

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

1	Présentation de l'<i>Internet des Objets</i>	4
1.1	Généralités	4
1.2	Caractéristiques des équipements de l' <i>IoT</i>	4
1.2.1	Domaines d'application	4
1.2.2	L'environnement <i>smarthome</i>	5
1.2.3	Exemples d'équipements	6
1.2.4	Restrictions des équipements	7
2	Présentations des pare-feux	8
2.1	Généralités	8
2.2	Différentes architectures	8
2.3	Types de pare-feu	10
2.3.1	Pare-feu de filtrage (sans état)	10
2.3.2	Pare-feu à état	10
2.3.3	Pare-feu applicatif	11
2.3.4	Pare-feu applicatif proxy	11
2.3.5	Pare-feu identifiant	12
2.4	Systèmes de détection d'intrusion (<i>IDS</i>)	12
2.5	Systèmes de prévention d'intrusion (<i>IPS</i>)	14
2.6	Les pare-feux nouvelle génération	14
2.7	Les pare-feux de référence	14
3	La protection dans l'<i>IoT</i>	15
3.1	Vulnérabilités liées à l' <i>IoT</i>	15
3.2	Possibilités d'amélioration	15
3.3	Solutions existantes	15
4	Les pare-feux et l'<i>IoT</i>	16
4.1	Différents types d'architecture	16
4.2	Les pare-feux domestiques	16
4.2.1	Caractéristiques d'un réseau domestique	16
4.2.2	Attaques possibles et conséquences	16
4.3	Application et implémentation	16
5	Mise en pratique : ébauche	17

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% [3] [2]. 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 équipées 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 scanners 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 attendant. 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-feux 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 préalable sur les pare-feux.

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'on 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 [6].

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.

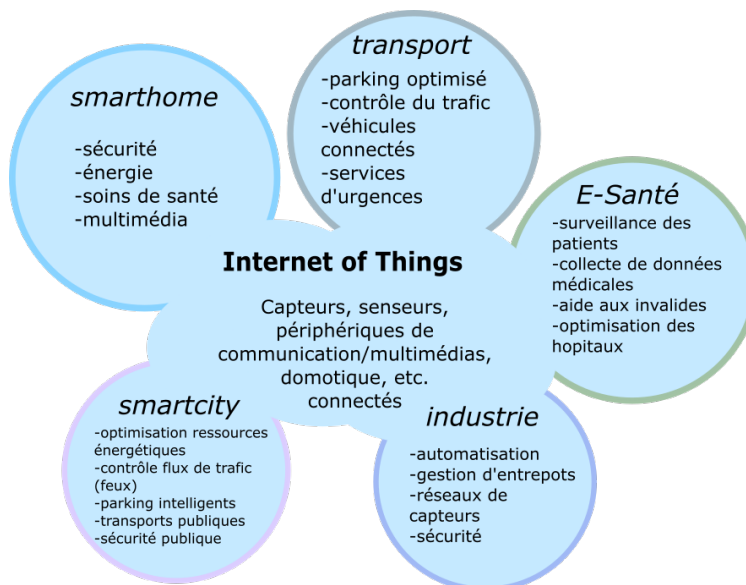


FIGURE 1 – Domaines d'application de l'IoT

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. [5] 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 [5]. 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.

