

Le contexte est celui de l'entreprise SODECAF. Vous travaillez dans l'équipe de la DSI de cette société, en tant que technicien systèmes et réseaux.

Vous êtes chargé notamment de la mise en œuvre d'un dispositif de sécurité, nommé **UTM (Unified Thread Management)**. Cet équipement émane de la société Stormshield spécialisée en sécurité des réseaux et des systèmes d'information.



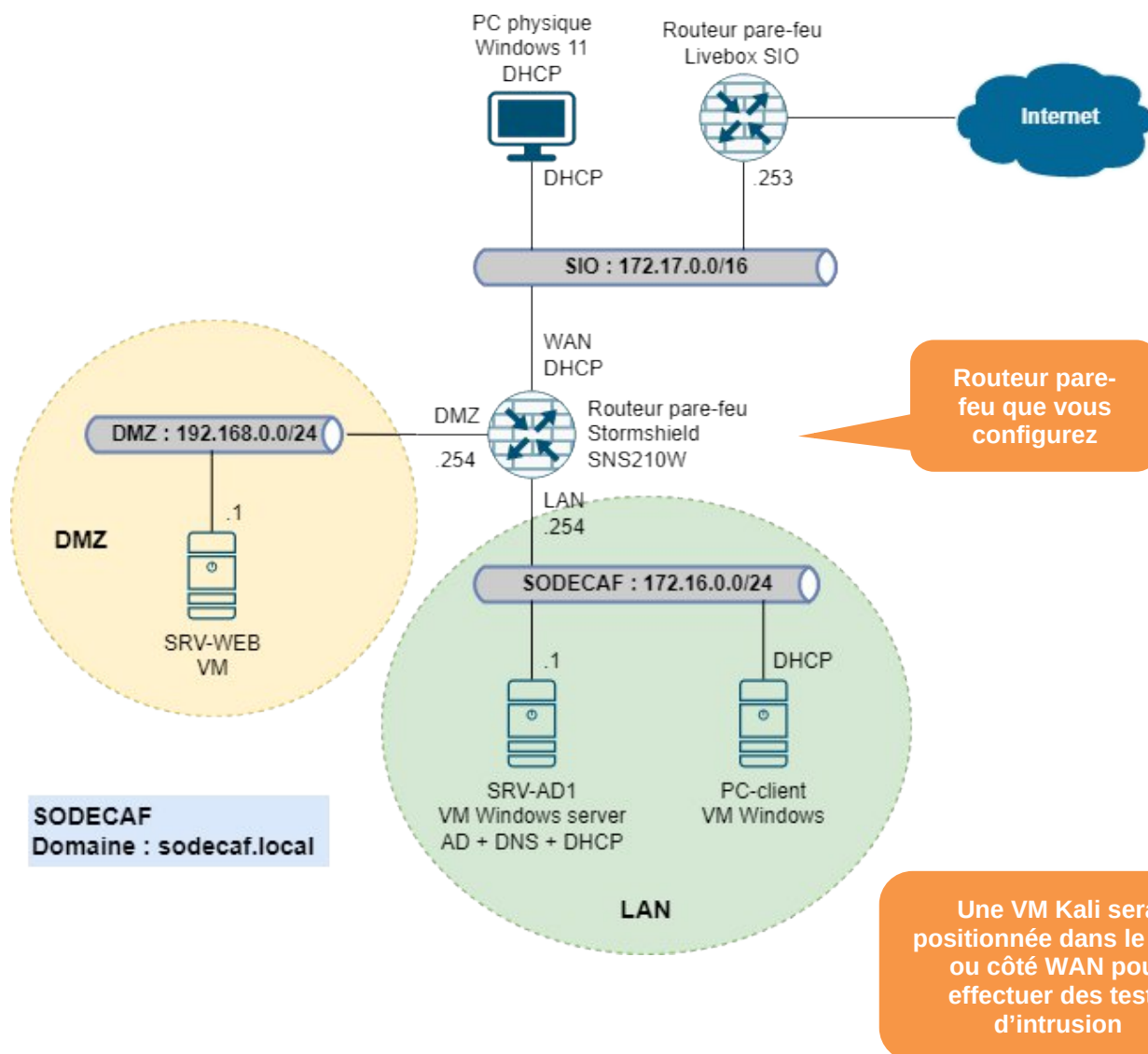
Stormshield est une entreprise française, sous-filiale d'Airbus, dont le siège social se situe à Issy-les-Moulineaux. Ainsi, elle est soumise à la loi française et à la loi européenne (loi informatique et libertés, RGPD, etc). L'outil de protection réseau Stormshield SNS a obtenu la certification ANSSI EAL4+.

