Etude de technologie

- Sauvegarde Open Source
- Le stockage NAS
- Infrastructure Internet
- Wifi 2,4 & 2,5 GHz
- Firewall

Sauvegarde Open Source

Définition open source :

L’Open Source est une méthode d’ingénierie logicielle qui consiste à développer un logiciel, ou des composants logiciels, et de laisser en libre accès le code source produit.

Il est très important de sauvegarder les données d’une machine ou d’une entreprise : en cas d’infection virale, d’attaques de pirates informatiques, ou de dysfonctionnement de matériel informatique. En cas de problème, on pourra donc effectuer une restauration des données.

Pour cela, il existe différents logiciels de sauvegardes de fichiers, Open Source ou non. En tant que logiciel Open Source de sauvegardes de fichiers, on a Duplicati, Areca Backup, Bacula ou encore Backup PC.

	Duplicati	Areca Backup	Bacula	Backup PC
Avantages	- Test régulier des sauvegardes - Gain de place avec sauvegardes incrémentales - Interface Web - Outil en ligne de commande - Permet la pause et la reprise des sauvegardes	- Navigation dans les versions des fichiers - Informations sur les sauvegardes - Outils en ligne de commande	- Outils en ligne de commande - Utilisation d'un SGBD libre - Peut gérer plus d'1 milliard d'objets sans perte de performance	- Outil en ligne d commande - Interface web poussée - Choix entre sauvegardes complètes ou incrémentales
Inconvénients	- Pas de guide d'installation sur NAS - Restauration obligatoire via l'outil - Stockage compressé en .zip - Versions 1.x non maintenues	- Logiciel non maintenu - Plugin payant pour effectuer des sauvegardes automatiques ou manuelles, même si le disque est en cours d'utilisation	- Peu de possibilités - Outils quasi entièrement limités au monde Unix	- Pas de planification avec date/heure - Format spécifique
Protocoles	- FTP, SSH, WebDAV	- FTP, FTPS, SSH,	TCP/IP, TLS, PKI, CRC, GZIP/LZO	FTP
Système d'exploitation	Windows, MacOS, Linux	Windows et Linux	Windows (licence), Linux et MacOS	Windows, Linux et MacOS

On peut effectuer une sauvegarde complète ou une sauvegarde incrémentielle.

Une sauvegarde complète sauvegarde la totalité des fichiers alors que la sauvegarde incrémentale sauvegarde seulement les fichiers modifiés depuis la dernière sauvegarde complète.

Le stockage NAS



Image : NAS QNAP

Nous allons parler des serveurs NAS. Il s’agit d’éléments clés au bon fonctionnement d’un parc informatique. Un serveur NAS (Network Attached Storage) est un serveur de stockage réseau, permettant de stocker des données et les partager dans un réseau informatique. C’est un appareil réseau contenant plusieurs disques durs qui sont partagés sur le réseau.

On les utilise pour partager des fichiers au sein du réseau (lecteurs réseaux), des stockages, héberger des applications (Bitwarden, Pi-hole...), NVR pour la vidéosurveillance...

Un élément important à prendre en compte lors de l'achat d'un NAS est le nombre de baies, qui correspond au nombre de disques que l'on peut utiliser avec le NAS. Sur l'image ci-dessus, il s'agit d'un NAS QNAP de 4 baies.

Le support du Gigabit et les types de RAID sont des éléments importants à prendre en compte.

Les deux marques les plus connus sont QNAP et Synology. Ils ont chacun leur logiciel propriétaire (DSM pour Synology).



Le NAS a plusieurs fonctions :

- Il permet de ne pas éparpiller les données sur plusieurs disques durs, Le NAS permet le regroupement des données dans un même emplacement réseau.
- Les données y sont accessibles. En effet, un utilisateur connecté sur le réseau a accès, selon ses droits, aux données stockés dans les disques du NAS.
- Le NAS permet de créer des sauvegardes, et permet la récupération de données.
- Le NAS permet également la sécurité des données via la RAID, employée pour sécuriser les données contre la défaillance des disques.

Existants depuis les années 1980, on distingue désormais plusieurs marques. La plus connue est Synology. On retrouve également QNAP, Asustor (filiale d’ASUS) ou encore NetApp.

