Département de génie informatique et génie logiciel

INF8402 - Sécurité des réseaux fixes et mobiles

Final Automne 2021

Le 18 Décembre 2021

Question 1 (50%):

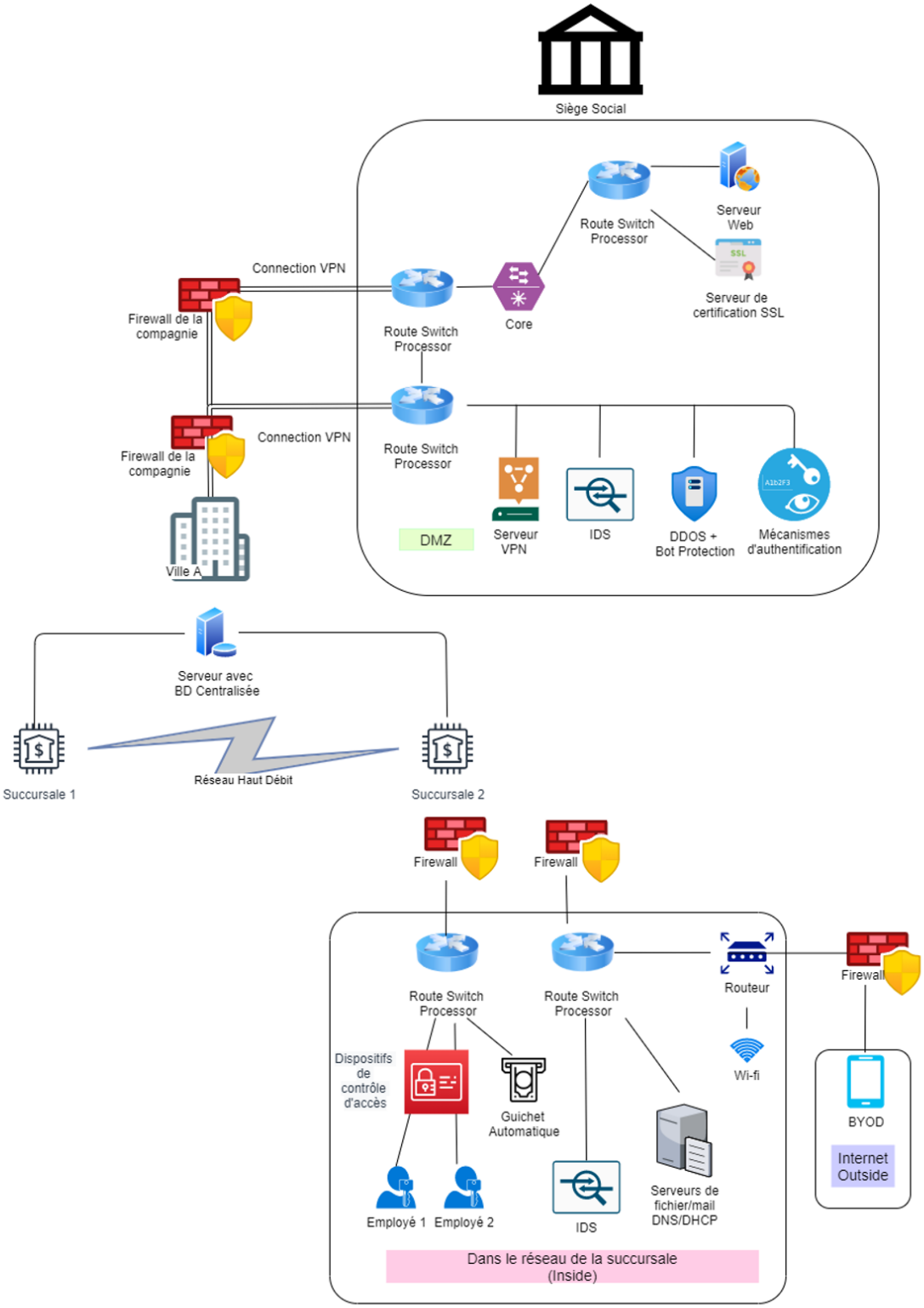

Figure 1 de l'architecture du siège social et l'interconnexion entre les villes et le siège social

