Compte Rendu du TP 7 ET 8 : Sécurité des Équipements Réseaux

EST Beni Mellal

Filière : Bachelor en Cybersécurité

Module : Sécurité Informatique

Professeur : H.KHALOUFI

Étudiant : Youssef HACHIMI

Année Universitaire : 2025-2026

TP 7 : Configuration de l'accès à distance VPN SSL SSL sans client ASA

1. Activation du service WebVPN sur l'interface OUTSIDE

Pour activer le service WebVPN sur l'interface externe (OUTSIDE), nous utilisons les commandes suivantes :

```
ASA# conf t
webvpn
enable outside
exit
```

```
ASA(config)#
ASA(config)#webvpn
ASA(config-webvpn)#en
ASA(config-webvpn)#enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
ASA(config-webvpn)#exit
```

- **webvpn** : Cette commande permet d'entrer en mode de configuration WebVPN (pour le VPN SSL).
- **enable outside** : Active le VPN SSL sur l'interface publique "outside".

2. Création d'un utilisateur local pour le VPN

Nous créons un utilisateur local dédié au VPN avec un mot de passe

```
username myvpnuser password vpn2026
```

```
exit
```

```
ASA(config)#username myvpnuser password vpn2026
```

- **username** myvpnuser **password** vpn2026 : Crée un utilisateur nommé "vpnuser" avec le mot de passe "vpn123". Cet utilisateur sera utilisé pour l'authentification lors des connexions VPN.

3. Création d'une Group Policy pour le VPN SSL

Nous définissons une politique de groupe interne pour le VPN SSL sans client :

```
conf t
```

```
group-policy SSL_GP internal
```

```
vpn-tunnel-protocol ssl-clientless
```

```
ASA(config)#group-policy SSL_GP internal
ASA(config)#group-policy SSL_GP attributes
ASA(config-group-policy)#vpn-tunnel-protocol ssl-clientless
ASA(config-group-policy)#exit
ASA(config)#
```

- **group-policy SSL_GP internal** : Crée une politique de groupe interne nommée "SSL_GP".
- **vpn-tunnel-protocol ssl-clientless** : Spécifie que le protocole de tunnel est SSL VPN sans client (clientless), ce qui signifie que la connexion se fait via un navigateur web sans logiciel dédié.

4. Création du Tunnel Group (Connection Profile)

Nous configurons un profil de connexion (Tunnel Group) pour les accès distants et l'associons à la politique de groupe :

```
exit

tunnel-group SSL_TUNNEL type remote-access

tunnel-group SSL_TUNNEL general-attributes

default-group-policy SSL_GP
```

```
ASA(config)#tunnel-group SSL_TUNNEL type remote-access
ASA(config)#tunnel-group SSL_TUNNEL general-attributes
ASA(config-tunnel-general)#default-group-policy SSL_GP
ASA(config-tunnel-general)#exit
```

- **tunnel-group SSL_TUNNEL type remote-access** : Crée un groupe de tunnel nommé "SSL_TUNNEL" pour les connexions d'accès distant.
- **default-group-policy SSL_GP** : Associe la politique de groupe "SSL_GP" par défaut à ce tunnel group.

5. Activation de l'accès clientless SSL et affichage de la liste des tunnels

Nous réactivons le service si nécessaire et activons l'affichage de la liste des tunnels :

```
enable outside

tunnel-group-list enable

exit
```

- **enable outside** : Réactive le WebVPN sur l'interface externe (déjà fait, mais répété pour confirmation).
- **tunnel-group-list enable** : Affiche la liste des tunnels disponibles sur la page de connexion WebVPN pour les utilisateurs.

