UMONS

Faculté des Sciences

Développement d'un pare-feu domestique

Pré-rapport de projet

Activité d' Apprentissage S-INFO-037

Rémy Decocq

Année Académique 2018-2019
Master en Sciences Informatiques, bloc 1
Faculté des Sciences, Université de Mons

Table des matières

Introduction

Depuis maintenant plusieurs années, la connectivité n'a cessé d'évoluer : en se limitant au domaine de l'Internet entre 2000 et 2015, une estimation de l'augmentation du pourcentage de la population mondiale l'utilisant avoisine 40% [2] [1]. Que ce soit dans le cadre d'infrastructures de type "mainframe" ou dans le contexte des ordinateurs personnels, les technologies et équipements relatifs au réseau et aux communications sont devenus indispensables. En conséquence, corrélé au fait de pouvoir de plus en plus s'interconnecter et rejoindre des réseaux de natures variées, le nombre de menaces potentielles pour une machine ainsi connectée augmente grandement. Heureusement, parallèlement à cette évolution, les performances des machines classiques qui en sont équipée ont également suivi une progression en terme de performances. Cela a permis d'en renforcer la sécurité à plusieurs niveaux, et surtout d'intercepter efficacement les menaces étrangères liées à l'utilisation des réseaux. À l'heure actuelle, les OS utilisés classiquement sur des machines desktop fournissent un pare-feu simple (*Windows Defender*, un utilitaire fournit de base dans MAC OS X, *iptables/Netfilter* ou autre pour les distributions Linux). Ce dernier tournant en arrière plan de façon quasi invisible car il demande peu de ressources par rapport à ce qu'une machine actuelle peut offrir.

En parallèle avec la montée en puissance de ces machines de type desktop, serveurs, etc. s'est développée depuis à peu près les années 2000 la tendance de l'≪ Internet des Objets ≫, ou encore plus communément abrégé IoT pour *Internet of Things*. Bien qu'assez large, cette dénomination regroupe beaucoup d'objets et de concepts, qu'ils soient virtuels ou non mais possédant un dénominateur commun : la capacité de communiquer en réseau avec d'autres équipements. Cela englobe par exemple la domotique, les outils et capteurs de mesures diverses, les imprimantes et scanneurs en réseau, etc. Tous ces éléments convergeraient idéalement vers une mise en réseau commune. Cela peut se faire par le réseau Internet, il n'est pas rare d'orienter ces connections vers un cloud permettant de traiter globalement et intelligemment la masse de données qu'il reçoit de ces équipements. Or, comme évoqué ci-dessus, plus on s'interconnecte et plus on s'ouvre à des attaquants potentiels, ce qui pose problème si rien n'est mis en place pour s'en protéger.

Ce travail aura pour objectif premièrement de faire un état de l'art des dispositifs de protection qui sont actuellement déployés dans l'IoT et plus particulièrement dans le cadre domestique. Il s'agit d'un monde beaucoup plus hétérogène et restreint en terme de ressources que celui des ordinateurs qu'on retrouve classiquement dans ce milieu, de fait il n'est pas toujours possible de réutiliser telles quelles toutes les technologies de protection y attenant. De plus, il faut prendre en considération les spécificités d'une habitation : au centre de tous ces équipements communiquant se trouve l'habitant, une personne n'étant pas forcément habilitée à manipuler et contrôler ces nouvelles technologies. Il sera également question d'établir une vision globale des différentes formes de pare-feus et sous quelles formes ceux-ci peuvent être implémentés dans les équipements d'une habitation classique. Deuxièmement, il sera question de mettre en pratique ces connaissances pour développer un système en lien avec ces nouvelles mesures de sécurité inhérentes à l'IoT. Celui-ci fera intervenir les connaissances acquises au préalables sur les pare-feus.