Vous avez, dans une activité précédente, mis en place le Stormshield SN210W, configuré les interfaces réseaux, le filtrage et le NAT.

Vous allez ici compléter la configuration de l'équipement avec :

- La détection des intrusions dans le SI de l'entreprise : **IDS et IPS** ;
- La mise en place d'un **portail captif** pour l'authentification des connexions sortantes vers internet ;

Schéma de l'infrastructure



Documents ressources sur le réseau

- Document du TP B3-Act5-TP1 Protection avancée avec un Stormshield SNS.pdf
- Fiches du Certa sur le Stormshield

La détection des intrusions dans le SI de l'entreprise : IDS et IPS

Un **système de détection d'intrusions** (*intrusion detection system - IDS*) est un outil logiciel ou matériel dont le rôle est de **repérer de manière passive les activités suspectes sur un réseau ou sur un hôte**, permettant ainsi aux administrateurs de réagir plus rapidement en cas d'attaque.

Un **système de prévention d'intrusions** (*intrusion prevention system - IPS*) est un **IDS** qui possède la capacité supplémentaire d'**agir de manière active sur les activités suspectes** (blocage de trames, de ports, blocage d'une tentative de modification du contenu d'un fichier, etc...).

Il existe essentiellement trois familles d'IDS/IPS :

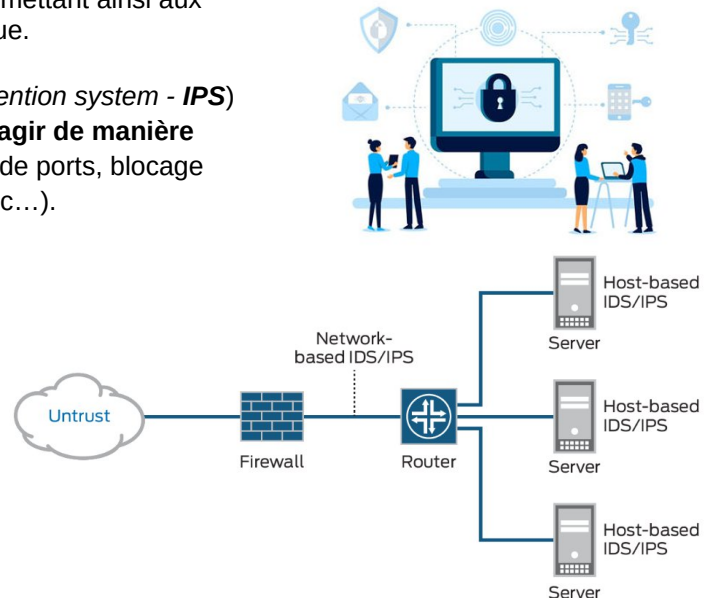
- Les **Network IDS / IPS (NIDS / NIPS)** qui analysent les flux sur le réseau et détectent les attaques en temps réel.
- Les **Host IDS / IPS (HIDS / HIPS)** qui analysent les activités des machines (OS) sur lesquels ils sont installés.
- Les **IDS / IPS hybrides**, qui centralisent l'analyse des flux réseaux et hôtes.

Le placement du système IDS est différent de l'IPS :

