**I - Contexte :**

**1.1 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

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.

**1.2 Présentation du prestataire informatique :**

Après quelques réunions, StadiumCompany charge 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.

Créée en 1989, NetworkingCompany est une société spécialiste en infrastructures systèmes et vente de matériel informatique pour professionnels de la vidéo.

Employant aujourd’hui 20 ingénieurs réseau, l’activité de NetworkingCompany s’établit à 1,8 millions d'euros de chiffre d’affaires. Son cœur de métier se situe au niveau de l’infrastructure informatique afin de garantir les besoins des activités « métiers ». NetworkingCompany est l’une des seules sociétés de services informatique qui accompagne réellement et jusqu’au bout ses clients dans le choix et la mise en œuvre de solutions.

NetworkingCompany intervient en mode Projet (Engagement de résultats), Régie (Engagement de moyens) et Infogérance des environnements Windows. Son outil de compétitivité et de productivité réside dans la capitalisation de son savoir-faire, le haut niveau de certification de ses partenariats ainsi qu’une veille technologiques active.

NetworkingCompany a développé une expertise forte dans les domaines de la virtualisation, les infrastructures d’accès (Application delivery), l’industrialisation du poste de travail (Itil, Supervision, Télédistribution), les annuaires et la gestion de l’identité.

Reconnu depuis 25 ans comme une entreprise innovante, et avec aujourd’hui plus de 300 collaborateurs, cette société répond avec flexibilité et efficacité à tous les besoins, qu’ils émanent de PME ou de grands comptes. Enfin, NetworkingCompany est en partenariat avec de nombreux gros groupes du monde de l’informatique, tout comme Microsoft, CISCO, HP, Huawei ou encore DELL, pour ne citer que les plus importants.

**1.3 Enseignements sur le système informatique de l’organisation :**

**Organisation de StadiumCompany :**

**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.

**Installations existantes et prises en charge :**

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 compte 90 personnes :

· 4 dirigeants

· 12 entraîneurs

· 14 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et

assistants financiers)

· 60 joueurs

L’équipe A dispose 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 estéquipée 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 sitesdistants 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.

**En résumé :**

Nombre de serveurs : 9 dont : (web, DHCP, commerce électronique, comptabilité(x3), paie)

Utilisateurs :

- 35 dirigeants

- 135 employés

- environs 80 intérimaires

- équipe A (90 personnes : 4 dirigeants, 12 entraineurs, 14 employé, 60 joueurs)

- équipe B

- équipe visiteurs

- restaurant

- fournisseur de concessions

- équipe B (4 dirigeants, 8 entraineurs, 12 employé, 40 joueurs)

- équipe visiteurs :

- fournisseur de concessions 5 employé 2 employé a temps partiel : intérimaire non défini

- restaurant de luxe : 4 dirigent, 2 employé,

- 20 loges de luxe

- 2 sites distants

Services : DNS, DHCP, web

- dirigeants : PC et téléphones connecter à un PABX

- personnel et sécurité : 50 téléphones et PC réparti dans le stade

- 12 téléphones analogiques répartis dans le stade qui prennent en charges la

télécopie, et d’autres offrant un accès direct aux services de police et pompier.

- locaux connecté par fibre optiques

- équipe A : 15 bureaux dont 5 partagé 24 PC et 28 téléphones dans ces bureaux ; vestiaire 5 téléphone, salon des joueurs : 15 téléphones

- équipe B : 12 bureaux dont 3 partagé, 19 PC et 22 téléphones, vestiaires 5 téléphones, salon des joueurs 15 téléphones

- équipe visiteur : salon et vestiaire doté de 10 téléphones

- fournisseur de concession : 2 bureau privée 5 PC et 7 téléphones, 32 stand permanent non équipé pour le moment.

- restaurant de luxe : 4 bureau privé, 6 téléphones + 2 utilisé en salle pour les réservations

- 20 loges de luxe : 20 téléphones

- zone de presse : 10 téléphones analogique, 2 ports de données réseaux + Wireless AP

- 2 sites distant : connecter Via VPN (router FAI x3 pour gérer la connexion StadiumCompany dispose d’un routeur de périmètre

Pas d’information sur les processus, contrats et chartes informatiques.

**II - Cahier des charges :**

Cette année, vous allez intégrer la division du stade de StadiumCompany. Vous

serez chargé de la maintenance des systèmes et réseaux informatiques.

StadiumCompany est composé de plusieurs sites :

Site 1 : Stade (hébergement informatique, siège social et centre administratif)

Site 2 : Billetterie (vente des billets)

Site 3 : Magasin (vente des souvenirs)

Les différentes solutions retenues pour l’étude du projet d’un point de vue général de

StadiumCompany pourront faire l’objet de documentations techniques suivant la

complexité de la mise en œuvre.

