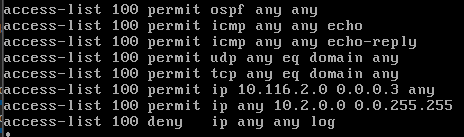
Jalon 48 - REMFW Firewall filtrage

Pour mettre le filtrage en place sur le REMFW, il faut déterminer des ACLs et les assigner à l’interface externe du réseau Remote. Voici les ACL mis en place :



access-list 100 permit ospf any any

* Autorise le trafic OSPF (protocole de routage) entre toutes les adresses IP.

access-list 100 permit icmp any any echo

* Autorise les paquets ICMP echo request (ping) depuis n'importe quelle source vers n'importe quelle destination.

access-list 100 permit icmp any any echo-reply

* Autorise les paquets ICMP echo reply (réponse au ping).

access-list 100 permit udp any eq domain any

* Autorise le trafic UDP pour le service DNS (port 53) depuis n'importe quelle source vers n'importe quelle destination.

access-list 100 permit tcp any eq domain any

* Autorise le trafic TCP pour le service DNS (port 53).

access-list 100 permit ip 10.116.2.0 0.0.0.3 any

* Autorise tout le trafic IP provenant de l'adresse réseau 10.116.2.0/30 vers n'importe quelle destination.
  + 0.0.0.3 correspond au masque wildcard pour 4 adresses.

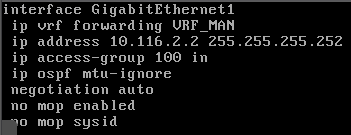
access-list 100 permit ip any 10.2.0.0 0.255.255.255

* Autorise tout le trafic IP vers le réseau 10.2.0.0/8 (grande plage d'adresses).

access-list 100 deny ip any any log

* Bloque tout le reste du trafic qui n'est pas explicitement autorisé ci-dessus et enregistre les logs pour audit.

Il faut ensuite assigner l’ACL a l’interface avec ip access-group 100 in :



En utilisant la commande show access-lists 100, on peut voir le nombre de fois que les ACL ont été utilisés.