vpn-ssl

```
    MARK RODERICK   -  VPN SSL
```

VPN = Virtual Private Network

Buts

- Connexion à distance
- Securiser connexion
- Confidentialité
- Authentification

- **IPsec VPN** → protège **tout le trafic réseau**, idéal pour relier deux sites ou donner un accès complet au réseau interne.
- **SSL VPN** → protège **uniquement certaines applications**, facile à utiliser depuis un navigateur, parfait pour les employés en télétravail ou sur des appareils personnels.

*types de vpn

📊 **Tableau comparatif : IPsec VPN vs SSL VPN**

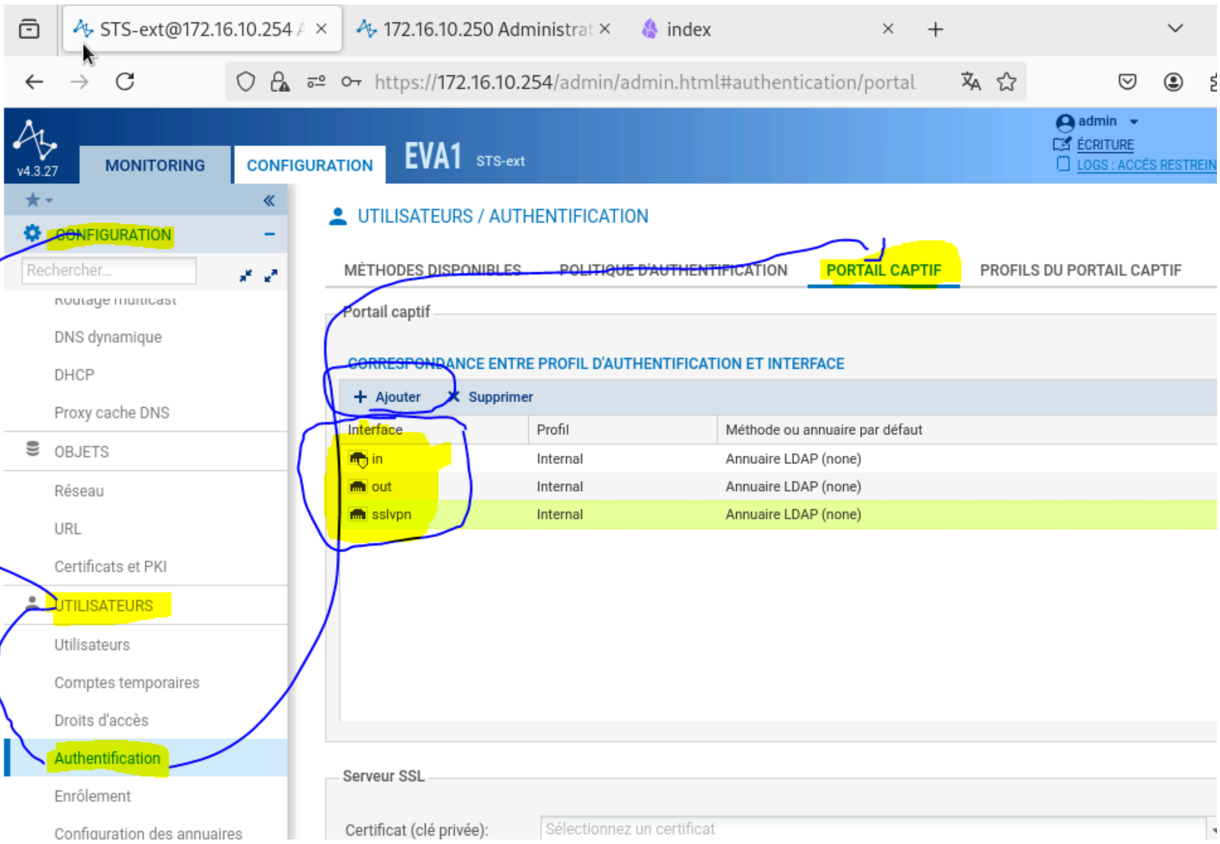
Caractéristique	IPsec VPN	SSL VPN
Couche OSI	Couche réseau (couche 3)	Couche transport (couche 4) via SSL/TLS
Portée du chiffrement	Tout le trafic réseau (IP complet)	Sessions/applications spécifiques
Client requis	Logiciel VPN dédié installé sur l'appareil	Navigateur web (aucun client supplémentaire)
Cas d'usage idéal	Connexion site-à-site, accès complet au réseau	Accès distant aux applications web
Maintenance	Plus complexe, nécessite configuration avancée	Plus simple, déploiement rapide
Performance	Très robuste pour gros volumes de données	Plus léger, adapté aux utilisateurs nomades

VPN sur le sts externe

Thème	Détails et Fonctionnement	Configuration & Prérequis
Modes de VPN	**1. Mode Portail :** Accès sans client (clientless) aux serveurs Web/HTTP via le portail captif. **2. Mode Tunnel (Complet) :** Accès transparent au réseau interne, nécessite un client installé.	Le mode tunnel utilise OpenVPN (gratuit) ou le client Stormshield.
Protocole & Réseau	Encapsulation de paquets IP dans un tunnel **TLS** (TCP ou UDP). Le réseau VPN est considéré comme "interne" et ne doit pas chevaucher l'existant.	**Adressage IP :** Le réseau VPN est découpé en sous-réseaux de **/30**. Le serveur prend les premières IP, chaque client reçoit un sous-réseau dédié.
Processus de Connexion	1. Authentification utilisateur sur le portail captif. 2. Vérification des droits (Access Privileges). 3. Téléchargement de la config (`.ovpn`, certificats). 4. Établissement du tunnel TLS.	Le client récupère automatiquement l'archive `Openvpn_client.zip` contenant la clé PKI et le fichier de configuration.
Prérequis Admin	Le service nécessite une **PKI** (Autorité de certification) configurée. Un **annuaire** (LDAP ou interne) doit être actif.	Un profil de **portail captif** doit être lié à l'interface d'entrée avec une méthode d'authentification valide.
Sécurité & Filtrage	L'accès n'est pas autorisé par défaut. Il faut modifier les **Privilèges d'accès** (Block → Allow) pour l'utilisateur/groupe.	Des **règles de filtrage explicites** sont obligatoires pour autoriser le trafic du tunnel (`net_ssl_vpn`) vers le réseau interne.
Clients Compatibles	**PC :** Windows, macOS, GNU/Linux. **Mobile :** Android, iOS.	Le client Stormshield (Windows uniquement) permet la gestion de carnets d'adresses.
Limitations	Le nombre maximum de tunnels simultanés dépend du modèle de l'équipement (ex: 5 pour SN160, 500 pour SNi40).	Limites spécifiques s'appliquent aussi aux appliances virtuelles (V-UTM).

