

Lab 9 – VPN SSL

Table des matières :

1. Création des objets réseau.....	2
2. Attribution du droit VPN SSL à l'utilisateur John Smith.....	3
3. Mise en place du filtrage.....	4
4. Téléchargement et utilisation du profil VPN SSL.....	5
5. Supervision et vérification de la connexion.....	7

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.

		Net_in_B	192.168.2.0/255.255.255.0
		Net_DMZ_B	172.16.2.0/255.255.255.0
		Net-SSLVPN_TCP	172.31.1.0/255.255.255.0
		NET-SSLVPN_UDP	172.30.1.0/255.255.255.0

		IANA_v6_multicast	/
		IANA_v6_teredo	/
		IANA_v6_uniquelocal	/
		Lan_in_A	192.168.1.0/255.255.255.0
		Net_in_A	192.168.1.0/255.255.255.0
		Net_DMZ_A	172.16.1.0/255.255.255.0
		NET-SSLVPN_TCP	172.31.2.0/255.255.255.0
		NET-SSLVPN_UDP	172.30.2.0/255.255.255.0

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.

USERS / AUTHENTICATION

AVAILABLE METHODS	AUTHENTICATION POLICY	CAPTIVE PORTAL	CAPTIVE PORTAL PROFILES
Captive portal			
AUTHENTICATION PROFILE AND INTERFACE MATCH			
+ Add X Delete			
Interface	Profile	Default method or directory	
in	Internal	Directory (a.net)	
out	External	Directory (a.net)	

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.

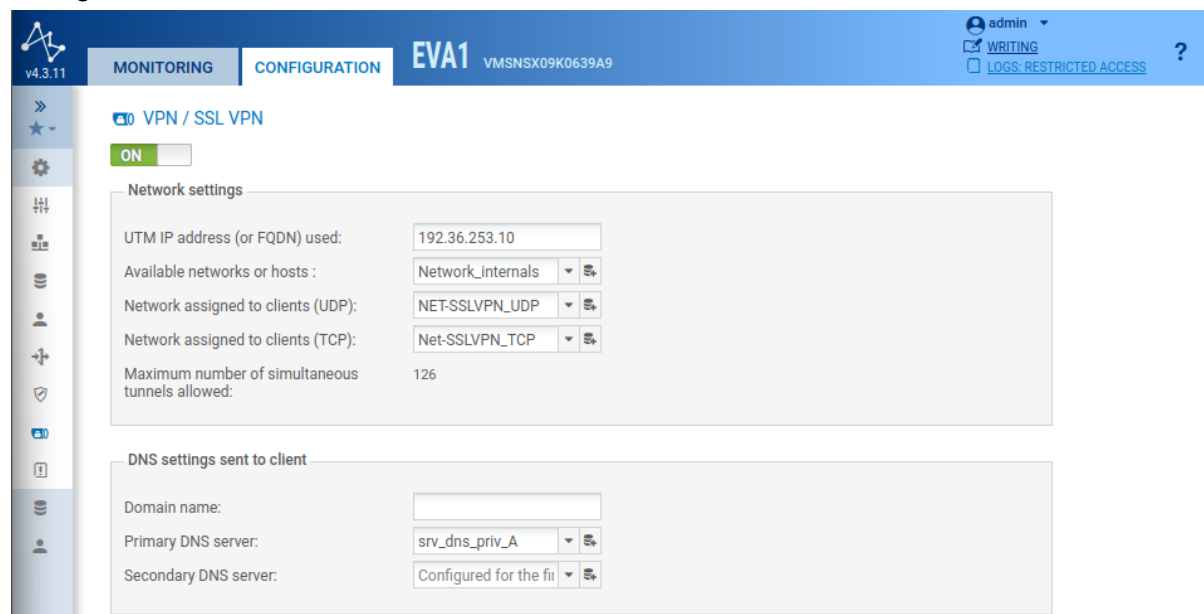
Cette étape permet à John de s'authentifier et d'utiliser le tunnel SSLVPN.

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT		ACCÈS DÉTAILLÉ	SERVEUR PPTP				
Rechercher...		+ Ajouter	X Supprimer	↑ Monter	↓ Descendre		
	Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Description
1	 Activé	 jsmith@b.net	 Interdire	 Interdire	 Autoriser	 Interdire	

