

Lab9 – VPN SSL

➤ Je copie la politique de filtrage LAB_8 en LAB_9 :

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(9) Lab_9 | Editer | Exporter | i

FILTRAGE NAT

Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ | Couper | Copier | Coller

| | État | Action | Source | Destination | Port dest. | Protocole | Inspection de sécurité | Comment... |
|---|------|--------|------------------------------------|-------------------|-----------------------|-------------------|------------------------|---------------|
| 1 | off | passer | Any | Any | Any | | IPS | Créée le 2... |
| 2 | on | passer | Any | Firewall | isakmp isakmp_natt | | IPS | Créée le 2... |
| 3 | on | passer | Any | Firewall | Any | vpn-esp | IPS | Créée le 2... |
| Inoming traffic from IPSec (contient 8 règles, de 4 à 11) | | | | | | | | |
| 4 | on | passer | Network | Lan_in_ DMZ_In | Any | icmp (requête Ech | IPS | Créée le 2... |
| 5 | on | passer | Lan_in_I interface: VT | Network | Any | icmp (requête Ech | IPS | Créée le 2... |
| 6 | on | passer | Lan_in_ DMZ_Ir via Tunnel VF | Networ Networ | Any | icmp (requête Ech | IPS | Créée le 2... |
| 7 | on | passer | Lan_in_ DMZ_Ir via Tunnel VF | srv_ftp_ | ftp | | IPS | Créée le 2... |
| 8 | on | passer | Lan_in_ DMZ_Ir via Tunnel VF | srv_web | http | | IPS | Créée le 2... |
| 9 | on | passer | Network | srv_ftp_ | ftp | | IPS | Créée le 2... |

Page 1 sur 1 | Page courante 1 - 43 sur 43

➤ Je permets aux utilisateurs externes de se connecter au portail captif :

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES | POLITIQUE D'AUTHENTIFICATION | **PORTAIL CAPTIF** | PROFILS DU PORTAIL CAPTIF

Portail captif

CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE

+ Ajouter | X Supprimer

| Interface | Profil | Méthode ou annuaire par défaut |
|-----------|----------|--------------------------------|
| in | Internal | Annuaire LDAP (a.net) |
| out | External | Annuaire LDAP (a.net) |

Portail captif

CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE

| + Ajouter X Supprimer | | |
|--------------------------|----------|--------------------------------|
| Interface | Profil | Méthode ou annuaire par défaut |
| in | Internal | Annuaire LDAP (b.net) |
| out | External | Annuaire LDAP (b.net) |

➤ Je créer sur A et B les objets réseau pour TCP et UDP :

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Nom de l'objet:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

➤ Je configure le serveur VPN SSL :

VPN / VPN SSL

ON

Paramètres réseaux

Adresse IP (ou FQDN) de l'UTM utilisée:

Réseaux ou machines accessibles:

Réseau assigné aux clients (UDP):

Réseau assigné aux clients (TCP):

Maximum de tunnels simultanés autorisés: 126

Paramètres DNS envoyés au client

Nom de domaine:

Serveur DNS primaire:

Serveur DNS secondaire:

ON

Paramètres réseaux

Adresse IP (ou FQDN) de l'UTM utilisée:

Réseaux ou machines accessibles:

Réseau assigné aux clients (UDP):

Réseau assigné aux clients (TCP):

Maximum de tunnels simultanés autorisés: 126

Paramètres DNS envoyés au client

Nom de domaine:

Serveur DNS primaire:

Serveur DNS secondaire:

Configuration avancée

➤ Je donne le droit VPN SSL à l'utilisateur John Smith :

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 <input checked="" type="checkbox"/> Activé | jsmith@a.net | <input type="radio"/> Interdire | <input type="radio"/> Interdire | <input checked="" type="radio"/> Autoriser | <input type="radio"/> Interdire | | | |

