Sécurité

Dans le cadre du projet IRS-SI, j'ai appliqué plusieurs recommandations de sécurité sur l'ensemble des services déployés.

1) Isolation réseau par VLAN

Le réseau visiteurs est isolé sur le VLAN 40 (192.168.10.192/27), séparé du LAN interne. Un visiteur connecté au SSID `Visiteurs-IRS` ne peut pas accéder aux ressources internes de l'entreprise.

2) Sécurité Wi-Fi

Le protocole WPA2 Personal a été retenu pour le réseau Wi-Fi visiteurs. Le protocole WEP, vulnérable aux attaques par dictionnaire, a été écarté. Le portail captif NoDogSplash ajoute une couche de contrôle supplémentaire en imposant une validation avant tout accès à internet. Son déploiement répond également à une obligation légale : en France, toute entreprise proposant un accès Wi-Fi visiteur doit conserver les logs de connexion pendant un an (LCEN).

3) Supervision sécurisée (SNMPv3)

La supervision des équipements réseau utilise SNMPv3 avec authentification SHA1 et chiffrement DES. Les versions SNMPv1 et SNMPv2c, qui transmettent les données en clair, ont été écartées. SHA1 et DES sont imposés par les capacités du firmware 1.1.4.0 du WAP150, dans un contexte où le remplacement du matériel serait possible, SHA-256 et AES-128 seraient recommandés.

4) Sécurité VoIP

L'accès au serveur Asterisk est restreint au VLAN 99 (LAN VMs). Chaque extension PJSIP est protégée par un mot de passe défini dans `pjsip.conf`. L'administration des VMs se fait exclusivement via SSH, évitant tout accès non chiffré.

5) Mises à jour

Les systèmes Debian 12 des trois VMs ont été mis à jour lors de leur déploiement. Le firmware du WAP150 a été mis à jour vers la version 1.1.4.0 pour corriger un bug de persistance des credentials SNMPv3.

Revision #3
Created 21 May 2026 10:08:06 by Mathéo
Updated 29 May 2026 08:54:26 by Mathéo