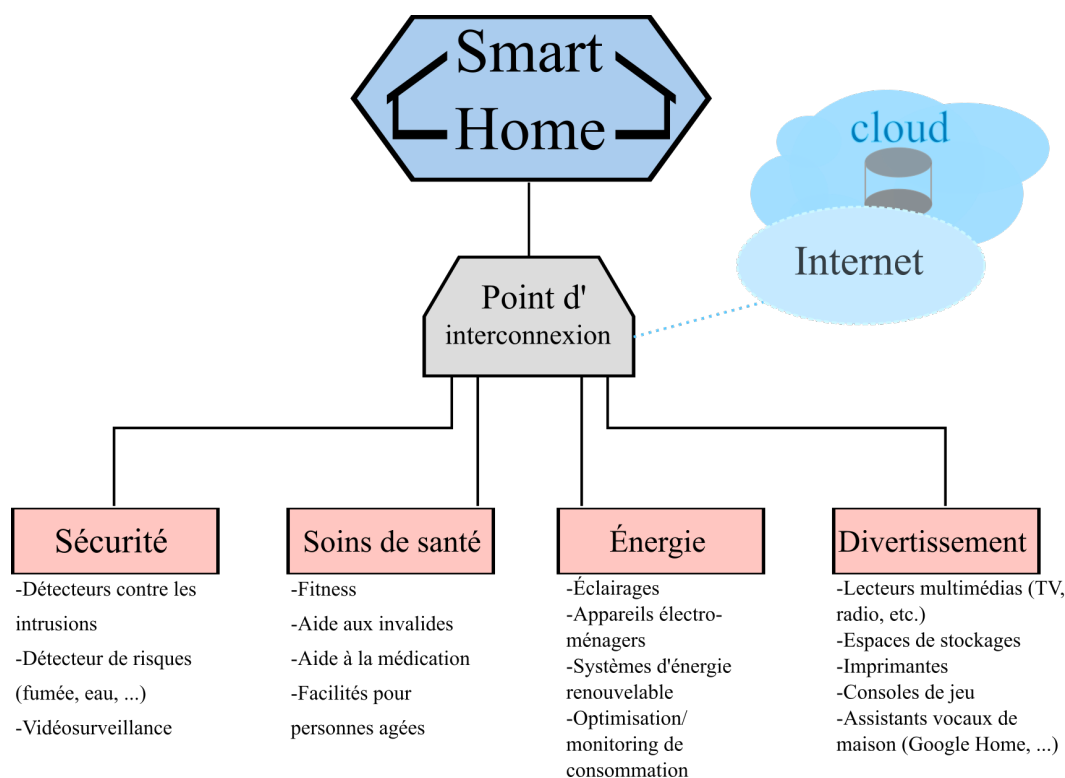


FIGURE 2 – Classification fonctionnelle des équipements *IoT* d'une *smarthome*

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* [6]. Il s'agit d'une erreur d'incompréhension, on peut tenter de l'explicitier 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.

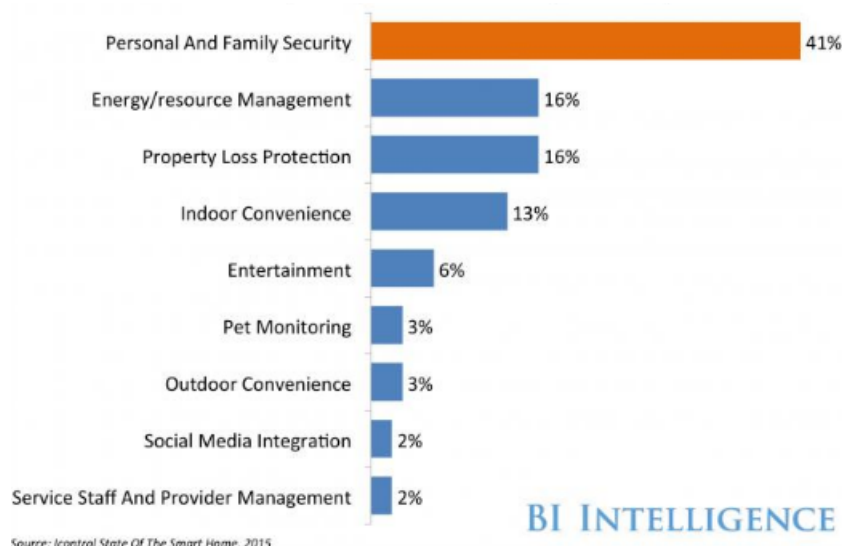


FIGURE 3 – Top des meilleurs apports des *smarthome* tel que perçu par les Américains

/— 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 scanners 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 [4]. 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) [10].

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 [9].

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 [10]. 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-feux

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-feux 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-feux sont distinguables en fonction de ce qu'ils visent à protéger. La description donnée en début de section correspond aux pare-feux 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* [7], 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-feux se présentent donc sous forme de software, directement intégrés 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-feux sont placés en bordure du réseau à protéger et sont directement liés aux machines qui font office de *gateway* (routeurs). 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-feux 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 fabricant du hardware sur lequel les deux parties opèrent et donc très optimisé pour garantir les performances requises.

À plus petite échelle, dans un réseau domestique par exemple, on retrouve également des pare-feux 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 à cette unique fonction.

