Mode Opératoire

Architecture du Wi-Fi pédagogique 802.1X, VLANs, portail captif et SSO

Code :	MO-NET-008
Version :	1.0
Date :	10 septembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	10/09/2026	Création initiale, validée par la mise en production effective des deux SSID (tests d'authentification, de session SSO et d'isolement réseau le 10/09/2026).

1 Objet

Ce mode opératoire documente l'**architecture complète du Wi-Fi pédagogique** du BTS SIO, mise en production le 10 septembre 2026. Il est écrit pour qu'un administrateur découvrant l'infrastructure — par exemple un collègue en l'absence de l'auteur — puisse **comprendre, exploiter, dépanner et, au besoin, reconstruire** la chaîne de bout en bout.

L'architecture répond à quatre exigences posées par l'équipe pédagogique :

— **Deux réseaux sans fil disjoints** : un pour les étudiants, un pour les professeurs (un seul chacun) ;

— **authentification individuelle** : chaque utilisateur se connecte avec son compte Active Directory — pas de mot de passe Wi-Fi partagé ;

— **simplicité d'usage** : aucune page de connexion supplémentaire une fois authentifié (ouverture de session Internet transparente, dite *SSO*) ;

— **isolation** : le réseau des étudiants n'a accès qu'à Internet et aux services qui l'y autorisent, pas aux ressources internes.

Les briques mises en jeu sont : les bornes UniFi et leur contrôleur (MO-NET-006), le serveur RADIUS **NPS** du contrôleur de domaine (802.1X / PEAP-MSCHAPv2), la segmentation **VLAN 240/241** sur les commutateurs (MO-NET-003), les services d'adressage, filtrage et portail captif du pare-feu **OPNsense** (MO-NET-004), et un collecteur **RSSO** (FreeRADIUS) qui ouvre automatiquement les sessions du portail captif à la réception de l'accounting 802.1X.

2 Champ d'application

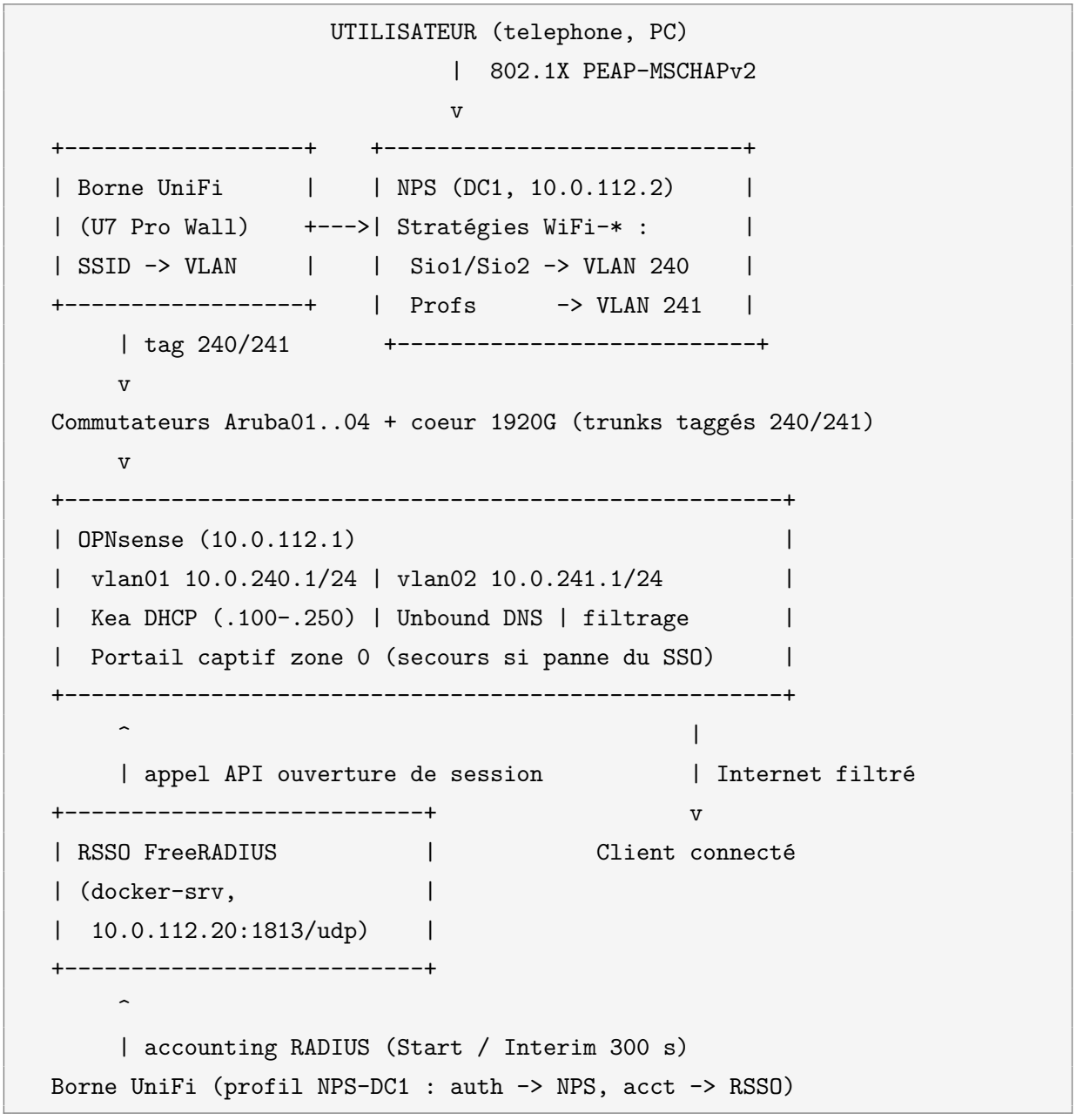
Public concerné	Administrateurs de l'infrastructure BTS SIO
SSID étudiants	`BTS SIO Etudiants` → VLAN 240, sous-réseau `10.0.240.0/24`
SSID professeurs	`BTS SIO Profs` → VLAN 241, sous-réseau `10.0.241.0/24`
Bornes déployées	`BTSSIOI109` (`10.0.230.2`), `BTSSIOI110` (`10.0.230.3`), `BTSSIOI111` (`10.0.230.5`) — salles i109, i110, i111
Population autorisée	Groupes AD `GGPromoSio1`, `GGPromoSio2` (étudiants) et `GGProfs`
Composants	UniFi Network 10.6 (MO-NET-006), NPS sur DC1, 6 commutateurs, OPNsense 26.7, FreeRADIUS 3.2.10
Classification	Usage interne — contient des identifiants techniques (aucun secret)