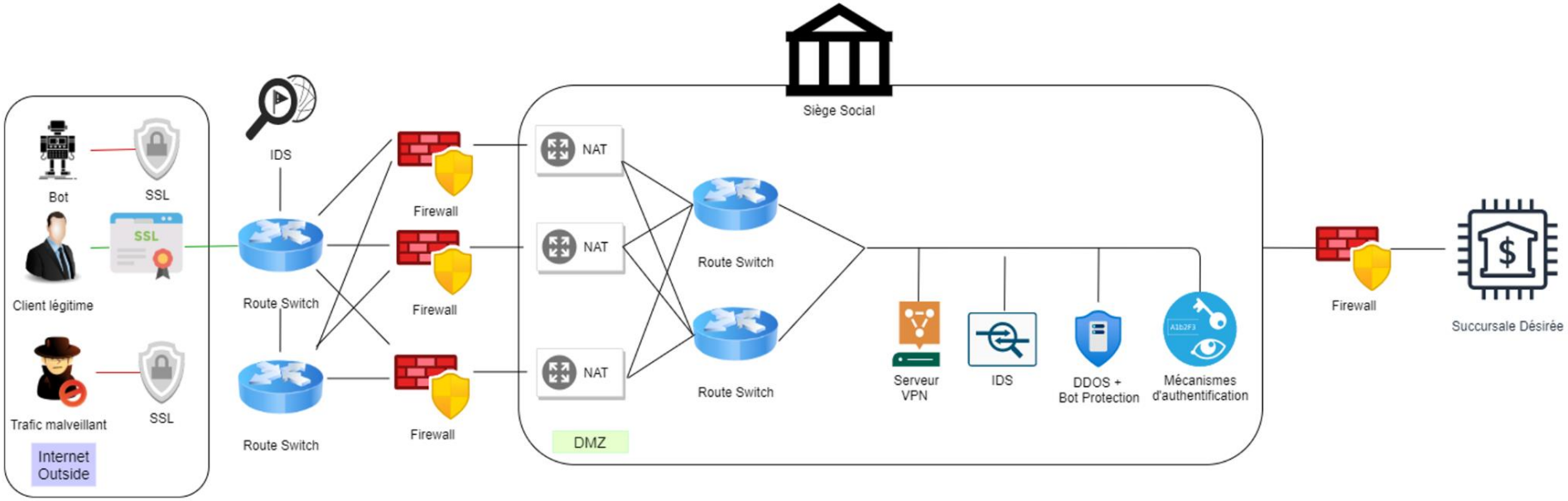

Figure 2 de l'architecture simplifiée d'un accès à une succursale X

J’ai fait le choix de mettre trois firewalls,trois NAT et deux Route switch entre Internet et la DMZ pour augmenter la fiabilité.

En effet, si un d’entre eux venait à ne plus fonctionner, nous en aurions toujours deux de fonctionnels. Nous avons ensuite plusieurs vérifications et méthodes pour sécuriser les transactions qui sont faites dans DMZ. D’ailleurs les firewalls servent également de DNS pour les machines se trouvant dans la DMZ.

Pour ce qui est des méthodes et vérifications nous avons par exemple, l’utilisation de SSL qui permet d’assurer l’intégrité des données qui seront échangées, l’authentification du serveur mais également celle du client. Comme nous pouvons le voir dans la 2e figure de façon simplifiée, sans cette authentification on ne peut pas accéder au réseau interne de la banque. On retrouve également un système de détection d’intrusion à plusieurs endroits pour diminuer les risques d’intrusion à plusieurs niveaux.

On remarque également que j’ai choisi de faire la plupart des vérifications de sécurité dans la DMZ avant d’envoyer le client vers le réseau interne qui contient les données plus confidentielles. Ainsi, un client malveillant ne pourrait pas accéder aux données se trouvant dans le réseau de la succursale sans avoir validé l’ensemble des mécanismes d'authentification et sécurité mises en place. Une fois que l’ensemble des vérifications ont été faites, le client peut accéder au réseau interne de la succursale en question.

