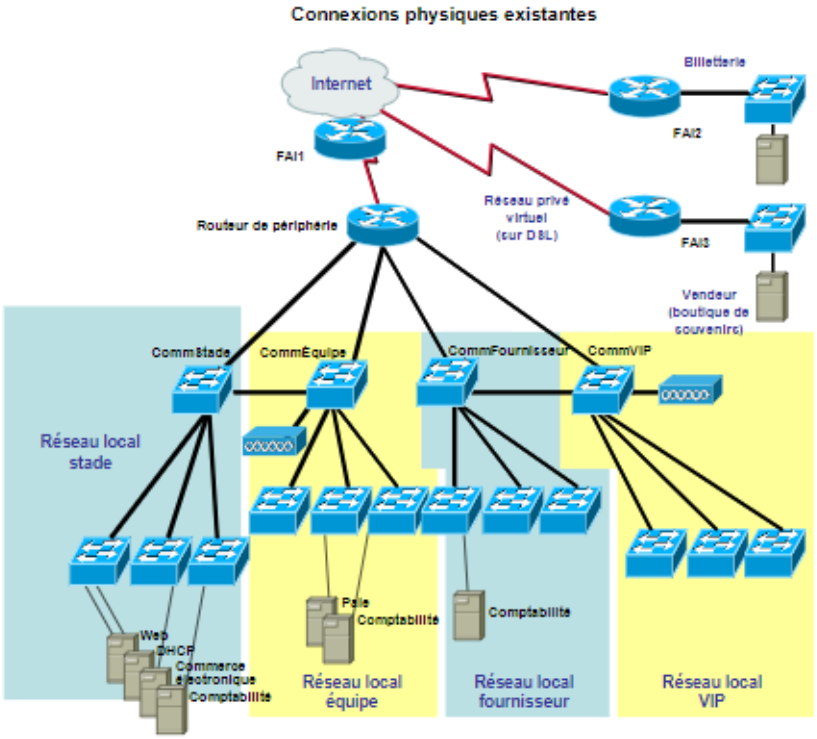
c)Information sur le système informatique

Téléphones et PC de StadiumCompany:

Tous les dirigeants et responsables de StadiumCompany utilisent des PC et téléphones connectés à un PABX vocal numérique. À l'exception des préposés au terrain à temps plein et des gardiens, tous les salariés utilisent également des PC et des téléphones.

Cinquante téléphones partagés sont répartis dans le stade pour le personnel de sécurité. On compte également12 téléphones analogiques, certains prenant également en charge les télécopies et d'autres offrant un accès direct aux services de police et des pompiers. Le groupe sécurité dispose également de 30 caméras de sécurité raccordées à un réseau distinct.

Schéma de l'état des lieux :



Serveur et service :

StadiumCompany propose des installations et une prise en charge de réseau pour deux équipes de sports (Équipe A et Équipe B), une équipe « visiteurs », un restaurant et un fournisseur de concessions.

Le stade mesure environ 220 mètres sur 375. Il est construit sur deux niveaux.

En raison de la taille des installations, plusieurs locaux techniques connectés par des câbles à fibre optique sont répartis sur l'ensemble du stade.

Les vestiaires des équipes A et B et les salons des joueurs sont situés au premier niveau de la partie sud du stade. Les bureaux des équipes occupent une surface d'environ 15 mètres par 60 au deuxième niveau.

Le bureau et le vestiaire de l'équipe « visiteuse

» sont également situés au premier niveau.

Les bureaux de StadiumCompany se trouvent dans la partie nord du stade, répartis sur les deux niveaux.

L'espace des bureaux occupe environ 60 mètres par 18 au premier niveau et 60 mètres par 15 au deuxième niveau.

Les équipes A et B sont engagées dans des compétitions sportives différentes, organisées à des dates différentes. Elles sont toutes les deux sous contrat avec

StadiumCompany pour leurs bureaux et services au sein du stade.

Organisation de l'équipe A

L'équipe A compté 90 personnes :

• 4 dirigeants

• 12 entraîneurs

• 14 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)

• 60 joueurs L'équipe A disposé de 15 bureaux dans le stade pour ses employés non joueurs.

Cinq de ces bureaux sont partagés. 24 PC et 28 téléphones sont installés dans les bureaux.