**Mission 5 :**

**Contexte**

Vous avez réalisé la mise en place de l’architecture réseau interne du site de Stade. Le DSI de

StadiumCompagny souhaite maintenant interconnecter le réseau de l’entreprise avec le réseau

Internet.

Les bénéfices sont multiples, mais ce vaste réseau et les technologies qui lui correspondent

ont ouvert la porte à un nombre croissant de menaces relatives à la sécurité contre lesquelles

l’entreprise doit se prémunir.

Maintenant, plus que jamais, il est impératif que l’entreprise intègre la sécurité au sein de son

architecture réseau afin de limiter les risques.

**Définition du besoin**

Le DSI de StadiumCompagny désire faire une étude générale sur les risques attachés à

l’accès au réseau Internet et souhaite prendre en compte les éléments de sécurité ci-dessous :

- Mise en place d’un réseau de type DMZ dans lequel on trouve un ensemble de

serveurs accessibles depuis l'extérieur, spécifiquement le serveur web.

- L'environnement du réseau interne de Stade doit être accessible aux seuls acteurs de

l'entreprise.

- L'entreprise a choisi d'héberger en interne les serveurs exécutant les applications et

besoins de StadiumCompagny.

- Un accès à l’Internet est autorisé aux collaborateurs à partir du réseau interne.

- Les utilisateurs du réseau Wifi Visiteurs ont un accès uniquement au réseau Internet.

**Travail à réaliser**

- Identifier les risques associés à une interconnexion avec le réseau Internet.

- Déterminer une démarche de limitation de ces risques.

- Définir la problématique de l’accès au réseau Internet à partir d’un réseau privé.

- Concevoir la politique de filtrage conformément au cahier des charges.

- Adapter la maquette en fonction de votre solution.

**III - Solution :**

Connexion par SSH et VPN

VPN

Il est essentiel d’installer un VPN (Virtual Private Network) pour avoir une communication sécurisé entre les machines et internet. Les VPN sont très bien sécurisés pour éviter que les serveurs ne tombent suite à une attaque. Ce qui permet de naviguer sur internet plus sereinement.

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers d’un réseau peu fiable, comme le réseau Internet. Cette technologie permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ce qui garantit aux utilisateurs d’un VPN qu’en cas d’interception malveillante les données soient illisibles.



Un VPN utilise des protocoles de tunnelisation (tunneling). Ce qui permet aux données d’être sécurisées par des algorithmes de chiffrage. Le serveur VPN nous connecte sur Internet en masquant notre adresse IP par sa propre adresse. Un client VPN chiffre et déchiffre les données du coté utilisateur. Un serveur VPN chiffre et déchiffre les données du côté de l’organisation.



Les VPN sont de nos jours de plus en plus utilisés, par exemple par les entreprises. Il est à noter qu’il existe de nos jours des services de VPN qui vous permettent d’installer ce type de réseau.

* L’intranet

L'intranet VPN relie des intranets entre eux. Ce type de VPN est utilisé par les entreprises possédant plusieurs sites. Le plus important avec ce type de VPN est de garantir la sécurité et l'intégrité des données.



* L’extranet

L’extranet VPN est utilisé pour communiquer avec ses clients en ouvrant son réseau local à ses clients ou à ses partenaires. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.



* Utilisation du VPN

Pour rendre notre connexion Internet privée, anonyme, protégée et cacher l’adresse IP sur Internet. La solution du VPN nous laisse la possibilité de construire des réseaux. De plus, réduit le coût de l’accès à Internet que ce soit à haut débit ou via une ligne téléphonique.

Nous avons exploré plusieurs solutions concernant le protocole VPN, nous avons hésité entre deux protocoles qui sont L2TP et PPTP. Nous avons conclu notre choix sur le protocole PPTP (Point-to-Point Tunneling Protocol) qui est un protocole de niveau 2 développé principalement par Microsoft. Nous avons donc choisi ce protocole car il est simple à installer et c’est le plus pratique puisque il fonctionne sur presque la totalité des appareils fixe et mobile quel que soit leurs système d’exploitation. Le protocole PPTP fonctionne sous Windows, MacOS et sur la plupart des systèmes mobiles.

ACL

Une ACL (Acces Control List) permet de filtrer les paquets IP. Elle permet de définir les actions possibles des utilisateurs réseau. Ainsi, une ACL va indiquer au routeur les paquets qu'il doit accepter et ceux qu'il doit refuser, notamment en fonction de leur adresse IP de provenance, leur IP destination et les ports source et destination.