Aucun secret dans ce document

Les secrets (mots de passe, clés API, secret RADIUS partagé) sont tous référencés par leur entrée dans le coffre Vaultwarden de l'équipe (`https://10.0.112.10`), jamais recopiés ici. La liste précise figure en annexe A.

3 Vue d'ensemble de l'architecture

3.1 Schéma fonctionnel



3.2 Le cycle de vie d'une connexion

1. **Association 802.1X** : le client choisit le SSID et saisit son identité AD (`p.nom` + mot de passe) dans la boîte de dialogue du système. La borne relaie l'authentification vers NPS (PEAP-MSCHAPv2), qui valide le mot de passe auprès de l'AD et l'appartenance au groupe autorisé, et renvoie l'attribut VLAN (240 ou 241).
2. **Adressage** : la borne marque le trafic du client avec le VLAN correspondant. Le client émet une requête DHCP qui aboutit au service **Kea** d'OPNsense sur l'interface du VLAN ; il reçoit une adresse en `10.0.24x.100-250`, passerelle et DNS = l'adresse d'OPNsense du VLAN.
3. **Ouverture de session SSO** : la borne envoie en parallèle un paquet *Accounting-Request Start* au collecteur RSSO. Celui-ci appelle l'API OPNsense (`/api/captiveportal/session/c` avec le nom d'utilisateur et l'IP : la **session du portail captif s'ouvre sans aucune saisie supplémentaire**.
4. **Navigation** : le trafic du client traverse les règles de filtrage du VLAN (isolation pour les étudiants, accès complet pour les professeurs).
5. **Maintien et fin** : la borne émet un accounting *Interim-Update* toutes les 300 s. À la déconnexion, la session du portail expire (délai d'inactivité 60 min, durée maximale 8 h).

Et si le collecteur RSSO tombe en panne ?

Les clients nouvellement connectés voient alors la page du portail captif et s'y authentifient avec leur compte AD (validé par NPS en PAP via la stratégie `WiFi-Portail`). Le service est dégradé, pas interrompu : c'est le rôle de secours du portail.