1 Présentation de l'*internet des objets*

1.1 Généralités

L'Internet des objets, qu'on désignera par *IoT* pour le terme plus répandu de *Internet Of Things*, représente un tout qui évolue maintenant en flèche depuis plusieurs années. Aucune définition formelle n'est acceptée globalement, mais plusieurs organismes ont tenté d'en établir une ébauche. Par exemple, l'ITU-T (ITU Telecommunication Standardization Sector) Y.2060 le définit comme tel :

"Global infrastructure for the society, enabling advanced services by inter-connecting (physical and virtual) things based on existing and evolving in-teroperable information and communication technologies."

Derrière cette définition très générale, on peut distinguer plusieurs sous-groupes d'objets connectés distincts, aux applications tant variées que hétérogènes, dans des domaines et secteurs également très différents. C'est ce qui fait la force et en même temps la faiblesse de cet ensemble d'équipements et services qu'on regroupe derrière le terme *IoT* et que des efforts considérables sont déployés pour inter-connecter au maximum. C'est un domaine d'étude intéressant car il représente littéralement ce qu'on pourrait considérer comme le futur de notre environnement technologique. De fait, les équipements que l'ont peut associer à une partie de l'IoT ont déjà fait leur apparition dans notre quotidien : en 2017 on comptait 8,4 milliards de machines en présentant les caractéristiques et les estimations pour l'année 2020 tendent vers 20,4 milliards d'objets connectés d'après la société d'analyse Gartner [5].

1.2 Caractéristiques des équipements de l'*IoT*

1.2.1 Domaines d'application

Les secteurs dans lesquels l'IoT s'est implanté ces dernières années sont nombreux et très variés : ils s'étendent de l'industrie au domaine des soins de santé en passant par la tendance des *Smart Home*. C'est ce dernier domaine qui est approfondi dans ce travail et qui sera le plus sous-entendu par la suite quand le terme *IoT* est utilisé. La Figure 1 présente une vision d'un schéma global des autres domaines qui gravitent autour du vaste monde de l'IoT.

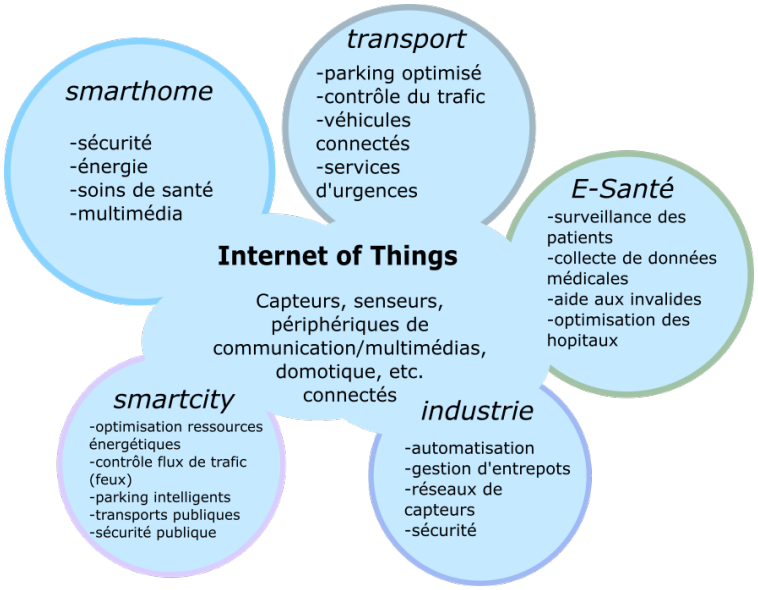

FIGURE 1 – Domaines d'application de l'IoT

1.2.2 L'environnement *smarthome*

Le terme émergeant *Smart Home* est une fois de plus très englobant et généra. Il n'en existe pas de définition formelle et communément acceptée. Basman M. Hasan et al. [4] en présentent plusieurs. Un résultat les unifiant pourrait être

« Une smarthome est un environnement lié au domicile particulier où plusieurs équipements ou sous-systèmes sont inter-connectés et où les informations qu'ils échangent sont collectées et utilisées afin de surveiller, réguler et automatiser l'écosystème du domicile ».

