04 - Sécurité

1) Choix du protocole de chiffrement Wi-Fi

L'un des premiers choix à effectuer pour sécuriser un réseau sans fil est le protocole de chiffrement. Contrairement aux réseaux filaires, les ondes radio se propagent au-delà des murs et peuvent être captées par tout équipement situé à portée. Sans chiffrement, toutes les données échangées seraient lisibles en clair par n'importe quel observateur passif.

Quatre générations de protocoles existent. Le tableau suivant les compare afin de justifier le choix retenu pour le projet IRS-SI.

Protocole	Chiffrement	Authentification	Niveau sécurité	Statut
WEP (1999)	**RC4 – 40/104 bits**	**Clé partagée**	**Très faible**	**Obsolète**
WPA-TKIP (2003)	**RC4 + TKIP**	**PSK / 802.1X**	**Faible**	**Déprécié**
WPA2-AES (2004)	**AES-CCMP 128 bits**	**PSK / 802.1X**	**Bon**	**Retenu ?**
WPA3-SAE (2018)	**AES-CCMP + SAE**	**SAE / 802.1X**	**Excellent**	**Non supporté**

WEP — Wired Equivalent Privacy (1999)
WEP est le premier protocole de sécurité Wi-Fi standardisé. Il utilise l'algorithme de chiffrement RC4 avec des clés de 40 ou 104 bits. Dès 2001, des chercheurs ont démontré que le vecteur d'initialisation (IV) de seulement 24 bits est réutilisé trop rapidement, ce qui permet à un attaquant de retrouver la clé en quelques minutes avec des outils comme aircrack-ng. WEP est formellement interdit dans tout réseau professionnel depuis 2004.

> Attention : WEP ne doit jamais être utilisé. Même un réseau sans données sensibles peut servir de point d'entrée vers l'infrastructure interne.

WPA-TKIP — Wi-Fi Protected Access (2003)
WPA avec TKIP a été conçu comme solution transitoire dans l'attente de WPA2. Il corrige les failles de WEP en ajoutant un compteur de séquence de trames et en renouvelant dynamiquement les clés. Cependant, des attaques de type TKIP MIC ont été publiées dès 2008, puis l'attaque Beck-Tews (2009) a permis de déchiffrer des paquets courts. WPA-TKIP est déprécié depuis 2012 par le standard 802.11.

WPA2-AES-CCMP — Protocole retenu pour le projet
WPA2 utilise le chiffrement AES (Advanced Encryption Standard) en mode CCMP (Counter Mode with CBC-MAC Protocol), avec des clés de 128 bits. AES est un algorithme symétrique standardisé par le NIST en 2001 et n'a à ce jour fait l'objet d'aucune attaque pratique sur des implémentations correctes. WPA2 est le standard de facto dans les environnements professionnels depuis 2006.

> Bonne pratique : WPA2-Personal avec AES-CCMP est retenu pour le SSID Visiteurs-IRS. Ce choix offre un niveau de sécurité adapté à un réseau invités tout en étant compatible avec l'ensemble des terminaux mobiles actuels.

WPA3-SAE — Évolution non déployée
WPA3, introduit en 2018, remplace l'échange de clé PSK par le protocole SAE (Simultaneous Authentication of Equals), basé sur l'échange Diffie-Hellman. SAE élimine les attaques par dictionnaire hors ligne sur le mot de passe, car chaque tentative d'authentification nécessite une interaction réseau. WPA3 n'est pas supporté par le firmware 1.1.4.0 du Cisco WAP150 et ne peut donc pas être déployé dans le cadre actuel du projet.

2) Authentification et contrôle d'accès

Le contrôle d'accès au réseau Wi-Fi repose sur deux mécanismes complémentaires : l'authentification au niveau du protocole Wi-Fi (WPA2-PSK) et le contrôle applicatif via le portail captif NoDogSplash, qui intervient après l'association au réseau.

WPA2 Personal (PSK) - Premier niveau

En mode WPA2-Personal, un mot de passe commun (Pre-Shared Key) est configuré sur le point d'accès. Tous les clients doivent le connaître pour s'associer au SSID. Cette méthode est adaptée à

un réseau visiteurs où les terminaux sont variés et non gérés par l'entreprise.

La clé PSK subit une dérivation cryptographique PBKDF2-HMAC-SHA1 avec 4096 itérations pour produire la PMK (Pairwise Master Key) de 256 bits. Cette PMK n'est jamais transmise sur le réseau.

Politique appliquée au mot de passe Wi-Fi

Critère	Règle appliquée
Longueur minimale	12 caractères
Composition	Majuscules + minuscules + chiffres
Durée de validité	Renouvellement mensuel recommandé
Diffusion	Via le portail captif après validation de l'identité
Stockage	Hash PBKDF2 côté WAP150, jamais en clair

Portail captif NoDogSplash - Second niveau de contrôle

Le portail captif constitue le deuxième niveau d'authentification. Même si un visiteur connaît le mot de passe WPA2, ses requêtes HTTP sont interceptées par la VM NoDogSplash jusqu'à ce qu'il accepte les conditions d'utilisation sur la page du portail.