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 <input checked="" type="checkbox"/> Activé | jsmith@b.net | <input type="radio"/> Interdire | <input type="radio"/> Interdire | <input checked="" type="radio"/> Autoriser | <input type="radio"/> Interdire | | | |

➤ J'ajoutes les règles de filtrage suivantes pour autoriser mon réseau à accéder aux autres firewalls :

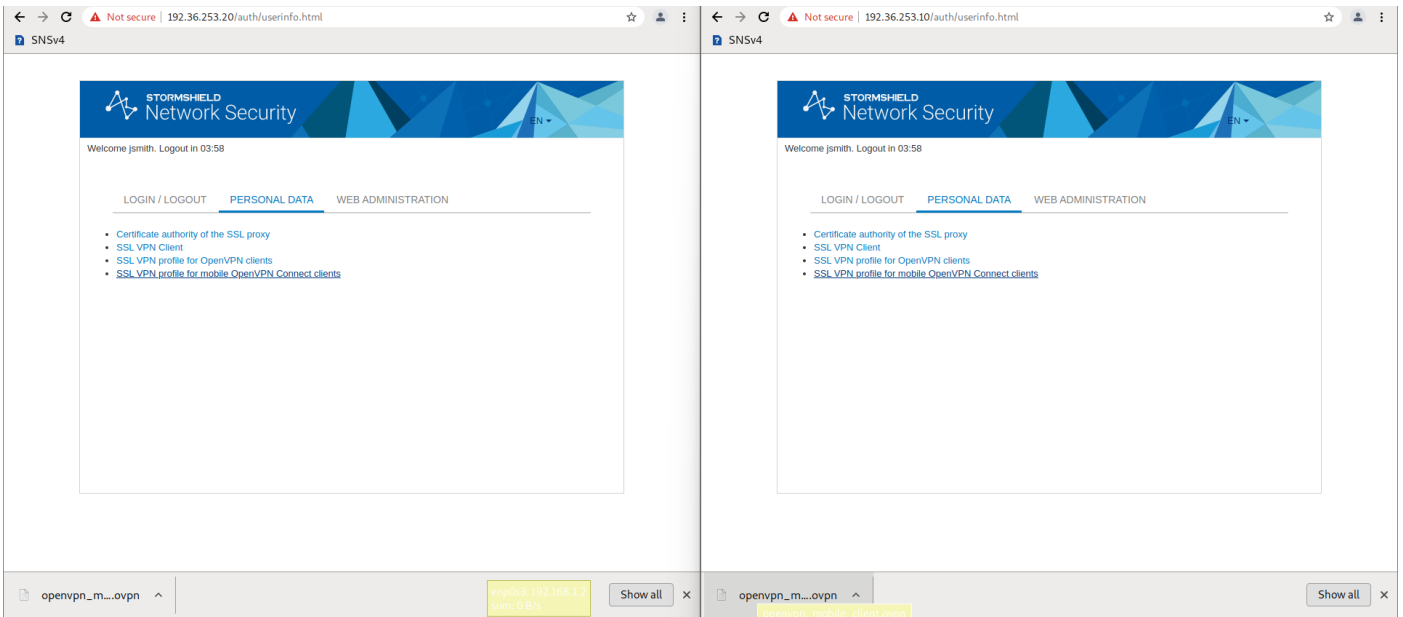
FILTRAGE NAT

| Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ | Couper | Copier | Coller | Chercher dans les logs | Chercher dans la supervision | | |
|--|---|--|-------------------|------------|-----------|--|---|------------------------------|--|--|
| Etat | Action | Source | Destination | Port dest. | Protocole | Inspection de sécurité | Commentaire | | | |
| 1 <input type="checkbox"/> off | <input type="radio"/> passer | Any | Any | Any | | <input type="checkbox"/> Off | Créée le 2025-10-02 13:24:20, par admin (192.168.1.2) | | | |
| 2 <input checked="" type="checkbox"/> on | <input checked="" type="radio"/> passer | Net-SSLVPN_UDP Net-SSLVPN_TCP via Tunnel VPN SSL | Network_internals | Any | | <input checked="" type="checkbox"/> On | Créée le 2025-10-09 14:19:02, par admin (192.168.1.2) | | | |
| 3 <input checked="" type="checkbox"/> on | <input checked="" type="radio"/> passer | Network_in | Fw_B | https | | <input checked="" type="checkbox"/> On | Créée le 2025-10-09 14:19:07, par admin (192.168.1.2) | | | |