L'utilisateur en tant que personne physique y vivant est donc au centre de cette architecture, et y siège comme le principal intervenant. Puisque dans l'idée où toute cette technologie est déployée dans le but d'améliorer sa qualité de vie, c'est lui qui devra interagir avec. La notion d'intelligence est intrinsèquement liée avec celle de l'interconnexion de tous ces senseurs et actuateurs déployés dans l'environnement du domicile : il s'agit d'en récolter et regrouper toutes les données en un point central doté d'une capacité de traitement plus évoluée afin qu'il puisse en tirer une optimisation globale du domicile et la proposer sous une forme donnée à l'habitant.

Une certaine classification fonctionnelle peut être établie pour distinguer de façon plus concrète les différents équipements qui peuvent intervenir dans l'écosystème d'une *smarthome*. Elle est schématisée par la Figure 2, inspirée de [4]. Ce qui est désigné par *point d'interconnexion* peut dépendre de l'architecture réelle d'une *smarthome*. Dans la plupart des cas il s'agit d'une machine faisant office de collecteur pour toutes les données transitant dans le domicile et de gateway vers le reste de l'Internet, éventuellement le cloud associé au domicile.

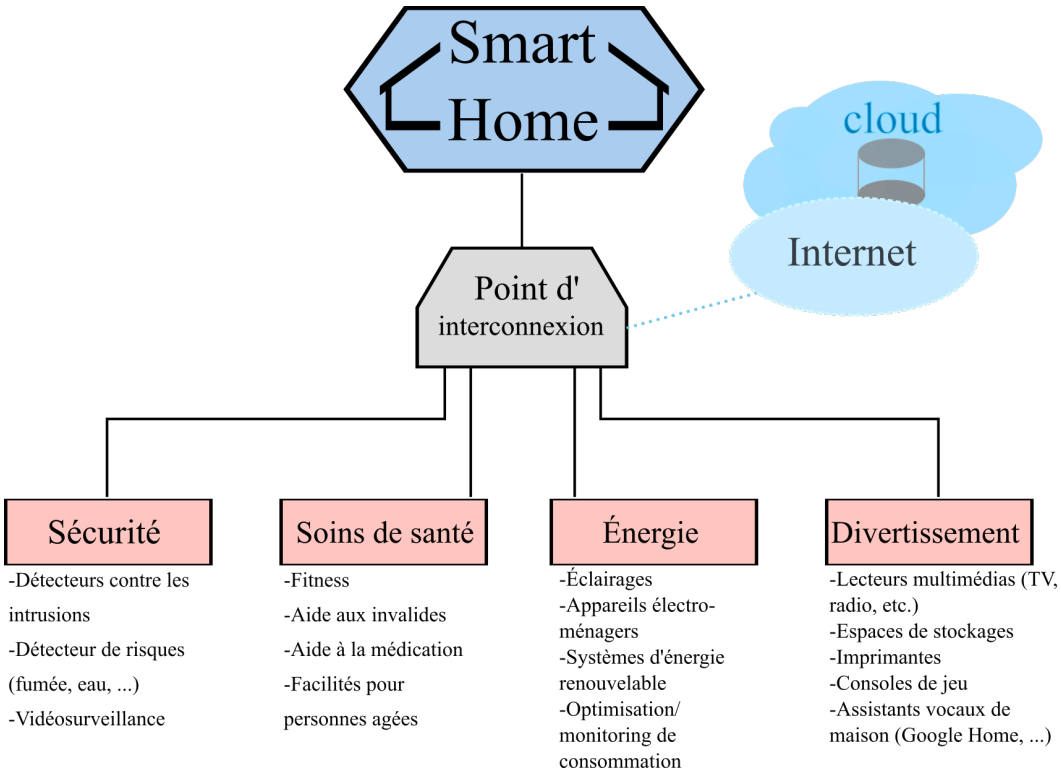

FIGURE 2 – Classification fonctionnelle des équipements *IoT* d'une smarthome

1.2.3 Exemples d'équipements

La perception de ce qu'est l'*IoT* par le grand public se résume énormément à l'environnement que constitue la *smarthome* [5]. Il s'agit d'une erreur d'incompréhension, on peut tenter de l'expliciter en analysant ce qui compose cette perception. La Figure 3 en donne une vision générale (tirée d'un sondage effectué aux États-Unis), qui va être étayée par les exemples concrets d'équipements la suivant.