3.3 Choix de conception

Option écartée	Raison du choix actuel
Mot de passe Wi-Fi partagé (PSK)	Aucune traçabilité individuelle, fuite irréversible, contraire aux recommandations ANSSI.
Portail captif seul (SSID ouvert)	Trafic radio non chiffré, association libre pour tout intrus à portée, identifiants AD exposés si la page n'est pas en HTTPS.
802.1X seul, sans portail	Fonctionne, mais sans point d'application du filtrage ni de la traçabilité de session par utilisateur.
802.1X + portail + RSSO (retenu)	Chiffrement WPA2/WPA3 par client, authentification AD, session filtrée ouverte automatiquement (SSO), portail en secours.

4 Composants détaillés

4.1 Contrôleur UniFi et bornes

Le contrôleur UniFi Network (MO-NET-006, `https://unifi.docker.bts.sio`) héberge la configuration sans fil. Objets en production :

Objet	Valeur	Détail
WLAN	`BTS SIO Etudiants`	WPA2/WPA3-Enterprise (transition), réseau `wifi-etudiants` (VLAN 240)
WLAN	`BTS SIO Profs`	idem, réseau `wifi-profs` (VLAN 241)
Réseaux	`wifi-etudiants` / `wifi-profs`	type *VLAN only*, tags 240 / 241
Profil RADIUS	`NPS-DC1`	auth `10.0.112.2:1812` (NPS), accounting `10.0.112.20:1813` (RSSO), interim 300 s
Groupe de bornes	*All APs*	les deux SSID sont émis par les 3 bornes

Le secret partagé entre les bornes et NPS (auth) ainsi qu'entre les bornes et le RSSO (accounting) est unique : entrée coffre « Wifi BTS SIO — Secret RADIUS bornes UniFi ». Les identifiants techniques (UUID) de ces objets figurent en annexe A.

API du contrôleur

L'authentification API se fait par `POST /api/login` (et non `/api/auth/login`, qui renvoie 401 sur cette version auto-hébergée). Compte administrateur en coffre (« UniFi Network Controller (docker-srv) »).

4.2 Active Directory, ADCS et NPS

Trois rôles sur le contrôleur de domaine `DC1` (`10.0.112.2`, `srv2022.bts.sio`) :

ADCS L'autorité « BTS SIO Root CA » (RSA 4096, valide jusqu'en 2036) émet les certificats de service. Elle est **publiée dans l'AD** : les postes du domaine la reconnaissent de confiance, ce qui rend la validation du certificat RADIUS transparente sur ces postes.

Certificat de serveur NPS présente un certificat émis par cette CA (`CN=Srv2022.bts.sio`). La validation côté client exige la CA « BTS SIO Root CA » et le domaine `bts.sio`.

NPS Quatre stratégies de réseau, évaluées dans l'ordre :

Stratégie	Ordre	Condition	Effet
`WiFi-Etudiants-Sio1`	1	Membre de `GGPromoSio1`	grant + Tunnel-Pvt-Group-ID `240`
`WiFi-Etudiants-Sio2`	2	Membre de `GGPromoSio2`	grant + `240`
`WiFi-Profs`	3	Membre de `GGProfs`	grant + `241`
`WiFi-Portail`	4	Les 3 groupes, méthode **PAP**	grant (authentification du portail de secours)

Les clients RADIUS déclarés sont les trois bornes (`BTSSIOI109/I110/I111`) et `OPNsense-Portail` (`10.0.112.1`), avec le même secret partagé qu'en 4.1. Tout compte AD hors des trois groupes est rejeté (*fail-closed*) : c'est notamment le cas des comptes TSTMG (groupe `GGSig`), volontairement exclus du Wi-Fi.

