ASSURMER

INSTALLATION ET CONFIGURATION DU RDS

PROCEDURE

Date de création : 22/10/2023

Version : 1.0

Pour validation : DSI

A destination : DSI

Mode de diffusion : Sharepoint

Nombre de page totale : 33

Sommaire

I. Les différents protocoles de sécurité WIFI

Il existe plusieurs protocoles de sécurité WiFi qui sont utilisés pour protéger les réseaux sans fil contre les accès non autorisés. Voici quelques-uns des principaux protocoles de sécurité WiFi :

WEP (Wired Equivalent Privacy) : C'était l'un des premiers protocoles de sécurité WiFi, mais il est maintenant largement obsolète en raison de ses vulnérabilités. Il est fortement déconseillé de l'utiliser.

WPA (Wi-Fi Protected Access) : WPA est une amélioration de WEP et propose des mécanismes de chiffrement plus robustes. Cependant, il existe différentes versions de WPA, telles que WPA, WPA2 et WPA3, chacune améliorant la sécurité par rapport à la précédente.

WPA2 (Wi-Fi Protected Access 2) : WPA2 est actuellement le protocole de sécurité le plus largement utilisé pour les réseaux WiFi. Il utilise le chiffrement AES (Advanced Encryption Standard) pour assurer une sécurité plus forte par rapport à WPA.

WPA3 (Wi-Fi Protected Access 3) : WPA3 est la dernière norme de sécurité WiFi, introduite pour améliorer encore la sécurité. Il offre des fonctionnalités telles que le chiffrement individuel des données, la protection contre les attaques par force brute, et d'autres améliorations par rapport à WPA2.

II. Avantages et inconvénients

A. WEP

Le protocole WEP (Wired Equivalent Privacy) était l'un des premiers protocoles de sécurité utilisés pour protéger les réseaux sans fil. Cependant, il est aujourd'hui largement obsolète en raison de ses nombreuses vulnérabilités. Voici quelques-uns de ses avantages et inconvénients

Avantages du WEP :

- Facilité de configuration : WEP était relativement facile à configurer, ce qui en faisait un choix attrayant pour les utilisateurs peu expérimentés.
- Compatibilité : Étant l'un des premiers protocoles de sécurité WiFi, le WEP a été largement pris en charge par de nombreux périphériques et routeurs plus anciens.

Inconvénients majeurs du WEP :

- Vulnérabilités de sécurité : Le WEP a des vulnérabilités majeures qui le rendent extrêmement faible face aux attaques. Des méthodes de craquage relativement simples, telles que l'attaque par fragmentation, permettaient à des attaquants de récupérer la clé de chiffrement WEP en peu de temps.
- Manque de confidentialité : Les clés WEP sont statiques et peuvent être facilement interceptées, compromettant ainsi la confidentialité des données transmises sur le réseau.

- Changement de clé manuel : Pour renforcer la sécurité, il était recommandé de changer régulièrement les clés WEP. Cependant, cela était souvent fastidieux et peu pratique, ce qui conduisait souvent à l'utilisation de clés statiques pendant de longues périodes.
- Absence d'authentification robuste : WEP ne propose pas d'authentification robuste des périphériques, ce qui signifie que même si un périphérique parvient à se connecter au réseau, il peut être difficile de garantir son identité.

B. WPA

Le WPA1 (Wi-Fi Protected Access 1) est également obsolète et a été remplacé par des versions plus sécurisées, comme WPA2 et WPA3. Cependant, voici quelques-uns des avantages et inconvénients associés au WPA1 :

Avantages du WPA1 :

- Meilleure sécurité que le WEP : Comme le WPA1 a été introduit pour remédier aux vulnérabilités du WEP, il offre une amélioration significative en termes de sécurité par rapport à son prédécesseur.
- Utilisation de TKIP : Le WPA1 utilise le protocole de chiffrement Temporal Key Integrity Protocol (TKIP), qui était considéré comme plus robuste que le WEP. TKIP a introduit des mécanismes pour renforcer la sécurité des clés de chiffrement.
- Authentification 802.1X : Comme le WPA1 prend en charge l'authentification 802.1X, il offre une méthode d'authentification plus avancée, notamment adaptée aux réseaux d'entreprise.

Inconvénients du WPA1 :

- Sensibilité aux attaques par force brute : Comme le WPA1 utilise une clé pré-partagée (PSK), il reste sensible aux attaques par force brute si des clés faibles ou prévisibles sont utilisées.
- Vulnérabilité de TKIP : Bien que TKIP ait offert une amélioration par rapport au WEP, il a également montré des vulnérabilités au fil du temps, ce qui a conduit à l'introduction ultérieure de WPA2.
- Obsolescence face à WPA2 : Avec l'introduction de WPA2, le WPA1 est devenu obsolète en matière de sécurité. WPA2 a introduit des améliorations significatives, notamment l'utilisation du chiffrement AES (Advanced Encryption Standard), offrant une sécurité plus robuste.

Il est fortement recommandé de ne pas utiliser le WPA1 et de mettre à niveau vers des protocoles plus récents, tels que WPA2 ou WPA3, pour garantir une sécurité optimale pour votre réseau sans fil.

C. WPA2

Bien que WPA2 ait été largement utilisé et soit encore en service dans de nombreux environnements, la transition vers WPA3 est recommandée pour bénéficier des dernières avancées en matière de sécurité WiFi.