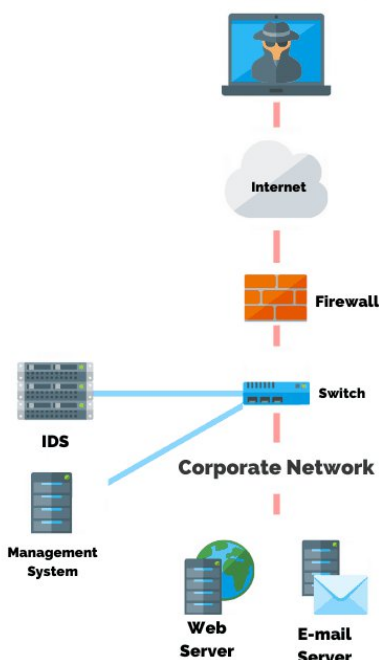
- **L'IDS est placé sur un réseau isolé et ne voit qu'une copie du trafic à surveiller.** L'IDS signale le trafic suspect.
- **L'IPS est placé en coupure sur le réseau, il analyse les données réelles.** L'IPS peut agir en temps réel et stopper le trafic suspect, en bloquant un protocole et/ou un port. L'inconvénient de l'IPS est qu'il peut bloquer un trafic légitime (faux positif).

IDS vs IPS

Whats the Difference & Why You Need them!

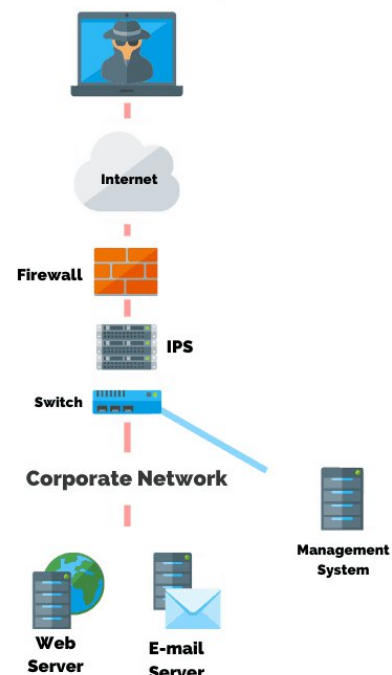


Intrusion Detection System (IDS)



VS

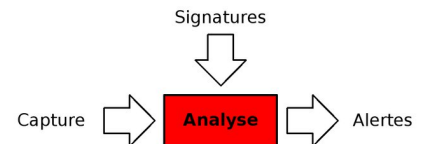
Intrusion Prevention System (IPS)



Les pare-feux UTM Stormshield sont dotés d'un NIDS/NIPS nommé ASQ (Active Security Qualification).

Ce service repose sur 3 phases :

- La capture ;
- L'analyse à partir d'une base de signatures, des RFC, de règles applicatives ;
- Les alertes et le blocage potentiel.



Sur les pare-feux Stormshield, le NIPS est activé par défaut. Cela renforce donc naturellement la sécurité car même en cas d'autorisation globale dans la table de filtrage de l'équipement, ce dernier inspecte et bloque les flux qu'il juge potentiellement dangereux. Bien évidemment, **ce service peut générer des faux positifs**. Dans le cadre d'un NIPS, les faux positifs sont des flux légitimes que le boîtier a bloqué estimant qu'ils étaient suspects. Suite aux remontées de terrain, les mises à jour (fix) permettent de minimiser les faux positifs et améliore la pertinence des alertes remontées.

Le NIPS est donc extrêmement complémentaire des autres solutions de sécurité mises en œuvre dans l'entreprise. Sur les pare-feux SNS, il est primordial, sauf cas particuliers, de le laisser activé. Dans le cas contraire, il est possible de basculer en mode IDS ou en mode pare-feu simple (c'est-à-dire filtrage couches 3 et 4).

Travail à effectuer :

A. Simulation d'une attaque ayant pour objectif de rendre le service web indisponible

- On vous demande, à partir d'une VM Kali placée dans le LAN de la SODECAF, d'utiliser les commandes suivantes à destination du serveur web situé en DMZ, afin de tester l'efficacité du NIPS/NIDS présent sur le pare-feu :

```
kali@kali:~$ sudo nmap -sS 192.168.0.1
kali@kali:~$ sudo nmap -sU 192.168.0.1
kali@kali:~$ sudo nmap -sV 192.168.0.1
```

- À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type d'attaque réalisé ainsi que la finalité de chacune de ces commandes.
- Visualisez les logs du Stormshield dans Monitoring > Audit logs > All logs ou Alarms. Le NIPS a-t-il été en mesure de détecter et de bloquer ces opérations ?