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



Débit d'inspection stateful (multiprotocole)	300 Mbps - 750 Mbps max
Débit max. App. Control (AVC) + IPS/NG IPS	125 Mbps
Débit max. VPN avec chiffrement 3DES/AES	100 Mbps
Nombre max. de sessions simultanées	50000

FIGURE 4 – Cisco ASA 5506H-X

Low: All connection attempts coming from the WAN or initiated from the LAN are permitted
Medium: All connection attempts coming from the WAN are rejected with the exception of those that have been authorized through port forwarding, DMZ or remote access configuration. All Services initiated from the LAN are permitted.
High: All connection attempts coming from the WAN are rejected with the exception of those that have been authorized through port forwarding, DMZ or remote access configuration. Services initiated from the LAN are restricted to the ones authorized via the rules set in the firewall (common services are covered by default).

FIGURE 5 – Pare-feu b-box 3V

Les pare-feux niveau hôte

Du fait que les pare-feux 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-feux 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 [8] 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 [7]

- 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-feux 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-feux puissants pour empêcher les propagations des attaques déclenchées. Dans le domicile, l'habitant utilise généralement le routeur fourni 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-feux 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-feux les plus rudimentaires dont le premier prototype remonte à celui élaboré par Jeffery Mogul en 1989 [12]. Généralement, ces pare-feux 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 attendant 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 modulables et facilement sujettes aux erreurs et oublis

Les paquets ICMP peuvent également faire l'objet d'un filtrage intelligent [7]. 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. Dès 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.

L'établissement d'une connexion se fait comme suit : lors de la réception du premier paquet TCP par le pare-feu, celui-ci va le soumettre à ses règles de filtrage définies comme dans un pare-feu sans état. Si le paquet est valide, il est retransmis pour poursuivre librement sa route et une entrée est ajoutée dans la table interne du pare-feu. Celle-ci va changer d'état à chaque paquet de la communication reçu, jusqu'à arriver dans un état *established* correspondant à la fin du 3-way handshake TCP. Tous les paquets suivants pourront alors être traités rapidement en faisant matcher les headers à ceux de l'entrée en état *established* dans la table. Cette façon de procéder est plus efficace que de soumettre chaque paquet individuellement aux règles de filtrage qui peuvent être complexes et demander beaucoup de travail.

Dans le cas d'une communication utilisant UDP, le contrôle possible est moins fin car il ne s'agit pas d'un protocole à état et les échanges ne sont pas bidirectionnels. Dans ce cas, quand le premier paquet d'une transmission arrive en entrée du pare-feu, il est soumis aux règles de filtrage. S'il est considéré comme correct, le pare-feu ajoute une entrée dans sa table pour les couple d'adresses et ports. Cette entrée expirera après un temps donné sans autre nouveau paquet la matchant.

2.3.3 Pare-feu applicatif

Ce type de pare-feu peut être considéré comme une extension complète aux simples pare-feux à états dans le but d'en améliorer la fiabilité. Là où ces derniers sont capables de déterminer quels protocoles sont utilisés et autorisés sur chaque port, les filtres ajoutés au niveau applicatif peuvent en plus déduire à quelles fins sont utilisés ces protocoles (l'inspection va jusqu'à la couche 7 du modèle OSI). Il s'agit cependant de plus que de simples filtres, c'est une technologie à part entière qui est utilisée : l'inspection profonde des paquets ou *deep packet inspection* (DPI). Les pare-feux utilisant la DPI mêlent les fonctionnalités d'un pare-feu à état avec les systèmes de détection et prévention d'intrusions (sous-sections 2.4 et 2.5). La décision de bloquer ou de laisser passer le paquet tient compte de ce qu'il contient réellement au niveau données et de l'interprétation qui en est faite pour déterminer s'il représente un danger.

Par exemple, les *Web Application Firewalls* (WAF) sont une sous-catégorie des pare-feux applicatifs qui opèrent un filtrage sur le trafic HTTP. Ils peuvent donc filtrer le trafic sur base de certaines règles d'accessibilités fixées en bloquant des requêtes aux URL douteuses ou considérées comme non éthiques vis-à-vis de l'organisme maintenant le réseau par lequel elles transitent. Outre cela, les WAFs permettent également de se protéger contre les attaques dites de type *parameter tampering* (injection SQL, cross-site scripting, etc.) [11], ainsi qu'inclure des filtres anti-spam pour les courriels [?].