4.3 Commutation : le chemin des VLANs

Les VLANs 240 (`wifi-etudiants`) et 241 (`wifi-profs`) sont créés sur les cinq commutateurs Aruba et le commutateur cœur HP 1920G. Le chemin physique entre les bornes et le pare-feu a été établi par LLDP et tables d'adresses MAC :

```
i111 : borne -> Aruba04 p10 -> Aruba04 p27 -> Aruba03 p26 -> Aruba03 p27
     -> Aruba02 p26 -> Aruba02 p27 -> Aruba01 p28 -> Aruba01 p24 -> OPNsense
i109 : borne -> Aruba01 p5  --\
i110 : borne -> Aruba01 p22 --+-> Aruba01 p28 -> (meme suite)
```

Commutateur	IP	Ports tagués 240+241 (rôle)
SwitchAruba01	`10.0.112.221`	p5 (borne i109), p22 (borne i110), p24 (OPNsense), p28 (vers Aruba02)
SwitchAruba02	`10.0.112.222`	p26 (vers Aruba03), p27 (vers Aruba01)
SwitchAruba03	`10.0.112.223`	p26 (vers Aruba04), p27 (vers Aruba02)
SwitchAruba04	`10.0.112.224`	p10 (borne i111), p20 (vers cœur), p27 (vers Aruba03)
Cœur HP 1920G	`10.0.112.213`	GE1/0/9 (vers Aruba04)

Tous ces ports conservent le VLAN 1 en *untagged* (continuité du réseau plat actuel) ; le marquage 240/241 est purement additif. La procédure générique de gestion des VLANs est décrite dans MO-NET-003 ; la création des interfaces VLAN du pare-feu dans MO-NET-004.

Chaînage fragile

Le chemin compte jusqu'à quatre commutateurs en cascade. Toute modification de câblage entre ces commutateurs casse le Wi-Fi pédagogique (symptôme type : association 802.1X réussie mais pas de DHCP). En cas de recâblage, reporter le marquage 240/241 sur les nouveaux ports et vérifier de proche en proche avec les tables MAC (section 7).

4.4 Pare-feu OPNsense

Quatre services sur `10.0.112.1` (v26.7) :

Interfaces `opt1` = `vlan01` (tag 240) **WIFIETUDIANTS** `10.0.240.1/24` ; `opt2` = `vlan02` (tag 241) **WIFIPROFS** `10.0.241.1/24`.

Kea DHCP actif sur les deux interfaces : pools `.100-.250`, passerelle et DNS = adresse de l'interface, bail 8 h.

Unbound DNS écoute globale ; résout pour les deux VLANs. Le DNS **système** du pare-feu pointe sur `10.0.112.2` (DC1), et une entrée statique Unbound (*host override*) relie `srv2022.bts.sio` à DC1.

Filtrage VLAN 240 (étudiants) : autoriser DNS vers le pare-feu, autoriser le portail (TCP 8000–8001), **bloquer tout destination RFC1918** (alias), autoriser le reste (Internet). VLAN 241 (professeurs) : tout autoriser.

Portail captif zone `0` sur les deux interfaces, authentification **RADIUS** (`NPS-DC1`, PAP), délai d'inactivité 60 min, durée maximale 8 h, connexions simultanées illimitées.

Un compte de service **svc-rsso** (privilège « Services : Captive Portal » uniquement) détient la clé API utilisée par le collecteur RSSO ; la clé et le secret sont en coffre (« OPNsense — svc-rsso (API portail captif) »).

4.5 Collecteur RSSO (FreeRADIUS)

Le collecteur est une stack Docker sur `docker-srv` (`/opt/docker/rsso`, image `freeradius/freeradi` `server:3.2.10`, port 1813/udp publié sur l'hôte `10.0.112.20`). Son unique fonction : à la réception d'un *Accounting-Request Start* ou *Interim-Update* contenant un nom d'utilisateur et une IP, appeler l'API OPNsense pour ouvrir la session du portail captif.

Fichiers de configuration (montés par fichier dans le conteneur) :

— `.env` : `RADSECRET` (secret partagé des bornes), `OPN_API_KEY`/`OPN_API_SECRET` (clé svc-rsso), `OPN_ZONE=0` ;

— `raddb/clients.conf` : clients autorisés = `localhost` et `10.0.230.0/24` (les bornes) ;

— `raddb/mods-enabled/rest` : module `rlm_rest` — POST vers `/api/captiveportal/session/conne` avec `data = "user=%{User-Name}&ip=%{Framed-IP-Address}"` en authentification basic (clé API) ;

— `raddb/sites-enabled/default` : section accounting déclenchant l'appel sur Start/Interim-Update, réponse systématique au NAS.