L'équipe A dispose également d'un vestiaire des joueurs, d'un grand salon pour les joueurs et d'une salle d'entraînement.

Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

Des rumeurs indiquent que l'équipe A aurait récemment installé un concentrateur sans fil dans le salon des joueurs.

Organisation de l'équipe B

L'équipe B compte 64 personnes :

• 4 dirigeants

• 8 entraîneurs

• 12 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)

• 40 joueurs L'équipe B dispose de 12 bureaux dans le stade pour ses employés autres que les joueurs.

Trois de ces bureaux sont partagés. 19 PC et 22 téléphones sont installés dans les bureaux. L'équipe B dispose également d'un vestiaire des joueurs et d'un grand salon pour les joueurs. Les employés non joueurs utilisent les locaux toute l'année.

Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

Accueil de l'équipe « visiteuse »

L'équipe « visiteuse » dispose d'un vestiaire et d'un salon équipés de 10 téléphones. Chaque équipe « visiteuse » demande des services provisoires le jour du match et quelques jours auparavant.

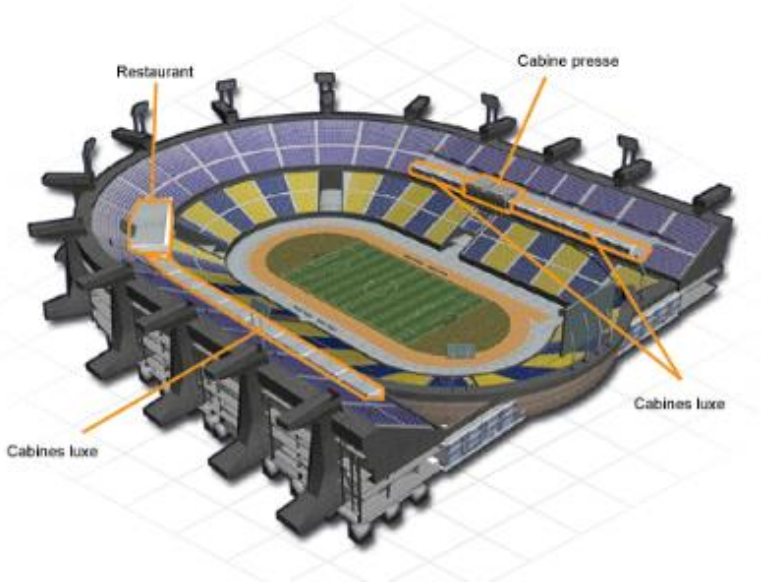
Les équipes « visiteuses » passent également un contrat avec StadiumCompany pour les bureaux et services au sein du stade.

Fournisseur de concessions

Un fournisseur de concessions gère les services proposés lors des matchs et événements. Il compte 5 employés à temps plein. Ils occupent deux bureaux privés et deux bureaux partagés équipés de cinq PC et sept téléphones. Ces bureaux se trouvent dans la partie sud du stade, entre les bureaux des équipes A et B. Deux employés à temps partiel prennent les commandes auprès des loges au cours des événements. Le concessionnaire de services emploie des intérimaires saisonniers pour gérer 32 stands permanents et autres services répartis sur l'ensemble du stade. Il n'y a actuellement aucun téléphone ni PC dans les zones de vente.

Organisation du restaurant de luxe

Le stade propose un restaurant de luxe ouvert toute l'année. En plus des salles et des cuisines, le restaurant loue des bureaux auprès de StadiumCompany. Les quatre dirigeants ont chacun un bureau privé. Les deux employés en charge des questions financières et comptables partagent un bureau. Six PC et téléphones sont pris en charge. Deux téléphones supplémentaires sont utilisés en salle pour les réservations.



Prise en charge des loges de luxe

Le stade compte 20 loges de luxe. StadiumCompany équipe chaque loge d'un téléphone permettant de passer des appels locaux et d'appeler le restaurant et le concessionnaire de services.