Plus généralement, les pare-feux applicatifs permettent de se protéger des virus, vers et tentatives d'*exploits* de faiblesses connues des systèmes à protéger [1] [11]. Un autre avantage d'analyser jusqu'à la couche 7 grâce au DPI est que certains protocoles (FTP par exemple) utilisent la couche applicative pour transmettre des informations relatives aux couches plus basses (IPs, ports, etc.) et qui seront impliquées dans des communications passant par le dispositif pare-feu [?]. Comme illustré par l'exemple des WAFs, le principal défaut inhérent à leur nature réside dans le fait que pour chaque type de trafic applicatif que l'on souhaite contrôler, un travail spécifique doit être opéré (établir des règles dédiées par exemple) [?].

2.3.4 Pare-feu applicatif proxy

Ces pare-feux mêlent l'inspection au niveau applicatif et le rôle de proxy pour les flux qui sont destinés à le traverser originellement. Ainsi, il devient réellement un intermédiaire entre les deux partis communiquant, interceptant les paquets pour les analyser puis les retransmettant vers le destinataire comme s'il en était la source [7]. Avant cette retransmission, le paquet peut être inspecté du point de vue de toutes ses couches et déterminé comme étant dangereux en fonction des opérations de filtrages décidées dans le proxy. Un contrôle très fin peut donc être opéré. Cela garantit un niveau de sécurité plus haut que les pare-feux de filtrage pur qui traitent les paquets à la volée [?].

Cette approche possède cependant trois gros désavantages :

- Clairement, l'impact sur les performances du réseau n'est pas insignifiant (surtout si le pare-feu n'est construit que au niveau software)
- À chaque nouveau protocole applicatif que l'on souhaite pouvoir filtrer de la sorte, un nouveau dispositif proxy correspondant doit être pensé et développé pour en filtrer le trafic
- Si un proxy présente une faille de sécurité, un assaillant peut l'utiliser comme un vecteur d'attaque et prendre le contrôle du système sur lequel il tourne. S'il parvient alors à désactiver les services relatifs au pare-feu, la voie vers ce qu'on souhaitait protéger se retrouve toute ouverte

2.3.5 Pare-feu identifiant

Pour ce type de dispositif, on veut pouvoir définir des règles de filtrage en fonction de l'utilisateur qui se cache derrière un paquet ou un flux. Plusieurs schéma d'association existent, définissant ce à quoi le notion d'un utilisateur correspond. Par exemple, certains de ces pare-feux placés sur un gateway exigent qu'avant d'autoriser un flux, l'utilisateur de l'hôte doit établir une connexion SSH avec ce dernier.

/—— A faire : Lire l'article <https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/access-idfw.pdf> ——\

2.4 Systèmes de détection d'intrusion (*IDS*)

Ce type de système, abrégé par IDS pour *intrusion detection system*, est analogue à un ce qu'est un système d'alarme intérieur dans l'environnement d'une habitation : quand les dispositifs de protection mis en place à l'entrée sont contournés (une présence non permise est détectée à l'intérieur), l'alarme est lancée et des actions sont éventuellement prises en conséquence. Les IDSs sont donc des sentinelles qui surveillent le réseau interne, logiquement placées après le pare-feu dans le sens entrant. Ces systèmes se présentent sous la forme d'outils spécialisés dans l'interprétation des logs des routeurs, pare-feux, serveurs et autres agents du réseau interne. Les IDSs sont épaulés par une base de données des signatures d'attaques déjà connues et y comparent le contenu des logs afin de trouver des *patterns* qui matchent. Dans une telle situation, plusieurs actions allant de simplement alerter l'administrateur réseau à couper les accès réseaux des machines peuvent être déclenchées, en fonction du degré de certitude (match fort entre les patterns) et de la menace.

Tout comme les pare-feux, les IDSs peuvent être des ressources software ou reposer sur du hardware spécifique. Dans le cas où il s'agit de software, ils sont établis sur la même machine que le pare-feu, les proxys ou autres dispositifs de bordure de réseau. S'ils se présentent sous forme d'équipements hardware spécifiques, ils sont installés de sorte à contrôler et surveiller de près un de ces dispositifs sensibles. Le trafic tant entrant que sortant peut être analysé par les IDSs, car les attaques peuvent autant venir de l'extérieur que se déployer depuis l'intérieur.