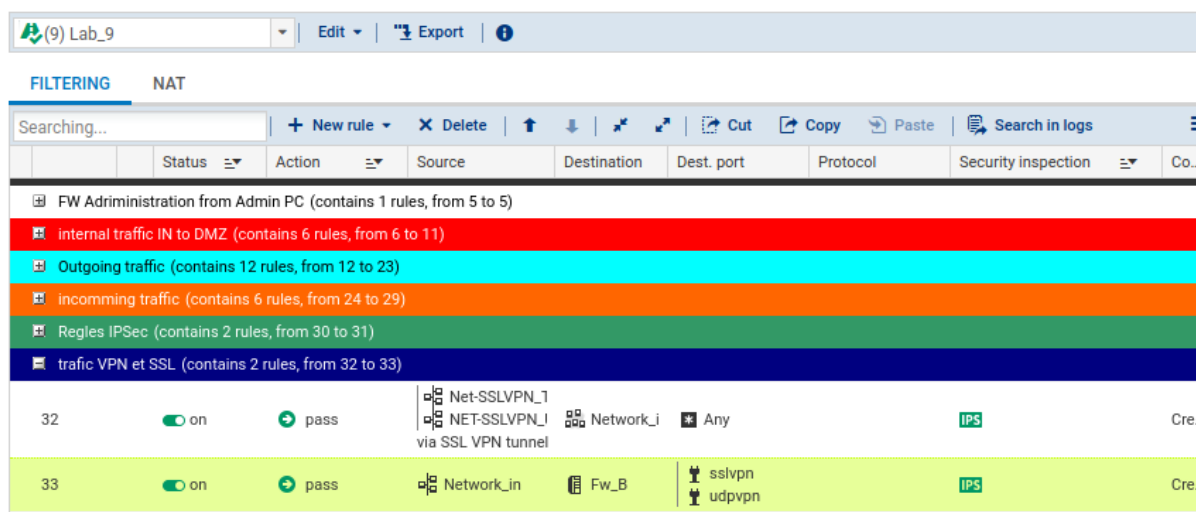
3. Mise en place du filtrage

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.

SECURITY POLICY / FILTER - NAT



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.

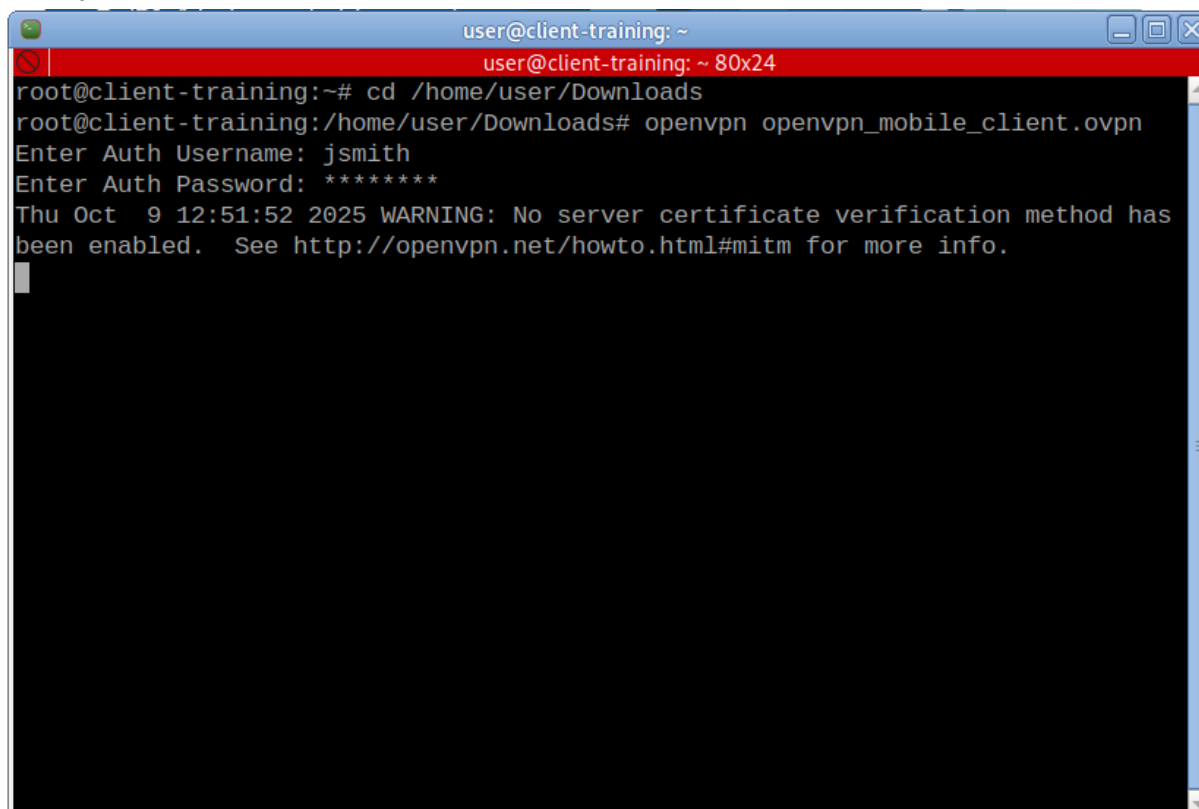
→ Nous nous connectons depuis le LAN A sur le portail captif du SNS B via son IP publique. Puis nous récupérons le fichier "Profil VPN SSL pour clients mobiles OpenVPN Connect"