Une liste d’accès est une liste d’actions d’autorisations (permit) ou d’interdiction (deny) sur des adresses ou des protocoles de couches supérieures. (Http, DNS, SMTP, FTP, Telnet, SSH, IMAP etc…)

Il existe différents types de listes d’accès :

* Standards (Une liste d'accès standard examinera seulement l'adresse IP source).
* Etendues (Une liste d'accès étendue pourra examiner les adresses IP et les ports aussi bien source que destination, ainsi que type de protocole (IP, ICMP, TCP, UDP)).
* Nommées
* Dynamiques

Utilité :

Une liste d'accès va servir :

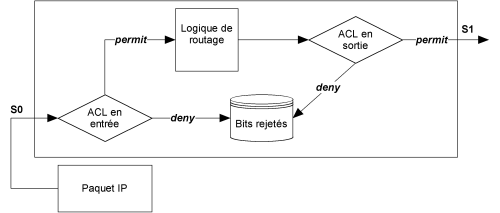
* A supprimer des paquets pour des raisons de sécurité (Pour du trafic de données ou des accès VTY)
* A filtrer des mises à jour de routage
* A filtrer des paquets en fonctions de leurs priorités (QOS)
* A définir du trafic intéressant pour des configurations spécifiques (NAT, ISDN, etc…)

Règles d’écritures :

* Il faut passer une commande pour chaque instruction permit ou deny
* Une nouvelle instruction est automatiquement insérée en fin de liste
* Ce n’est pas possible de supprimer une ligne de la liste
* Pour modifier une liste d’accès standard ou étendue, il faut d’abord la supprimer puis recréer
* Une liste de contrôle d’accès ne se termine toujours pas une instruction deny any implicite
* Il faut placer les instructions les plus globales

Logique :

Une liste d'accès, comportant une suite d'instructions de filtrage, va être appliquée sur une interface du routeur, pour le trafic entrant ou pour le trafic sortant. Il va falloir appliquer une logique sur les interfaces en sortie ou en entrée.



Certificat SSL

Un certificat SSL est un fichier de données qui lie une [clé cryptographique](https://www.globalsign.fr/fr/centre-information-ssl/choisir-la-bonne-taille-de-cle/) aux informations d'une organisation ou d'un individu. Installé sur un serveur, le certificat active le cadenas et le protocole « https » (via le port 443) dans les navigateurs, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur.  
Généralement, le [SSL](https://www.globalsign.fr/fr/centre-information-ssl/definition-ssl/) est utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions, telles que les noms d'utilisateur et les mots de passe. Récemment, le SSL est devenu la norme pour sécuriser l'utilisation de sites de réseaux sociaux. Les certificats SSL lient ensemble :

* Un nom de domaine, un nom de serveur, un nom d’hôte
* L’identité de l’organisation (de l’entreprise) et le lieu

L'organisation doit installer le certificat SSL sur son serveur web afin d'initialiser des sessions sécurisées avec les navigateurs. L'organisation devra se soumettre à une vérification auprès de l'Autorité de Certification, dont le degré va varier selon le [type de certificat SSL](https://www.globalsign.fr/fr/centre-information-ssl/types-certificats-ssl/) pour lequel elle a effectué une demande. Une fois le certificat SSL installé sur un site, les visiteurs pourront accéder à celui-ci à travers une connexion « https » qui indique au serveur qu'il doit établir une connexion sécurisée avec le navigateur. Lorsque la connexion sécurisée est établie, l'ensemble du trafic entre le serveur et le navigateur sera sécurisé. Les visiteurs d'un site web sont assurés que celui-ci est sécurisé grâce à différents indicateurs visuels de confiance.

Signatures de certificat :

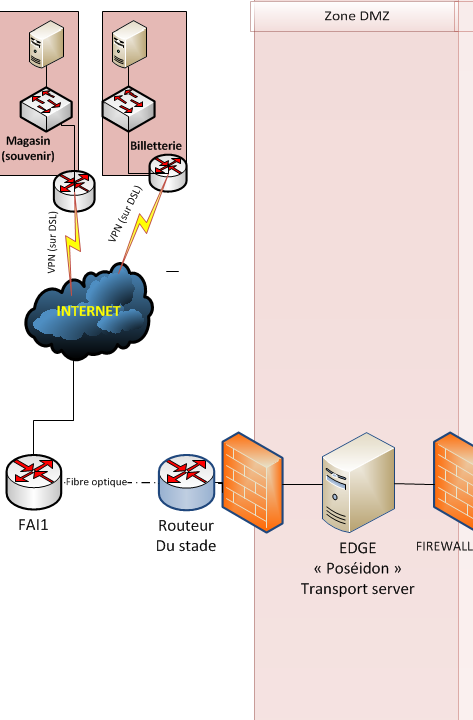
On distingue différents types de certificats selon le niveau de signature :

* Les **certificats auto-signés** sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.
* Les **certificats signés par un organisme de certification** sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.

