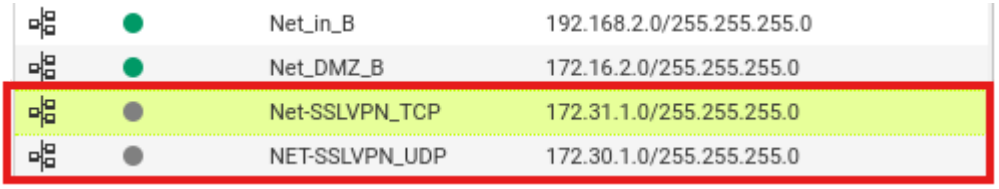
Lab 9 – VPN SSL

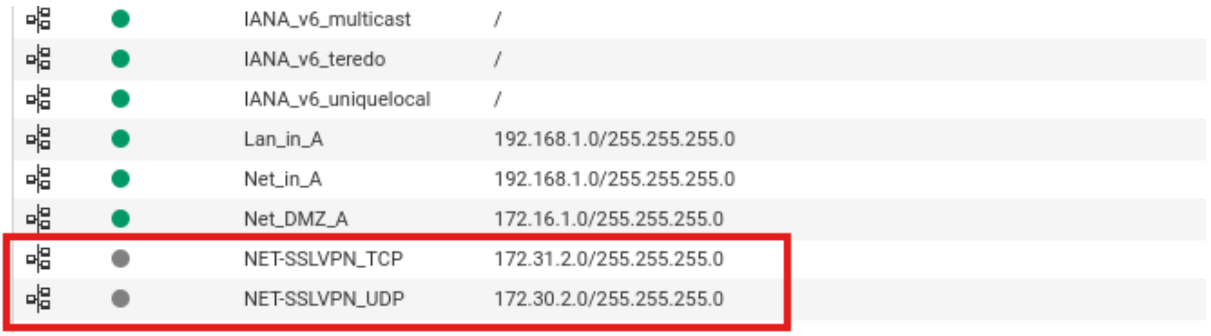
Table des matières :

1. Création des objets réseau

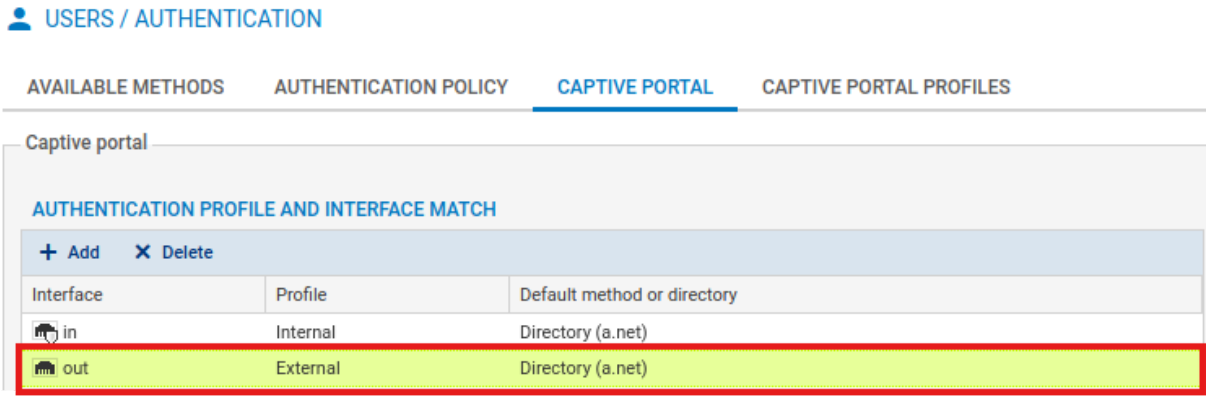
▪ Nous avons créé deux objets réseau pour le VPN SSL :
- Net-SSLVPN_TCP (172.31.x.0/24)
- Net-SSLVPN_UDP (172.30.x.0/24)

Ces réseaux servent à identifier les sous-réseaux utilisés par les connexions VPN SSL.
Nous avons aussi autorisé les utilisateurs externes à accéder au portail captif du pare-feu.





Ces réseaux servent à identifier les sous-réseaux utilisés par les connexions VPN SSL.
Nous avons aussi autorisé les utilisateurs externes à accéder au portail captif du pare-feu.

