

# Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

## Situation 6 : Portail captif et pare-feu authentifiant

### Fiches Stormshield associées :

- Fiche 10 – Utilisateurs et authentification
- Fiche 11 – Infrastructures à clés publiques

### Documents :

- Document 1 : qu'est-ce qu'un portail captif ?
- Document 2 : différences entre une authentification LDAP, invités, comptes temporaires, parrainages et enrôlement

Le RSSI souhaite qu'un certain nombre de règles de filtrage soit appliqué suite à une authentification préalable des utilisateurs sur le portail captif (voir document 1) **dans le sous-réseau « Administration systèmes et réseaux »**.

## I Authentification sur le pare-feu via un couple login/mot de passe

1. Créer et activer un annuaire interne ayant pour nom de domaine « <votre\_agence>.cub.fr ». Vous lui associez dès la création le profil d'authentification sur l'interface correspondante au sous-réseau « Administration systèmes et réseaux » et vous permettez l'enrôlement des utilisateurs.
2. Tester l'accès au portail captif.

Vous vous assurerez que l'annuaire par défaut utilisé est bien l'annuaire interne au pare-feu et que la possibilité d'enrôlement est bien activée.

3. Créer dans l'annuaire interne au firewall l'utilisateur Denis Ritchie :
  - Identifiant : dritchie
  - Mot de passe : dmac1969
  - Mail : dritchie@agence.cub.fr (ou agence correspond au nom de votre agence)
4. À l'aide de la fonction d'enrôlement, créer l'utilisateur Ken Thompson (en fonction des versions de firmware utilisées, un message « erreur interne » peut apparaître et empêcher la création d'un utilisateur par enrôlement) :
  - Mail : kthompson@agence.cub.fr
  - Mot de passe : foobar1991
5. Adapter 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.
6. Concernant l'utilisateur Dennis Ritchie, seul l'accès aux sites de la catégorie IT sera autorisé. Pour le reste des utilisateurs authentifiés, la politique de filtrage http et https créée dans la mission précédente restera appliquée.
7. Compléter la politique de filtrage afin d'autoriser les requêtes SSH provenant de votre LAN vers l'extérieur uniquement à l'utilisateur Ken Thompson une fois ce dernier authentifié sur le portail captif. Cette règle devra lever une alarme mineure.

## II Authentification sur le pare-feu à l'aide d'un certificat X509

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 concernant ce sous-réseau afin de pouvoir appliquer cette nouvelle politique.

### 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 :

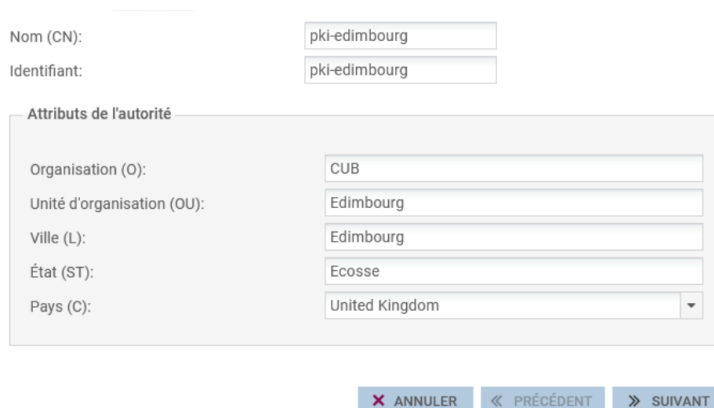
```
CONFIG AUTH HTTPS tlsv1=0  
CONFIG AUTH ACTIVATE
```

### Généralités

1. Pourquoi la RSSI envisage une authentification par certificat X509 plutôt que par simple couple identifiant et mot de passe ?
2. Expliquer la différence entre authentification faible, authentification multi-facteur et authentification forte. Donner plusieurs exemples de systèmes d'authentification forte.  
*Il est conseillé de consulter le guide de l'ANSSI <https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification-multifacteur-et-mots-de-passe.pdf>*

### Cahier des charges

3. Créer la PKI relative à votre agence et la définir par défaut sur le même modèle que celle d'Edimbourg



4. Créer un nouvel utilisateur Kévin Mitnick dans votre annuaire interne :
  - Identifiant : kmitnick
  - Mot de passe : H4xor2600
  - Mail kmitnick@agence.cub.fr.