Dans un second temps, réalisez l'opération depuis le réseau de SIO, vers l'adresse IP externe du pare-feu.

```
kali@kali:~$ sudo hping3 --flood -S -p 80 172.17.XX.YY
```

- À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type d'attaque réalisé ainsi que la finalité de la commande.
- Le NIPS a-t-il été en mesure de détecter et de bloquer cette opération ? Votre service web est-il toujours disponible ?

B. Analyses protocolaires

Le NIPS du Stormshield peut effectuer une analyse précise de protocoles et d'appliquer différents niveaux de sécurité.

- Afin de n'accepter que les paquets IP chiffrés en SSL/TLS avec un niveau de sécurité élevé, vérifiez que le chiffrement SSL/TLS accepté est « Haut uniquement ».
- Afin de vous prévenir d'une exfiltration de données de la zone DNS de la SODECAF vers l'extérieur, bloquez les actions de type transfert de zone (AXFR et IXFR) au niveau du protocole DNS.

C. Protections applicatives

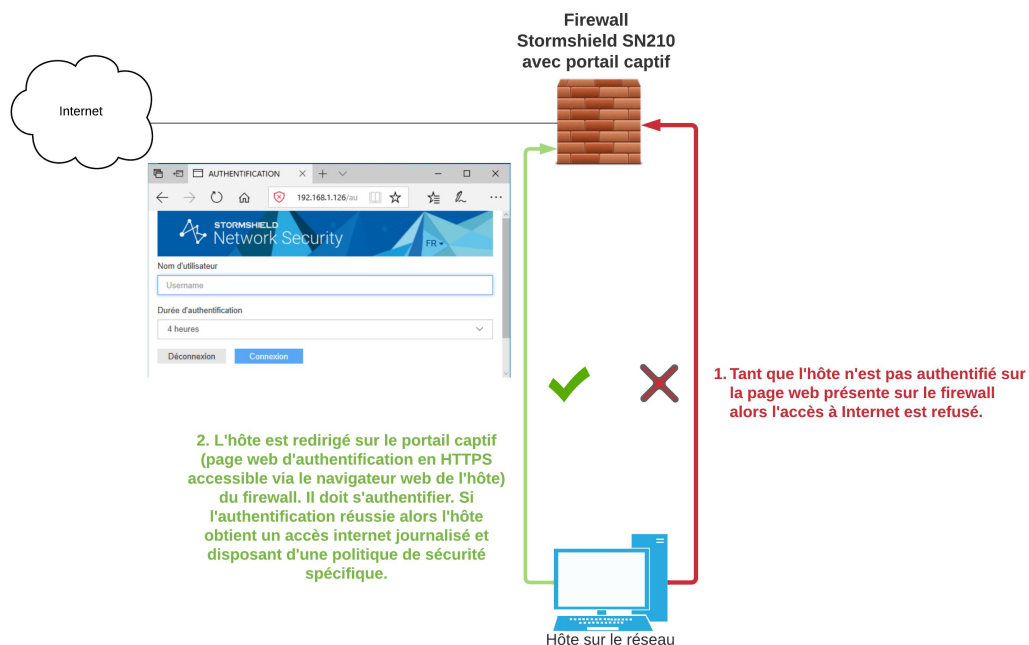
- Depuis votre réseau interne, interdisez l'utilisation des jeux dans l'application Facebook.
- Interdisez toute action concernant la plateforme de jeu Steam, et le VPN FrozenWay provenant de votre réseau d'entreprise et levez une alerte mineure lorsque cela se produit.

Le portail captif

Le portail captif, ou portail d'authentification, est une page web embarquée sur le pare-feu et accessible via une connexion HTTPS. Il est possible, dans l'usage d'un réseau Wifi ou filaire, **d'imposer aux utilisateurs une authentification** sur cette page web afin d'obtenir un accès à Internet ou à certaines ressources précises sur le réseau.

Cette technologie est souvent utilisée dans le cadre de réseaux Wifi publics ou invités mais aussi parfois sur des réseaux filaires.