L'analyse des événements repose communément sur deux techniques. La première, la détection par signature (*signature detection*), utilise une base de données de signatures d'attaques déjà connues et se base sur le trafic et les patterns observés pour établir un match avec ces signatures. La seconde approche est celle de la détection d'anomalies (*anomaly detection*). Il est question d'utiliser des heuristiques afin de distinguer les situations et comportements anormaux, sur base de profils types construits par analyses statistiques, agencement de règles ou réseaux neuronaux. Outre la technique utilisée, trois catégories d'IDSs existent en fonction de leur place dans l'architecture réseau (leur mode de fonctionnement diffère en conséquence) :

- Surveillance du réseau (*NIDS : Network-based IDS*)
- Surveillance des systèmes du réseau (*HIDS : Host-based IDS*)
- Surveillance distribuée du réseau (*NIDS : Distributed IDS*)

Les NIDSs

Ces dispositifs surveillent le réseau, ou un segment de ce réseau sous forme d'un équipement intermédiaire de capture (ses interfaces réseaux sont en mode écoute de l'entièreté du trafic transitant par le segment). Il est important d'avoir plusieurs unités de surveillance distinctes dans le cas où le réseau est scindé en plusieurs modules. Par exemple, un serveur web d'une entreprise pourrait être infecté et servir de plateforme de lancement d'une attaque depuis le réseau interne, vers un autre module contenant des serveurs internes.

Deux manières de procéder à l'analyse sont possibles : soit en mode *in-line* soit en *off-line*. Le cas de la capture du trafic par interface décrit ci-dessus correspond au mode *in-line*. Le trafic est analysé en temps réel, ce qui permet une plus grande réactivité mais peut constituer un goulot d'étranglement si le processus

de décision est coûteux. Le mode off-line est donc plus avantageux à ce niveau, puisque le processus d'analyse et de décision est opéré sur des données stockées et non pas à traiter à la volée. Une inspection plus fine est alors envisageable, cependant le principal défaut inévitable de ce mode de fonctionnement reste le manque de réactivité à une attaque.

Les HIDSs

Les IDSs orientés systèmes sont élaborés dans le but de protéger uniquement l'hôte sur lequel ils sont déployés. Ils ciblent également de façon précise le trafic qu'ils doivent surveiller en fonction de la nature du système. Par exemple, si l'hôte ne maintient aucun service DNS, il est inutile d'analyser des requêtes DNS qui lui parviendraient pour y déceler une menace exploitant une faille connue dans le protocole DNS. Puisque les HIDSs vont s'exécuter sous forme d'un processus (*daemon*) sur la machine hôte qui fonctionne sous un OS classique, un lien doit être établi entre les deux pour que l'HIDS puisse surveiller le système et les interfaces réseaux. Certains vont même jusqu'à rechercher les intrusions dans le noyau de l'OS.

D'une part, un HIDS peut surveiller le comportement du système dynamiquement en récupérant des informations que ce dernier met à sa disposition à la manière d'un antivirus. Différents indicateurs sont à interpréter :

- Activité de la machine même : processus qui y vivent, ressources qu'ils consomment (CPU, RAM, réseau etc.), modification dans les comptes des utilisateurs
- Activité des utilisateurs : commandes entrées, programmes lancés, tentatives d'accès à des ressources non autorisées, passage au compte administrateur
- Patterns d'exécution ou de procédure de déploiement des ver, virus, chevaux de Troie (shell ouvert simultanément à l'ouverture d'un fichier, accès aux interfaces réseau anormaux, ...)

D'autre part, certaines sections plus critiques du système peuvent être intéressantes à analyser finement, car c'est généralement là qu'un attaquant voulant prendre le contrôle de la machine va laisser des traces en y installant son software. Un HIDS voulant s'assurer que des sections critiques (système de fichiers, registres, ...) ne sont pas infectées, va maintenir une base de données de leur évolution dans le temps sous forme d'attributs et sommes de contrôles (*checksums*). Ces dernières permettent d'assurer l'intégrité des ressources concernées en comparant les valeurs régulièrement dans le temps, et notifiant les différences observées.