Prise en charge de la zone de presse

StadiumCompany propose un espace presse avec trois zones partagées :

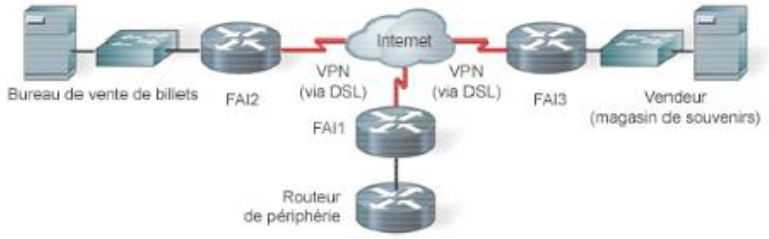
• La zone presse écrite accueille généralement 40 à 50 journalistes au cours d'un match. Cette zone partagée est équipée de 10 téléphones analogiques et de deux ports de données partagés. On sait qu'un journaliste stagiaire apporte un petit point d'accès sans fil lorsqu'il couvre un match.

• La zone de presse pour les radios peut accueillir 15 à 20 stations de radio. Elle est équipée de 10 lignes téléphoniques analogiques.

• La zone de presse télévisée accueille généralement 10 personnes. Elle est équipée de 5 téléphones.

Prise en charge de site distant

StadiumCompany compte actuellement deux sites distants : une billetterie en centre-ville et une boutique de souvenirs dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local.



Le stade est connecté au FAI local à l'aide de FAI1, un routeur de services gérés qui appartient au FAI. Les deux sites distants sont connectés au même FAI par les routeurs FAI2 et FAI3, fournis et gérés par le FAI. Cette connexion permet aux sites distants d'accéder aux bases de données situées sur les serveurs dans les bureaux de StadiumCompany.

StadiumCompany dispose également d'un routeur de périmètre, nommé Routeur de périphérie, connecté au routeur FAI1 du stade.

II) Cahier des charges

Mission 1 :

Vous intégrez le service informatique du centre administratif de stade. Sur ce site sont effectuées toutes les opérations concernant la gestion du personnel, et l'administration du stade. On y trouve 7 grands services :

- Service Administration (170 personnes)
- Service Equipes (164 personnes)
- Service Wifi (100 personnes)
- Service Caméra IP (80 caméras)
- Service VIP-Presse (80 personnes)
- Service Fournisseurs (44 personnes)
- Service Restaurant (14 personnes)

Le réseau de StadiumCompany doit comporter plusieurs périmètres de sécurité

- Adressage réseau et attribution de noms faciles à mettre à niveau : 172.20.0.0/22
- Un système de cloisonnement du réseau devra être testé. Les commutateurs devront être facilement administrables afin de propager les configurations rapidement et aisément
- Solution permettant l'interconnexion des différents sites (stade, billetterie et magasin). Les différents commutateurs ainsi que le routeur doivent disposer de réglages de base homogènes. La solution doit se faire avec les équipements réseau CISCO !

Mission 2 :

StadiumCompagny possède le nom de domaine StadiumCompagny.com

Les principaux serveurs sont hébergés au stade au centre d'hébergement informatique.

Selon les cas, certains services sont répliqués sur les sites eux-mêmes. Par exemple, les services d'annuaire Active Directory sont généralement répliqués sur le site de stade. Le réseau de magasin et le réseau de billetterie sont tous composés de la même manière :

•X Postes pour les employés

•Le site du stade dispose d'un service Active Directory, d'un service DHCP, et d'un DNS primaire sur une machine sous Windows 2012 Server.

Celle-ci permet aussi le stockage des fichiers utilisateurs. Un serveur RSync et DNS secondaire sous Linux Debian.

Annuaire du site de stade :

Les utilisateurs sont authentifiés via le serveur Active Directory du domaine Stadiumcompagny.local. Il est configuré en regroupant les utilisateurs par service. Les UO suivantes sont présentes sur le serveur : Admin, Wifi, ...

Chaque UO contient les utilisateurs du service concerné, un groupe d'utilisateurs dont le nom est au format G_xxxx où xxxx=le nom du service, un groupe regroupant les utilisateurs avec pouvoir du

service GP_Admin (directeurs et responsables notamment) et une GPO permettant d'imposer des contraintes d'utilisation et d'habilitations sur les machines du réseau.

Extrait d'une GPO : service equipes → gpo_equipes

•Accès au panneau de configuration, l'accès aux paramètres réseau est interdit

•Un script de démarrage Equipesstart.bat permet la connexion des lecteurs réseaux accédant aux dossiers partagés.