Pour ce qui est du réseau de la succursale choisie, j’ai mis des dispositifs de contrôle d’accès pour pouvoir identifier les employés et éviter que quelqu’un puisse rentrer dans la banque et avoir accès à des pièces ou machines qu’il n’aurait pas le droit d’utiliser.C’est ce qu’on appelle une protection de l'infrastructure. Une autre protection peut être observée dans la 1e figure, un utilisateur voulant se connecter au réseau à l’aide du “bring your own device” doit d’abord passer par le pare-feu ce qui va nous permettre de savoir s' il respecte la politique de sécurité du réseau. Si c’est le cas, il aura accès au réseau interne et passera par un routeur qui nous permettra d’éviter des attaques IP spoofing en vérifiant qu’aucun paquet entrant a une adresse “interne”. Il pourra ensuite à l’aide de l’interface de faire les opérations qu’il souhaite. Les requêtes seront traitées par le serveur visible dans la figure. J’ai regroupé le serveur mail, de fichier, DHCP et DNS ensemble pour rendre la figure un peu plus compacte.

Nous pouvons également retrouver dans les figures des NAT qui permettent de cacher les adresses de l’intérieur. Les NAT sont souvent inclus dans les route switch mais j’en ai mis deux visibles dans la 2e figure pour montrer un exemple.

J’ai mis un serveur VPN qui recevra les données cryptées et procédera au décryptage et transmettra ces données au serveur Web.

Ce serveur permet d’éviter que nos renseignements se retrouvent dans un format clair et lisible.

Nous pouvons également voir une couche coeur “core” dans la première figure. Celle-ci permet de relier entre eux les différents segments du réseau.

Question 2 (50%):

1) a) L'article **« Decentralized Self-Enforcing Trust Management System for Social Internet of Things »** prend en compte la confidentialité des utilisateurs lors de la conception d'un système de gestion de la confiance pour protéger les informations privées des utilisateurs individuels. Les systèmes de gestion de confiance existants préservent la confidentialité des utilisateurs en utilisant trois méthodes principales : l'anonymisation, la perturbation des données et la cryptographie.

Le système de gestion de la confiance est auto-exécutoire, les participants du système exécutent les étapes du protocole pour calculer les scores de confiance de tout le monde dans le système d'une manière vérifiable publiquement sans impliquer de partie tiers. Aussi, l'utilisation de preuves à connaissance nulle (ZKP) oblige efficacement chaque participant à suivre honnêtement les spécifications du protocole.

Notons ainsi que tout mauvais comportement sera publiquement accessible et leurs scores de confiance se dégradent progressivement jusqu'à un point extrême tel que les parties se comportant mal seront automatiquement expulsées du réseau.

Aussi, la confidentialité de l'utilisateur a été protégée en utilisant des techniques de cryptage homomorphes qui permettent à un utilisateur de fournir des scores de confiance sous forme cryptée et seul le résultat global est décrypté. Plusieurs systèmes d'évaluation de la confiance ont été proposés pour garantir que la confidentialité des nœuds IoT reste préservée pendant le processus de calcul, nous retrouvons le système de cryptage homomorphe additif et le système de cryptage pallier additif pour la préservation des valeurs de confiance des nœuds IoT. Ainsi que le schéma de partage de données privées dans le réseau IoT pour protéger la vie privée, celui-ci utilisant le « cloud storage ». Enfin, le MEDiSN framework, qui accumule les données des capteurs dans le réseau de capteurs sans fil.

La technologie blockchain a également été utilisée pour assurer la confidentialité des utilisateurs dans un réseau IoT. Nous retrouvons ainsi le Privacy-preservation model pour la répartition des tâches dans un environnement de « crowdsourcing », le modèle basé sur la blockchain pour distribuer « the reputation score » entre les nœuds d'un réseau IoT distribué, et enfin, le IoT Passport permettant aux appareils IoT d'une plate-forme différente de collaborer les uns avec les autres à l'aide du système de blockchain.

L'article **« On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things »** propose le modèle subjectif et modèle objectif pour l'évaluation de la fiabilité. Ainsi, en combinant l'évaluation de la fiabilité directe et indirecte, nous obtenons un modèle de confiance adaptative. Ils présentent ainsi les mesures de similarité sociale pour maximiser les performances de l'application, ainsi que le filtrage adaptatif pour contrôler les paramètres de pondération afin de prévenir les attaques malveillantes.

La méthode basée sur la réputation est également utilisée dans le modèle de confiance. Le retour de satisfaction des transactions ou des services est adopté comme information liée à la confiance dans le modèle basé sur la réputation. Certaines approches typiques de calcul de réputation sont largement appliquées pour quantifier la confiance. Certains indicateurs, tels que la complexité de calcul, le temps de convergence, le taux de réussite, sont utilisés comme mesures de l'efficacité des méthodes ci-dessus.

