PERFORMANCE NUMÉRIQUE

Votre rendez-vous mensuel

Mettre en place le wifi dans son entreprise

Avec l'essor des smartphones et des tablettes puis à présent celui des objets connectés, les besoins en connexion sans fil ne cessent d'augmenter.

Le wifi (contraction de Wireless Fidelity) permet de mettre en place un réseau local sans fil (ou WLAN: Wireless Local Area Network) avec un investissement matériel relativement faible lorsqu'il existe peu d'obstacles aux ondes électromagnétiques.

Cette technologie peut être utilisée en interne (wifi privé) ou être ouverte à des personnes extérieures (wifi public). En interne, le wifi permet de faciliter le travail de ses collaborateurs qui peuvent accéder au réseau local de l'entreprise via leurs smartphones et tablettes. Les utilisateurs de ces terminaux ont aussi la possibilité de s'affranchir des réseaux mobiles dont la couverture fait parfois défaut et dont l'usage s'avère payant. Enfin, un réseau sans fil présente un moyen de piloter facilement et sans liaison filaire des équipements tels qu'une imprimante ou un système d'alarme.

Le wifi public permet quant à lui d'apporter un service aux personnes extérieures à l'entreprise en leur offrant une connexion Internet gratuite. Dans des secteurs comme l'hôtellerie, la présence d'un point d'accès wifi devient même déterminante dans le choix d'un établissement.

Cette notice explique en trois points les fondamentaux d'un projet de déploiement du wifi dans une entreprise.

Un réseau wifi efficace

> Fonctionnement du Wifi

La mise en place d'un réseau wifi nécessite à minima un modem connecté à Internet et un routeur wifi. Souvent modem et routeur ne font qu'un sous forme d'une « box » fournie par l'opérateur (de la même manière que les offres grand public).

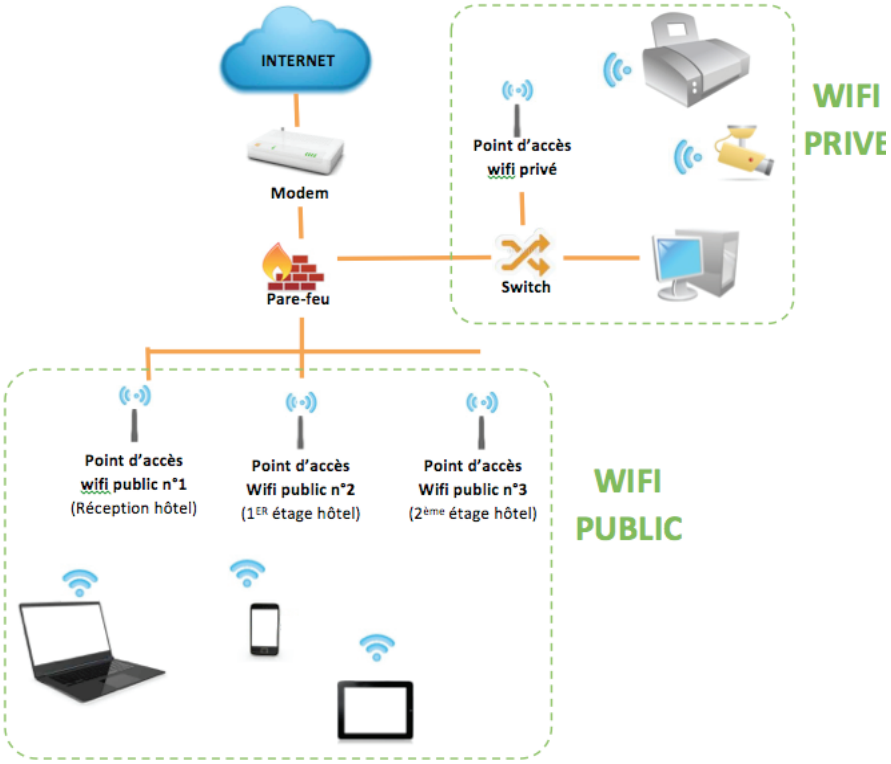
A ce système peuvent s'ajouter un ou plusieurs points d'accès wifi si de nombreux utilisateurs (plus de 10 pour les équipements de base) se connectent en même temps au WLAN afin de garantir la qualité du débit[1]. Tous les modèles d'AP (access points) ne se valent pas, les versions entrée de gamme acceptent généralement moins de connections simultanées et rencontrent des problèmes avec les effets de bascule d'un AP à l'autre (par exemple quand on marche dans un couloir).

Un réseau wifi est dit privé lorsqu'il est utilisé seulement par le personnel de l'entreprise. On parle de wifi public lorsqu'il est mis à disposition de personnes extérieures.
Sa présence est alors signalée par le logo suivant :

[1] Une connexion wifi permet un débit théorique de 11Mbit/s.

Voici deux possibilités de configuration d'un réseau wifi :

a. Configuration à partir d'une box d'accès Internet



b. Configuration d'un réseau structuré

> Installer un WLAN

La mise en place d'un réseau wifi peut s'avérer techniquement très pointue en raison d'éventuels problèmes de couverture (murs épais, environnement perturbé par des ondes électromagnétiques…). C'est pourquoi il peut être intéressant de faire appel à un professionnel.

D'autant plus qu'un paramétrage amateur du réseau wifi risquerait de compromettre la sécurisation de tout le système d'information de l'entreprise (logiciels, données,…).

Les équipements grand public fonctionnent bien mais restent pauvres en fonctionnalités. Les solutions professionnelles permettent par exemple de verrouiller l'accès au wifi en dehors des heures d'ouverture d'un établissement, de limiter le temps de connexion ou la bande passante, de bloquer un utilisateur ou de superviser les connexions en cours.