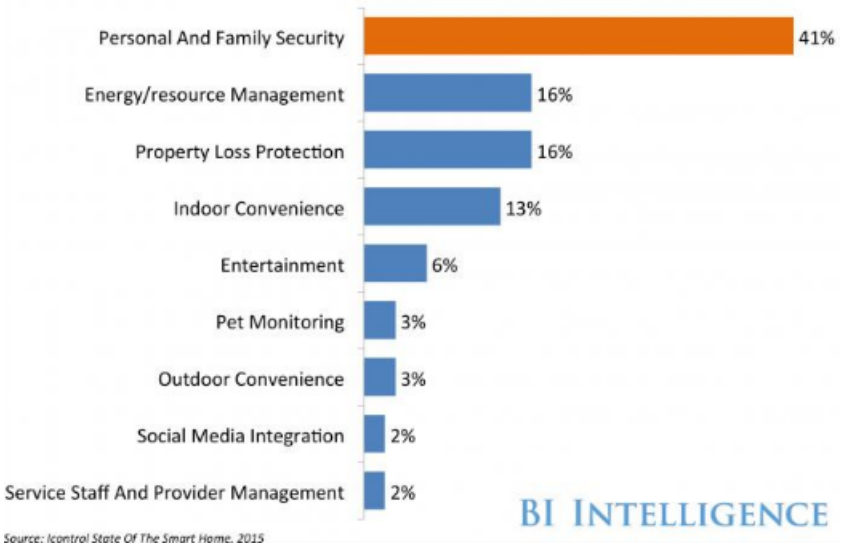

FIGURE 3 – Top des meilleurs apports des *smarthome* tel que perçu par les Américains

/—— A faire : Remplacer par une section plus pertinente ——\

Appartenant à la classe sécurité

- Caméras de vidéosurveillance dites IP
- Systèmes de gestion d'alarme à distance
- Verrous de portes intelligents
- Simulateurs de présence et occupation du domicile

Appartenant à la classe soins de santé

- Surveillance des patients à leur domicile (contrôle des mesures médicales)
- Accessoires de fitness : montres, balances connectées et autres
- Outils divers d'aide aux personnes invalides (fauteuils, bracelets de secours, ...)

Appartenant à la classe des énergies

- Luminaires intelligents/automatisés contrôlables à distance
- Frigos, lave-vaisselles, etc.
- Thermostats connectés, compteurs et senseurs énergétiques

Appartenant à la classe du divertissement & multimédia

- Outils de communication : smartphones, babyphones, etc.
- SmartTV, consoles, casques connectés et lecteurs multimédia divers
- Imprimantes et scanneurs en réseau
- Assistants vocaux de maison comme le *google home*

1.2.4 Restrictions des équipements

Malgré le fait que l'ensemble des objets considérés comme appartenant à l'IoT soit très hétérogène, on peut distinguer plusieurs caractéristiques communes à beaucoup d'entre eux. Elles tendent généralement vers ce qui est vu comme une restriction par rapport à un ordinateur type classique (*desktop*). Ces éléments constituent les plus gros freins au développement de la sécurité sur de tels système [3]. Les conséquences de ces restrictions sont discutées plus en détail dans la section 3 de ce document.