Différentes des méthodes ci-dessus, l'article propose le degré de relation sociale (DoSR) pour mesurer la confiance des informations relatives à la confiance provenant de différentes sources. Ainsi que les nouvelles métriques, y compris DoI et DoC pour quantifier la compétence et la volonté. La construction des métriques et des fonctions ci-dessus améliorera l'efficacité et la résistance aux attaques dans le processus d'évaluation de la fiabilité et de délégation de service.

En sommes, selon moi les principaux critères à prendre en compte sont la **fiabilité** qui doit garantir le bon fonctionnement du réseau sans interruption, la **disponibilité** qui doit garantir que les services de réseau sont fournis malgré les attaques, et la **confidentialité** qui doit être préservée lorsque les informations des utilisateurs sont collectées pour l'évaluation de la confiance. De mon point de vue, le modèle de l'article [2] est meilleur car il prend en compte les trois critères.

1) b) L'article **« Decentralized Self-Enforcing Trust Management System for Social Internet of Things »** traite d'un mécanisme où les appareils et leurs utilisateurs évaluent la fiabilité des autres appareils et utilisateurs avant de faire confiance aux informations qu'ils envoient. La confidentialité des participants au SIoT est protégée en utilisant un cryptage homomorphe dans le cadre décentralisé.

Le système de gestion de confiance se compose de trois entités fonctionnelles : les utilisateurs, objets IoT et un PBB (panneau d'affichage public), ainsi, c'est en établissant une relation sociale entre les objets, que les appareils IoT peuvent interagir de manière autonome les uns avec les autres sans intervention humaine.

Dans ce cas, les utilisateurs reçoivent des informations des objets IoT et fournissent une évaluation basée sur la réponse positive ou négative des objets IoT ; Les objets IoT fournissent un service aux utilisateurs, par exemple, en fournissant des conditions routières, etc. ; Les utilisateurs évaluent les objets IoT ; Le panneau d'affichage public (PBB) doit fournir la possibilité aux utilisateurs authentifiés de publier les paramètres cryptographiques, les commentaires cryptés et les scores de preuve de rétroaction NIZK et doit mettre les données à la disposition de tous pour calculer la fiabilité agrégée du objets ; Ainsi, la fonctionnalité du panneau d'affichage public peut être distribuée ou centralisée et est gérée par n'importe quelle entité de l'écosystème SIoT.

Dans l'article **« On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things »** le paradigme SIoT a été appliqué dans divers segments de

l'industrie, tels que les réseaux de véhicules, les soins de santé omniprésents et la surveillance de la santé, le crowdsourcing et le crowdsensing mobile, etc.

Comme vu précédemment, le SIoT est supérieur dans la découverte, l'allocation et le partage d'informations et de ressources réseau car les objets IoT ont des caractéristiques sociales similaires à celles de l'humain, ce qui les aidera à établir de manière autonome des relations sociales ; la structure de SIoT améliore la navigabilité et l'évolutivité du réseau, ce qui améliorera la découverte de services et l'acquisition de ressources ; et les méthodes théoriques du réseau social peuvent être convergées dans la gestion des objets IoT, y compris la reconnaissance d'identité, le partage d'informations, etc.

Cependant, la plupart des méthodes existantes quantifient le degré de confiance en fonction des caractéristiques fixes des objets IoT, telles que leur emplacement et leur propriété. Un tel degré de confiance doit être évalué de manière dynamique car les relations entre les objets sont modifiables au cours des interactions de service. Les capacités d'un SP (les fournisseurs de services) à fournir un service seront susceptibles de varier en fonction, par exemple, des caractéristiques de ce SP et des propriétés d'une tâche spécifique.

En sommes, l'article [1] propose un modèle plus adapté sachant que dans l'article [2] il manque une analyse minutieuse sur la manière d'examiner les informations relatives à la confiance provenant de différentes sources. De plus, les problèmes de sécurité dans l'environnement SIoT réel causés par des comportements malveillants restent en suspens.

2)

L'article [1] présente un aperçu des différentes techniques/modèles pour la gestion de la confiance dans l'Internet des objets ('IoT') que sont la précision, l'adaptabilité, la disponibilité, l'hétérogénéité, l'intégrité, la confidentialité, la fiabilité et l'évolutivité.