Pièges connus du module rest

Le template `%{urlencode:...}` n'est pas supporté par le build FreeRADIUS utilisé : ne pas le réintroduire (les identifiants AD sont déjà URL-sûrs). Et `docker run -env-file` ne supprime pas les guillemets des valeurs (contrairement à `docker compose`) : pour un lancement de debug à la main, utiliser un fichier d'environnement sans guillemets.

5 Mise en service initiale (rappel de l'ordre des phases)

La construction s'est faite dans l'ordre suivant, qui est aussi l'ordre de reconstruction. Chaque phase renvoie au MO dédié lorsqu'il existe :

1 Socle d'authentification (AD)

Créer l'autorité ADCS « BTS SIO Root CA » sur DC1, installer le rôle NPS, émettre le certificat de serveur (`CN=Srv2022.bts.sio`), créer les stratégies de réseau (ordre, groupes, attributs VLAN, PEAP-MSCHAPv2) et les clients RADIUS des bornes.

2 Contrôleur UniFi

Déployer la stack (MO-NET-006), adopter les bornes (réinitialisation physique préalable si elles sont gérées par une autre console), créer les réseaux *VLAN only* 240/241 et le profil RADIUS `NPS-DC1` (auth vers NPS, accounting vers le RSSO).

3 Commutation

Créer les VLANs 240/241 sur tous les commutateurs et marquer en *tagged* tous les ports du chemin bornes → OPNsense (table de la section 4.3), en conservant le VLAN 1 untagged. Sauvegarder

chaque configuration (MO-NET-003).

4 **Pare-feu**

Créer les VLANs sur l'interface LAN d'OPNsense, les assigner en interfaces opt1/opt2 avec adresses statiques, appliquer les changements, activer Kea sur ces interfaces, configurer les règles de filtrage, créer le serveur d'authentification RADIUS et la zone de portail captif (MO-NET-004), créer l'utilisateur API svc-rsso et sa clé.

5 **Collecteur RSSO**

Déployer la stack FreeRADIUS avec le `.env` réel, vérifier le traitement d'un *Accounting-Request* de test (procédure de la section 7), puis basculer l'accounting du profil RADIUS UniFi vers le collecteur.

6 **Bascule et validation**

Mapper les WLAN sur les réseaux VLAN, créer le SSID professeurs, et valider avec deux comptes de test (un étudiant, un professeur) : authentification, adressage dans le bon VLAN, session SSO automatique, accès Internet, isolement.

6 Exploitation courante

6.1 Vérifier l'état de santé (5 minutes)

Vérification

- ☐ **Contrôleur UniFi : les 3 bornes sont *Connected* (UI → Devices).**
- ☐ **OPNsense → Services : Kea et Unbound *running* ; Services → Captive Portal → Sessions : les utilisateurs connectés apparaissent avec *authenticated_via = API*.**
- ☐ **Conteneur `rsso` sur `docker-srv` : `docker ps` → *healthy*.**
- ☐ **Test réel : connecter un poste au SSID avec un compte autorisé → IP en `10.0.24x.100+` et Internet direct.**

6.2 Ajouter une borne Wi-Fi

7 Raccorder et référencer

Raccorder la borne à un port de commutateur PoE tagué 240+241 (procédure MO-NET-003). Relever son adresse MAC et son IP sur le contrôleur UniFi.

8 Réinitialiser si nécessaire

Si la borne est gérée par une autre console (étiquette ou état *Connection Interrupted*), la réinitialiser : bouton *reset* enfoncé 5–10 s jusqu'au clignotement de la LED (pas plus de 15 s, sinon mode TFTP).

9 Adopter et déclarer

L'adopter sur le contrôleur (*forget* préalable si elle y figure encore), la laisser se provisionner (firmware auto). La déclarer comme client RADIUS dans NPS (même secret partagé) avec le nom

> **`BTSSIOI<salle>`. Les SSID et le profil RADIUS s'appliquent automatiquement (groupe *All APs*).**

6.3 Ajouter un SSID ou une population

Créer le WLAN sur le contrôleur (sécurité `wpaeap`, profil `NPS-DC1`, réseau cible), créer le réseau *VLAN only* correspondant si nouveau tag, câbler le VLAN jusqu'à OPNsense (interfaces, Kea, règles), et ajouter la stratégie NPS du groupe AD concerné avec l'attribut `Tunnel-Pvt-Group-ID` adéquat. Toute nouvelle population s'ajoute par groupe AD : inutile de toucher au Wi-Fi, la stratégie NPS fait foi.