Dans le cadre des tarifs, le prix évolue selon le nombre de baies du NAS, du processeur intégré, de la mémoire RAM et de la capacité maximale.

Pour un NAS de 2 baies, il faut compter en moyenne 200 Euros. Pour un 4 baies, il faut compter entre 300 et 400 Euros (hors disques).

Infrastructure Internet



Dans le cadre d’une entreprise, l’accès Internet est primordial. Dans la plupart des cas, un seul accès internet n’est pas suffisant. Par exemple, en cas de panne du routeur Internet, l’entreprise n’aura plus accès à Internet.

Cependant, il existe des solutions à ce problème.

Qu’est-ce que le WAN ?

Un WAN (pour Wide Area Network, en français Réseau étendu) est un réseau couvrant une zone géographique de grande envergure. Le routeur Internet envoie et reçoit des informations depuis et vers Internet via son port WAN.

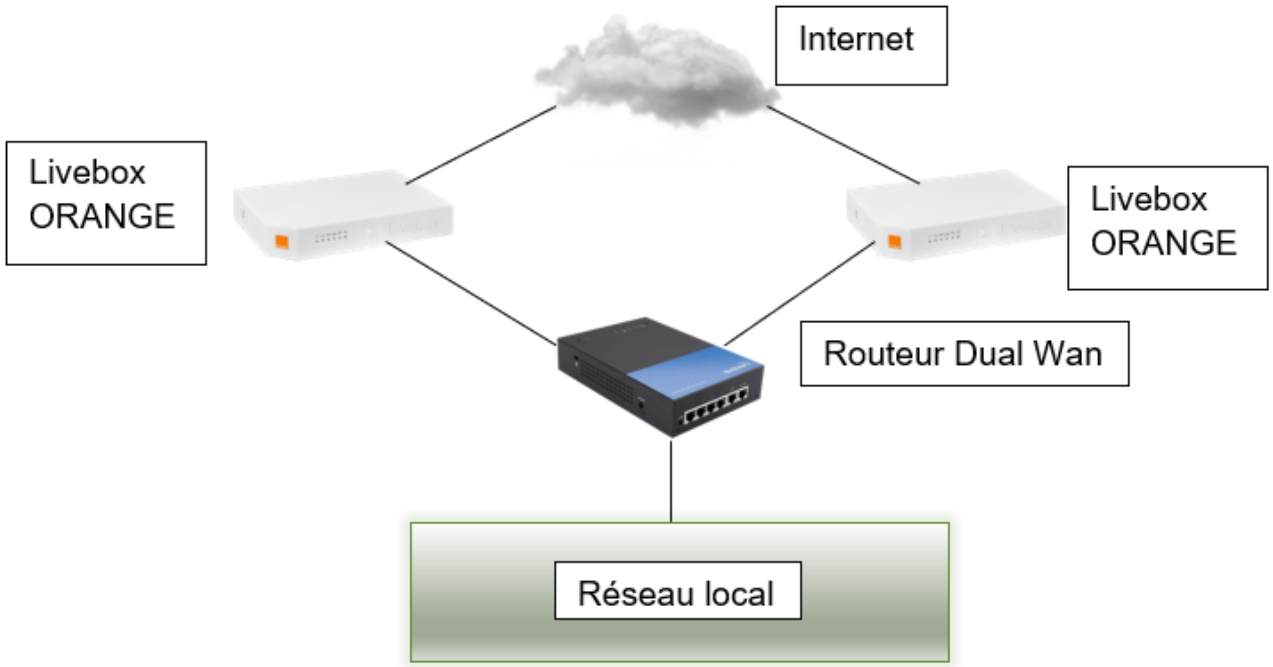
Dans le cadre d’une Livebox de chez Orange, nous avons une interface WAN reliée à l’ADSL, VDSL ou encore la fibre ; une ou plusieurs interfaces LAN pour l’accès au réseau local. Si un poste souhaite aller sur internet, la communication passe par l’interface LAN puis WAN.

L’accès internet est fourni par des FAI (Fournisseurs d’Accès Internet) comme Orange, SFR, Free ou OVH.