Les DIDSs

Les DIDSs se présentent sous la forme d'une architecture distribuée d'IDS (surveillant réseaux et/ou hôtes), et d'une unité centrale de management qui récolte toutes les informations de ces dispositifs déployés. Ainsi, la machine centrale peut maintenir une vaste base de données centralisée, représentant l'état global du réseau à protéger. Cette approche présente plusieurs avantages :

- moins de faux positifs car plus de données pour justifier une prise de décision (agrégation des événements et attaques)
- mises à jour et distribution aisées de la base de données des signatures
- centralisation des alertes/logs, contrôle global
- réponses aux événements plus efficaces, IDSs plus simples à administrer en conséquence (ajout de nouvelles règles suite à des brèches découvertes, blacklisting d'IPs, etc.)

Afin de transmettre les alertes générées avec l'unité centrale efficacement, les différents nœuds IDSs du réseau devraient communiquer de façon homogène. À cette fin, un standard a été écrit sous le nom de format IDMEF (*Intrusion Detection Message Exchange Format*, RFC 4765). Ce langage d'alertes est lisible par l'humain, utilisant le format XML. Utilisé par tous les nœuds qui effectuent la tâche de détection d'intrusion

(quelque soit le type et l'implémentation), l'unité centrale qui récolte toutes les alertes peut utiliser un outil de pilotage de la sécurité du réseau global comme Prelude. Ce outil normalise, trie, agrège, corrèle et en tire les conclusions sur des décisions à prendre pour protéger le réseau, tout en fournissant une interface (et des logs) sur laquelle l'administrateur peut surveiller ce qui se passe globalement.

2.5 Systèmes de prévention d'intrusion (*IPS*)

Dans la section précédente, il était question de détection des attaques et pour certaines d'entre elles des actions à effectuer en contre-mesure pour bloquer la menace. Cela relève du domaine d'application des systèmes de prévention d'intrusion, aussi abrégé IPS pour *intrusion prevention systems*. Tout comme les IDS, deux types d'IPS peuvent être distingués en fonction de leur place dans l'architecture réseau : les *host-based IPS* agissent au niveau local pour un hôte, tandis que les *network-based IPS* défendent un réseau ou un de ses segments internes. De fait, IDSs et IPSs vont de paires puisque les contre-mesures prises par un dispositif IPS sont basées sur ce que l'IDS détecte et lui transmet comme information.

En plus de lancer une alerte à destination d'un administrateur et écrire des logs complets, les actions qu'un IPS peut effectuer suite à la détection d'une menace sont généralement les suivantes :

- Jeter les paquets détectés comme contribuant à cette attaque
- Bloquer tout trafic issu de la même adresse IP/du même utilisateur que celui considéré comme attaquant (mettre fin à la connexion TCP impliquée)
- Reconfigurer le pare-feu associé pour qu'il puisse à l'avenir bloquer le trafic relatif à cette attaque
- Si l'IPS est lié à un dispositif faisant du proxy, il peut agir sur le contenu des paquets pour neutraliser la menace (par exemple ôter un fichier infecté joint à un mail)

2.6 Les pare-feux nouvelle génération

2.7 Les pare-feux de référence

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] Application firewall. Wikipedia article, URL : https://en.wikipedia.org/wiki/Application_firewall.
- [2] Cable broadband technology gigabit evolution. Dernière lecture le 27/11/2018.
- [3] Internet growth statistics par internet world stats. <http://www.ti.com/lit/ml/swrb028/swrb028.pdf>. Dernière lecture le 26/11/2018.
- [4] 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.
- [5] 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.
- [6] Dan-Radu Berte. Defining the IoT. *De Gruyter*, 2018.
- [7] Robert J. Shimonski, Debra Littlejohn Shinder, and Thomas W. Shinder, editors. *The Best Damn Firewall Book Period*. Syngress, Burlington, 2003.
- [8] Kalle Kokko. Next-generation firewall case study. Master's thesis, South-Eastern Finland University of Applied Sciences, 2017.
- [9] Engin Leloglu. A review of security concerns in Internet of Things. *Journal of Computer and Communications*, 2017.
- [10] Huichen Lin and Neil Bergmann. IoT privacy and security challenges for Smart Home environments. *Information (online MDPI journal)*, 2016.
- [11] Dariusz Pałka and Marek Zachara. Learning web application firewall - benefits and caveats. pages 295–308, 01 2011.
- [12] Alaauddeen Shieha. *Application Layer Firewall Using OpenFlow*. PhD thesis, University of Colorado, 2014.