•Les utilisateurs démarrent avec un bureau imposé (barre de menu, fond d'écran...)

•Les utilisateurs ont des logins construits sur la base suivante - pnom – p=première lettre du prénom et nom=nom de famille. S'il y a homonymie un chiffre de 1 à 10 sera ajouté. Chaque utilisateur possède un dossier personnel et un profil centralisé.

Une stratégie de complexité des mots de passe est définie au niveau domaine.

DNS :

Les serveurs DNS sont configurés pour résoudre la zone directe stadiumcompagny.local et la zone inverse du 172.20.0.x/24. Le serveur primaire est hébergé sur une machine Windows Server et le DNS secondaire sur une Linux Debian.

DHCP :

Une plage est définie sur le 172.20.0.x/24 avec des options de routeur renvoyant vers la passerelle/pare-feu. Les serveurs DNS sont aussi transmis via les options DHCP.

Mission 3 :

Solution permettant l'administration à distance sécurisée 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 Magasin.
- La solution retenue devra être administrable à distance via un accès sécurisé par SSH

SSH et RDP uniquement depuis administration vers AD

VPN entre site et billetterie et magasins

ACL pour autoriser les flux que depuis réseau administration

III) Solutions

Test des solutions :

Proxy :

Pour les petites structures aux données peu sensibles et avares de leur bande passante, un proxy associé à un bon antivirus peut suffire. Il masque les adresses IP en insérant une IP anonyme. En complément, les Smart DNS ont ajouté la possibilité de supprimer les données de localisation.

Idéalement, il faudrait un chiffrement entre le poste de travail et le proxy, et les informations d'identification devraient pouvoir s'effacer après utilisation (les antivirus le proposent).

Les proxys sont souvent gratuits. Mieux vaut s'assurer de l'intégrité de la plateforme qui les propose.

Des fournisseurs comme Team Viewer proposent des solutions "tout-en-un" équivalente pour l'accès à distance d'un poste Windows ou Mac, à un tiers du coût d'un VPN. Elles permettent de partager des fichiers importants et d'accéder aux serveurs de l'entreprise à distance. On peut également les éteindre ou les rallumer à distance. Et une fonction "écran noir" permet de cacher l'ordinateur distant.

Liaisons louées, MPLS ou autres réseaux privés :

A l'opposé, certaines grandes organisations – défense, aéronautique, spatial – ont encore les moyens de supporter le coût d'un réseau privé reposant sur des liaisons spécialisées (LS) chèrement louées aux opérateurs. C'est le cas des offres MPLS (Multiprotocol label switching). Il y a aussi le cas d'infrastructures entièrement privées sur fibre noire, typiquement des réseaux métropolitains (MAN) fermés ou PPN (Physically private networks).

Le VPN :

En informatique, un réseau privé virtuel1,2 (RPV) ou réseau virtuel privé2 (RVP), plus communément abrégé en VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

Concernant notre infrastructure, nous allons nous intéresser à deux types de VPN et expliquer pourquoi nous favorisons une des solutions. Il existe des VPN SSL et des VPN IPSEC.

SSL (pour Secure Locket Layer) est un protocole cryptographique qui permet l'authentification, et le chiffrement des données qui transitent entre des serveurs, des machines et des applications en réseau.

IPSec (Internet Protocol Security) a été normalisé en 1995 par l'IETF (Internet Engineering Task Force). IPsec regroupe un ensemble de protocoles de communication sécurisée conçue pour la protection des flux réseaux et en particulier pour établir une communication privée (un tunnel) entre des entités distantes, séparées par un réseau public ou non sûr ou public comme Internet.

La différence :

La différence entre les deux protocoles se situe au niveau des couches réseaux dans lesquelles s'effectuent les étapes d'authentification de chiffrement.

Par encapsulation IPsec garantit la confidentialité et l'intégrité d'un flux au niveau de la couche réseau (couche « Internet » de la pile TCP/IP ou couche 3 « réseau » du modèle OSI). SSL/TLS agit lui beaucoup plus haut dans la pile réseau qu'IPsec, en se plaçant au-dessus de la couche transport réalisée par TCP. C'est un protocole conçu pour garantir la sécurité des communications Web sur Internet en fournissant un « socket sécurisé » pour protéger les paquets IP entre le navigateur et le serveur Web lorsque le flux de données transmis via HTTP nécessite d'être chiffré).