Conçus pour satisfaire une unique fonction

Le meilleur exemple est celui des capteurs : un capteur a pour objectif de faire une mesure d'une grandeur physique (température, pression, etc.), d'en tirer une valeur numérique et de faire remonter via son interface avec le réseau cette information vers une unité centrale qui la traitera. Ce genre d'équipement est généralement minimaliste au possible et ne peut donc pas remplir d'autre tâche.

Requièrent une faible consommation énergétique

Les systèmes embarqués n'ont pas toujours accès à une source illimitée d'énergie, et auront donc une durée de vie limitée à celle de leur batterie. En conséquence, il est souhaitable d'économiser un maximum, ce qui peut se faire en réduisant les temps d'éveil de l'équipement et en optimisant le nombre d'opérations effectuées quand il tourne à plein régime. Dés lors, certains protocoles et algorithmes doivent être adaptés (relatifs aux communications réseaux mais aussi à la sécurité) [7].

Sont contraints en ressources CPU, mémoires et radios Ces contraintes sont aussi identiques à celles des systèmes embarqués classiques. En plus de celles-ci, on peut mettre en évidence le fait que les radios (quand il s'agit d'une interface sans fil) sont assez faibles et ne permettent pas des communications à haut débit. En résulte également que des techniques comme le saut de fréquence et les algorithmes de chiffrement de type asymétrique sont plus compliquées à mettre en œuvre [6].

Sont programmés à un bas niveau d'abstraction

Étant conçus pour ne remplir que des fonctions spécifiques, certains équipements ne sont pas programmables en utilisant des langages de haut niveau. Par conséquent, ce sont souvent des boîtes noires difficilement manipulables et statiques : les mises à jour et patch de sécurité ne sont pas déployables aisément par les constructeurs [7]. Les seules interactions que l'utilisateur peut avoir avec l'équipement sont celles prévues par l'interface de ce dernier s'il y en a une.

2 Présentations des pare-feus

2.1 Généralités

Un pare-feu est un dispositif, virtuel ou matériel, qui surveille et contrôle le lien entre un réseau dit de confiance et un réseau extérieur non fiable. Typiquement, ce réseau potentiellement dangereux est Internet et la zone à protéger est le réseau interne d'une entreprise ou d'une habitation. L'existence des pare-feus est une conséquence du besoin d'outils de protection aux bordures de réseaux distincts contrôlés par des entités différentes. D'une part, il faut garantir que des données internes confidentielles restent à l'intérieur du réseau de confiance. D'autre part, il est nécessaire de filtrer les données entrantes dans ce réseau de sorte qu'aucune menace ne s'y infiltre par des flux, même initiés depuis l'intérieur du réseau de confiance. Ces filtres sont créés et assemblés à partir de *politiques* ou *règles* définies par défaut ou par les personnes compétentes liées à l'entité gérant le réseau.

2.2 Différentes architectures

Deux classes de pare-feus sont distinguables en fonction de ce qu'ils visent à protéger. La description donnée en début de section correspond aux pare-feus au niveau réseau (*network firewalls*), situés en bordure de LANs, WANs et intranets. Ceux-ci, de par leur nature de barrière entre réseaux, peuvent également fournir des services plus évolués : système de NAT, gestion de *zones démilitarisées*, service DHCP, etc. La seconde classe agit au niveau des nœuds du réseau eux-mêmes (*host-based firewalls*), protégeant une machine physique et non pas un réseau entier. Ces pare-feus se présentent donc sous forme de software, directement intégré au niveau du système d'exploitation ou installés à un plus haut niveau.