FILTRAGE NAT

| Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ | Couper | Copier | Coller | Chercher dans les logs | Chercher dans la supervision | | |
|--|---|--|-------------------|------------|-----------|--|---|------------------------------|--|--|
| Etat | Action | Source | Destination | Port dest. | Protocole | Inspection de sécurité | Commentaire | | | |
| 1 <input type="checkbox"/> off | <input type="radio"/> passer | Any | Any | Any | | <input type="checkbox"/> Off | Créée le 2025-10-02 13:21:28, par admin (192.168.2.2) | | | |
| 2 <input checked="" type="checkbox"/> on | <input checked="" type="radio"/> passer | Net-SSLVPN_UDP Net-SSLVPN_TCP via Tunnel VPN SSL | Network_internals | Any | | <input checked="" type="checkbox"/> On | Créée le 2025-10-09 14:22:56, par admin (192.168.2.2) | | | |
| 3 <input checked="" type="checkbox"/> on | <input checked="" type="radio"/> passer | Network_in | Fw_A | https | | <input checked="" type="checkbox"/> On | Créée le 2025-10-09 14:22:58, par admin (192.168.2.2) | | | |

- Depuis la machine A je me connecte au firewall de B et vice-versa et je récupère le fichier openvpn des deux côtés :



- Dans un terminal je me connecte en tant que jsmith, je vois que des routes se sont ajoutées pour communiquer avec les réseaux des sites B pour A et A pour B :

```
user@client-training:~$ su -
Password:
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 15:21:25 2025 WARNING: No server certificate verification method has
been enabled.  See http://openvpn.net/howto.html#mitm for more info.
Thu Oct  9 15:22:30 2025 WARNING: No server certificate verification method has
been enabled.  See http://openvpn.net/howto.html#mitm for more info.

user@client-training: ~
user@client-training: ~ 80x24
user@client-training:~$ ip route show
default via 192.168.1.254 dev enp0s3
172.16.2.0/24 via 172.31.2.5 dev tun0
172.30.2.0/24 via 172.31.2.5 dev tun0
172.31.2.0/24 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
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.2
192.168.2.0/24 via 172.31.2.5 dev tun0
user@client-training:~$
```

```

user@client-training: ~
user@client-training: ~ 80x24
user@client-training:~$ su -
Password:
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 15:22:13 2025 WARNING: No server certificate verification method has
been enabled.  See http://openvpn.net/howto.html#mitm for more info.
Thu Oct  9 15:23:18 2025 WARNING: No server certificate verification method has
been enabled.  See http://openvpn.net/howto.html#mitm for more info.
user@client-training:~$ ip route show
default via 192.168.2.254 dev enp0s3
172.16.1.0/24 via 172.31.1.5 dev tun0
172.30.1.0/24 via 172.31.1.5 dev tun0
172.31.1.0/24 via 172.31.1.5 dev tun0
172.31.1.1 via 172.31.1.5 dev tun0
172.31.1.5 dev tun0 proto kernel scope link src 172.31.1.6
192.168.1.0/24 via 172.31.1.5 dev tun0
192.168.2.0/24 dev enp0s3 proto kernel scope link src 192.168.2.2
user@client-training:~$

```

➤ Je consulte la liste des utilisateurs authentifiés ainsi que les logs relatifs au VPN SSL :