Pourquoi nous favorisons IPsec :

Le protocole IPsec est plus sécurisé (recommandé par l'ANSSI). Les raisons que l'ANSSI met en avant :

- Surface d'attaque d'IPsec plus réduite.
- Le choix d'algorithme entre le client et le serveur plus robuste en IPsec qu'en TLS.
- Gestion par défaut des autorités de certification autorisées.
- Détection de plusieurs vulnérabilités récentes concernant les implémentations de protocoles SSL et TLS.

Mise en place de protocole SSH :

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.

Mise en place de protocole TELNET :

Telnet (terminal network ou télécommunication network, ou encore teletype network) est un protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte.

Créé en 1969, telnet est un moyen de communication très généraliste et bi-directionnel. Il appartient à la couche application du modèle OSI et du modèle ARPA. Il est normalisé par l'IETF (RFC 15, 854 et 855).

Connexion à distance RDP :

Remote Desktop Protocol (RDP) est un protocole qui permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services. Des clients existent pour la quasi-totalité des versions de Windows, et pour d'autres systèmes d'exploitation, comme les systèmes GNU/Linux. Le serveur écoute par défaut sur le port TCP 3389.

Choix de la solution :

-Nous choisirons le SSH puisqu'il est plus sécurisé que telnet, Telnet transfère les données tel quel en texte, SSH crypte les données et les envoie sur canal sécurisée, qui demande une autorisation.

-Nous choisirons le Vpn plutôt que la prise en main à distance puisqu'elle est plus sécurisée que la prise en main à distance avec un poste hors domaine non fournies par l'entreprise

Vanfleteren, Lazare, Ayadi, Li, Canto **IRIS MEDIASCHOOL**

IV)PROJET

Objectif et but du projet

Sécurisation et accès à distance d'un réseau d'entreprise

Phases du projet :

En premier lieu, nous mettrons en place un protocole SSH, puis un VPN

SSH :

1. Définir un compte utilisateur avec le doublet (login/mot de passe) router> enable router# configure terminal router(config)# username user1 password Bts2023$ Ici on définit un utilisateur nommé "user1" dont le mot de passe associé est "Bts2023$"

```
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname
% Incomplete command.
Router(config)#hostname R-FAI2
R-FAI2(config)#username user1 password Bts2023$
R-FAI2(config)#
```

2. Définir un hostname à son équipement switch ou routeur, qui sera utilisé pour générer la clé de chiffrement router(config)# hostname R1-Stade R1-Stade(config)# Cette commande permet de mettre un hostname particulier à votre équipement, ici "R1". Ce hostname est par ailleurs utilisé pour générer la clé de chiffrement RSA, créée plus bas

3. Définir un nom de domaine, qui sera utilisé pour générer la clé de chiffrement R1-Stade (config)# ip domain-name stadiumcompagny.com Cette commande permet de définir un nom de domaine (DNS – Domain Name Server) à votre routeur. Il s'appellera désormais "stadiumcompagny.com", qui est tout simplement la concaténation du hostname "R1" avec le nom de domaine "stadiumcompagny.com ". Ce nom de domaine est aussi utilisé pour générer la clé de chiffrement RSA, créée juste à l'étape suivante.

```
R-FAI2(config)#ip domain-name stadiumcompany.com
```

4. Générer la clé de chiffrement R1-Stade(config)# crypto key generate rsa modulus 1024 Cette commande génère une clé de chiffrement RSA utilisé par le processus SSH pour générer la clé de session. La variable "modulus 1024" définit la taille de votre clé. A titre d'information, pour une clé asymétrique, 1024 est une taille correcte.