Les pare-feux niveau réseau

Afin de remplir leur fonction, ces pare-feus sont placés en bordure du réseau à protéger et sont directement liés au machines qui font office de *gateway*. Tout le trafic passe donc par le pare-feu afin d'être analysé et filtré, ce qui peut représenter beaucoup de données à traiter. Le pare-feu doit offrir une vitesse de traitement proportionnelle aux débits et à la qualité des liens qui le traversent afin de ne pas être un goulot d'étranglement. C'est pourquoi ces pare-feus doivent être très efficaces et sont communément situés (partiellement) au niveau hardware. On parle de *hardware-based firewall appliances*, qui sont des machines physiques dont le seul objectif est de remplir les tâches d'un pare-feu le plus efficacement possible. On y retrouve deux composants : la partie applicative software ou firmware remplissant la fonction de pare-feu, qui repose sur la deuxième partie plus basse constituée de juste ce qu'il faut d'un OS particulier (*jeOS - just enough Operating System*). Cet OS est généralement propriétaire, lié au fabriquant du hardware sur lequel les deux parties opèrent et donc très optimisé pour garantir les performances.

À plus petite échelle, dans un réseau domestique par exemple, on retrouve également des pare-feus directement implémentés dans le routeur qui fait office de *gateway* pour l'habitation. Ceux-ci sont fatalement moins efficaces et complets que les matériels spécialement dédiés.

/—— A faire : Faire vrai tableau de comparaison ——\

FIGURE 4 – Cisco ASA 5550

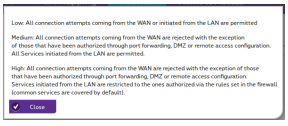

FIGURE 5 – Another figure

Les pare-feux niveau hôte

Du fait que les pare-feus de cette classe sont généralement déployés sur des machines de type desktop, la dénomination *pare-feu personnel* est aussi utilisée. Ces ordinateurs sont généralement munis de tels pare-feus par défaut ou peuvent tout du moins supporter leur installation par l'utilisateur si l'OS utilisé est classique (Windows, MAC OS X, ...). Le pare-feu agit jusqu'au niveau applicatif [**?**] et sous forme d'un *service* ou d'un *daemon* en fonction du système d'exploitation utilisé. Cela permet une proximité étroite avec l'OS et les processus. Le pare-feu personnel est donc capable de contrôler le trafic réseau demandé par chaque application et de détecter les menaces engendrées par certains flux. Ces dernières peuvent être entrantes ou sortantes : une machine extérieure qui tente d'établir une connexion suspecte ou un exécutable sur la machine à protéger qui initie un trafic avec une cible blacklistée, par exemple.

Les principales fonctionnalités d'un pare-feu personnel devraient être au minimum les suivantes :

- Bloquer les attaques et comportements dangereux du réseau extérieur : scanning des ports ouverts, attaques par fragmentation, *IP Spoofing*, etc.
- Empêcher les menaces venant de l'intérieur : un exécutable comme un *malware* ou un *spyware* qui tente d'établir une connexion vers l'extérieur doit être bloqué et mis en quarantaine
- Présenter de l'automatisation, d'une part car un utilisateur non-expérimenté pour sa configuration doit quand même rester protégé et d'autre part il doit se mettre à jour automatiquement
- Agir au niveau applicatif : un malware pourrait utiliser le port web 80 pour se répandre par exemple, pour détecter cela il faut analyser les payload des paquets et disposer d'une base de données à jour pour y déceler des patterns malicieux
- Alerter l'utilisateur quand un événement survient, et le logger avec suffisamment d'informations pour qu'il puisse prendre une décision adaptée
- Éviter les *faux-positifs* (bloquer du trafic légitime)

Que ce soit en entreprise ou dans une habitation, il est donc probable que l'on retrouve des pare-feus appartenant à ces deux classes distinctes là où ils sont efficaces. Il ne s'agit que d'échelles différentes, qui impliquent également des intervenants différents. En entreprise l'administrateur sécurité configure du matériel spécifique afin de sécuriser les frontières de son réseau tout en préservant ses performances. Il est aussi possible qu'il introduise dans les machines internes des pare-feus puissants pour empêcher les propagations des attaques déclenchées . Dans le domicile, l'habitant utilise généralement le routeur fournit par son FAI qui inclut un pare-feu réseau par défaut. S'il est un minimum expérimenté, il sera à même d'installer et configurer des pare-feus personnels sur chacun de ses équipements connectés.