4. Pour cet utilisateur, créer un certificat X509 personnel.
5. Exporter ce certificat utilisateur sur un poste Windows 10/11 présent dans le LAN et l'intégrer dans le navigateur (magasin de certificat d'un navigateur ou du système).
6. Ajouter et configurer la méthode d'authentification « Certificat SSL » dans les paramètres du portail captif et désignez-la comme méthode par défaut.
7. Tester cette nouvelle méthode d'authentification sur le portail captif en permettant à l'utilisateur Kevin Mitnick de s'authentifier sur le portail captif par l'intermédiaire de son certificat X509 sans mot de passe.

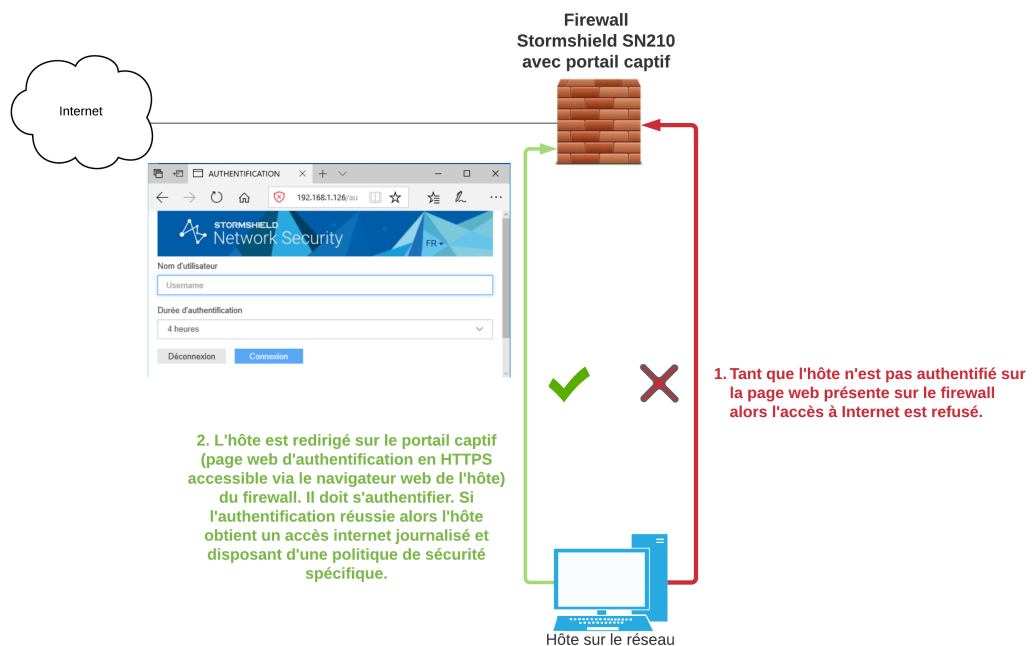
## Documents

### Document 1 : Qu'est-ce qu'un portail captif ?<sup>1</sup>

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 Wi-Fi 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 utilisation au détriment du protocole 802.1x suscite parfois des polémiques.<sup>2</sup>

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.

<sup>1</sup> Source « Livre de formation CSNA Stormshield »

<sup>2</sup> Pour plus d'informations sur le sujet : <https://www.bortzmeyer.org/8910.html>

## Document 2 : différences entre une authentification LDAP, invités, comptes temporaires, parrainages et enrôlement

**L'authentification LDAP** permet de vérifier l'identité d'un utilisateur auprès d'un annuaire interne au boîtier Stormshield ou externe comme un annuaire OpenLDAP ou Active Directory.

**L'utilisation d'une authentification de type invité** permet à un utilisateur d'accéder au réseau après validation des conditions générales d'utilisation présentes sur le portail captif. Il doit fournir une adresse e-mail et un nom, mais ces informations ne sont pas vérifiées. Cette méthode est généralement utilisée dans les lieux publics tels que les hôtels ou les gares.

**Les comptes temporaires** permettent à des utilisateurs de s'authentifier sur le portail captif du pare-feu en utilisant un couple login, mot de passe fourni par l'administrateur. Ces comptes ont généralement une validité limitée dans le temps et ne sont pas ajoutés au sein d'un annuaire.

**Le parrainage** permet à un utilisateur identifié par son nom et prénom d'accéder au réseau grâce au parrainage d'un utilisateur local déjà existant et disposant des droits pour cela. L'utilisateur est invité, depuis le portail captif, à saisir son nom, prénom et l'adresse mail du parrain. Ce dernier reçoit alors un mail contenant un lien pour valider la demande.

**L'enrôlement** permet à des utilisateurs, par l'intermédiaire du portail captif, de remplir un formulaire de création de compte qui sera soumis à l'approbation de l'administrateur.