Qu’est-ce que le LAN ?

Le LAN (pour Local Area Network, en Français réseau local) désigne les appareils connectés dans le domicile ou l’entreprise. On parle de réseau d’entreprise ou personnel. Le LAN est l’opposé du WAN.

Qu’est-ce que le Dual WAN ?



Le dual Wan est une norme permettant à un appareil, par deux prises, de se connecter à deux connections Internet comme le schéma ci-dessus.

Cela permet d’améliorer la connexion, donc le débit. Cela est intéressant dans les zones où la connexion est mauvaise (ADSL par exemple) ou dans le cadre d’une entreprise avec beaucoup de salariés qui accèdent à Internet au même moment.

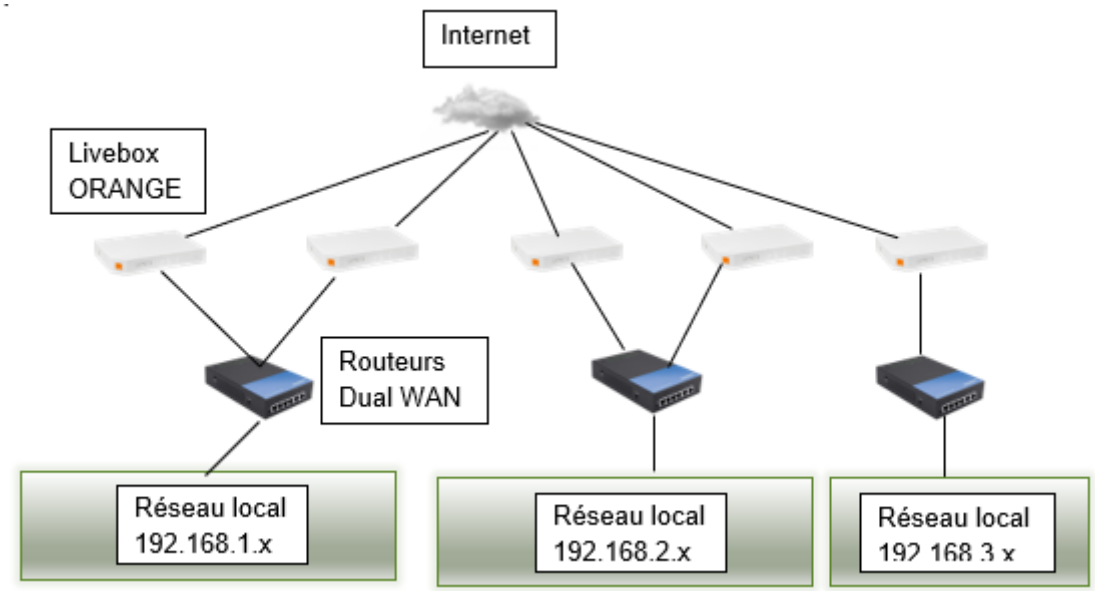
Le Dual Wan permet également d’assurer la connexion Internet. En cas de panne d’un modem d’accès internet, le deuxième sera toujours fonctionnel.

Qu’est-ce que le multi WAN ?

Le multi WAN reprend le principe du dual WAN, mais au lieu d'avoir deux accès internet, on en a 3, 10, 50… Cela est très utilisé dans les grands bâtiments, les grandes entreprises…

En multipliant le nombre de connexions, on multiplie le nombre d'utilisateurs possibles avec un bon confort d'utilisation.

Le débit est donc amélioré pour chacun, qui permet l'envoie ou la réception de données plus rapidement.



Qu'est-ce que le LOAD BALANCING WAN ?

Le Load Balancing consiste à répartir la charge des connexions. On peut dédier un routeur pour un ou plusieurs usages ou connexions, limiter la charge de chaque utilisateur, de manière automatique, intelligente ou manuellement.

Attribuer des services à certains routeurs permet en cas de panne de garantir une certaine sécurité, puisque les autres routeurs, et donc services associés continueront de fonctionner parfaitement.

Il permet d’augmenter la qualité des services, leur temps de réponse, palier la défaillance d’une ou plusieurs machines et la possibilité d’ajouter des serveurs dans interruption de service.