Son principe général de fonctionnement est le suivant :



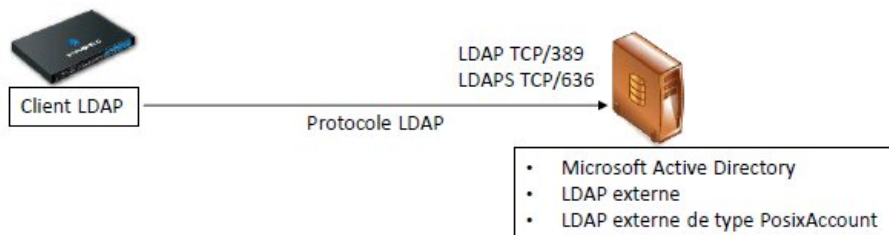
Les usages du portail captif sur un pare-feu Stormshield sont les suivants :

- authentifier des utilisateurs pour accéder au réseau ;
- enrôler de nouveaux utilisateurs ;
- créer et télécharger un certificat ;
- télécharger le client VPN SSL et sa configuration ;
- faire une demande de parrainage pour accéder au réseau.

A. Authentification sur le pare-feu via un couple login/mot de passe sur l'AD de la Sodecaf

Nous souhaitons mettre en place un **portail captif**, permettant d'autoriser l'accès internet depuis les réseaux internes de l'entreprise, seulement aux personnes authentifiées avec leur compte présent dans l'Active Directory.

Nous allons, dans un premier temps, lier le pare-feu à l'annuaire LDAP de notre serveur Active Directory :



- Créez, dans l'UO users, un compte utilisateur simple *stormshield-ldap* dans l'annuaire AD de la Sodecaf. Le Stormshield utilisera ce compte pour accéder à l'annuaire.
- Utilisez la fiche 10 pour effectuer le lien entre le Stormshield et l'annuaire AD de la Sodecaf. Testez ce lien.
- Dans l'annuaire AD, créez une UO Employés_Sodecaf et à l'intérieur une UO Commercial avec un utilisateur « Flore Diaz »

- Dans le menu Utilisateurs > Authentification > Portail Captif, configurez le portail captif en l'activant sur l'interface IN.
- Dans le menu Utilisateurs > Authentification > Profils du portail captif, vérifiez que l'annuaire LDAP est la méthode par défaut.
- Dans le menu Utilisateurs > Authentification > Politique d'authentification, créez une politique d'authentification pour tous les utilisateurs de la Sodecaf, sur l'interface IN, en utilisant la méthode LDAP.
- Adaptez la politique de filtrage http et https afin que tous les utilisateurs soient redirigés vers le portail captif lorsqu'ils tentent d'accéder à des sites Web, en créant une nouvelle règle d'authentification.
- Effectuez le bon fonctionnement du portail captif pour Flore Diaz. Si l'écran du portail captif ne s'affiche pas dans le navigateur web, vous pouvez l'ouvrir à l'adresse <https://172.16.0.254/auth>.

- Dans l'annuaire AD ; ajoutez une UO « Admins » dans l'UO « Employés_Sodecaf ». Créez un utilisateur pdupond dans cette UO admins.
- Accordez le droit aux connexions SSH vers l'extérieur pour les membres de l'UO Admins et pas aux autres utilisateurs. Faire un test de connexion ssh vers le serveur web.

B. Authentification sur le pare-feu à l'aide d'un certificat X509

La solution précédente mise en place pose deux problèmes en matière de sécurité :

- Utilisation de l'annuaire AD pour l'authentification du portail captif. Nous avons vu que l'ANSSI préconise d'utiliser un annuaire dédié.
- Utilisation du couple login/mot de passe qui est déconseillée en matière d'authentification.

Au lieu d'utiliser les traditionnels login et mot de passe pour s'authentifier sur le firewall, il est possible de le faire à l'aide de certificats X509 associés aux utilisateurs. Le service RSSI souhaite expérimenter cette fonctionnalité et vous êtes en charge de son implémentation sur le pare-feu de votre agence. Il vous est demandé de désactiver les règles existantes afin de pouvoir appliquer cette nouvelle politique.



- Créez et activez un annuaire LDAP interne ayant pour nom de domaine « sodecaf.stormshield ». Vous lui associez dès la création le profil d'authentification sur l'interface correspondante au sous-réseau « LAN SODECAF » et vous permettez l'enrôlement des utilisateurs.
- Modifiez la configuration du portail captif afin qu'il utilise ce nouvel annuaire dédié.
- Créez le compte de Flore Diaz dans ce nouvel annuaire.
- Faites un test du portail captif sur la machine cliente. L'authentification doit fonctionner avec le couple login/mot de passe configuré dans l'annuaire interne du Stormshield.