Types d’usages :

Les certificats servent principalement dans trois types de contextes :

* Le **certificat client**, stocké sur le poste de travail de l'utilisateur ou embarqué dans un conteneur tel qu'une carte à puce, permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte d'identité numérique utilisant une paire de clé asymétrique d'une longueur de 512 à 1024 bits.
* Le **certificat serveur** installé sur un serveur web permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL.
* Le **certificat VPN** est un type de certificat installé dans les équipements réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IPSEC.

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 .

Le protocole SSH

Il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :

•Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

•Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing)

L'établissement d'une connexion SSH se fait en plusieurs étapes :

•Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).

•Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session.

Mise en place du canal sécurisé

La mise en place d'une couche de transport sécurisée débute par une phase de négociation entre le client et le serveur afin de s'entendre sur les méthodes de chiffrement à utiliser. En effet le protocole SSH est prévu pour fonctionner avec un grand nombre d'algorithmes de chiffrement, c'est pourquoi le client et le serveur doivent dans un premier temps échanger les algorithmes qu'ils supportent.

Ensuite, afin d'établir une connexion sécurisée, le serveur envoie sa clé publique d'hôte (host key) au client. Le client génère une clé de session de 256 bits qu'il chiffre grâce à la clé publique du serveur, et envoie au serveur la clé de session chiffrée ainsi que l'algorithme utilisé. Le serveur déchiffre la clé de session grâce à sa clé privée et envoie un message de confirmation chiffré à l'aide de la clé de session. A partir de là le reste des communications est chiffré grâce à un algorithme de chiffrement symétrique en utilisant la clé de session partagée par le client et le serveur.

Toute la sécurité de la transaction repose sur l'assurance qu'ont le client et le serveur de la validité des clés d'hôte de l'autre partie. Ainsi, lors de la première connexion à un serveur, le client affiche généralement un message demandant d'accepter la connexion (et présente éventuellement un condensé de la clé d'hôte du serveur) :

**Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?**

Afin d'obtenir une session véritablement sécurisée, il est conseillé de demander oralement à l'administrateur du serveur de valider la clé publique présentée. Si l'utilisateur valide la connexion, le client enregistre la clé hôte du serveur afin d'éviter la répétition de cette phase.

A l'inverse, selon sa configuration, le serveur peut parfois vérifier que le client est bien celui qu'il prétend être. Ainsi, si le serveur possède une liste d'hôtes autorisés à se connecter, il va chiffrer un message à l'aide de la clé publique du client (qu'il possède dans sa base de données de clés d'hôtes) afin de vérifier si le client est en mesure de le déchiffrer à l'aide de sa clé privée (on parle de challenge).

L'authentification

Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès. Il existe plusieurs méthodes :

•la méthode la plus connue est le traditionnel mot de passe. Le client envoie un nom d'utilisateur et un mot de passe au serveur au travers de la communication sécurisé et le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide.

•une méthode moins connue mais plus souple est l'utilisation de clés publiques. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge et donner un accès au client si ce dernier parvient à déchiffrer le challenge avec sa clé privée.

(Pour l’installation voir annexe SSH)

Mise en place du VPN

La sécurité du système d’information devra être renforcée entre le site du stade et les sites distants Billetterie et le Magasin. Pour rendre notre connexion Internet privée, anonyme, protégée et cacher l’adresse IP sur Internet. La solution du VPN nous laisse la possibilité de construire des réseaux. De plus, réduit le coût de l’accès à Internet que ce soit à haut débit ou via une ligne téléphonique.

Nous avons exploré plusieurs solutions concernant le protocole VPN, nous avons hésité entre deux protocoles qui sont L2TP et PPTP. Nous avons conclu notre choix sur le protocole PPTP (Point-to-Point Tunneling Protocol) qui est un protocole de niveau 2 développé principalement par Microsoft. Nous avons donc choisi ce protocole car il est simple à installer et c’est le plus pratique puisque il fonctionne sur presque la totalité des appareils fixe et mobile quel que soit leurs système d’exploitation. Le protocole PPTP fonctionne sous Windows, MacOS et sur la plupart des systèmes mobiles.