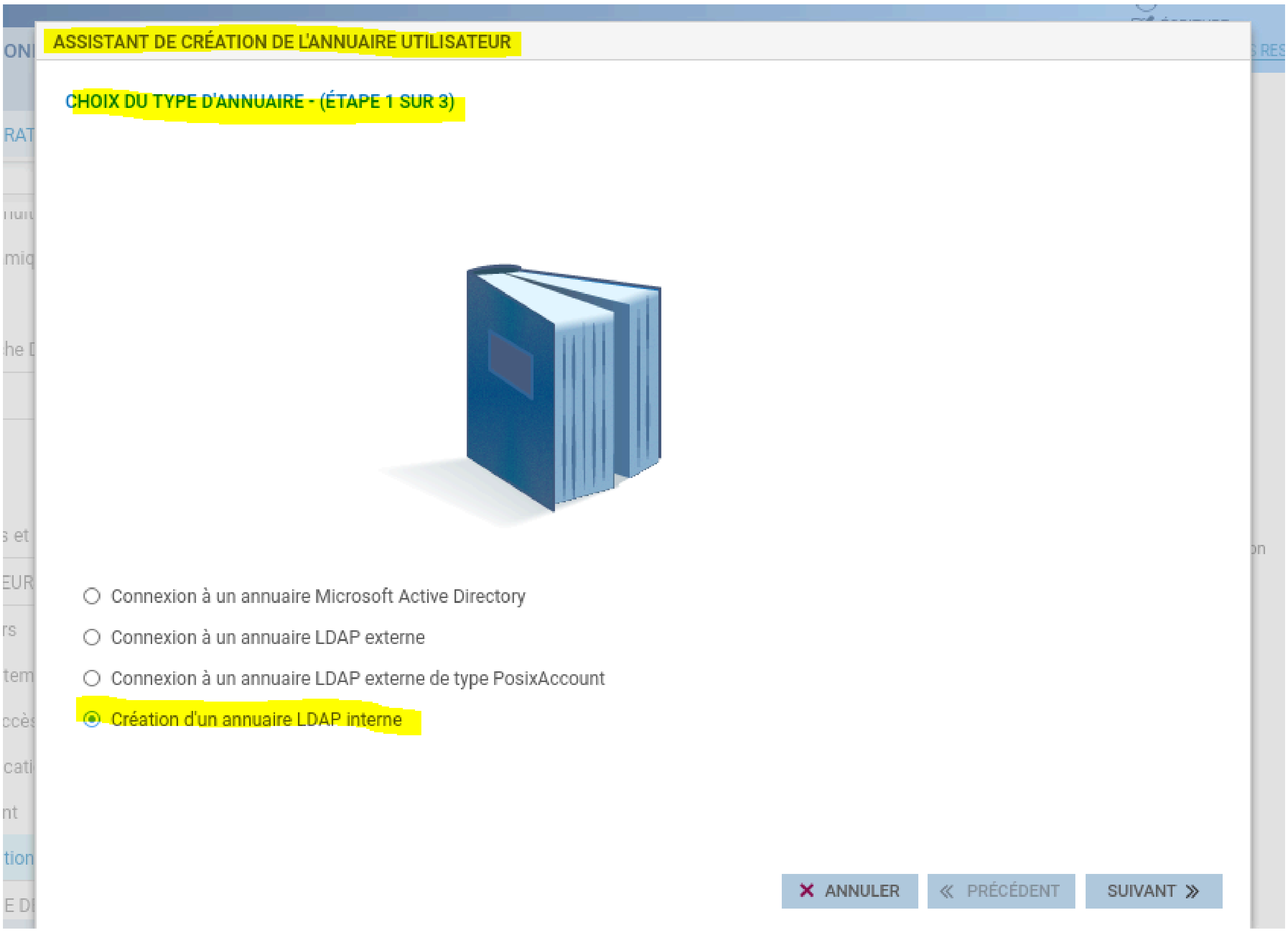
STS eExterne SSL VPN

L'onglet Utilisateurs > Authentification



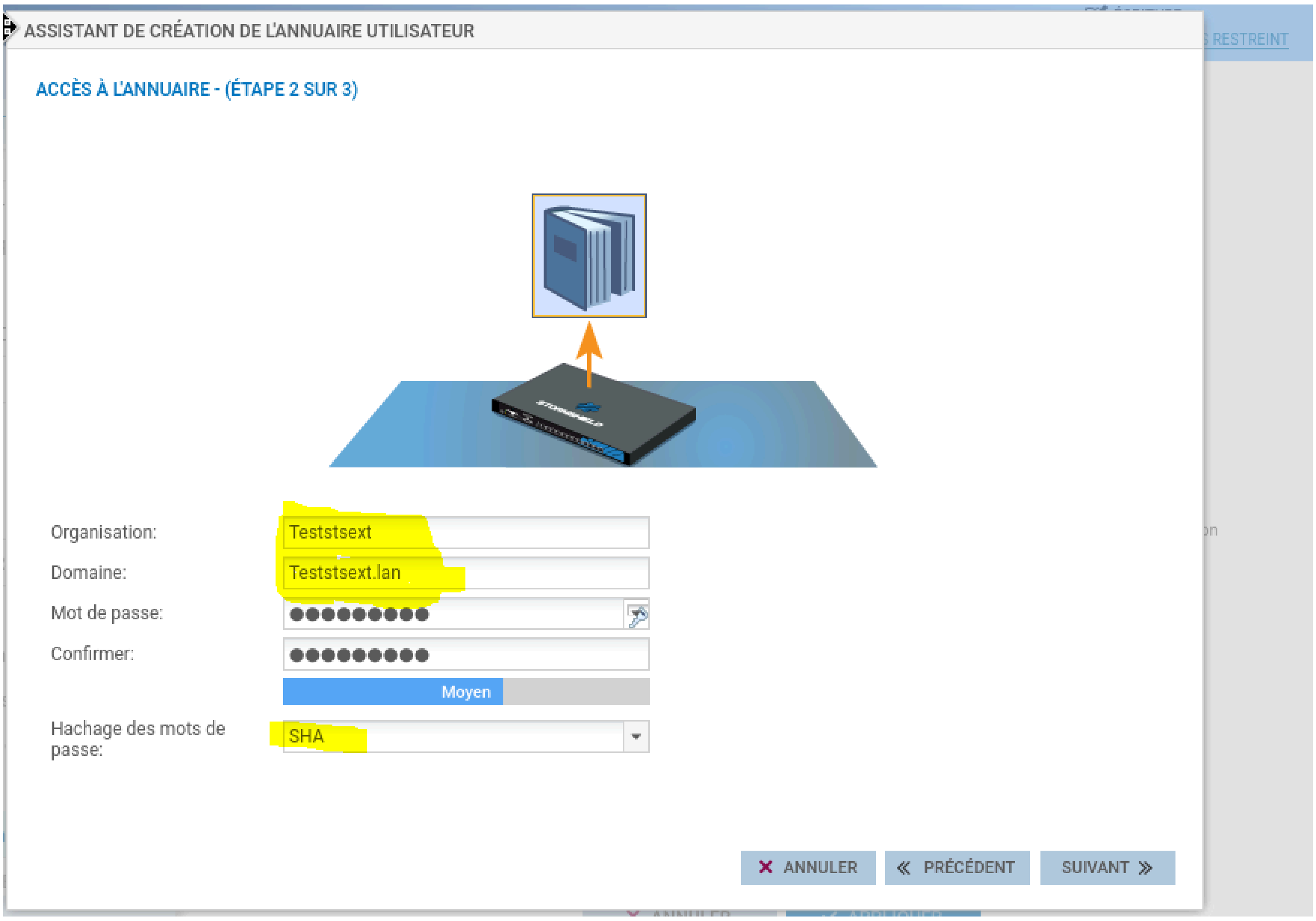
ds

LDAP

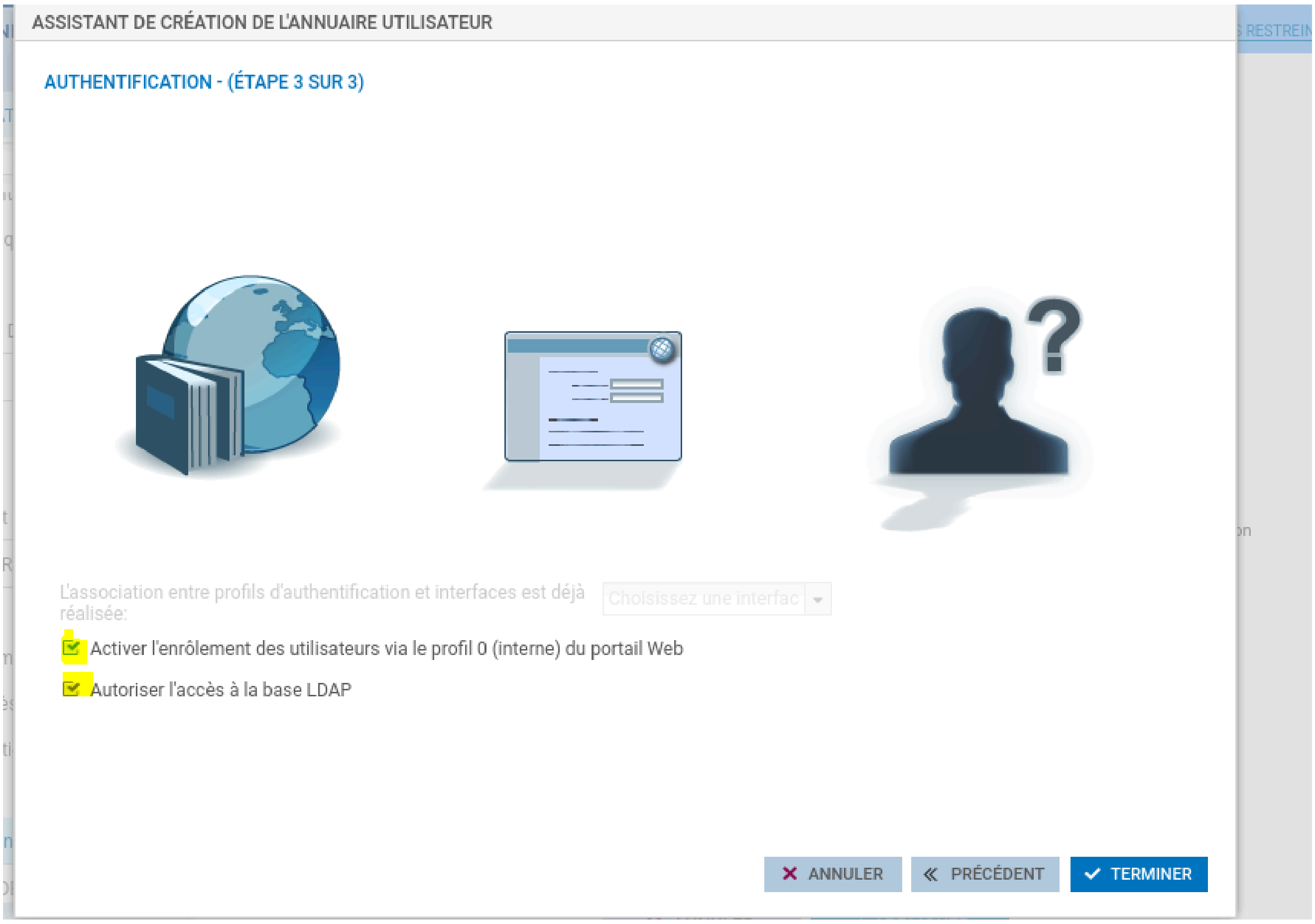


etape 2

mdp :Azerty123



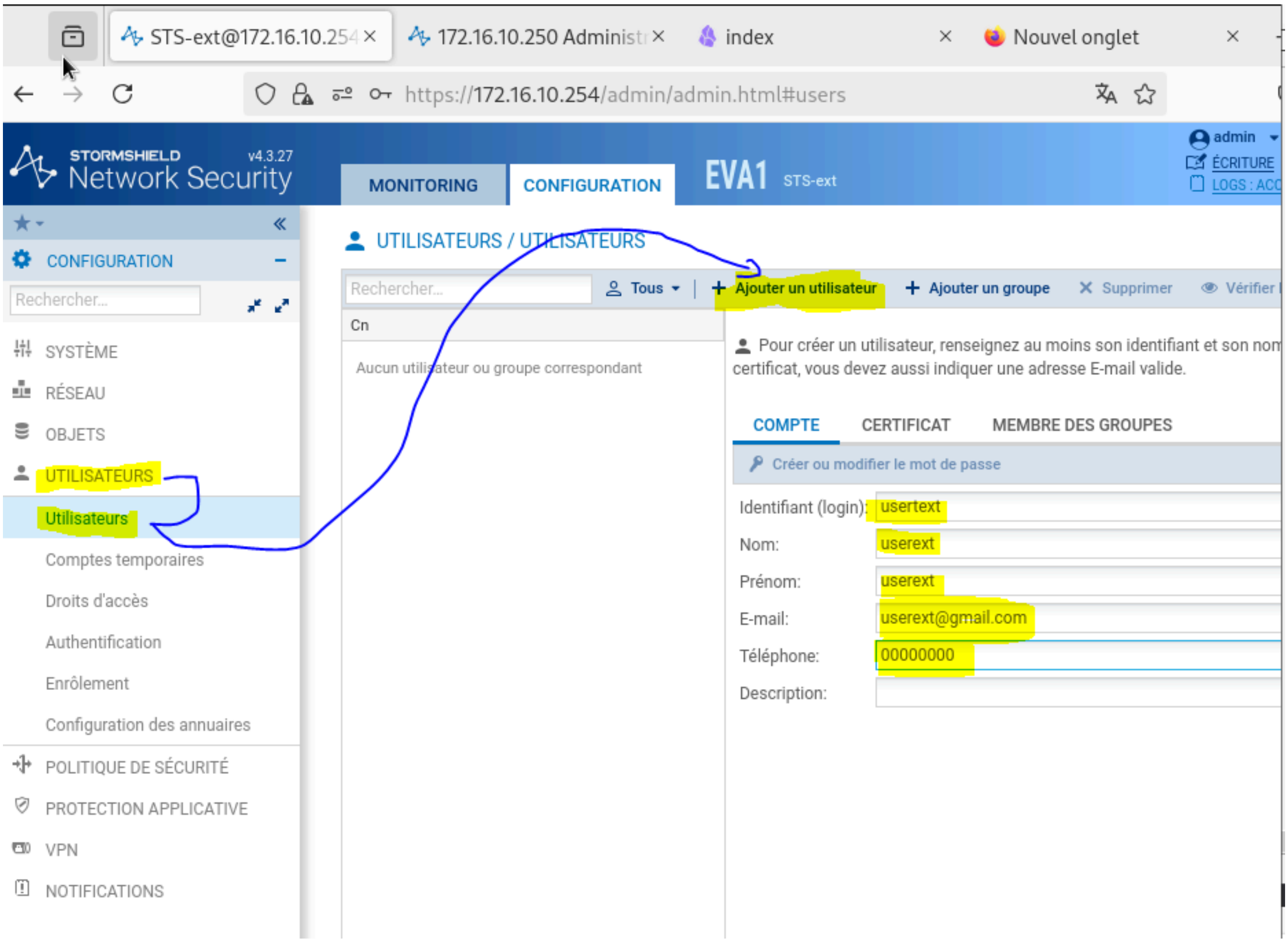
etape 3



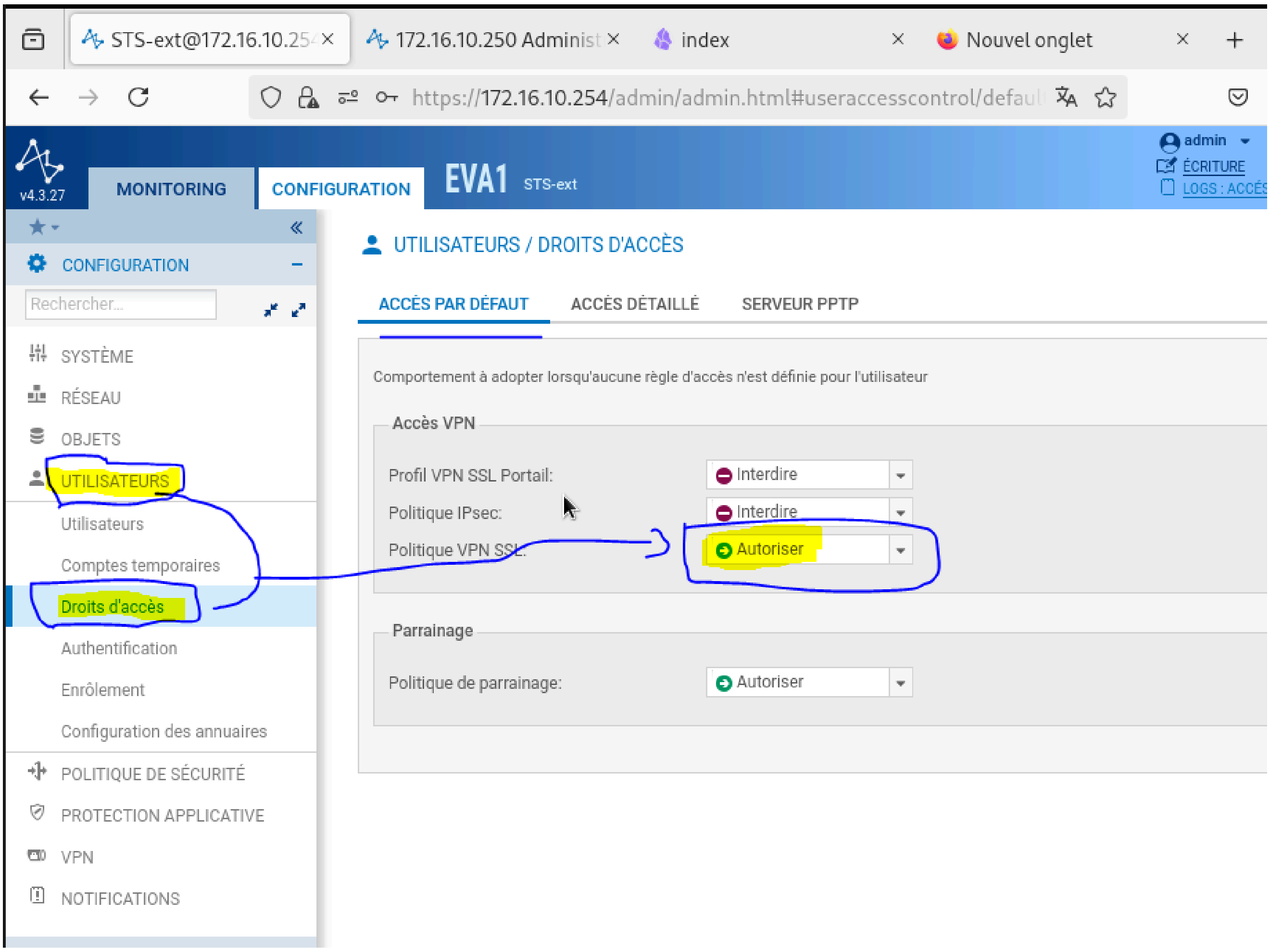
users

pour y acceder via l'application open vpn

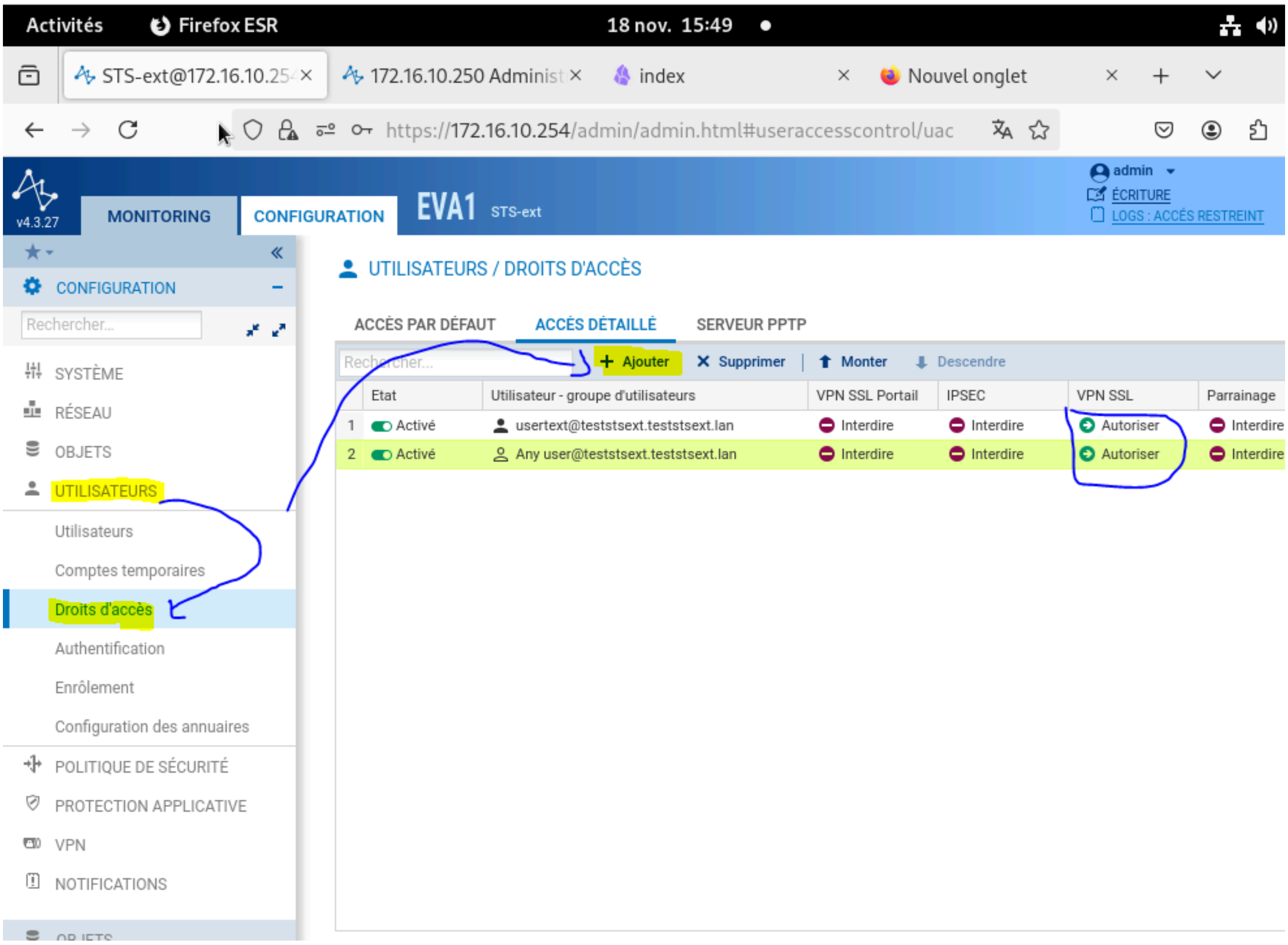
login : usertext
mdp : Azerty123



droit access