La répartition de charge est très utilisée au niveau des serveurs web, afin d’assurer la connexion. La répartition permet d’éviter la surcharge des serveurs, tout en augmentant la vitesse de traitement des requêtes.

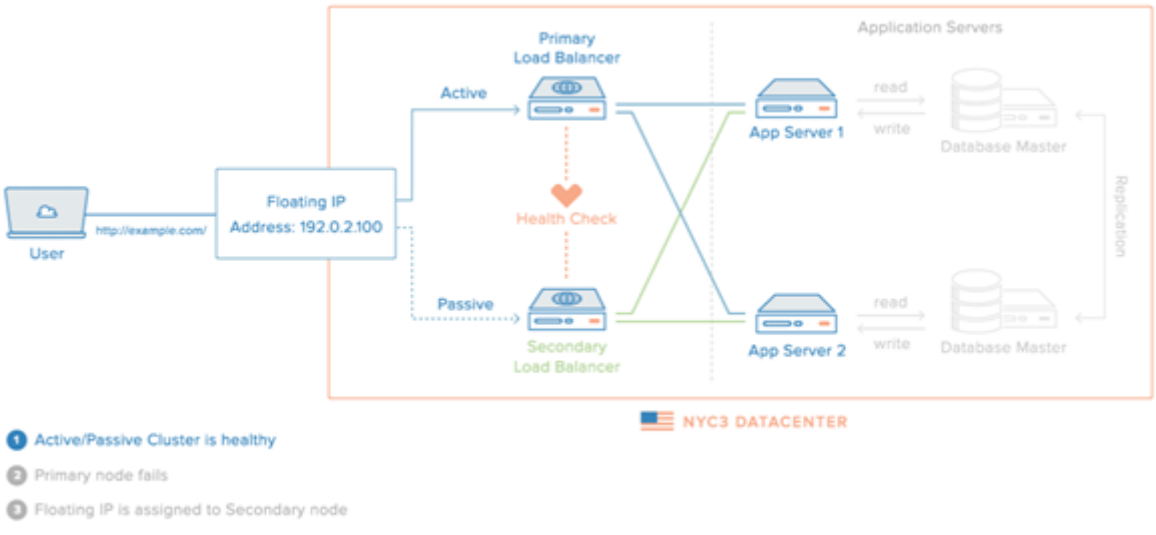
Le répartiteur peut être un routeur, un switch, un serveur ou un logiciel.

Par exemple, s’il on envoie une requête à un serveur web, celle-ci ne va pas aller directement au serveur. Elle va passer par un « Load Balancer » ou répartiteur de charge, qui va affecté la requête à un serveur Backend (derrière le Load Balancer), dans le but de réduire la latence et d’assurer le traitement. On peut également créer une affinité avec une adresse IP et un serveur Backend.

Cependant, avec ce système, on a toujours un risque que le Load Balancer tombe en panne et que le réseau ne fonctionne plus. On va donc ajouter un ou plusieurs Load Balancer afin de former un « Cluster » qui va permettre une redondance.

Si un des Load Balancer est défectueux, le serveur DNS va rediriger le traffic vers un autre Load Balancer. Or, une modification DNS peut prendre du temps à se diffuser. On va donc utiliser un système d’adresse IP flottante, évitant le problème du DNS.

Un exemple d’une infrastructure à deux Load Balancer :



Si le Load Balancer primaire tombe en panne, le secondaire prend le relais. La connexion est assurée.

Conclusion

Ainsi, ces différents types de WAN permettent une redondance de la connexion, assurant un meilleur confort d'utilisation via un débit amélioré. Ce système est très utilisé dans les grandes entreprises, afin d'assurer un service adaptés aux nombres d'utilisateurs.

Sources

https://www.digitalocean.com/community/tutorials/what-is-load-balancing

https://le-routeur-wifi.com/multi-wan-load-balancing/

https://forum.peplink.com/t/multi-wan-basic-questions/8215

http://techgenix.com/multi-wan-routers/

Wifi 2,4 & 2,5 GHz

Le Wi-Fi

Le Wi-Fi est un ensemble de protocoles de communication sans fil. Un réseau Wi-Fi relie plusieurs appareils informatiques au sein d’un réseau informatique par des ondes radio. Depuis sa création en 1997, il existe plusieurs normes.