6. Sauvegarde de la configuration

Pour enregistrer les modifications :

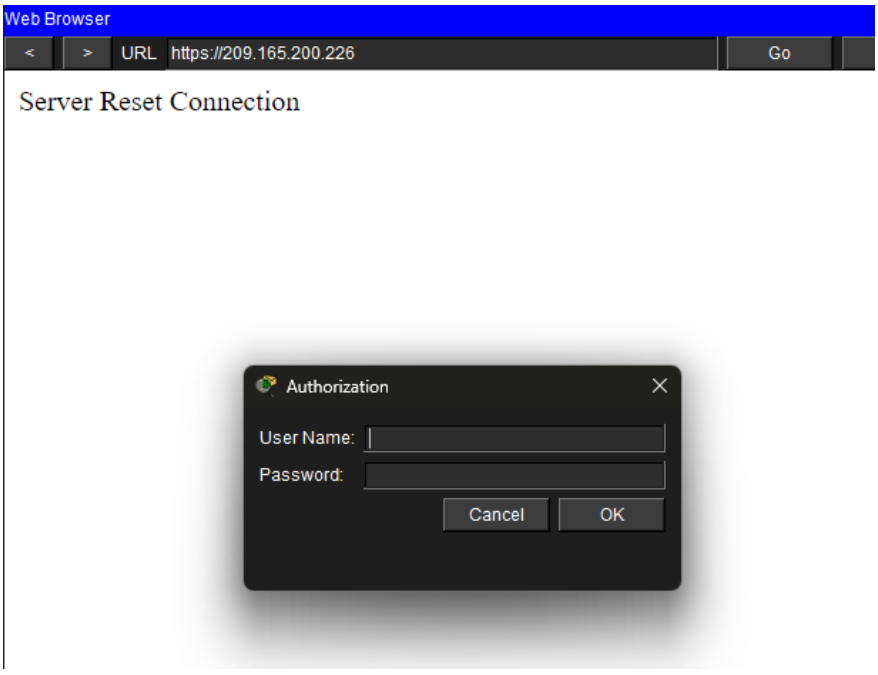
```
exit
```

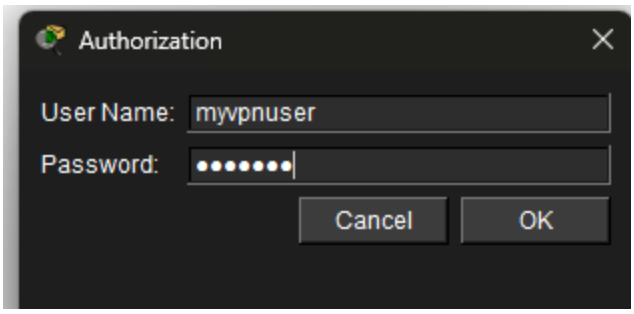
```
write memory
```

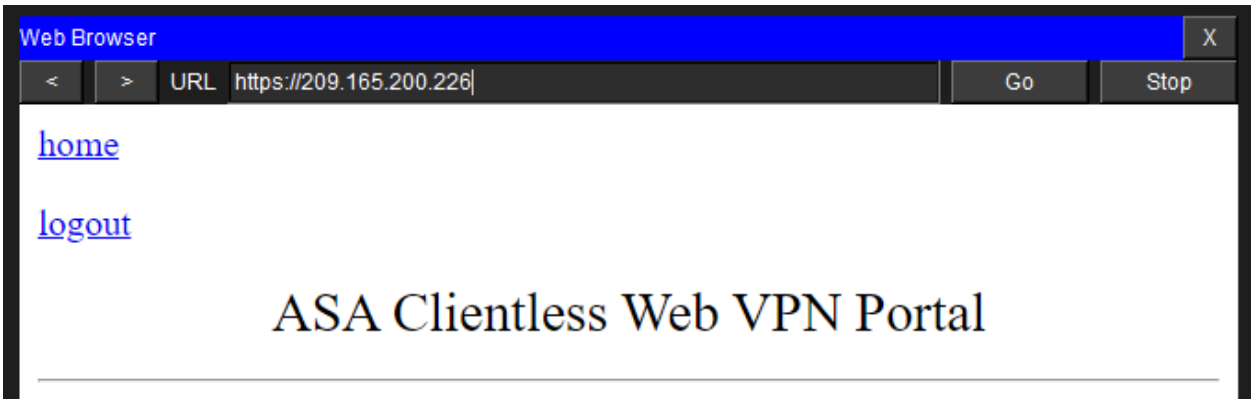
```
ASA(config)#tunnel-group SSL_TUNNEL type remote-access
ASA(config)#tunnel-group SSL_TUNNEL general-attributes
ASA(config-tunnel-general)#default-group-policy SSL_GP
ASA(config-tunnel-general)#exit
```

7. Test de la configuration VPN SSL

La configuration est testée en accédant à l'URL du portail WebVPN https://209.165.200.226 via un navigateur. L'utilisateur "myvpnuser" avec mot de passe "vpn2026" peut se connecter. Le portail affiche "ASA Clientless Web VPN Portal".