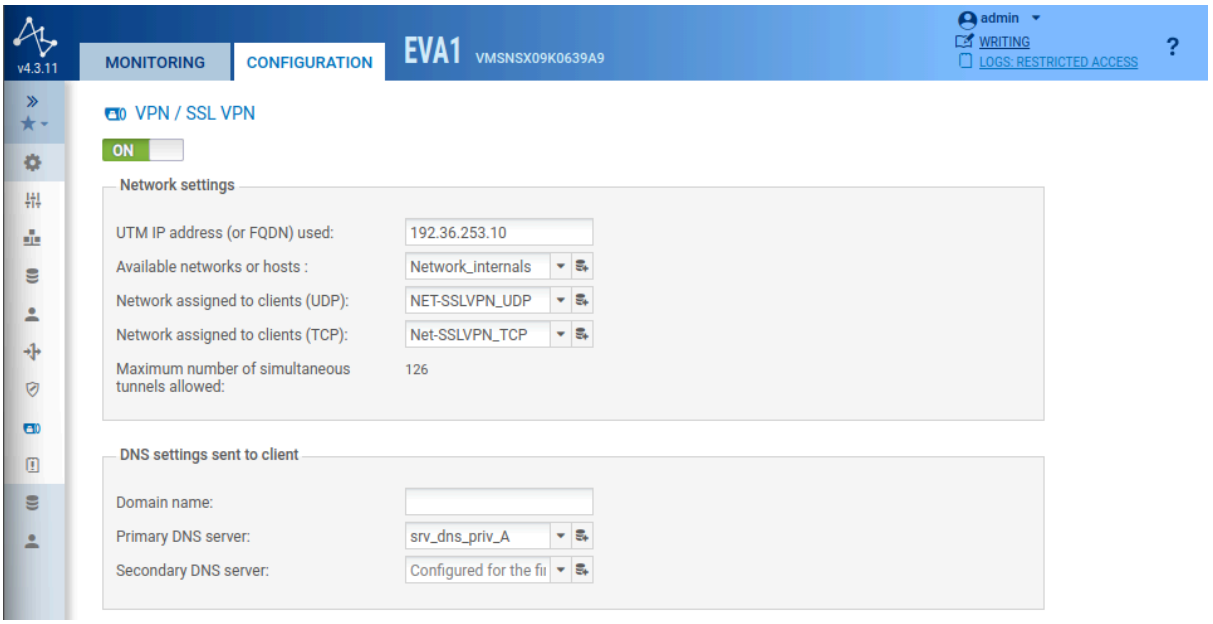


2. Attribution du droit VPN SSL à l'utilisateur John Smith

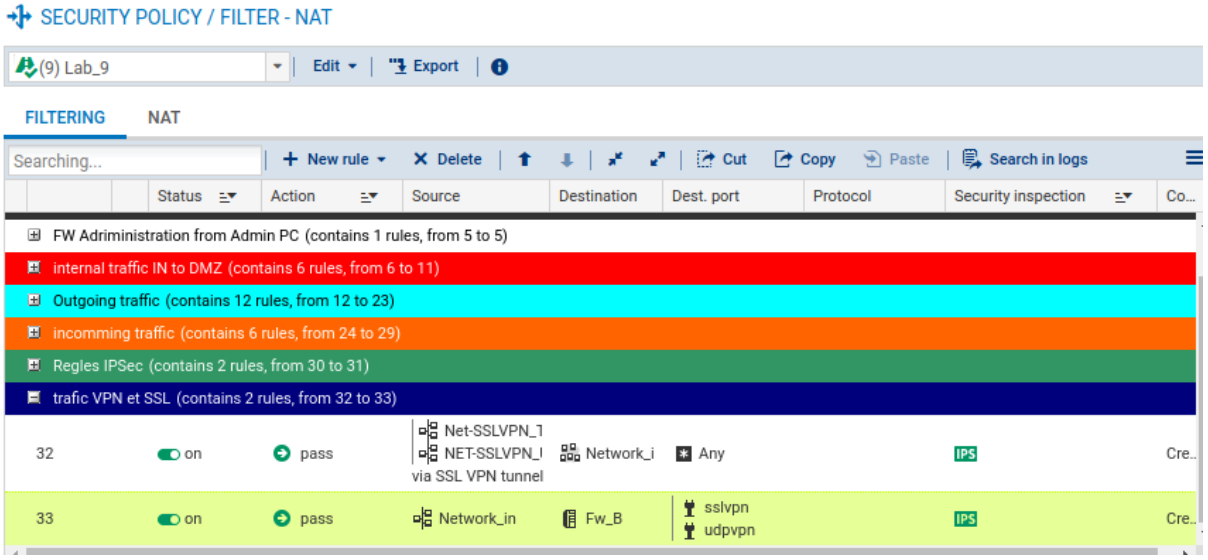
▪ J'ai attribué le droit d'accès VPN SSL à l'utilisateur John Smith via le menu Configuration → Utilisateurs → Droits d'accès → Accès détaillé.
Cette étape permet à John de s'authentifier et d'utiliser le tunnel SSLVPN.