acces par defaut faut autoriser SSL

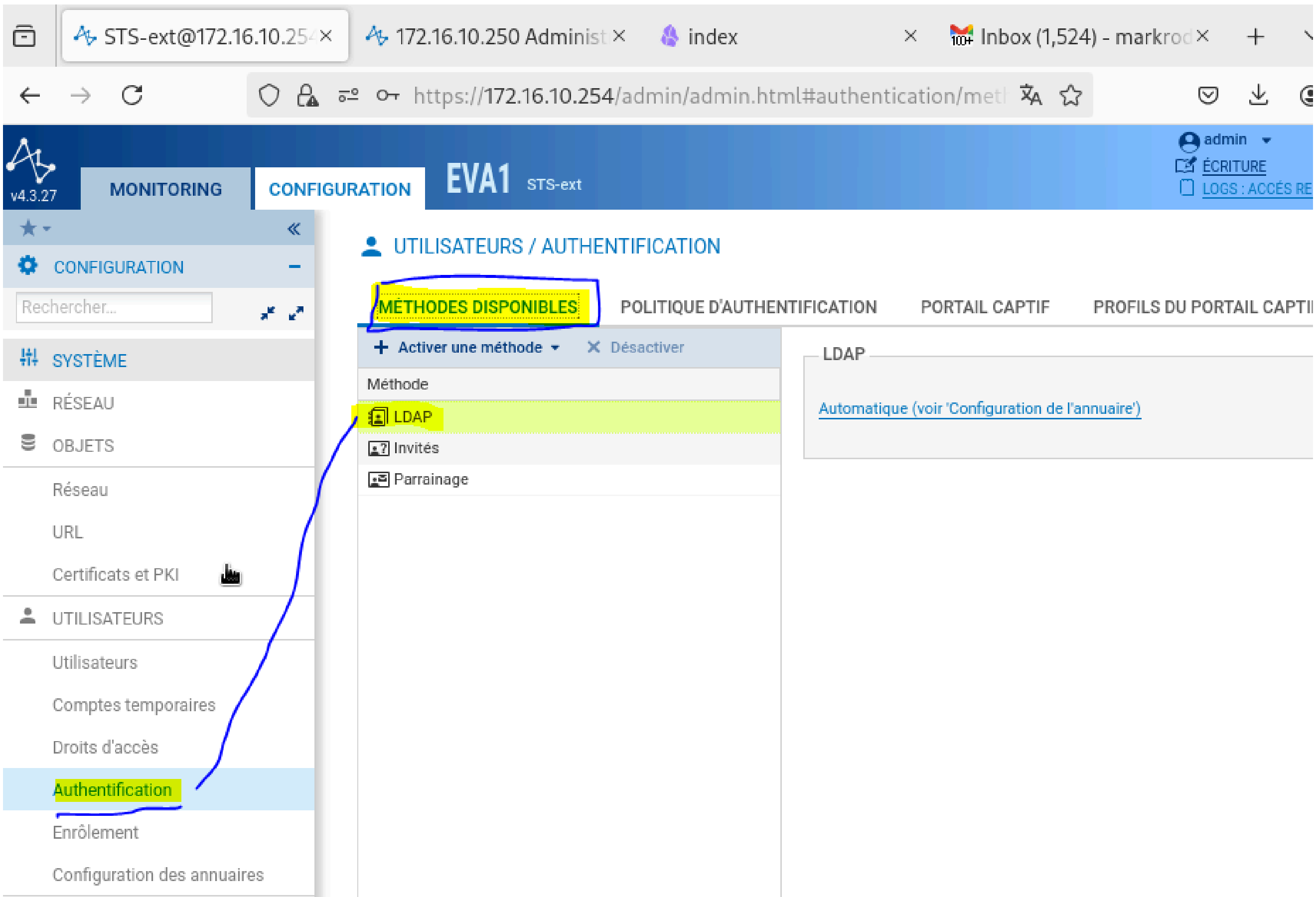


PUIS ACCCESS detailler

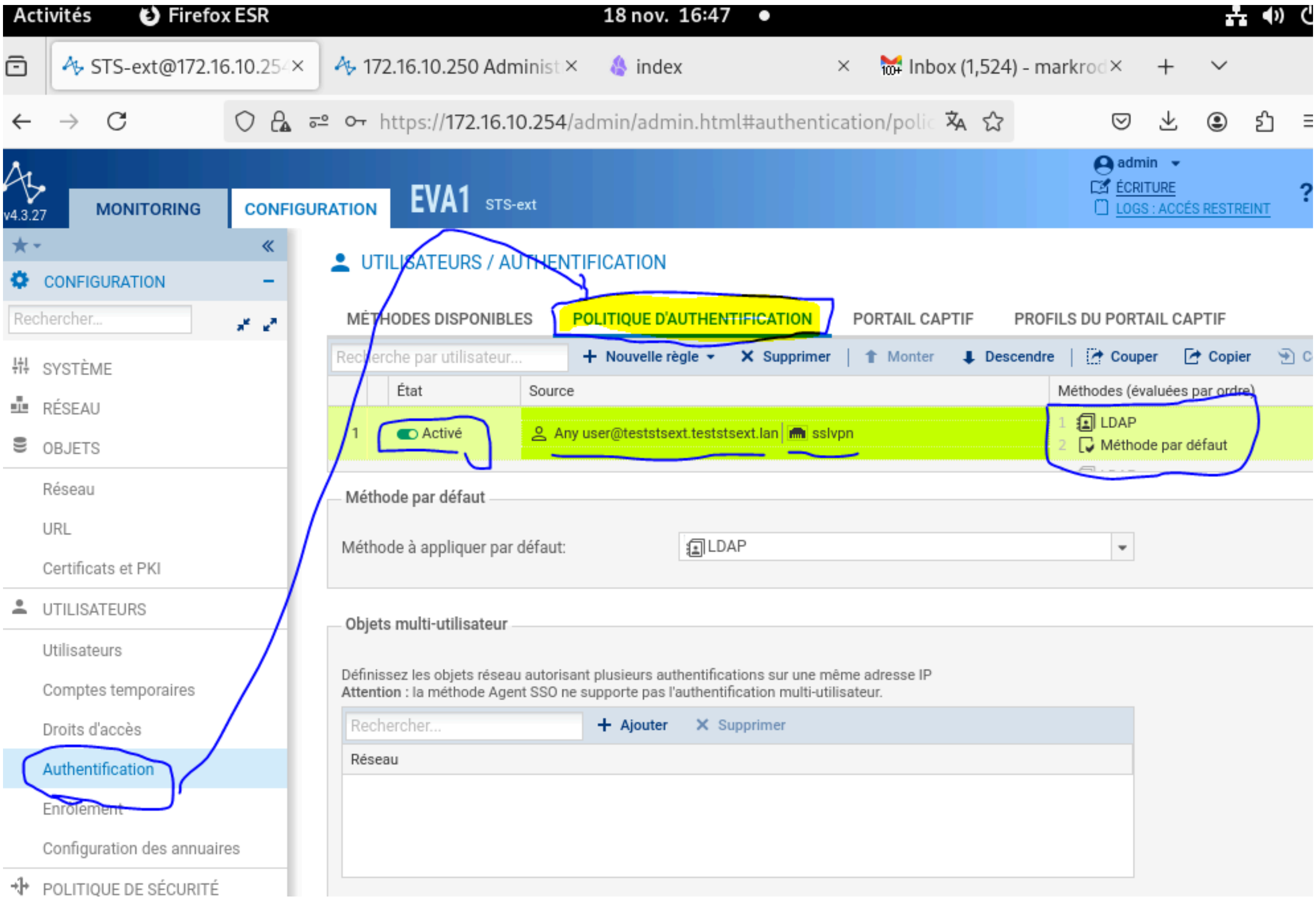


Authentification

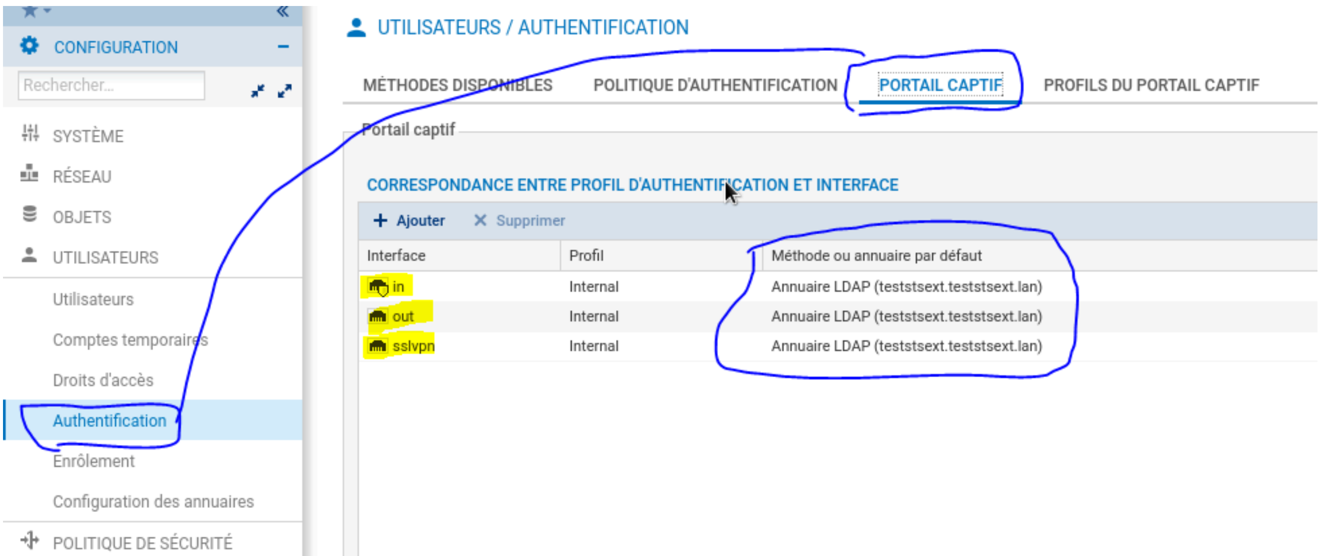
methodes disponibles faut choisir LDAP



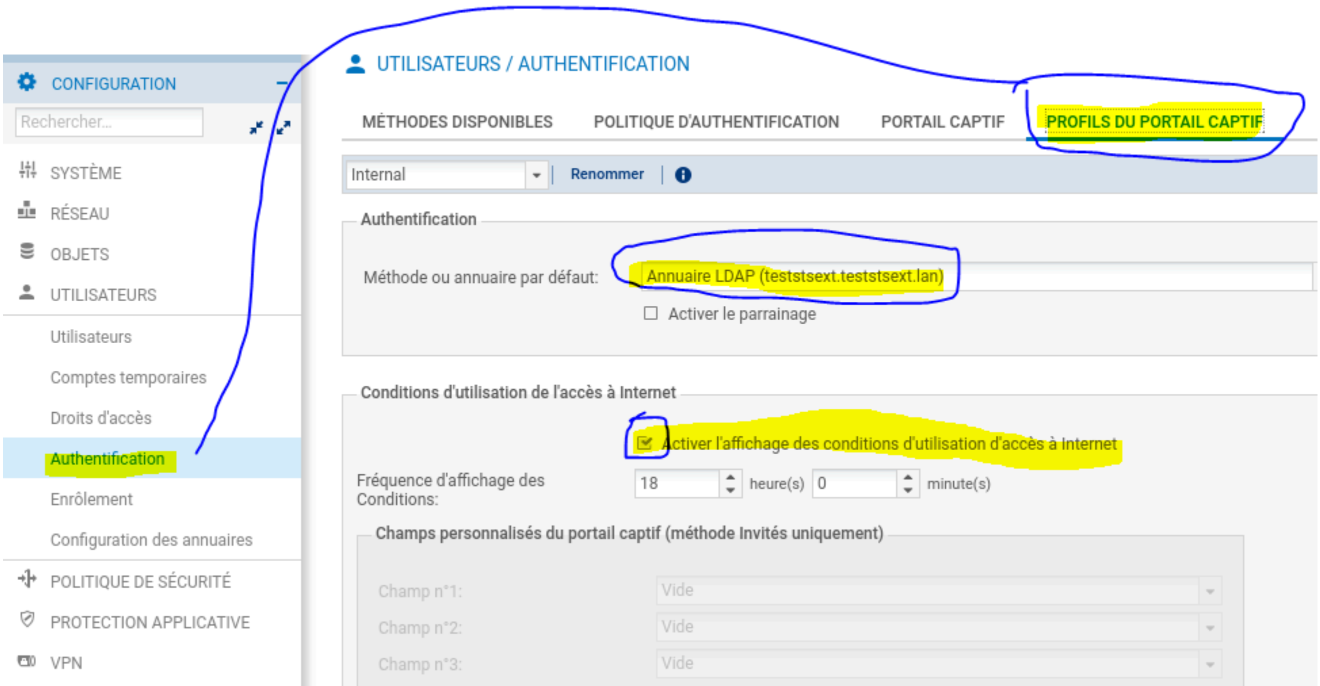
Politique authentification



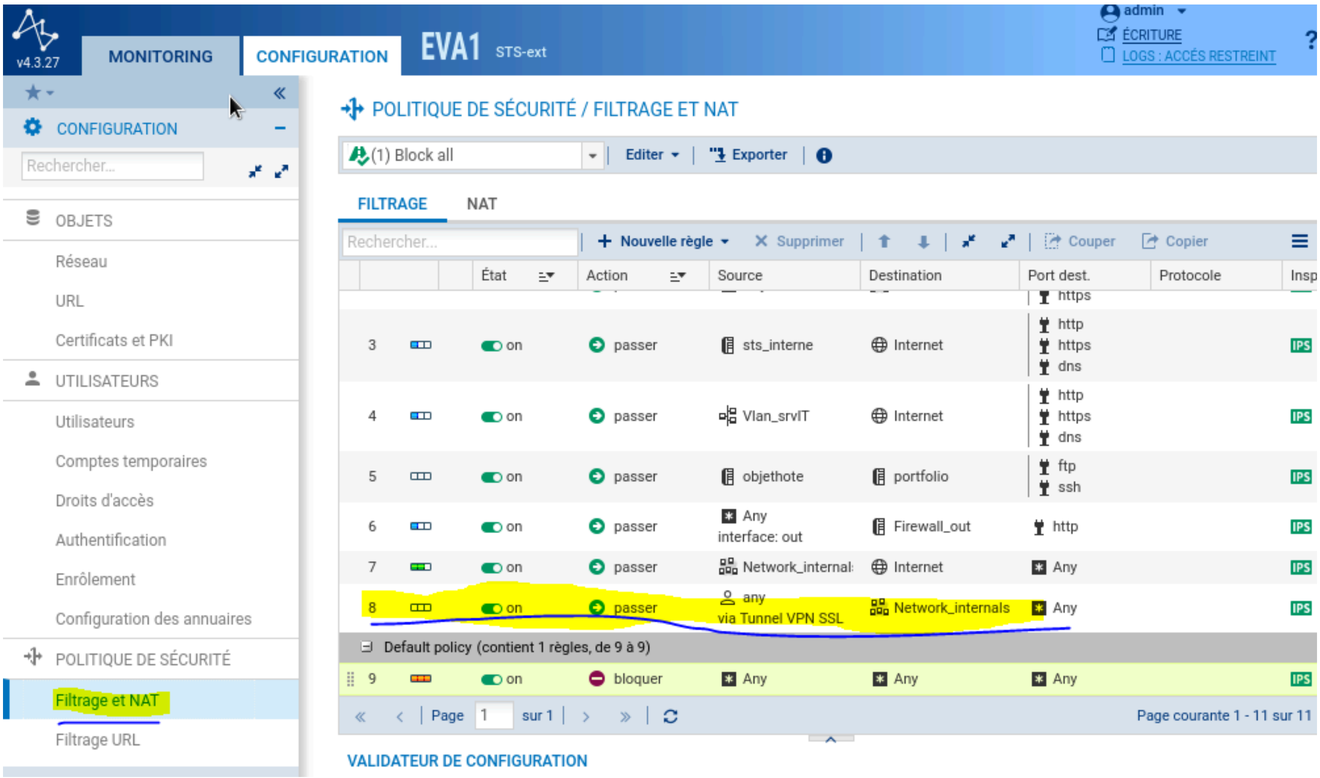
portail captif



profil portail captif

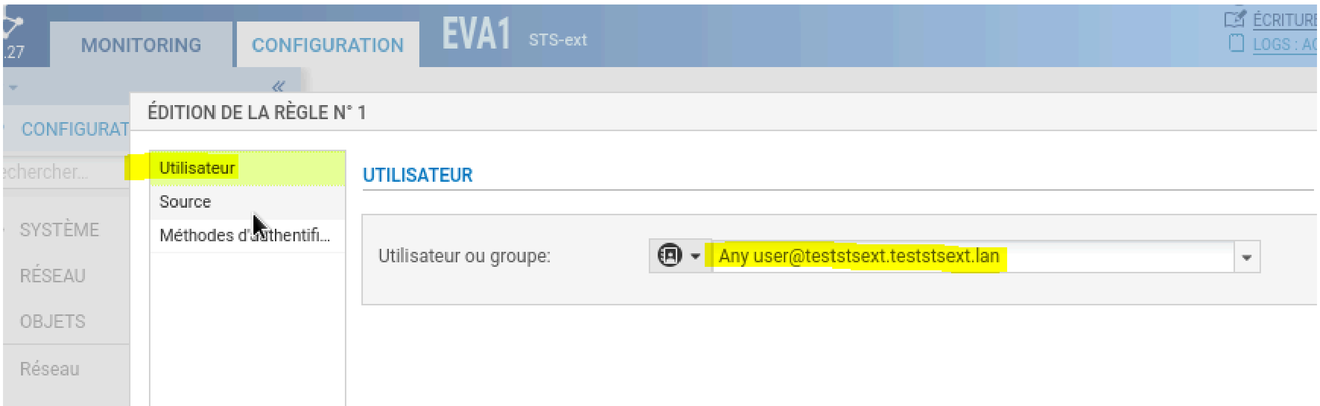


Politique de securité > Filtrage et Nat