Flux d'authentification

Le flux complet d'un client visiteur se déroule en cinq étapes :

1. Association Wi-Fi : le terminal se connecte au SSID Visiteurs-IRS avec le mot de passe WPA2.
2. Obtention d'une adresse IP : le serveur DHCP du VLAN 40 attribue une adresse dans la plage 192.168.10.196–222/27.
3. Interception HTTP : NoDogSplash redirige toute requête HTTP vers sa page d'accueil (port TCP 2050).
4. Validation : le visiteur accepte les conditions d'utilisation sur le portail.
5. Accès autorisé : NoDogSplash lève le blocage et laisse passer le trafic du client vers internet.

3) Isolation et segmentation réseau

La segmentation réseau est le principe de défense qui consiste à diviser l'infrastructure en zones étanches. Même si un attaquant pénètre dans l'une d'elles, il ne peut pas accéder aux autres sans franchir des contrôles supplémentaires.

Isolation des clients Wi-Fi

L'isolation des clients interdit toute communication directe entre les terminaux connectés au même SSID. Sans cette mesure, deux visiteurs sur le même réseau pourraient s'attaquer mutuellement via des techniques comme l'ARP spoofing ou le scan de ports.

Lorsque l'isolation est activée sur le WAP150, le point d'accès bloque au niveau de la couche 2 (Ethernet) tout échange de trames entre clients. Un client ne peut envoyer des trames qu'en direction de la passerelle par défaut (la VM NoDogSplash, 192.168.10.194). Les trames destinées à d'autres clients sont silencieusement supprimées par le WAP150.

Segmentation par VLAN 40

Le réseau Wi-Fi visiteurs est entièrement isolé du réseau de production par l'utilisation du VLAN 40. Ce VLAN est dédié exclusivement aux clients sans fil et n'est pas routé vers les VLAN internes (VLAN 10 Gestion, VLAN 20 Administration, VLAN 30 Commercial, etc.).

VLAN	Usage	Réseau	Accès depuis VLAN 40
VLAN 10	**Gestion**	**192.168.10.0/27**	**Interdit**
VLAN 20	**Administration**	**192.168.10.32/27**	**Interdit**
VLAN 30	**Commercial**	**192.168.10.64/27**	**Interdit**
VLAN 40	**Wi-Fi visiteurs**	**192.168.10.192/27**	**Natif — DHCP 196-222**
VLAN 99	**LAN VMs / gestion**	**192.168.10.128/26**	**Interdit (sauf passerelle)**

Le routeur Cisco ISR 4321 est configuré pour bloquer tout routage inter-VLAN depuis le VLAN 40 vers les VLAN de production. Seul le trafic à destination d'internet (ou des ressources explicitement autorisées) est permis après validation sur le portail captif.

Rôle de la VM NoDogSplash comme point de contrôle unique

La VM NoDogSplash (Debian 12) est le seul point de transit entre le VLAN 40 (Wi-Fi visiteurs) et le reste du réseau. Son architecture réseau est la suivante :

Interface VM	VLAN	Adresse IP	Rôle
ens18	VLAN 99	Adresse DHCP	Gestion / supervision Zabbix
ens19	VLAN 40	192.168.10.194/27	Passerelle des clients Wi-Fi

Les clients Wi-Fi utilisent 192.168.10.194 comme passerelle par défaut. Tout leur trafic transite obligatoirement par la VM, qui peut ainsi appliquer des règles iptables pour filtrer ou journaliser les connexions avant de les transmettre.

3) Supervision

La supervision permet de détecter des comportements anormaux (saturation de la bande passante, nombre inhabituel de clients associés, perte de connectivité) et d'alerter l'administrateur avant qu'un incident ne se transforme en incident de sécurité majeur.

Choix de SNMPv3

Le protocole SNMP (Simple Network Management Protocol) est le standard de supervision des équipements réseau. Trois versions coexistent, avec des niveaux de sécurité très différents :

Version	Authentification	Chiffrement	Recommandation
SNMPv1	**Community string en clair**	**Aucun**	**À proscrire**
SNMPv2c	**Community string en clair**	**Aucun**	**Déconseillé**
SNMPv3 noAuthNoPriv	**Utilisateur, sans auth**	**Aucun**	**Insuffisant**
SNMPv3 authNoPriv	**SHA-1 ou MD5**	**Aucun**	**Acceptable**
SNMPv3 authPriv	**SHA-1**	**DES / AES**	**Retenu ?**

SNMPv1 et v2c transmettent le nom de communauté (équivalent d'un mot de passe) en clair sur le réseau. Un simple sniffeur (Wireshark) suffit à l'intercepter et à prendre le contrôle de l'équipement. SNMPv3 en mode authPriv apporte une authentification forte par HMAC-SHA1 et un chiffrement du contenu des échanges par DES ou AES.

Configuration SNMPv3 appliquée

Paramètre	Valeur configurée
Utilisateur SNMP	zabbix
Niveau de sécurité	authPriv (authentification + chiffrement)
Protocole authentification	SHA-1 (HMAC)
Protocole chiffrement	DES (Data Encryption Standard)
Mot de passe auth	Zabbix123 (à renforcer en production)
Mot de passe chiffrement	Zabbix123 (à renforcer en production)
Version SNMP côté Zabbix	SNMPv3
OID supervisés	ifInOctets, ifOutOctets, ifOperStatus, sysUpTime

Revision #7
Created 24 March 2026 09:35:14 by Mathéo
Updated 9 June 2026 17:18:17 by Mathéo