



Cybersécurité

Paramétrage d'un pare-feu Cisco

BTS CIEL

Semestre 1
2025_2026

1^{ère} partie : Initialisation du Cisco ASA 5505

Connexion à l'ASA :

Brancher un câble console entre un PC et l'ASA.

Ouvrir le terminal avec les paramètres suivants :

- Baud rate : 9600.
- Data bits : 8.
- Parity : None.
- Stop bits : 1.
- Flow control : None.

Réinitialiser le pare-feu :

```
enable  
write erase  
reload
```

Accéder au mode de configuration :

```
enable  
configure terminal
```

Configurer les interfaces :

Configurer les interfaces inside (LAN) et outside (WAN) :

```
interface Vlan1  
nameif inside  
security-level 100  
ip address 192.168.100.1 255.255.255.0  
no shutdown  
  
interface Vlan2  
nameif outside  
security-level 0  
ip address 172.20.40.100 255.255.0.0  
no shutdown
```

Configurer les routes statiques :

```
route outside 0.0.0.0 0.0.0.0 172.20.100.1
```

2^{ème} partie : Configuration des règles de pare-feu

Créer des ACL (Access Control Lists) pour bloquer YouTube :

Identifier les adresses IP utilisées par YouTube (ou utiliser des expressions régulières pour les noms de domaine).

Exemple pour bloquer les domaines via une ACL :

```
access-list BLOCK_YOUTUBE extended deny tcp any any eq 443
access-list BLOCK_YOUTUBE extended deny tcp any any eq 80
access-list BLOCK_YOUTUBE extended deny udp any any eq 53
access-list BLOCK_YOUTUBE extended deny tcp any host youtube.com
access-list BLOCK_YOUTUBE extended permit ip any any
```

Appliquer cette ACL à l'interface inside :

```
access-group BLOCK_YOUTUBE in interface inside
```

Configurer l'inspection du trafic DNS pour bloquer les requêtes vers YouTube :

```
class-map youtube_block
match regex youtube_block_regex dns
match string "youtube.com"

policy-map youtube_block_policy
class youtube_block
drop

service-policy youtube_block_policy interface inside
```

3^{ème} partie. Configurer le NAT pour le réseau local

Permettre au trafic interne de sortir tout en appliquant les règles de filtrage.

```
object network LAN
subnet 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface
```

4^{ème} partie : Vérification et test

Sauvegarder la configuration :

```
write memory
```

Tester la connexion Internet :

S'assurer que les postes du réseau peuvent accéder à Internet.

Tester le blocage de YouTube :

Essayer d'accéder à [YouTube](https://www.youtube.com) à partir d'un poste client. Cela doit être bloqué.

5^{ème} partie : Surveillance et débogage

Vérifier les logs :

```
show log
```

Observer le trafic bloqué :

```
show access-list BLOCK_YOUTUBE
```