Avantages du WPA2 :

- Chiffrement robuste : WPA2 utilise le chiffrement Advanced Encryption Standard (AES), qui est considéré comme plus robuste et sécurisé que les protocoles utilisés dans le WPA1.
- Protection contre les attaques par force brute : WPA2 intègre des mécanismes de protection contre les attaques par force brute, ce qui rend plus difficile pour les attaquants de deviner ou de craquer la clé de sécurité.
- Authentification 802.1X : WPA2 prend en charge l'authentification 802.1X, offrant une méthode d'authentification plus robuste, particulièrement adaptée aux environnements d'entreprise.
- Résistance aux attaques de rejeu : WPA2 inclut des mécanismes pour résister aux attaques de rejeu, renforçant ainsi la sécurité des échanges de données sur le réseau sans fil.
- -Compatibilité avec des anciens périphériques : WPA2 a été conçu pour être compatible avec les anciens périphériques prenant en charge WPA, facilitant ainsi la transition vers un protocole de sécurité plus avancé.

Inconvénients du WPA2 :

- Vulnérabilités possibles : Bien que WPA2 soit considéré comme très sécurisé, des vulnérabilités, telles que la faille de sécurité KRACK (Key Reinstallation Attacks), ont été découvertes en 2017. Les correctifs ont été mis en place, mais cela souligne la nécessité de maintenir le firmware des périphériques à jour.
- Limitations de l'authentification PSK : Lors de l'utilisation de WPA2 avec une clé pré-partagée (PSK), il reste sensible aux attaques par force brute si des clés faibles ou prévisibles sont utilisées.
- Obsolescence face à WPA3 : Avec l'introduction de WPA3, WPA2 peut être considéré comme obsolète en termes de sécurité. WPA3 apporte des améliorations supplémentaires pour répondre aux nouvelles menaces et renforcer la sécurité des réseaux sans fil.

D. WPA3

Le WPA3 (Wi-Fi Protected Access 3) représente une évolution significative des protocoles de sécurité WiFi par rapport au WEP, WPA1, et WPA2. Voici une liste des avantages et inconvénients associés au protocole de sécurité WPA3 :

Avantages du WPA3 :

- Chiffrement plus fort : WPA3 utilise le chiffrement de données individuel (Individual Data Encryption, IAE), offrant un niveau de confidentialité plus élevé en chiffrant chaque connexion entre les périphériques du réseau sans fil.
- Protection contre les attaques par force brute : WPA3 renforce la protection contre les attaques par force brute en imposant des limitations sur le nombre de tentatives d'authentification, ce qui rend plus difficile pour les attaquants de deviner ou de craquer la clé de sécurité.
- Protection contre les attaques de dictionnaire : WPA3 résiste davantage aux attaques de dictionnaire en utilisant un protocole appelé Simultaneous Authentication of Equals (SAE), qui protège contre les attaques de type offline.

- Sécurité accrue pour les réseaux ouverts : WPA3 propose des améliorations pour les réseaux ouverts, où il peut utiliser le protocole Opportunistic Wireless Encryption (OWE) pour chiffrer les communications, même sans authentification.
- Protection de la confidentialité des réseaux publics : WPA3 propose des améliorations pour la confidentialité des réseaux publics en introduisant le protocole Enhanced Open, qui sécurise davantage les communications.

Inconvénients potentiels du WPA3 :

- Compatibilité avec les anciens périphériques : Certains périphériques plus anciens pourraient ne pas prendre en charge WPA3. Cependant, de nombreux périphériques récents prennent en charge WPA3, et la prise en charge devrait augmenter à l'avenir.
- Mise à jour du matériel nécessaire : La mise en œuvre complète de WPA3 peut nécessiter une mise à jour matérielle, et tous les appareils ne pourront peut-être pas bénéficier de toutes les fonctionnalités de sécurité sans une mise à jour matérielle appropriée.
- Lente adoption : Bien que WPA3 représente une amélioration significative en matière de sécurité, son adoption peut être lente, en particulier dans les environnements où les dispositifs plus anciens sont toujours utilisés.

En résumé, WPA3 offre des améliorations substantielles en matière de sécurité par rapport aux versions précédentes, mais il peut y avoir des considérations de compatibilité et d'adoption à prendre en compte lors de sa mise en œuvre.

III. Différence WPA personnel / WPA entreprise

WPA2 personnel / WPA2 entreprise se réfèrent généralement aux deux modes d'utilisation principaux de WPA2.

1. **WPA2-Personnel (WPA2-PSK - Wi-Fi Protected Access 2 - Pre-Shared Key)** : Il s'agit du mode de sécurité dans lequel une clé pré-partagée (pre-shared key, PSK) est utilisée pour authentifier les périphériques sur le réseau. Cette clé est généralement partagée entre tous les périphériques autorisés qui se connectent au réseau.

2. **WPA2-Entreprise** : Ce mode utilise généralement le protocole 802.1X (EAP) pour l'authentification des utilisateurs. Contrairement à WPA2-Personnel, WPA2-Entreprise nécessite un serveur d'authentification externe, tel qu'un serveur RADIUS (Remote Authentication Dial-In User Service). Chaque utilisateur a des identifiants uniques, et l'authentification est gérée de manière centralisée.

L'utilisation de WPA2-Personnel est plus courante dans les environnements domestiques et de petites entreprises, car il est plus simple à configurer. En revanche, WPA2-Entreprise est souvent utilisé dans les grandes entreprises et les institutions qui nécessitent une gestion centralisée des utilisateurs et une sécurité renforcée.