LOG / VPN

Dernière heure Actualiser Rechercher... Recherche avancée Actions

RECHERCHE DU - 09/10/2025 16:25:48 - AU - 09/10/2025 17:25:48

| Enregistré à | Message | Utilisateur | Nom de la source |
|---------------------|-------------------------|-------------|------------------|
| 09/10/2025 17:23:19 | SSL tunnel created | jsmith | 192.36.253.20 |
| 09/10/2025 17:23:19 | User authenticated i... | jsmith | 192.36.253.20 |

DÉTAILS DE LA LIGNE DE LOG

| Dates | |
|----------------|---------------------|
| Enregistré à | 09/10/2025 17:23:19 |
| Date et heure | 09/10/2025 17:23:19 |
| Décalage GMT | +0200 |
| Destination | |
| Réseau distant | 172.31.1.6 |

LOG / VPN

Dernière heure Actualiser Rechercher... Recherche avancée Actions

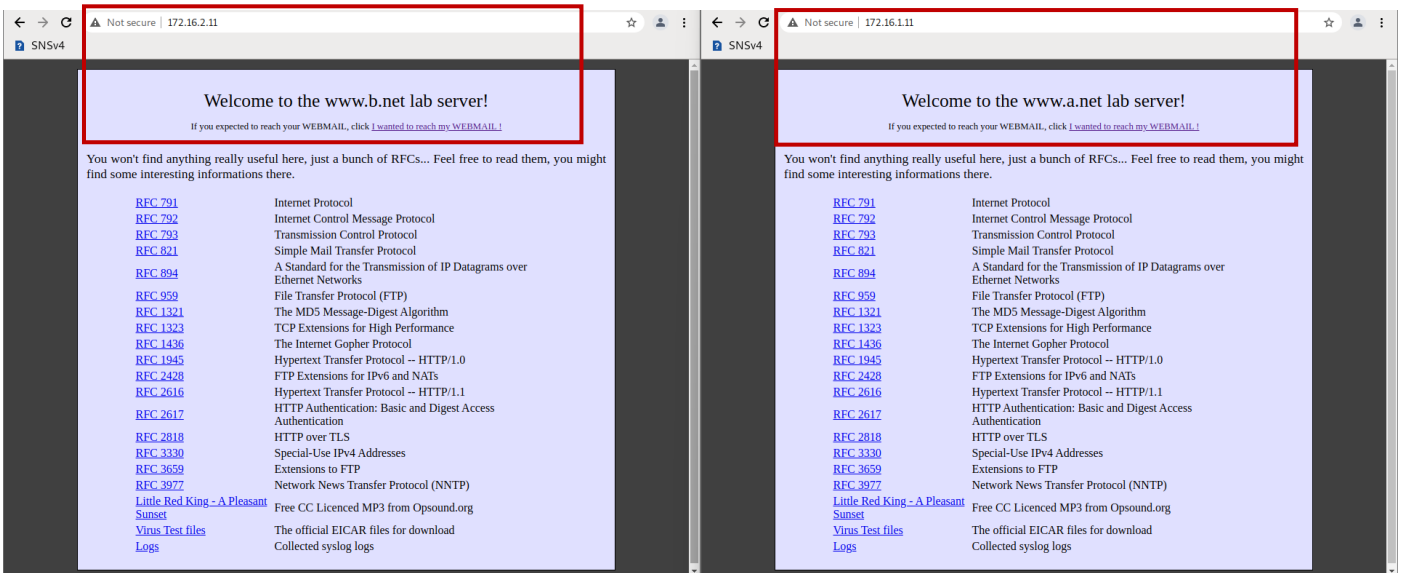
RECHERCHE DU - 09/10/2025 16:24:53 - AU - 09/10/2025 17:24:53

| Enregistré à | Message | Utilisateur | Nom de la source |
|---------------------|-------------------------|-------------|------------------|
| 09/10/2025 17:22:31 | SSL tunnel created | jsmith | 192.36.253.10 |
| 09/10/2025 17:22:31 | User authenticated i... | jsmith | 192.36.253.10 |