Authorization
User Name:
myvpnuser
Password:
Cancel
OK


Web Browser
X
<
>
URL
https://209.165.200.226
Go
Stop
home
logout
ASA Clientless Web VPN Portal

TP 8 : Configuration d'un VPN de site à site entre l'ASA et l'ISR

Configuration sur l'ASA

1. Configuration de la Phase 1 (IKEv1)

Nous configurons la politique IKEv1 pour la négociation initiale :

```
conf t
crypto ikev1 policy 10
encryption aes-256
hash sha
authentication pre-share
group 5
lifetime 86400
```

```
ASA#conf t
ASA(config)#crypto ikev1 policy 10
ASA(config-ikev1-policy)#encryption aes-256
ASA(config-ikev1-policy)#hash sha
ASA(config-ikev1-policy)#authentication pre-share
ASA(config-ikev1-policy)#group 5
ASA(config-ikev1-policy)#lifetime 86400
ASA(config-ikev1-policy)#exit
ASA(config)#crypto ikev1 enable outside
ASA(config)#
```

- **crypto ikev1 policy 10** : Crée une politique IKEv1 avec priorité 10.
- **encryption aes-256** : Utilise le chiffrement AES 256 bits pour une sécurité élevée.
- **hash sha** : Utilise SHA pour vérifier l'intégrité des données.
- **authentication pre-share** : Authentification via une clé pré-partagée.
- **group 5** : Groupe Diffie-Hellman 5 pour l'échange de clés (sécurité moyenne-élevée).

- **lifetime 86400** : Durée de vie de la clé en secondes (24 heures).

2. Activation d'IKEv1 sur l'interface

```
crypto ikev1 enable outside
```

- Active IKEv1 sur l'interface "outside" pour permettre les négociations VPN.

3. Configuration de la Phase 2 (IPsec)

Nous définissons l'ensemble de transformation pour IPsec :

```
crypto ipsec ikev1 transform-set TS esp-aes-256 esp-sha-hmac
```

```
ASA(config)#crypto ipsec ikev1 transform-set TS esp-aes-256 esp-sha-hmac
```

- **esp-aes-256** : Chiffrement AES 256 bits.
- **esp-sha-hmac** : Intégrité via HMAC-SHA.

4. Configuration du tunnel IPsec site-à-site

```
tunnel-group 1.1.1.1 type ipsec-l2l
```

```
WARNING: l2l tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication method is
Digital Certificates and/or The peer is configured to use
Aggressive Mode
```

```
tunnel-group 1.1.1.1 ipsec-attributes
ikev1 pre-shared-key Cisco123
exit
```

```
ASA(config)#tunnel-group 1.1.1.1 type ipsec-l2l
WARNING: L2L tunnel-groups that have names which are not an IP
address may only be used if the tunnel authentication
method is Digital Certificates and/or The peer is
configured to use Aggressive Mode
ASA(config)#tunnel-group 1.1.1.1 ipsec-attributes
ASA(config-tunnel-ipsec)#ikev1 pre-shared-key Cisco123
ASA(config-tunnel-ipsec)#exit
ASA(config)#
```

(Note : "ipsec-l21" est une faute de frappe ; il s'agit de "ipsec-l2l" pour lan-to-lan.)

- **tunnel-group 1.1.1.1 type ipsec-l2l** : Définit un tunnel site-à-site avec le peer à l'adresse IP 1.1.1.1.
- **ikev1 pre-shared-key Cisco123** : Définit la clé pré-partagée pour l'authentification.