6.4 Sauvegardes

— **OPNsense** : export XML de la configuration (**Système** → **Configuration** → **Sauvegardes** → **Télécharger**) après chaque modification ;
— **contrôleur UniFi** : sauvegarde intégrée (MO-NET-006, section exploitation) ;
— **commutateurs** : bouton Save de chaque interface web après modification ;
— **NPS** : la configuration vit dans `C:\Windows\System32\ias\ias.xml` — en faire une copie avant toute retouche (elle est couverte par la sauvegarde System State du DC, MO-AD-006) ;
— **RSSO** : le dossier `/opt/docker/rsso` est inclus dans les sauvegardes vzdump du CT (MO-PLT-016).

7 Dépannage

Symptôme	Causes probables et conduite à tenir
Le SSID n'apparaît pas	Borne hors ligne (contrôleur → Devices), borne non adoptée, ou coupure PoE/switch en amont. Vérifier l'état dans l'UI UniFi et le port du commutateur (lien, PoE 13 W).
« Impossible de se connecter » à l'association	Mot de passe AD erroné, compte hors des groupes autorisés (rejet fail-closed), certificat RADIUS refusé (CA non installée sur le client ou domaine `bts.sio` non renseigné sur Android). Vérifier le journal NPS (`C:\Windows\System32\LogFiles\IN*.log`).
Association réussie mais **pas d'adresse IP**	Rupture du chemin VLAN (cause nř1). Vérifier de proche en proche la présence de la MAC du client dans les tables MAC des commutateurs (Diagnostics → MAC Table), puis les logs Kea (**Services** → **Kea DHCP** → **Leases** + journaux).
Pas de DHCP sur *tous* les VLANs	Kea arrêté ou interfaces VLAN sans adresse IP au niveau OS : vérifier **Interfaces** → **Overview** puis appliquer les changements d'interface en attente (bannière Apply changes).
IP obtenue mais **page de portail** affichée	Le SSO n'a pas ouvert la session : conteneur `rsso` arrêté, accounting UniFi mal configuré (profil NPS-DC1 → acct `10.0.112.20:1813`), ou appel API en échec (clé svc-rsso révoquée/expirée). Se connecter une fois via le portail (compte AD) en attendant la réparation.
IP obtenue, Internet direct, mais **session absente** du portail	Cosmétique si le surf fonctionne : l'accounting Interim (300 s) recréera la session. Sinon vérifier les journaux du conteneur RSSO.
Le portail refuse les identifiants	Le serveur d'authentification du portail est `NPS-DC1` (RADIUS) : vérifier la stratégie `WiFi-Portail` (ordre 4, méthode PAP) et le client RADIUS `OPNsense-Portail` dans NPS.

Test de la chaîne accounting

Depuis un poste du LAN, on peut émettre un *Accounting-Request Start* de synthèse vers `10.0.112.20:1813` (secret partagé des bornes requis) : la réponse *Accounting-Response* et l'apparition de la session dans Captive Portal →

Sessions prouvent la chaîne complète RSSO → API → portail, indépendamment des bornes.

8 Reconstruction complète (sinistre)

En cas de perte totale d'un composant, reconstruire dans cet ordre (chaque élément a sa sauvegarde ou son MO) :

1. **OPNsense** : restaurer la configuration XML (export le plus récent) → toute la couche VLAN/DHCP/filtrage/portail revient d'un bloc. Recréer l'utilisateur svc-rsso et sa clé API si l'export est antérieur à sa création.
2. **Commutateurs** : ressaisir VLANs et marquages selon la table de la section 4.3 (MO-NET-003).
3. **Contrôleur UniFi** : restaurer la sauvegarde du contrôleur (MO-NET-006) ou recréer les objets selon la section 4.1 et l'annexe A.
4. **NPS** : restaurer `ias.xml` (sauvegarde System State, MO-AD-006) puis redémarrer le service IAS ; vérifier les clients RADIUS.
5. **RSSO** : redéployer la stack depuis `/opt/docker/rsso` (sauvegarde vzdump) et réarmer le `.env` depuis le coffre.
6. Valider avec la checklist de la section 6.1 puis un test utilisateur réel par SSID.