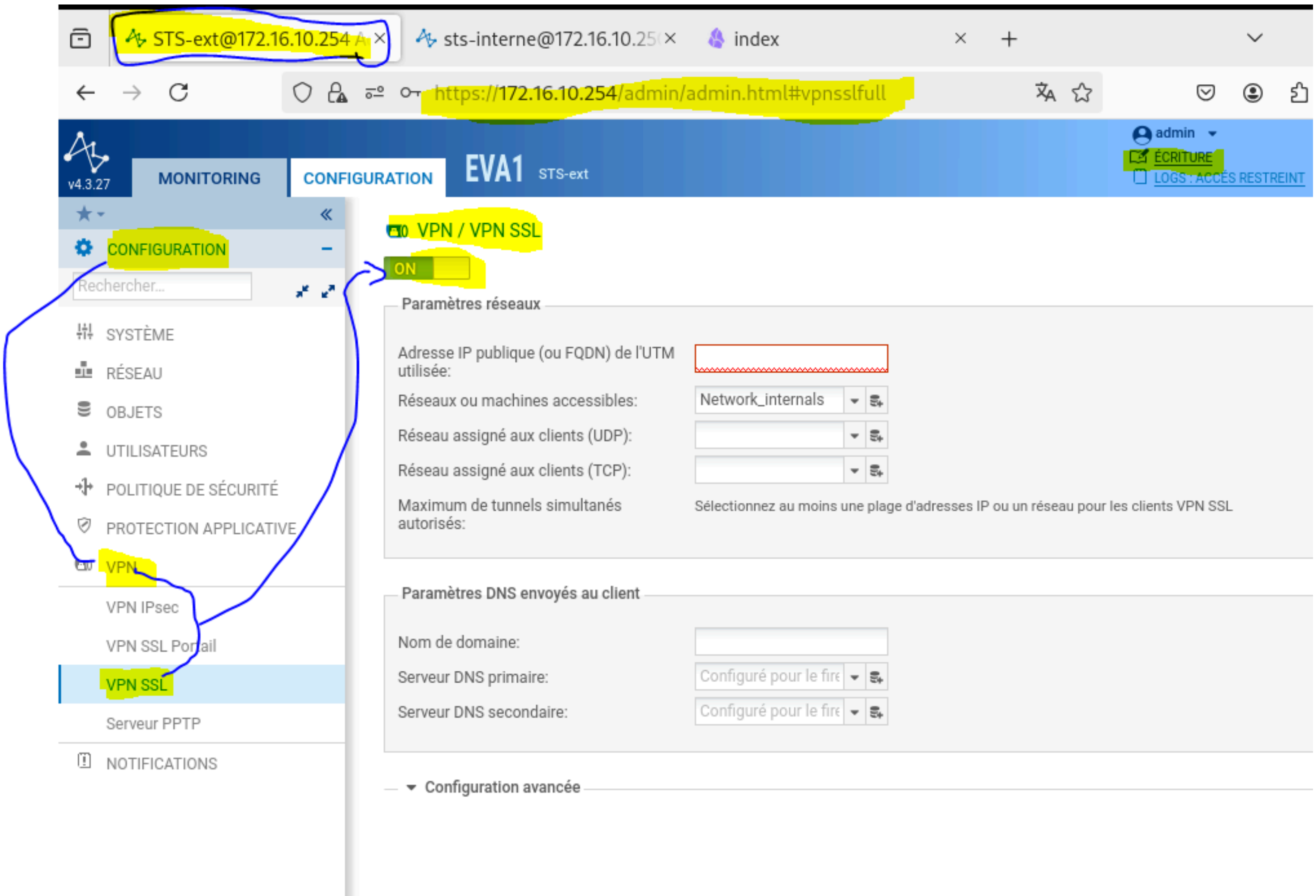


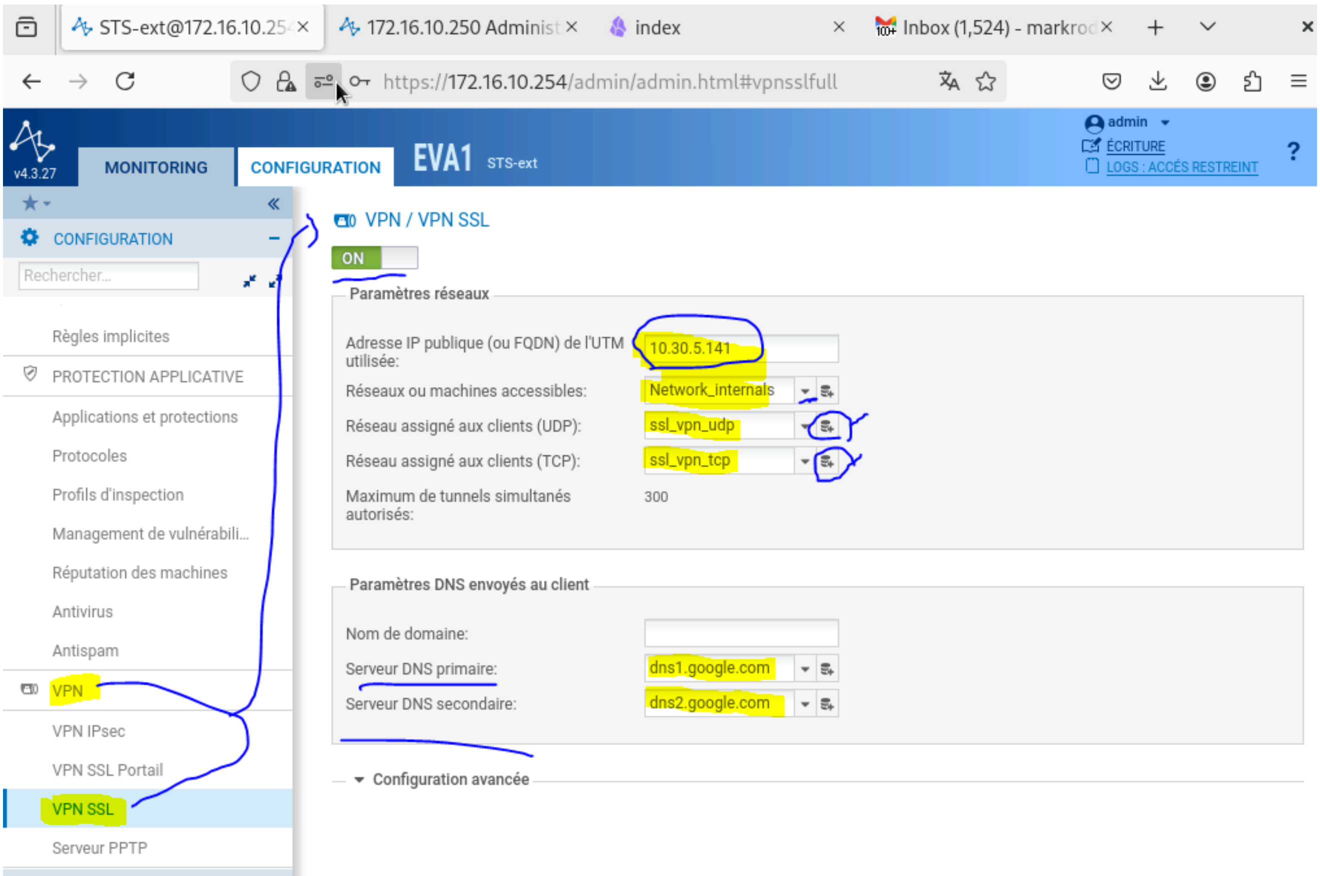
cette regle sur le stormshield

source

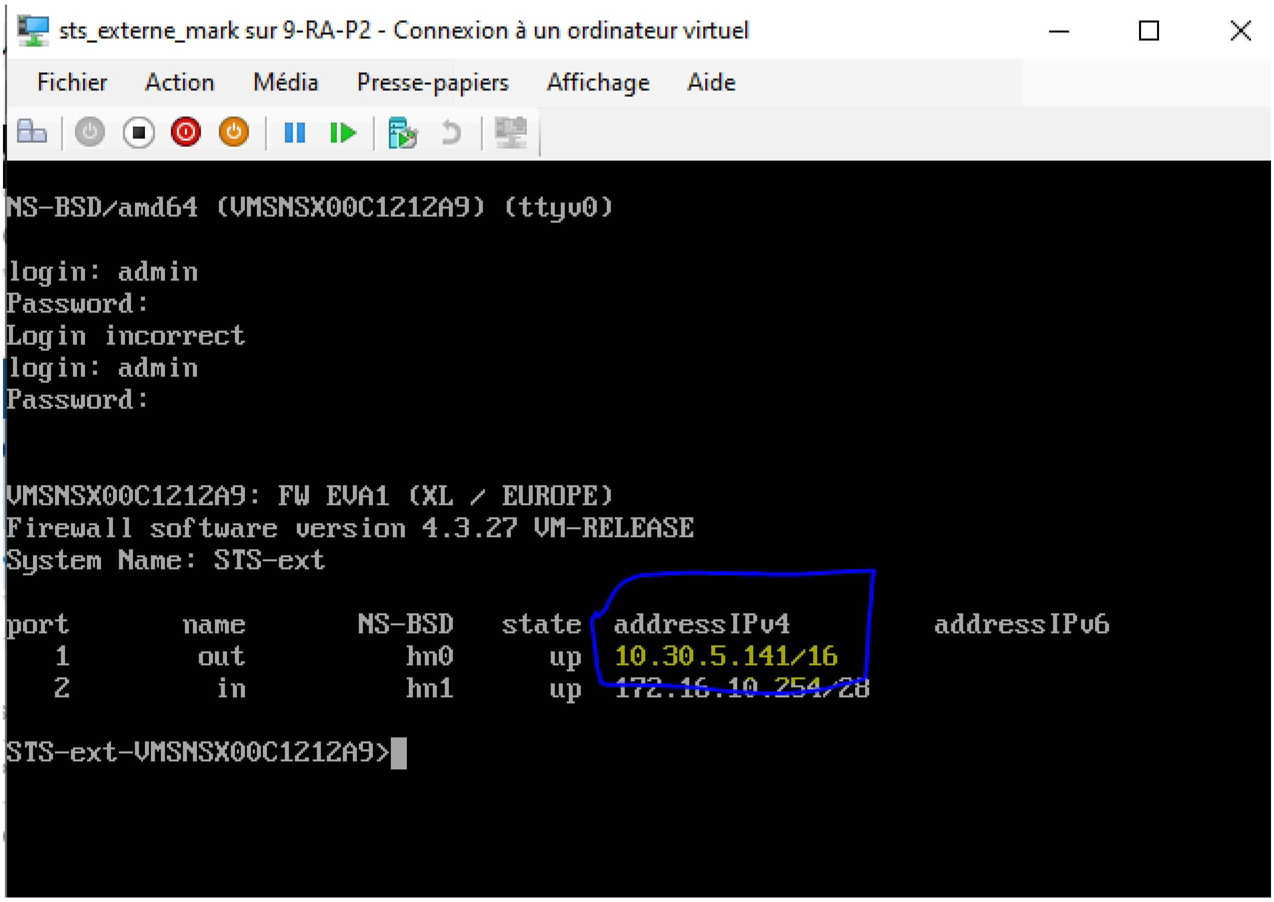


VPN SSL


STS-ext@172.16.10.254
sts-interne@172.16.10.25
index
https://172.16.10.254/admin/admin.html#vpnsslfull
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
CONFIGURATION
Rechercher...
SYSTÈME
RÉSEAU
OBJETS
UTILISATEURS
POLITIQUE DE SÉCURITÉ
PROTECTION APPLICATIVE
VPN
VPN IPsec