5. Définition du trafic à chiffrer (ACL)

```
access-list VPN-TRAFFIC extended permit ip 192.168.1.0
255.255.255.0 172.16.3.0 255.255.255.0

access-list VPN-TRAFFIC extended permit ip 192.168.2.0
255.255.255.0 172.16.3.0 255.255.255.0
```

- L'ACL "VPN-TRAFFIC" spécifie le trafic à chiffrer : les réseaux 192.168.1.0/24 et 192.168.2.0/24 vers 172.16.3.0/24.

```
ASA(config)#access-list VPN-TRAFFIC extended permit ip 192.168.1.0
255.255.255.0 172.16.3.0 255.255.255.0
ASA(config)#access-list VPN-TRAFFIC extended permit ip 192.168.2.0
255.255.255.0 172.16.3.0 255.255.255.0
ASA(config)#
```

6. Création et application de la crypto-map

```
crypto map VPN-MAP 10 match address VPN-TRAFFIC

crypto map VPN-MAP 10 set peer 1.1.1.1

crypto map VPN-MAP 10 set ikev1 transform-set TS

crypto map VPN-MAP interface outside
```

```
ASA(config)#crypto map VPN-MAP 10 match address VPN-TRAFFIC
ASA(config)#crypto map VPN-MAP 10 set peer 1.1.1.1
ASA(config)#crypto map VPN-MAP 10 set ikev1 transform-set TS
ASA(config)#crypto map VPN-MAP interface outside
```

- **match address VPN-TRAFFIC** : Associe l'ACL au map.
- **set peer 1.1.1.1** : Définit l'IP du peer.
- **set ikev1 transform-set TS** : Utilise l'ensemble de transformation défini.
- **interface outside** : Applique la crypto-map sur l'interface externe.

Configuration sur R3 (Cisco ISR)

1. Configuration de la Phase 1 (ISAKMP/IKE)

```
R3# conf t
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encr aes 256
R3(config-isakmp)# hash sha
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# lifetime 86400
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encr aes 256
R3(config-isakmp)#hash sha
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#grou
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 86400
R3(config-isakmp)#exit
R3(config)#crypto isakmp key Cisco123 address 209.165.200.226
R3(config)#
```

- Similaire à l'ASA : Politique IKE avec chiffrement AES-256, hash SHA, pré-shared key, groupe 5, lifetime 86400.

2. Clé pré-partagée pour l'authentification

```
R3(config-isakmp)# crypto isakmp key Cisco123 address
209.165.200.226
```

- Définit la clé "Cisco123" pour le peer à l'adresse 209.165.200.226 (doit matcher celle de l'ASA).

3. Configuration de la Phase 2 (IPsec)

```
R3(config)# crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
```

- Similaire à l'ASA : Chiffrement AES-256 et intégrité HMAC-SHA.

4. Définition du trafic à chiffrer (ACL de crypto)

```
R3(config)# access-list 100 permit ip 172.16.3.0 0.0.0.255
192.168.1.0 0.0.0.255

R3(config)# access-list 100 permit ip 172.16.3.0 0.0.0.255
192.168.2.0 0.0.0.255
```

```
R3(config)#crypto isakmp key Cisco123 address 209.165.200.226
R3(config)#crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
R3(config)#access-list 100 permit ip 172.16.3.0 0.0.0.255 192.168.1.0
0.0.0.25
R3(config)#access-list 100 permit ip 172.16.3.0 0.0.0.255 192.168.1.0
0.0.0.255
R3(config)#access-list 100 permit ip 172.16.3.0 0.0.0.255 192.168.2.0
0.0.0.255
R3(config)#
```

- ACL 100 : Trafic de 172.16.3.0/24 vers 192.168.1.0/24 et 192.168.2.0/24 (miroir de l'ACL ASA).

5. Création de la crypto-map

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer and
a valid access list have been configured.

R3(config-crypto-map)# set peer 209.165.200.226

R3(config-crypto-map)# set transform-set TS

R3(config-crypto-map)# match address 100

R3(config-crypto-map)# exit
```

```
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 209.165.200.226
R3(config-crypto-map)#set transform-set TS
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#interface G0/0
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
```

- **set peer 209.165.200.226** : Peer ASA.
- **set transform-set TS** : Ensemble de transformation.
- **match address 100** : Associe l'ACL.

6. Application de la crypto-map sur l'interface

```
R3(config)# interface G0/0

R3(config-if)# crypto map VPN-MAP

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

- Applique la crypto-map sur l'interface GigabitEthernet0/0 pour activer le chiffrement du trafic.