3. Mise en place du filtrage

Cela garantit la communication entre les clients VPN et les ressources internes.



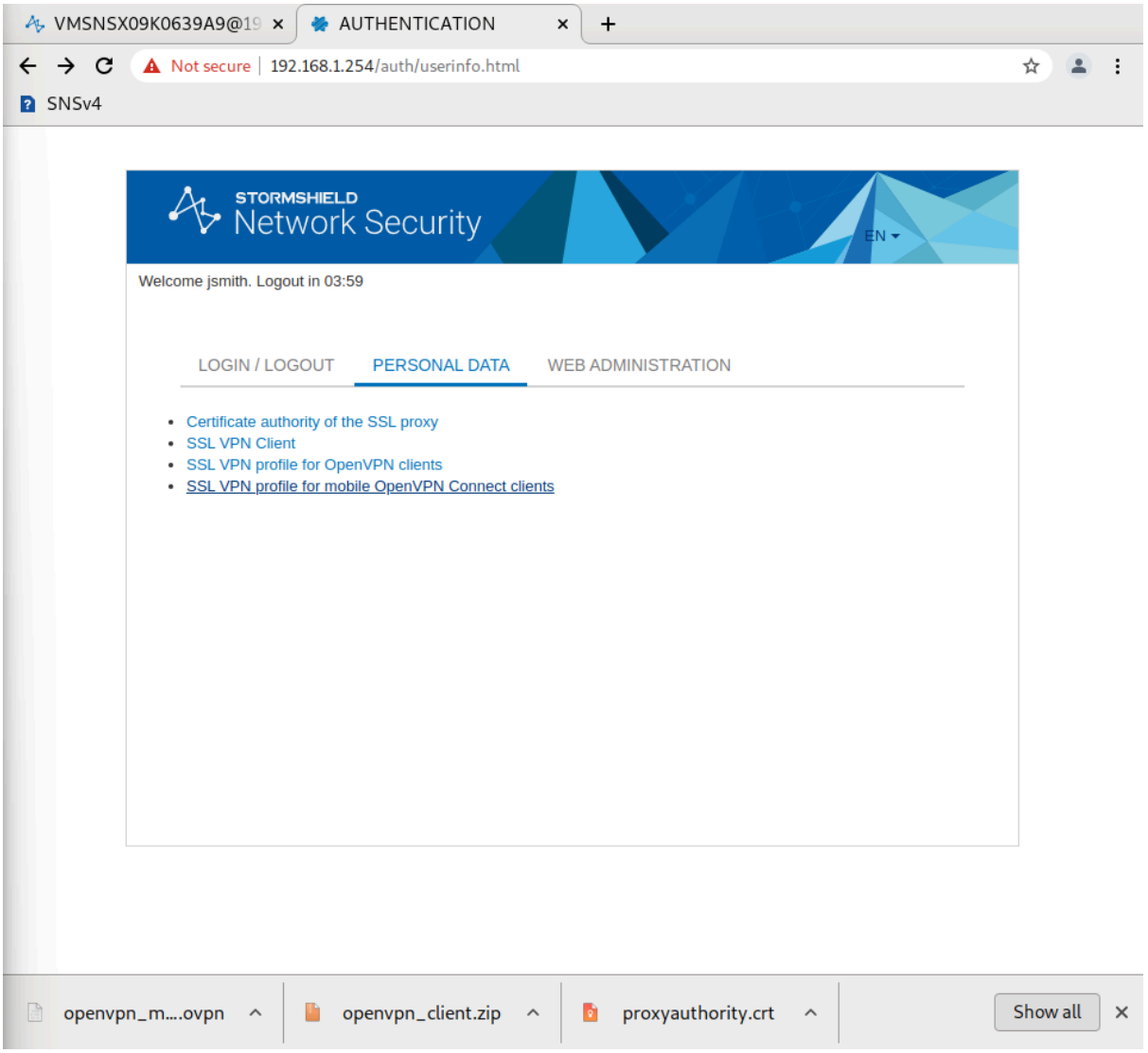
- Nous avons ajouté des règles de filtrage autorisant :
  - notre réseau à accéder aux firewalls voisins sur les ports SSLVPN et UDPVPN,
  - les réseaux Net-SSLVPN_TCP et Net-SSLVPN_UDP à atteindre les réseaux internes.