DÉTAILS DE LA LIGNE DE LOG

| Dates | |
|----------------|---------------------|
| Enregistré à | 09/10/2025 17:22:31 |
| Date et heure | 09/10/2025 17:22:31 |
| Décalage GMT | +0200 |
| Destination | |
| Réseau distant | 172.31.2.6 |
| Divers | |

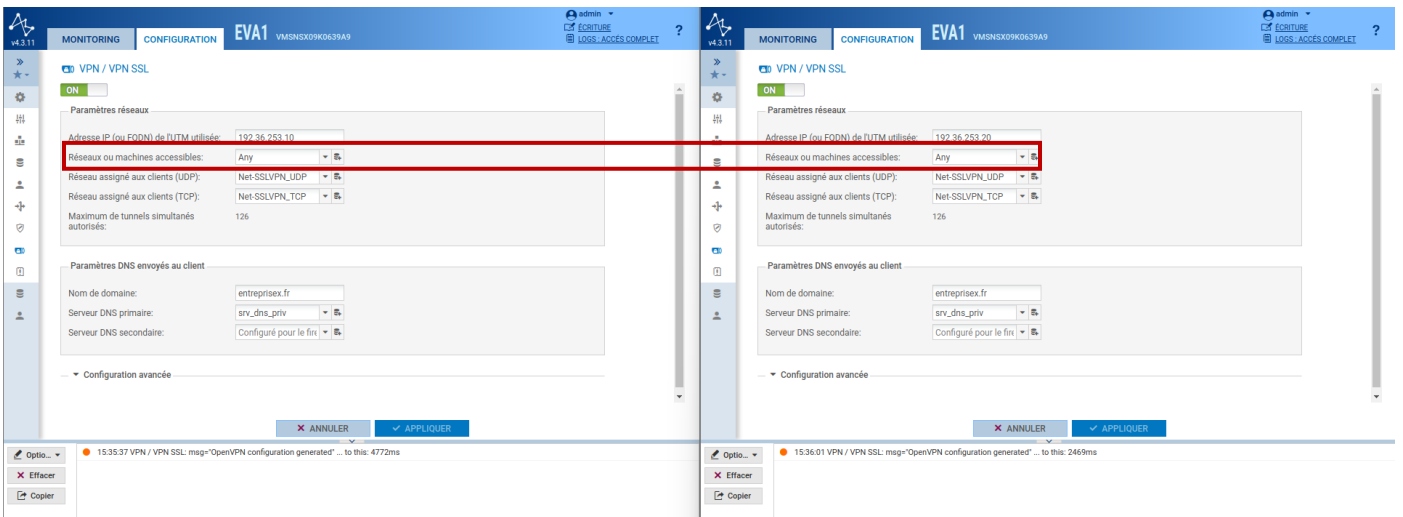
➤ Je teste l'accès aux serveur web des deux côtés (172.16.x.11) :



