Problème établissement connexion vpn SSL

Avantage VPN SSL : Logiciel gratuit

Facilité de connexion les ports 443 sont ouvert de partout

SSL est capable de garantir la confidentialité, l'authentification et le contrôle d'intégrité des données en utilisant des mécanismes classiques de cryptographie (encryptions symétrique, asymétrique et fonction de « hachage »).

Inconvenant VPN SSL : Moins sécurisé que le VPN SSL en termes de sécurité. IPSEC est capable de changer régulièrement la clé de session symétrique lors de la même session alors que SSL garde la même. IPSEC supporte l'algorithme AES pour le chiffrement des données alors que la majorité des applications SSL ne l'ont pas encore implémenté. Alors qu'il est « facile » d'effectuer une attaque de type « Man in the Middle » sur SSL

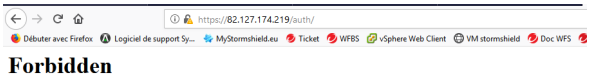
Etape 1 :

- Tester l'authentification sur le portail captif : IP publique/auth

Le portail s'affiche :

- Tester l'authentification avec l'utilisateur et le mot de passe
  - Ok passer à l'étape 2

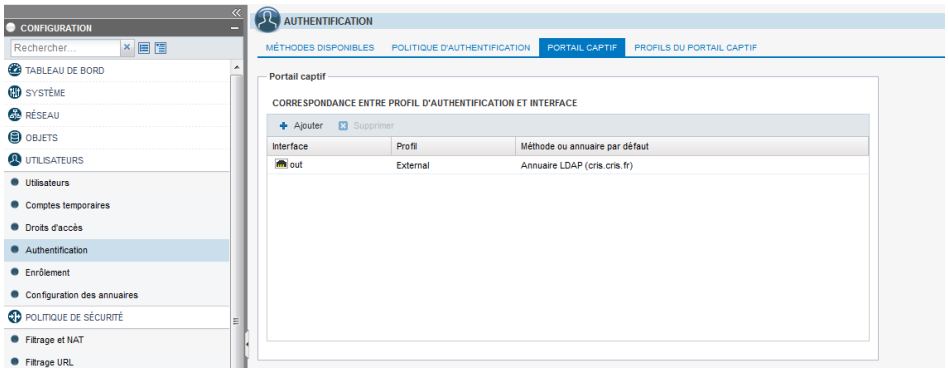
Le portail ne s'affiche pas :



- Vérifier les interfaces du portail captif

Utilisateur – Authentification – portail captif

Indiquer l'interface externe (qui peut être out ou ppoe)



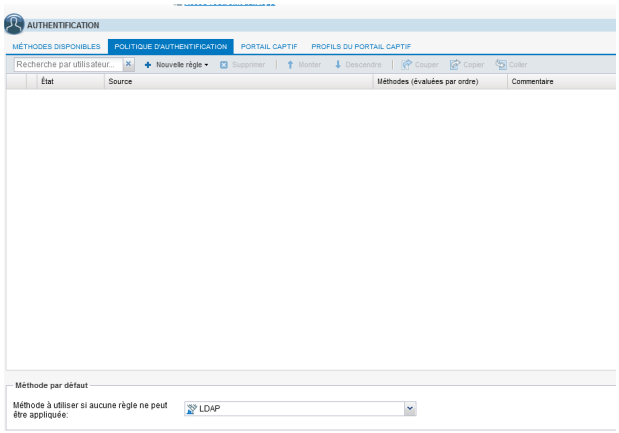
Message forbiden sur le portail captif malgré l'interface out de renseigner sur le portail

- Relancer les services nrestart sld et nrestart openvpn en SSH

- Authentification refusée : vérifier les droits d'accès du vpn SSL

Dans *utilisateurs – droit d'accès VPN – accès VPN*

Vérifier dans *utilisateurs → Authentification → politique d'authentification* méthode par défaut LDAP

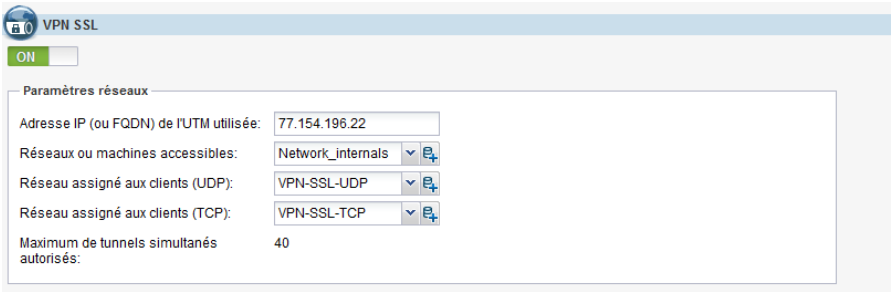


- Authentification réussie sur le portail captif

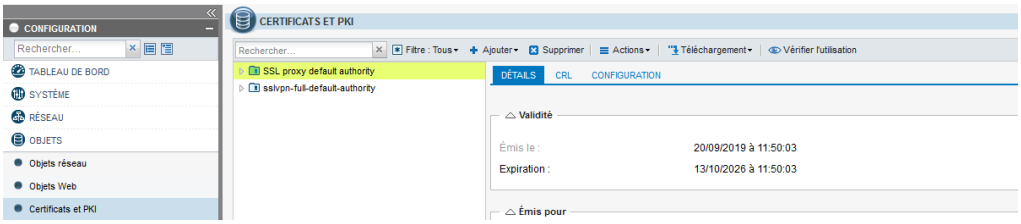
    - Tester avec le client vpn SSL

<u>Etape 2 : connexion sur le client VPN SSL</u>

- <u>Message Echec TLS – error</u> :
    - Vérifier l'adresse IP de l'UTM utilisée



    - Vérifier la plage réseau si elle n'est pas trop grande (réseau assigné aux clients – mettre /24)
    - Indiquer le réseau assigné au client dans le champ TCP, si pas mieux tester avec uniquement dans le champ UDP
    - Vérifier l'heure et la date du certificat



- Suivre la procédure ci-dessous

- Supprimez le répertoire associé à l'autorité de certification sslvpn-full-default-Authority, à l'aide de la commande suivante :

rm -rf ~ / ConfigFiles / Certificates / sslvpn-full-default-author

- Régénérer les certificats avec la commande

sslinit

- Recharger la configuration openvpn à partir de l'interface graphique Web en désactivant / activant la configuration SSL VPN

- Authentification correcte sur le portail captif et authentification failed sur le client malgré les droits de connexion au vpn ssl
  - Redémarrer le boitier → problème connu de consommation de SHM (shared memory) sur le produit.

- Je suis connecté au vpn SSL mais je n'ai plus accès à internet
  - Vérifier les DNS utiliser

  Dans la configuration avancée du vpn ssl décocher
  - Utiliser les serveurs DNS fournis par le firewall
  - Interdire l'utilisation de serveur DNS tiers

  Si on veut laisser les DNS du poste local

- Message sur le client VPN SSL : fichier de configuration non disponible
  - Vérifier les DNS utiliser par le Firewall

- Pas d'accès aux ressources en local
  - Vérifier le filtrage