### Règles de l’ANSSI

## 1 Règle de l’ANSSI



Figure 1 logo ANSSI

L'ANSSI préconise quelques Règles concernant l'installation d'un réseau Wifi

***R1*** N’activer l’interface WiFi que lorsqu’elle celle-ci doit être utilisée.

***R2*** Afin de garder le contrôle sur la connectivité du terminal, désactiver systématiquement l’association automatique aux points d’accès WiFi configurés dans le terminal.

***R4*** Éviter tant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance.

***R5*** Bloquer, par configuration du pare-feu local, les connexions entrantes via l’interface WiFi.

***R6*** Respecter la politique de sécurité de l’entité, en particulier s’agissant des moyens cryptographiques d’authentification ainsi que de protection en confidentialité et en intégrité qui doivent être mis en œuvre.

***R9*** Plus largement, lorsque des données sensibles doivent être véhiculées via un réseau WiFi, l’utilisation d’un protocole de sécurité spécifique, tel que TLS ou IPsec, doit être mis en oeuvre.

***R11*** Lorsque l’accès au réseau WiFi n’est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier mais également de contrôler sa diffusion.

En particulier, il convient de :

– ne pas communiquer le mot de passe à des tiers non autorisés (prestataires de services

par exemple) ;

– ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non

autorisé ;

– changer le mot de passe régulièrement et lorsqu’il a été compromis.

***R12*** Pour les réseaux WiFi en environnement professionnel, mettre en œuvre WPA2 avec une infrastructure d’authentification centralisée en s’appuyant sur WPA-Entreprise (standard

802.1X et protocole EAP), ainsi que des méthodes d’authentification robustes.

***R13*** Configurer le Private VLAN invité en mode isolated lorsque que le point d’accès WiFi prend en charge cette fonctionnalité.

***R14*** Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle.

***R17*** Configurer le point d’accès pour que les évènements de sécurité puissent être supervisés. En environnement professionnel.

il est préférable de rediriger l’ensemble des évènements générés par les points d’accès vers une infrastructure centrale de supervision.

***R19*** Ne jamais sous-estimer la zone de couverture d’un réseau WiFi. Ne jamais penser être à l’abri de tout risque du fait de l’isolement géographique du point d’accès WiFi.

***R20*** En environnement professionnel, isoler le réseau WiFi du réseau filaire et mettre en place des équipements de filtrage réseau permettant l’application de règles strictes et en adéquation avec les objectifs de sécurité de l’organisme.

Comme pour le point d’accès, l’équipement de filtrage doit être paramétré pour que puissent être supervisés les évènements de sécurité.

***R21*** Si un réseau WiFi "visiteurs" doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive.

***R23*** Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au WiFi par GPO (nom de réseau, clé d’accès, certificats éventuels si la méthode EAP le nécessite, etc.).