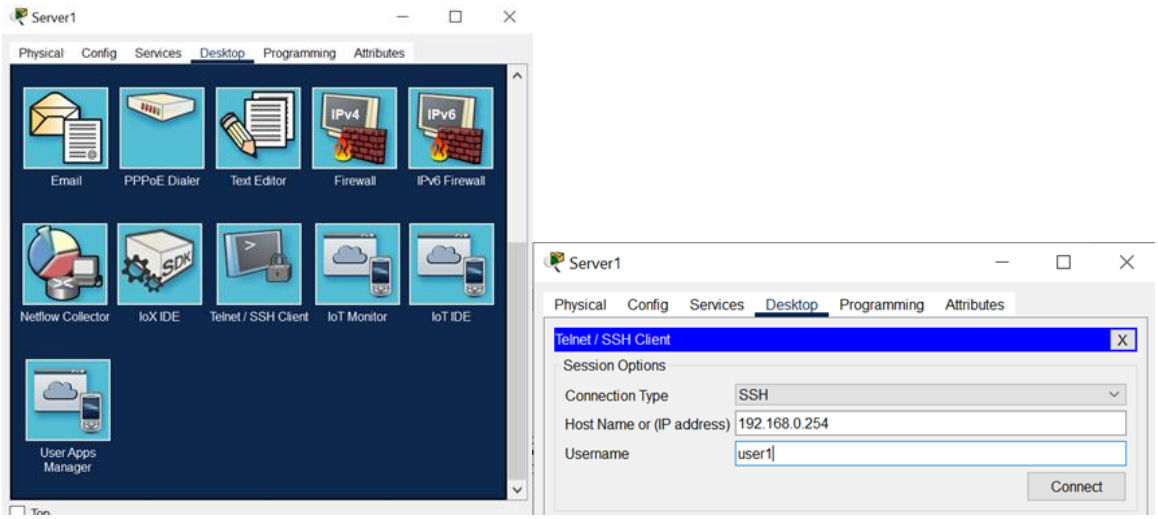
```
R-FAI2(config)#crypto key generate rsa
The name for the keys will be: R-FAI2.stadiumcompany.com
Choose the size of the key modulus in the range of 360 to
2048 for your
  General Purpose Keys. Choosing a key modulus greater than
512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
```

5. Activer le SSH R1-Stade (config)# line vty 0 4 R1-Stade (config-line)# transport input ssh R1-Stade (config-line)# login local R1-Stade (config-line)# exit Pour accéder en telnet ou ssh à un équipement

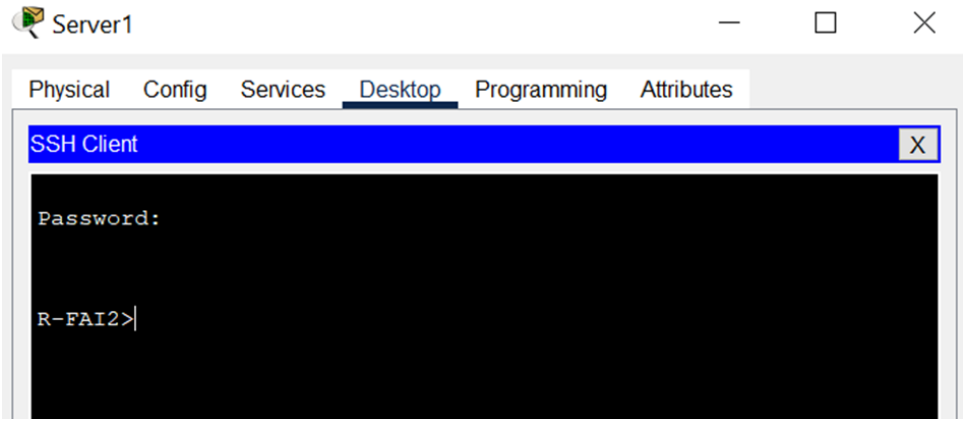
Cisco, il faut configurer les lignes “virtuelles” de l’équipement. En effet, quand je fais un telnet vers un routeur, je peux arriver de n’importe quelles interfaces actives du routeur

```
R-FAI2(config)#line vty 0 4
*Mar 1 0:33:9.219: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-FAI2(config-line)#transport input ssh
R-FAI2(config-line)#login local
R-FAI2(config-line)#exit
```