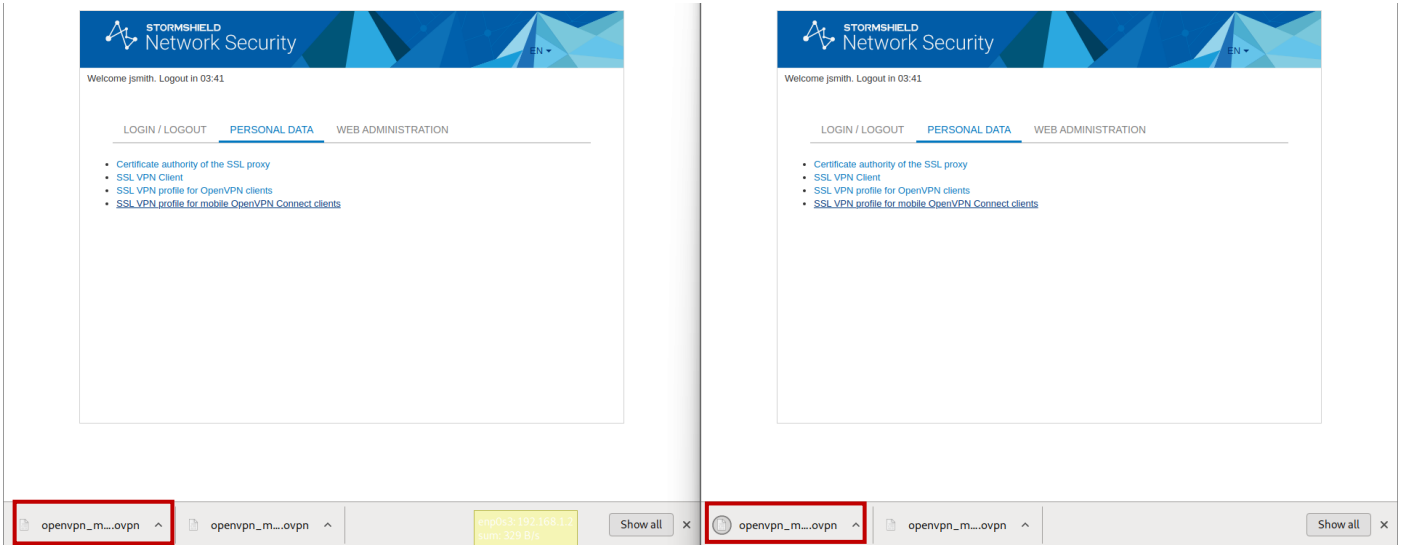
A

B

➤ Je modifie la configuration du VPN SSL pour donner l'accès à l'objet « Any » :

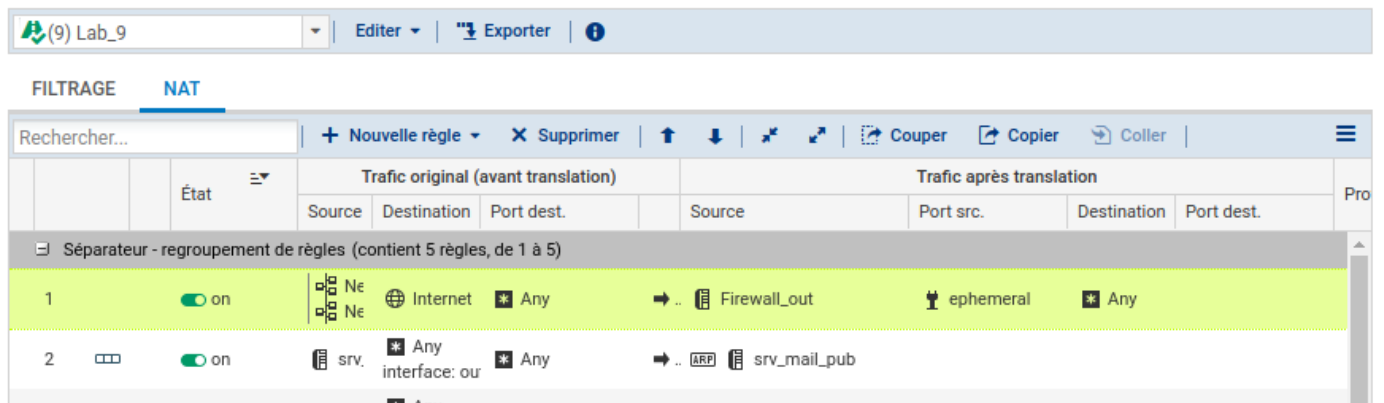
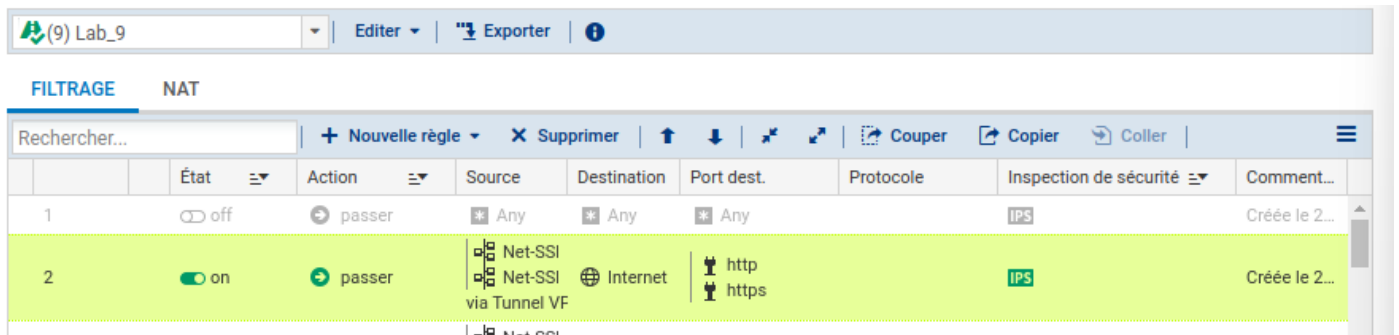