Dans l'article **« Decentralized Self-Enforcing »** :

- ➔ **Précision :** Propose un système de réputation préservant la confidentialité: utilisation d'un système de cryptage homomorphe additif et un cryptosystème de Pallier pour la préservation des valeurs de confiance des nœuds IoT.
- ➔ **Adaptabilité :** Context-aware framework pour le calcul de la fiabilité des nœuds IoT dans le SIoT. Le système prend en compte les concepts de la science sociale et physiologique pour calculer la confiance entre les objets IoT et leurs propriétaires.
- ➔ **Disponibilité :** Importance de l'évaluation de la fiabilité des appareils IoT ainsi que des utilisateurs afin d'empêcher les entités malveillantes de diffuser du contenu malveillant ou de perturber le réseau : en faisant appel à des entités pour fournir des commentaires sur leur interaction avec certains appareils et utilisateurs IoT.
- ➔ **Hétérogénéité :** Les objets IoT fournissent un service aux utilisateurs, par exemple, en fournissant des conditions routières, etc.
- ➔ **Intégrité :** Plusieurs systèmes homomorphes ont été proposés dans le cadre du crowdsourcing et des réseaux P2P : un système de réputation qui masque l'identité des

consommateurs en utilisant des identités anonymes pour garantir la confidentialité et l'intégrité des avis soumis par les consommateurs.

- ➔ **Confidentialité :** Les systèmes de gestion de la confiance existants préservent la confidentialité des utilisateurs en utilisant trois méthodes principales telles que l'anonymisation, la perturbation des données et la cryptographie.
- ➔ **Fiabilité :** Le système de gestion de la confiance utilise des ZKP non interactifs, de sorte que l'adversaire malveillant ne sera pas en mesure de produire des commentaires correspondant à des entrées hors de portée à moins qu'il ne puisse briser la sécurité du système de preuve NIZK qui ne se produit qu'avec une probabilité négligeable.
- ➔ **Évolutivité :** l'environnement IoT est flexible et modifiable dans certaines fonctionnalités. La confiance des appareils change en fonction de l'environnement, des circonstances et des scénarios. Ainsi, un certain nombre de caractéristiques environnementales et sociales ont été identifiées.

Dans l'article **« A Comprehensive Study »** :

- ➔ **Précision :** Méthode de détection sécurisée et fiable basée sur des informations contextuelles et des données IOT anormales, cependant les nouveaux dispositifs peuvent être considérés comme un nœud malveillant.
- ➔ **Adaptabilité :** en utilisant la prise de décision basée sur la confiance basée sur la fiabilité, le risque et la probabilité de perte de santé, notons ainsi que l'hétérogénéité n'est pas considérée.
- ➔ **Disponibilité :** utilisation d'une architecture de clustering où chaque cluster implique les objets ayant le même intérêt pour former une communauté d'intérêt, notons également que l'hétérogénéité n'est pas considérée.
- ➔ **Hétérogénéité :** utilisation d'un modèle d'évaluation de la fiabilité où chaque objet calcule la fiabilité des autres objets en fonction de son expérience et de l'opinion des objets communs, cependant cette méthode ignore la disponibilité et la fiabilité.
- ➔ **Intégrité :** utilisation d'un modèle d'évaluation de confiance centré sur les données basé sur plusieurs couches, y compris des données basées sur plusieurs couches, y compris l'extraction de métriques de confiance de données, l'agrégation de confiance de date, l'évaluation et la prédiction.
- ➔ **Confidentialité :** propose une architecture en couches basée sur des couches de capteur, de cœur et d'application pour la gestion de la confiance dans l'IOT, cependant cette architecture ne considère pas l'hétérogénéité et la fiabilité.
- ➔ **Fiabilité :** propose une méthode combinée en combinant certaines méthodes telles que SC et MRC, avec un bas niveau d'évolutivité.
- ➔ **Évolutivité :** propose une gestion de confiance centralisée et fournit un modèle de confiance évolutif basé sur l'aspect dynamique de l'IOT mais ne considère pas l'hétérogénéité et de la fiabilité.

En sommes, les deux articles respectent l'ensemble des critères établies, mais le second nous donne des contraintes, donc le meilleur article est le premier.