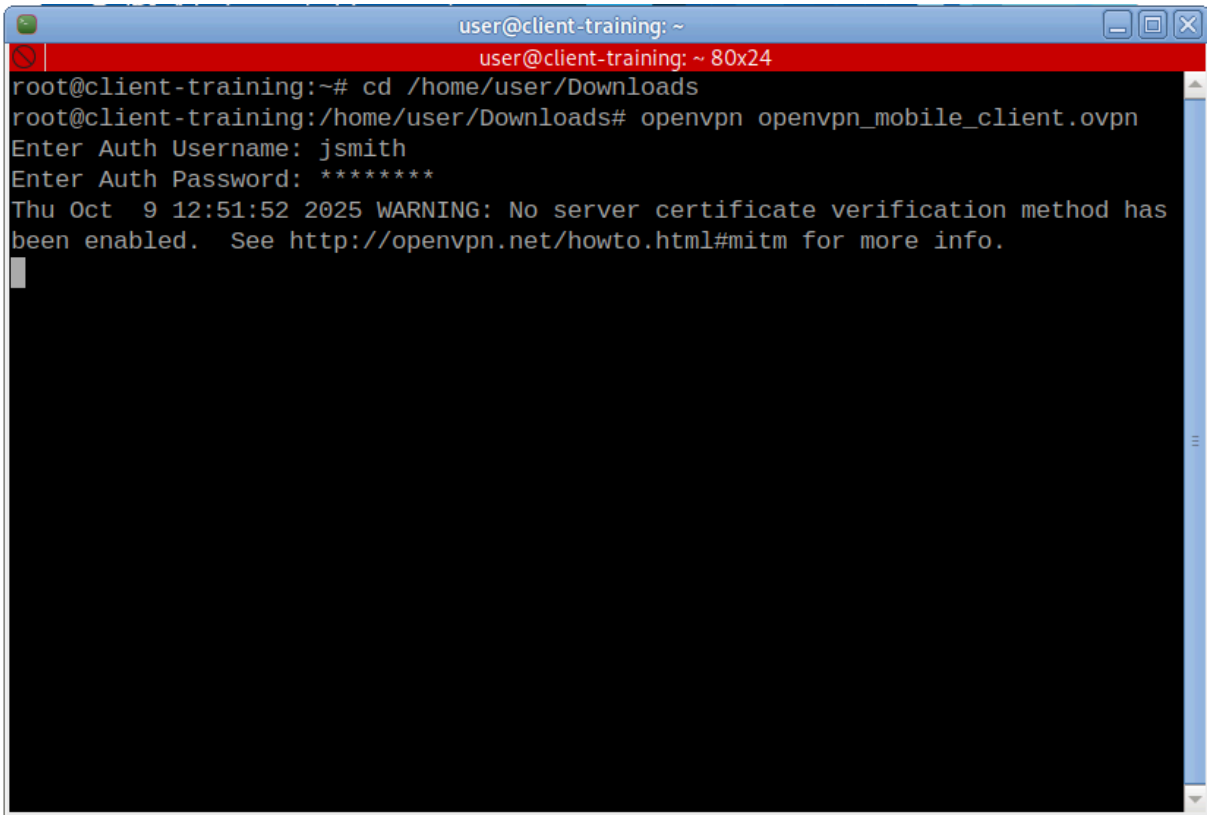
4. Téléchargement et utilisation du profil VPN SSL

Depuis le LAN A, je me suis connecté au portail captif du site B via son IP publique.
J'ai ensuite téléchargé le profil OpenVPN (.ovpn) et l'ai exécuté sur le client pour établir la connexion.