VPN SSL Portail
VPN SSL
Serveur PPTP
NOTIFICATIONS
VPN / VPN SSL
ON
Paramètres réseaux
Adresse IP publique (ou FQDN) de l'UTM utilisée:
Réseaux ou machines accessibles:
Network_internals
Réseau assigné aux clients (UDP):
Réseau assigné aux clients (TCP):
Maximum de tunnels simultanés autorisés:
Sélectionnez au moins une plage d'adresses IP ou un réseau pour les clients VPN SSL
Paramètres DNS envoyés au client
Nom de domaine:
Serveur DNS primaire:
Configuré pour le fire
Serveur DNS secondaire:
Configuré pour le fire
Configuration avancée


STS-ext@172.16.10.25
172.16.10.250 Administ
index
Inbox (1,524) - markroc
https://172.16.10.254/admin/admin.html#vpnsslfull
v4.3.27
MONITORING
CONFIGURATION
EVA1
STS-ext
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
CONFIGURATION
Rechercher...
Règles implicites
PROTECTION APPLICATIVE
Applications et protections
Protocoles
Profils d'inspection
Management de vulnérabili...
Réputation des machines
Antivirus
Antispam
VPN
VPN IPsec
VPN SSL Portail
VPN SSL
Serveur PPTP
VPN / VPN SSL
ON
Paramètres réseaux
Adresse IP publique (ou FQDN) de l'UTM utilisée:
10.30.5.141
Réseaux ou machines accessibles:
Network_internals
Réseau assigné aux clients (UDP):
ssl_vpn_udp
Réseau assigné aux clients (TCP):
ssl_vpn_tcp
Maximum de tunnels simultanés autorisés:
300
Paramètres DNS envoyés au client
Nom de domaine:
Serveur DNS primaire:
dns1.google.com
Serveur DNS secondaire:
dns2.google.com
Configuration avancée

10.30.5.141


sts_externe_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
NS-BSD/amd64 (VMSNSX00C1212A9) (ttyv0)
login: admin
Password:
Login incorrect
login: admin
Password:
VMSNSX00C1212A9: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.27 VM-RELEASE
System Name: STS-ext
port name NS-BSD state addressIPv4 addressIPv6
1 out hn0 up 10.30.5.141/16
2 in hn1 up 172.16.10.254/28
STS-ext-VMSNSX00C1212A9>