➤ Je réinstalle les fichier open vpn :



➤ J'ajoute les règles de filtrage NAT et filtrage permettant aux réseaux Net-SSLVPN_TCP et Net-SSLVPN_UDP d'accéder à Internet une fois le tunnel monté :

Sur A :



Sur B :

| | État | Action | Source | Destination | Port dest. | Protocole | Inspection de sécurité | Comment... |
|---|------|--------|-----------------------|-------------|---------------|-----------|------------------------|---------------|
| 1 | off | passer | Any | Any | Any | | IPS | Créée le 2... |
| 2 | on | passer | Net-SSL via Tunnel VF | Internet | http https | | IPS | Créée le 2... |

| | État | Trafic original (avant translation) | | | Trafic après translation | | | |
|---|------|-------------------------------------|----------------------------|------------|--------------------------|-----------|-------------|---------|
| | | Source | Destination | Port dest. | Source | Port src. | Destination | Port de |
| STATIC NAT - regroupement de règles (contient 5 règles, de 1 à 5) | | | | | | | | |
| 1 | on | Net-SSLVPN_TCP Net-SSLVPN_UDP | Internet interface: out | Any | Firewall_out | ephemeral | Any | |
| 2 | on | srv_ftp_priv | Internet | Any | srv_ftp_pub | | | |
| 3 | on | Internet interface: out | srv_ftp_pub | Any | | | srv_ftp_ | |
| 4 | on | srv mail priv | Any | Any | srv mail c | | | |

➤ J'ajoute une politique de filtrage URL pour que seul l'accès aux sites des groupes « it » et « news » soit autorisé :

| État | Action | Catégorie d'URL | Commentaire |
|------|--------------|-----------------|-------------|
| 1 on | Passer | it | |
| 2 on | Passer | news | |
| 3 on | BlockPage_00 | Any | |

Mes test n'ont pas fonctionné, par conséquent je me suis arrêté là.

Quiz :

Q1—Les utilisateurs s'authentifient avec des certificats uniques sur le VPN SSL :

B. Faux

Q2—Le pare-feu peut gérer simultanément des connexions UDP et TCP au VPN SSL :

A. Vrai

Q3—Le VPN SSL est une implémentation non standard, spécifique Stormshield :

B. Faux

Q4– Les utilisateurs connectés en VPN SSL sont automatiquement authentifiés sans devoir passer par le portail captif :

A. Vrai

Q5–Pour qu'un utilisateur puisse se connecter en VPN SSL, je dois :

A. Autoriser l'accès au VPN pour cet utilisateur

B. Lui fournir l'adresse IP publique de mon firewall

C. Activer le portail captif sur l'interface externe

D. Avoir un annuaire lié à mon pare-feu