Les normes Wi-Fi

Voici les principales normes Wi-Fi :

802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
Wi-Fi 1 (a)	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
Wi-Fi 2 (b)	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
Wi-Fi 3 (g)	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
Wi-FI 4 (n)	2,4 GHz	288 Mbps	Bonne	Elevée	20 MHz	Non
Wi-FI 4 (n)	5 GHz	600 Mbps	Correcte	Faible	20 ou 40 MHz	Oui
Wi-Fi 5 (ac)	5 GHz	5 300 Mbps	Correcte	Faible	20, 40, 80 ou 160 MHz	Oui
Wi-Fi 6 (ax)	2,4 et 5GHz	10 530 Mbps	Correcte	Très faible	20, 40, 80 ou 160 MHz	
ad	60 GHz	6 757 Mbps	Très faible	Faible	2 160 MHz	Oui (+MU-MIMO)

Les plus utilisées sont le 802.11b, 802.11g, 802.11n et 802.11ac.

Le standard 802.11ac est l’évolution du 802.11n, la première norme de Wi-Fi haut débit. Il s’agit de la plus connue des normes Wi-Fi car elle intervient dans notre usage quotidien des réseaux sans fil que ce soit avec notre smartphone, tablette ou ordinateur portable.

Comment limiter les interférences en choisissant convenablement ses canaux

et quel canal wifi choisir pour optimiser son débit ?

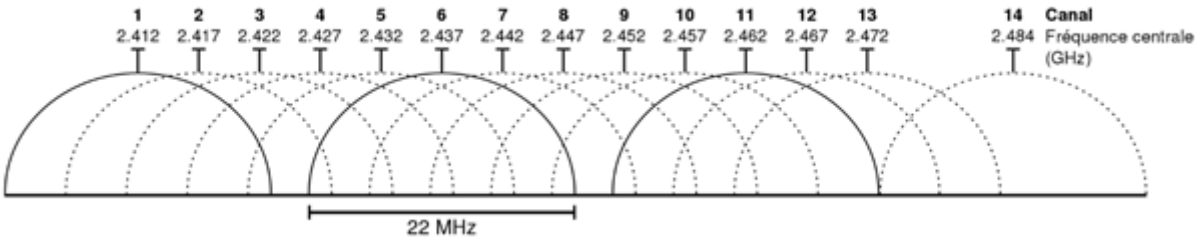
Dans le tableau ci-dessus, toutes les bandes de fréquence (à part le 802.11ad) sont en 2.4GHz ou 5GHz.

Pour ces deux bandes, il existe des canaux, qui représentent chacun une certaine fréquence.

La bande des 2.4GHz

Canal	Fréquence (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

La représentation graphique des canaux :



On remarque ici que les canaux se chevauchent entre eux. C'est pour cela qu'il est recommandé d'utiliser le canal 1, 6 et 11 pour éviter ce chevauchement.

Cependant, certains canaux sont également utilisés par d'autres types d'équipements, comme les radioamateurs du canal 1 à 8, les canaux 1, 5, 9 et 13 pour les transmetteurs et webcams

analogiques et numériques, et pour finir les fours à micro-ondes qui utilisent les canaux 7 à 10.

Pour résoudre ce problème, les normes 802.11n & 802.11ac sont créées. Celles-ci utilisent la bande des 5GHz, évitant ainsi le chevauchement.

La bande des 5GHz

Canal	Fréquence Centrale (MHz)	Fréquence (MHz)
32	5160	5150–5170
36	5180	5170–5190
40	5200	5190–5210
44	5220	5210–5230
48	5240	5230–5250
52	5260	5250–5270
56	5280	5270–5290
60	5300	5290–5310
64	5320	5310–5330
68	5340	5330–5350
96	5480	5470–5490
100	5500	5490–5510
104	5520	5510–5530
108	5540	5530–5550
112	5560	5550–5570
116	5580	5570–5590
120	5600	5590–5610
124	5620	5610–5630
128	5640	5630–5650
132	5660	5650–5670
136	5680	5670–5690
140	5700	5690–5710
144	5720	5710–5730
149	5745	5735–5755
153	5765	5755–5775
157	5785	5775–5795
161	5805	5795–5815
165	5825	5815–5835