9 Retour arrière

Pour désactiver le Wi-Fi pédagogique sans tout démonter :

— **Retour au réseau plat** : remapper le WLAN `BTS SIO Etudiants` sur le réseau *Default* du contrôleur (annule la segmentation, les clients retombent en DHCP plat) — réversible en une minute ;

— **arrêt du portail** : désactiver la zone 0 dans OPNsense (les règles et le DHCP continuent de fonctionner) ;

— **arrêt du SSO** : repointer l'accounting du profil `NPS-DC1` vers NPS (`10.0.112.2:1813`) et arrêter le conteneur `rsso` ;

— **arrêt complet** : désactiver les deux WLAN sur le contrôleur, désactiver Kea sur opt1/opt2, retirer les marquages VLAN des ports (MO-NET-003).

10 Annexe A — Référentiel des identifiants techniques

10.1 Objets UniFi (site `default`)

Objet	Identifiant
WLAN `BTS SIO Etudiants`	`6a9abdbbae5521a3531f4e3e`
Réseau `wifi-etudiants` (VLAN 240)	`6a9ea9de1b0ca8c7e88aa6b0`
Réseau `wifi-profs` (VLAN 241)	`6a9ea9de1b0ca8c7e88aa6b3`
Réseau `Default` (plat, rollback)	`6a96b183ae5521a3531f4dcf`
Profil RADIUS `NPS-DC1`	`6a9e955e1b0ca8c7e88aa651`
Groupe de bornes *All APs*	`6a96b183ae5521a3531f4dd4`
Groupe d'utilisateurs par défaut	`6a96b183ae5521a3531f4dd0`

10.2 Entrées du coffre Vaultwarden

Entrée	Contenu
Wifi BTS SIO — Secret RADIUS bornes UniFi	Secret partagé bornes ↔ NPS et bornes ↔ RSSO
UniFi Network Controller (docker-srv)	Compte administrateur du contrôleur
OPNsense — svc-rsso (API portail captif)	Clé + secret API du compte svc-rsso
OPNsense — root (firewall principal)	Compte root du pare-feu
AD — Compte de service svc-ldap-opnsense	Compte de bind LDAP (réservé, portail LDAP non retenu)
Wifi BTS SIO — Compte de test 802.1X (wifitest / wifiprof)	Comptes AD de validation
CT 200 docker-srv	Accès SSH root de l'hôte des conteneurs
SwitchAruba01 … 06	Comptes `admin` locaux des commutateurs

10.3 Paramètres clients (téléphones, PC hors domaine)

Paramètre	Valeur
Sécurité	WPA2-Enterprise (802.1X)
Méthode EAP	PEAP
Authentification de phase 2	MSCHAPv2
Identité	Compte AD (`p.nom`) + mot de passe AD
Certificat CA	« BTS SIO Root CA » (installée d'office sur les postes du domaine)
Domaine	`bts.sio` (champ exigé par Android)

11 Annexe B — Extraits de configuration RSSO

11.1 docker-compose (rappel)

La stack est décrite dans `/opt/docker/rsso/docker-compose.yml` (image `freeradius/freeradius-server:3.2.10`, port `1813/udp` publié, montages par fichier des trois configurations, volume de logs, `env_file`). Le healthcheck vérifie la présence du processus `freeradius`.

11.2 Module rest (extrait corrigé)

```
accounting {
    uri = "${..connect_uri}/api/captiveportal/session/connect/$ENV{OPN_ZONE}"
    method = 'post'
    body = 'post'
    data = "user=%{User-Name}&ip=%{Framed-IP-Address}"
    auth = 'basic'
    username = "$ENV{OPN_API_KEY}"
    password = "$ENV{OPN_API_SECRET}"
    force_to = 'plain'
    timeout = 4.0
    tls = ${..tls}
}
```

11.3 Vérification de la chaîne en mode debug

```
# Sur docker-srv : instance de debug en réseau hôte, env SANS guillemets
docker run --rm --name rsso-debug --network host \
  -v /opt/docker/rsso/raddb/clients.conf:/etc/freeradius/clients.conf:ro \
  -v
    /opt/docker/rsso/raddb/mods-enabled/rest:/etc/freeradius/mods-enabled/rest:ro
    \
  -v
    /opt/docker/rsso/raddb/sites-enabled/default:/etc/freeradius/sites-enabled/default:ro
    \
  --env-file /tmp/rsso-debug.env \
  freeradius/freeradius-server:3.2.10 freeradius -X
```

12 Références