/—— A faire : Schéma récapitulatif de la place des FW dans l'architecture d'une entreprise ——\

2.3 Types de pare-feu

2.3.1 Pare-feu de filtrage (sans état)

Aussi désigné dans la littérature par le terme *stateless*. Il s'agit des pare-feus les plus rudimentaires dont le premier prototype remonte à celui élaboré par Jeffery Mogul en 1989 [**?**]. Généralement, ces pare-feus sont rapides mais peu efficace car facilement dupé. Un pare-feu de ce type inspecte chaque paquet individuellement et détermine s'il peut passer sur base d'un certain ensemble de règles écrites que ses headers matchent ou non. Il s'agit des headers TCP/IP (également UDP), des options y attenant et de l'interface d'entrée principalement. Plus en détail : les adresses IP sources et destination, les ports sources et destination au minimum seront soumis aux filtres du pare-feu. Il y a plusieurs problèmes avec cette approche :

— Il n'y a aucune vérification au dessus de la couche transport : la partie applicative peut contenir n'importe quoi
— Le pare-feu n'est pas dynamique : il n'apprend rien du trafic qu'il laisse passer. Aucun état n'est retenu, alors que TCP est un protocole lié à une machine à état dont il pourrait être possible de garder une trace
— Les règles sont très redondantes à écrire pour être efficace, très peu modulable et facilement sujettes aux erreurs et oublis

Ce type de pare-feu tombe en désuétude car ils sont trop simple à duper par des attaquants.

2.3.2 Pare-feu à état

Le but de ce type de pare-feu dit *stateful* est d'améliorer les techniques de filtrage sans état en maintenant de l'information sur les flux passant au travers, principalement TCP. Effectivement, au contraire d'UDP, TCP est un protocole qui garde un état qui se traduit dans certains champs de ses headers. Dés lors, le pare-feu peut accéder à cette information, l'analyser et l'utiliser pour en déduire dans quel état est actuellement la connexion entre les deux processus communiquant sur les deux hôtes impliqués. Cela peut se traduire par l'inspection des flags (SYN, FIN, ...), des numéros de séquences et acquittements qui permettent au pare-feu de contrôler en conséquence le contenu d'une table interne des connexions.

Une fois une connexion

2.3.3 Pare-feu applicatif

2.3.4 Pare-feu applicatif proxy

2.3.5 Pare-feu à inspection profonde

2.3.6 Pare-feu identifiant

2.3.7 Pare-feu nouvelles génération

2.4 Ressources logicielles importantes

3 La protection dans l'*IoT*

3.1 Vulnérabilités liées à l'*IoT*

3.2 Possibilités d'amélioration

3.3 Solutions existantes

4 Les pare-feux et l'*IoT*

4.1 Différents types d'architecture

4.2 Les pare-feux domestiques

4.2.1 Caractéristiques d'un réseau domestique

4.2.2 Attaques possibles et conséquences

4.3 Application et implémentation

5 Mise en pratique : ébauche

Conclusion

Références

[1] Cable broadband technology gigabit evolution. Dernière lecture le 27/11/2018.

[2] Internet growth statistics par internet world stats. http://www.ti.com/lit/ml/swrb028/swrb028.pdf. Dernière lecture le 26/11/2018.

[3] Security in the Internet of Things. https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf, 2015.

[4] Alhafidh Basman M.Hasan and William Allen. Design and simulation of a smart home managed by an intelligent self-adaptive system. *Int. Journal of Engineering Research and Application*, 2016.

[5] Dan-Radu Berte. Defining the IoT. *De Gruyter*, 2018.

[6] Engin Leloglu. A review of security concerns in Internet of Things. *Journal of Computer and Communications*, 2017.

[7] Huichen Lin and Neil Bergmann. IoT privacy and security challenges for Smart Home environments. *Information (online MDPI journal)*, 2016.