The screenshot shows a web browser window with the address bar displaying "192.168.1.254/auth/userinfo.html". The page title is "VMSNSX09K0639A9@19 AUTHENTICATION". The main content area is titled "STORMSHIELD Network Security" and includes a welcome message "Welcome jsmith. Logout in 03:59". Below the header, there are three tabs: "LOGIN / LOGOUT", "PERSONAL DATA", and "WEB ADMINISTRATION". The "PERSONAL DATA" tab is active, showing a list of links:

- [Certificate authority of the SSL proxy](#)
- [SSL VPN Client](#)
- [SSL VPN profile for OpenVPN clients](#)
- [SSL VPN profile for mobile OpenVPN Connect clients](#)

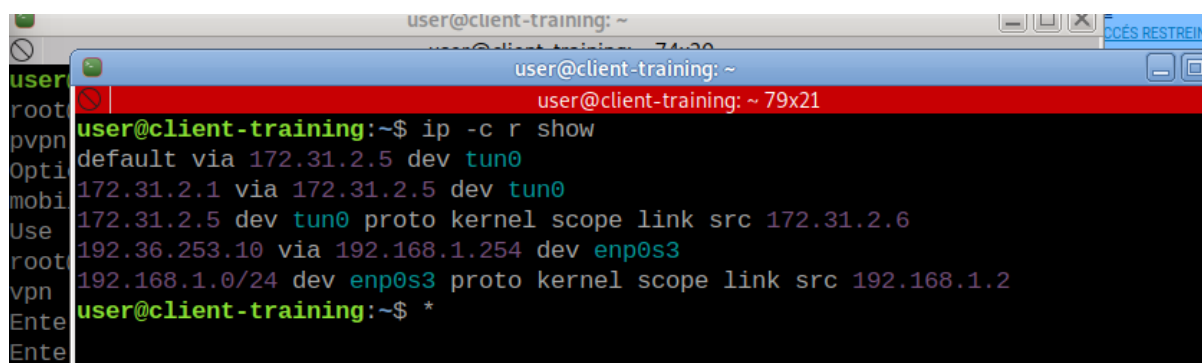
At the bottom of the browser window, the file manager shows three downloaded files: "openvpn_m....ovpn", "openvpn_client.zip", and "proxyauthority.crt". A "Show all" button is visible next to the file list.

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



```
user@client-training: ~  
user@client-training: ~ 80x24  
root@client-training:~# cd /home/user/Downloads  
root@client-training:/home/user/Downloads# openvpn openvpn_mobile_client.ovpn  
Enter Auth Username: jsmith  
Enter Auth Password: *****  
Thu Oct 9 12:51:52 2025 WARNING: No server certificate verification method has  
been enabled. See http://openvpn.net/howto.html#mitm for more info.
```

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



```
user@client-training: ~  
user@client-training: ~ 74x20  
user@client-training: ~ 79x21  
root@client-training:~$ ip -c r show  
default via 172.31.2.5 dev tun0  
172.31.2.1 via 172.31.2.5 dev tun0  
172.31.2.5 dev tun0 proto kernel scope link src 172.31.2.6  
192.36.253.10 via 192.168.1.254 dev enp0s3  
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.2  
user@client-training:~$ *
```

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	OK	Firewall_VTL_vers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTL_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	OK	Firewall_VTL_vers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTL_B
Type : Politiques d'exception (bypass) (1)							
Bypass		rfc5735_loopback	localhost		localhost		any

STORMSHIELD Network Security v4.3.11

MONITORING CONFIGURATION EVA1 VM5NSX09W0639A9

admin

LOGS - JOURNAUX ...

RAPPORTS

SUPERVISION

Rechercher...

Matériel / Haute Disponibil...

Système

Interfaces

QoS

Machines

Utilisateurs

Connexions

SD-WAN

DHCP

LOG / VPN

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 13/10/2025 12:20:17 - AU - 13/10/2025 13:20:17

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destination	Réseau distant
13/10/2025 13:10:35	SSL tunnel created	jsmith	192.168.1.2	172.31.2.5		172.31.2.6
13/10/2025 13:10:35	User authenticated in ASD	jsmith	192.168.1.2	172.31.2.5		172.31.2.6
13/10/2025 12:55:19	IPSEC SA established		Firewall_out	192.168.120.0..	Fw_B	192.168.120.1..
13/10/2025 12:55:19	IKE SA established		Firewall_out		Fw_B	
13/10/2025 12:55:14	IPSEC SA established		Firewall_out	192.168.120.0..	Fw_B	192.168.120.1..
13/10/2025 12:55:14	IKE SA established		Firewall_out		Fw_B	
13/10/2025 12:55:07	Charon daemon started					
13/10/2025 12:55:07	Charon configuration reloaded					
13/10/2025 12:55:07	Reloading charon configuration					

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