Test SSH



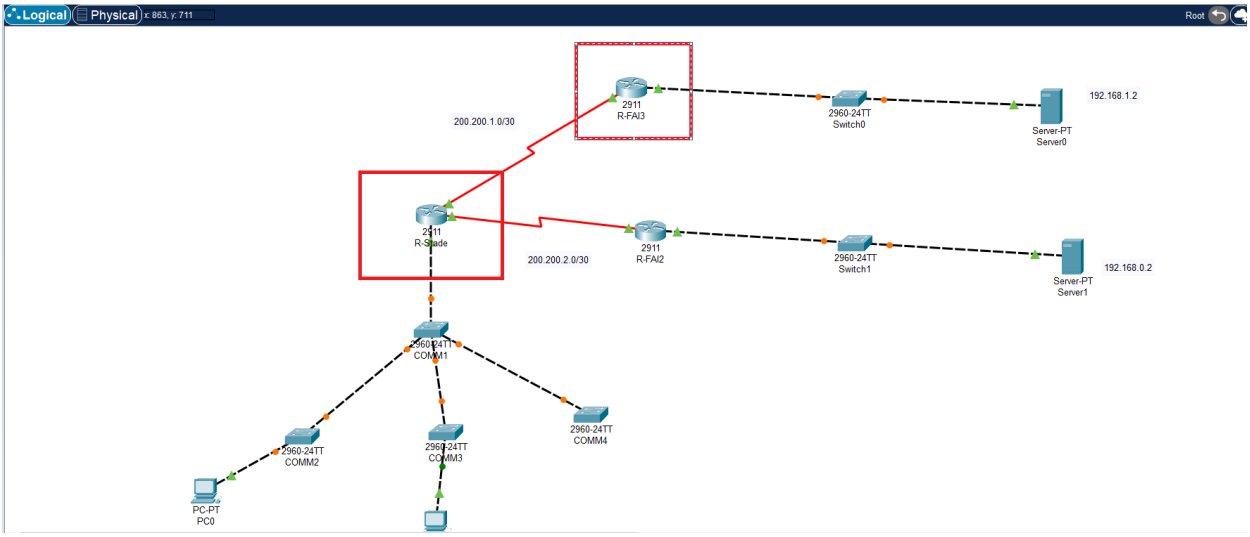
Saisir le mot de passe



Connexion effectuée

VPN :

Concernant l’installation voici l’infrastructure que nous prenons :



La mise en place du VPN se fait entre le routeur R-FAI3 (magasin de souvenir) et le routeur stade.

La liste des commandes à passer sur le routeur R-FAI3 :

- Première étape :

Vérifier que l'IOS de vos routeurs supporte le VPN.
Activer ensuite les fonctions crypto du routeur :

```
R1(config)#crypto isakmp enable
```

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

- Deuxième étape :
-

Configurer la police qui détermine quelle chiffrement on utilise, quelle Hash, quelle type d'authentification, etc.

```
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
```

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 configurer la clef :

```
R1(config)#crypto isakmp key mot_de_passe address 10.2.2.1
```

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

```
R1(config)#crypto isakmp key 6 mot_de_passe address 10.2.2.1
```

- Quatrième étape :

Configurer les options de transformations des données :

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

esp : Signifie **Encapsulation Security Protocol**

N'oubliez pas d'utiliser les mêmes protocoles de chiffrement et de Hash utilisés dans la première étape.
Dans notre cas :
Chiffrement : 3des
hash : md5

Fixer ensuite une valeur de Lifetime :

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

- Cinquième étape :

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

```
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

- Sixième étape :

Dans cette dernière étape, configurer la crypto map qui va associer l'access-list, le traffic et la destination :

```
R1(config)#crypto map nom_de_map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 10.2.2.1
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
```

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

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#crypto map nom_de_map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Même principe sur le routeur R3.

V)Conclusion

VI)Compétences acquises

Activité	Résultat attendu /production	Vécu/simulé /observe
"Participation à un Projet"	Projet de refonte du réseau de StadiumCompany	Vécu/simulé/observé
"Maquettage et prototypage d'une solution d'infrastructure"	Réalisation de schémas d'infrastructures	Simulé
"Rédaction d'une Documentation technique"	Rédaction d'un dossier de projet	Vécu/simulé/observé
"Administration sur site ou à distance des éléments d'un réseau, de serveurs, etc."	Configuration des éléments d'interconnexion et implantation des serveurs	Vécu/simulé/observé