Source : wikipedia

Chaque canal a une largeur de 20 MHz espacés de 20 MHz qui ne sont pas superposés (contrairement à ceux de la bande des 2,4 GHz) et peuvent être agrégés par groupe de 2 (norme 802.11n) ou par groupes de 2, 4 ou 8 (norme 802.11ac). Un seul terminal Wi-Fi, compatible avec la norme 802.11ac, doit pouvoir utiliser 80 MHz et optionnellement jusqu’à 160 MHz de largeur de bande.

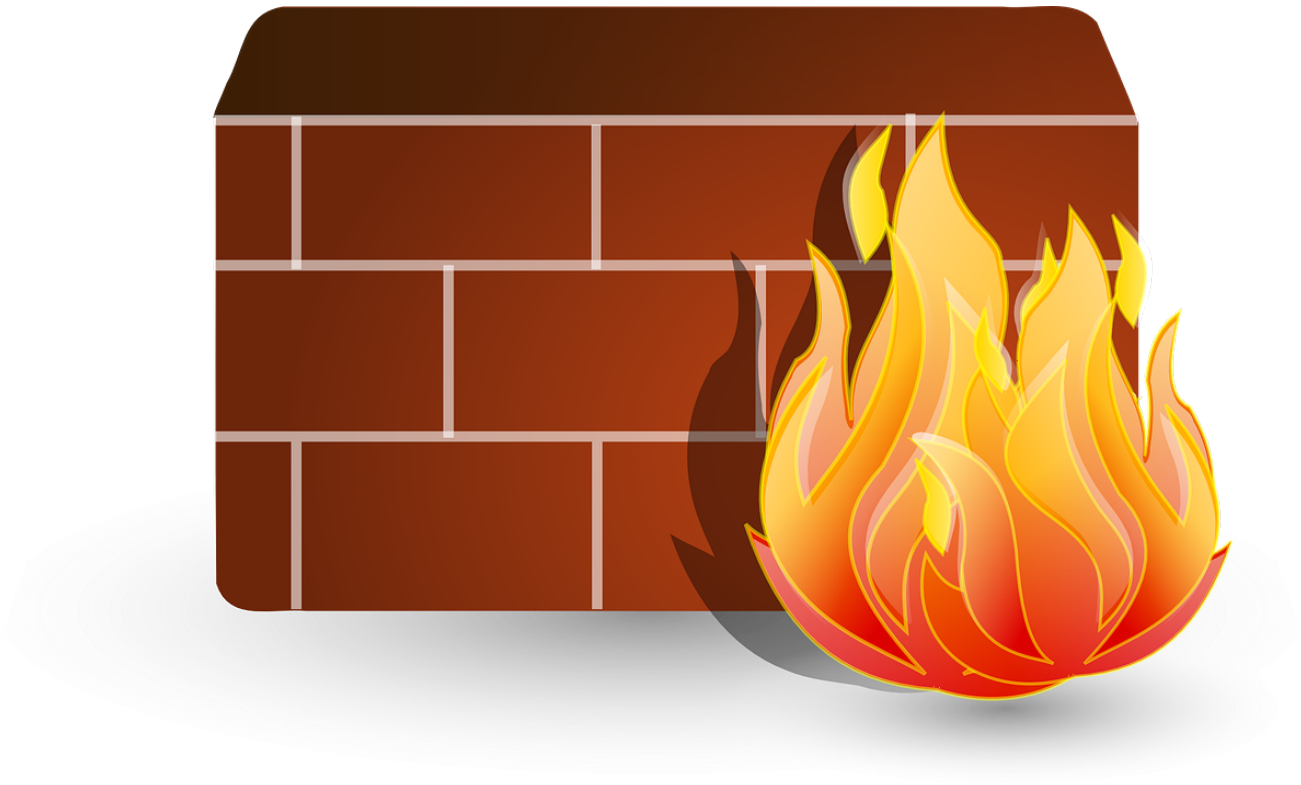
Si le point d’accès wifi est compatible ainsi que les équipements qui seront amenés à se connecter à la norme 802.11ac ou 802.11n, il est important d’utiliser la bande des 5GHz. En effet, les interférences y sont plus faibles car on trouve bien plus de canaux que la bande des 2.4GHz. De

plus, le débit est plus important.