Une mauvaise qualité de service peut impacter négativement l'image de l'entreprise (hôtel).

Un réseau wifi sécurisé

Tout comme un accès filaire à Internet, le wifi doit être contrôlé par un firewall[2] afin de protéger le système d'information de l'entreprise d'éventuelles intrusions.

Les précautions nécessaires s'avèrent néanmoins différentes selon que l'accès soit privé ou ouvert au public.

> Sécuriser un accès wifi privé

Limiter l'accès au wifi

Dans le cas où le wifi est destiné à être utilisé par le personnel de l'entreprise, la sécurisation du WLAN consiste notamment à limiter strictement son accès aux personnes autorisées.

Pour ce faire, il est d'abord conseillé de masquer le nom du réseau wifi aussi appelé SSID (Service Set Identifier). Autrement dit, les appareils équipés en wifi ne détecteront pas la présence du point d'accès.

Il est également possible d'autoriser l'accès au wifi uniquement à certains équipements. Tous les appareils équipés d'une carte réseau (ordinateur, smartphone, tablette, imprimante/fax wifi…) sont identifiés par une suite de lettres et de chiffres séparés par des doubles points « : » ou des tirets « - » et appelée adresse MAC (Media Access Control). On peut utiliser ces caractères d'identification pour filtrer les terminaux tentant de se connecter à l'accès wifi.

Enfin il est possible d'utiliser un routeur wifi équipé d'une antenne directionnelle afin d'éloigner le signal de l'extérieur.

Crypter les échanges de données

Il existe plusieurs systèmes de cryptage du wifi qui consistent à chiffrer l'accès au réseau au moyen d'un mot de passe complexe appelé « clé numérique ». Le protocole WEP utilise une clé composée de 10 ou 26 caractères. Plus le nombre de caractère est élevé et plus l'accès au wifi est sécurisé.

Le WEP ne doit cependant plus être utilisé car trop facilement piratable, le WPA et le WPA2 lui sont préférables. Ces deux derniers systèmes de cryptage fonctionnent également avec une clé de cryptage mais aussi un serveur d'authentification.

> Sécuriser un accès wifi public

La création d'un point d'accès wifi public nécessite impérativement :

- **D'isoler le réseau de l'entreprise** de celui destiné aux clients afin de circonscrire une éventuelle infection par un virus et d'éviter des intrusions sur le réseau privé de l'entreprise.
- **De rendre invisibles les utilisateurs entre eux**. Une personne connectée au point d'accès wifi ne doit pas avoir la possibilité d'identifier un autre appareil connecté lui aussi.

Il existe trois types d'accès wifi public:

- L'accès libre sans mot de passe: les utilisateurs sont invités à accepter des conditions générales d'utilisation ou à saisir une adresse email. Cette solution est cependant peu sécurisée.
- L'accès via un mot de passe unique. Ce système convient aux établissements ayant un turnover important tels que les bars ou les restaurants.
- L'accès individuel : un mot de passe différent est créé pour chaque utilisateur

La durée de chaque type d'accès peut-être limitée dans le temps. Par ailleurs, il est recommandé de bloquer l'accès à des sites illégaux et d'exclure certains services (téléchargement de gros fichiers, peer to peer,…).

Les aspects légaux d'un accès wifi

> Obligations légales

Dans tous les cas, un réseau wifi ne doit pas dépasser une puissance maximale à l'intérieur et à l'extérieur d'un bâtiment[3]. L'Autorité de Régulation des Communications Electroniques et des Postes (ARCEP) fixe deux limites selon la bande de fréquence utilisée.

> Cas spécifiques de l'accès wifi public

Au regard de la loi, la mise à disposition d'une connexion Internet à des clients fait d'une entreprise un fournisseur d'accès. A ce titre, elle a l'obligation de conserver les données de connexion des utilisateurs pendant un an : adresse IP de l'ordinateur, date, heure et durée de chaque connexion.

Cette obligation résulte d'un ensemble de lois[4] visant à faciliter la recherche et la poursuite des infractions pénales. L'entreprise quant à elle pourra prouver son absence de responsabilité dans le cas où l'accès wifi public serait utilisé à des fins illégales (activité pédophile, téléchargements illégaux, spam, piratage, propos diffamatoires, xénophobes, antisémites,…).

[2] En français « Pare-feu » - Voir l'excellent article sur CCM http://goo.gl/dhQ5Ql

[3] http://bit.ly/1E0KCUN

[4] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet dite HADOPI 2

L'entreprise qui fournit un accès wifi public n'est pas tenue de relever et de conserver l'identité des clients. En revanche, si elle choisit de le faire, ces données devront également être conservées pendant un an et respecter les exigences de la CNIL sur les données personnelles.

Quel que soit le type d'accès wifi choisi, il est recommandé de faire accepter à tout utilisateur une charte dans laquelle il s'engage à ne pas commettre d'actes interdits sur Internet.

> Cas spécifiques de l'accès wifi privé

Une entreprise n'est pas concernée par l'obligation de conservation des données techniques. Néanmoins, il lui appartient de veiller à ce qu'aucune infraction ne soit commise sur son réseau par un des salariés, en bloquant l'accès à certains sites par exemple.

En revanche, les collaborateurs doivent impérativement être informés de l'existence d'un dispositif de filtrage de sites ou de surveillance automatisée contrôlant le bon fonctionnement du réseau. Un paragraphe pourra ainsi être ajouté dans la charte informatique de l'entreprise.

Votre prochain rdv numérique :
« Qu'est-ce qu'un objet connecté ? »

VOTRE CONTACT

Samuel COSTE

05 53 35 80 31 - 06 20 42 97 58
s.coste@dordogne.cci.fr
www.dordogne.cci.fr

CCI DORDOGNE