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 2)



Organisation:	sodecaf
Domaine:	stormshield
Mot de passe:	*****
Confirmer:	*****
	Bon
Hachage des mots de passe:	SSHA256

Configuration du navigateur des postes clients

Préalable : depuis le firmware 4.2.2 et l'intégration de TLS v1.3, la méthode d'authentification par certificat (SSL) n'était pas fonctionnelle. Ce problème a été corrigé sur le pare-feu grâce à l'ajout du support du Post-Handshake Authentication.

Le navigateur Web utilisé doit également autoriser le Post-Handshake Authentication pour que la méthode soit fonctionnelle.

Sur Firefox

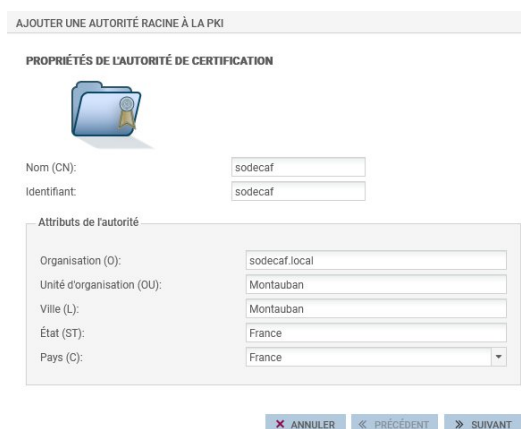
- Saisir about:config dans la barre de recherche du navigateur.
- Passer la valeur de « security.tls.enable_post_handshake_auth » à « true ».

Il est aussi possible d'effectuer une modification côté pare-feu uniquement en désactivant le support du TLS 1.3 pour cette partie (le pare-feu utilisera donc la version 1.2, ce qui n'est pas conseillé) via ces commandes CLI :

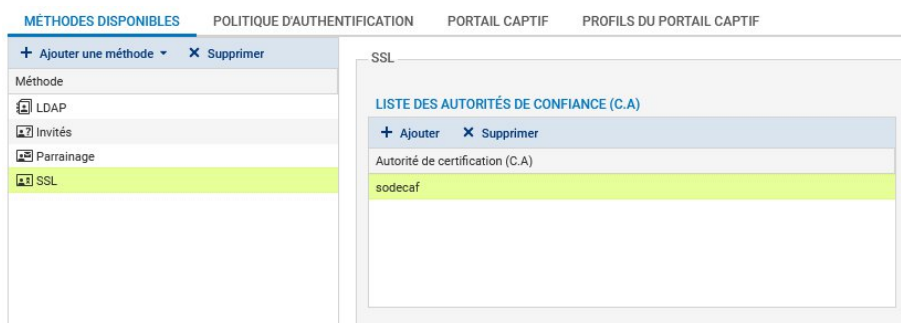
```
CONFIG AUTH HTTPS tlsv1=0
```

```
CONFIG AUTH ACTIVATE
```

- En utilisant la fiche 11, créez la PKI (Public Key Infrastructure) relative à votre agence et la définir par défaut sur le même modèle que celle ci-dessous :



- Définissez par défaut l'autorité de certification créée.
- Dans Utilisateurs > Utilisateurs, créez un certificat X509 personnel pour Flore Diaz.
- Dans Objets > Certificats et PKI, exportez ce certificat utilisateur (télécharger > identité > format p12) et importez le sur le poste Windows 10/11 présent dans le LAN et intégrez le dans le navigateur (magasin de certificat d'un navigateur ou du système).
- Ajoutez et configurez la méthode d'authentification « Certificat SSL » dans les paramètres du portail captif et désignez-la comme méthode par défaut.



- Testez cette nouvelle méthode d'authentification sur le portail captif en permettant à l'utilisateur Flore Diaz de s'authentifier sur le portail captif par l'intermédiaire de son certificat X509 sans mot de passe. Lors de la première connexion, vous devez entrer uniquement l'identifiant. Le certificat est « trouvé » via l'identifiant « mail » correspondant à l'utilisateur. Il est demandé, lors d'une première connexion, de le valider.