Dans le cas où il y a des équipements non compatibles, il faut utiliser la bande des 2.4GHz donc la norme 802.11n qui est compatible avec cette fréquence. Le nombre de canaux est moins important, pouvant ainsi augmenter le nombre d'interférences.

Dans les deux cas, il est important d'utiliser un canal le moins utilisé par d'autres appareils, afin d'éviter ces interférences. Les points d'accès Wi-Fi sont capables d'analyser les canaux présents aux alentours pour choisir le meilleur canal à utiliser. Cela est d'autant plus important pour la norme 802.11n en 2.4GHz. Les interférences seront ainsi moins importantes, permettant d'avoir un meilleur débit.

Firewall



Un Firewall (pare-feu en français) est un appareil de protection de réseaux. Il surveille le trafic entrant/sortant, et autorise ou bloque le trafic basé sur un ensemble de règles définies au préalable.

Il existe plusieurs types de pare-feu : le pare-feu sans état, avec état, applicatif, et de nouvelle génération.

- Les pare-feu sans-état utilisent des informations concernant la destination d'un paquet de données, sa provenance et d'autres paramètres pour déterminer si les données présentent une menace. Ces paramètres doivent être saisis par un administrateur ou par le fabricant au moyen de règles qu'ils ont définies au préalable. Si un paquet de données sort des paramètres considérés comme acceptables, le pare-feu sans état peut identifier la menace et restreindre ou bloquer les données qui l'hébergent.
- Un pare-feu avec état inspecte tout ce qui se trouve dans les paquets de données, les caractéristiques des données et leurs canaux de communication. Les pare-feu avec état examinent le comportement des paquets de données et, si quelque chose semble anormal, ils peuvent filtrer les données suspectes. En outre, un pare-feu peut apprendre comment les données se comportent, en cataloguant les modèles de comportement.
  Si l'examen d'un paquet de données révèle un comportement suspect - même si ce type de comportement n'a pas été saisi manuellement par un administrateur - le pare-feu peut le reconnaître et traiter la menace. Il peut être utilisé à la périphérie d'un réseau ou à

l'intérieur, comme c'est le cas d'un pare-feu à segmentation interne (ISFW), qui protège des segments spécifiques du réseau au cas où un code malveillant s'y introduirait.

- Un pare-feu d'application Web aide à protéger les applications Web en filtrant et en surveillant le trafic HTTP entre une application Web et Internet. Il protège généralement les applications Web contre les attaques telles que la falsification intersites, le cross-site-scripting (XSS), l'inclusion de fichiers et l'injection SQL, entre autres. C'est une défense de la couche 7 du protocole (dans le modèle OSI), et n'est pas conçu pour se défendre contre tous les types d'attaques. Cette méthode d'atténuation des attaques fait généralement partie d'une suite d'outils qui, ensemble, créent une défense globale contre une série de vecteurs d'attaque.
- Les NGFW (Next Generation Firewall) sont la dernière génération de pare-feu.
  Ils vérifient non seulement la conformité complète d'un paquet, mais aussi qu'il correspond au protocole attendu. Ainsi, un paquet qui veut passer par le port TCP 80 devra utiliser le protocole HTTP. De même, ils permettent la gestion de la qualité de service (QOS : Quality Of Service), le blocage d'URL, l'inspection approfondie des paquets (DPI : Deep packet inspection), SSL / SSH ou la détection de malwares. Les options sont si nombreuses que la configuration d'un tel dispositif peut devenir très complexe et nécessiter l'intervention de spécialistes.
  En bref, les NGFW ont la capacité de comprendre et de prendre des décisions en analysant les détails du trafic. Ceci a deux implications majeures : tout d'abord, un traitement gourmand en temps de calcul (en fonction du débit binaire). Deux éléments, un besoin de mises à jour régulières afin de pouvoir contrôler les dernières menaces.