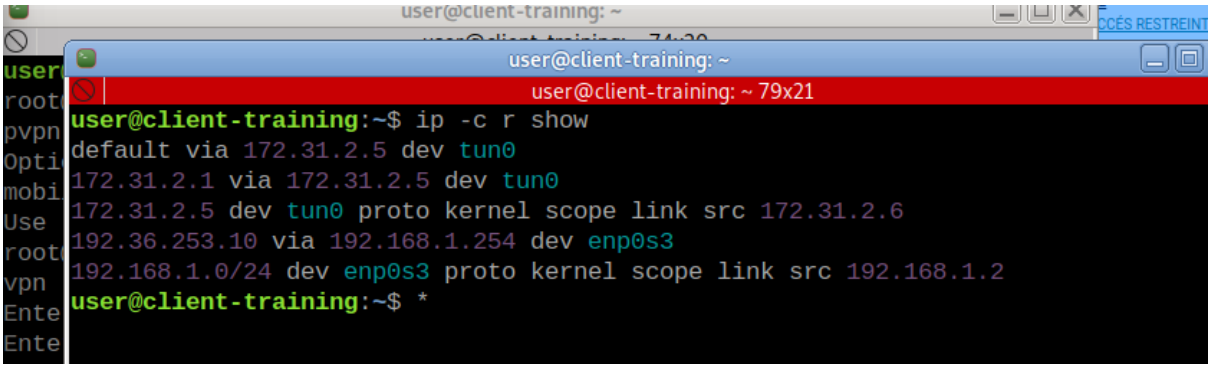
→ Nous nous connectons depuis le LAN A sur le portail captif du SNS B via son IP publique. Puis nous récupérons le ficher "Profil VPN SSL pour clients mobiles OpenVPN Connect"



▪ Après authentification avec jsmith, de nouvelles routes vers les réseaux internes du site B sont ajoutées automatiquement.



▪ Nous constatons l'ajout de routes nous permettant de communiquer avec les réseaux internes du site B.



5. Supervision et vérification de la connexion

▪ Nous avons vérifié dans la supervision du pare-feu que l'utilisateur jsmith était bien connecté au VPN SSL.

MONITOR / TUNNELS VPN IPSEC

Actualiser | Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic l...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic ...
Type : Tunnels site à site (1)							
	OK	Firewall_VTI_vers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTI_B
Type : Politiques d'exception (bypass) (1)							
	Bypass	rfc5735_loopback	localhost		localhost		any

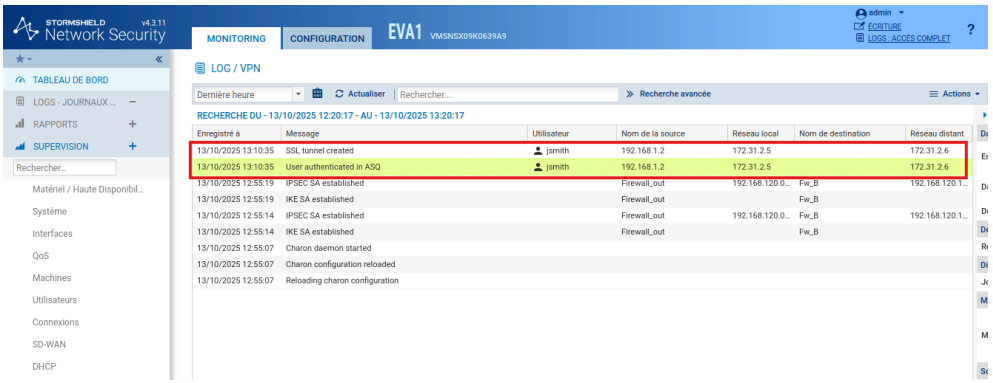
▪ Les journaux VPN confirment l'établissement du tunnel et le trafic vers les serveurs internes.

MONITOR / TUNNELS VPN IPSEC

Actualiser | Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic l...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic ...
Type : Tunnels site à site (1)							
	OK	Firewall_VTI_vers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTI_B
Type : Politiques d'exception (bypass) (1)							
	Bypass	rfc5735_loopback	localhost		localhost		any



▪ Les tests de ping et d'accès au serveur web de la DMZ ont confirmé la réussite de la configuration.