***Les règles de filtrage ACL***

Il y a deux types d’ACL :

* Les ACL standards
* Les ACL étendues
* Les ACL sont des scripts installés dans le routeur qui permettent de filtrer le trafic entrant ou sortant d’une interface.

Une ACL est activé à la suite de la configuration de cette ACL sur cette interface

* Creation des règles de filtrage (identification de ces règles)
* Application de ces règles sur l’interface.
* L e filtrage de paquet (routeur filtrent FN routeur) opère sur la couche de protocole

TCP/IP et non sur les données utiles.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Type  IP/ICMP/ARP |  | Protocole  TCP/UDP |  | @ip  SRC | @ip  Dest | Port  SRC | Port  Dest |  | donnée |

N2 liaison N3 reseau N4 transport Appli

* L’ACL comprend un certain nombre de lignes qui regroupent les règles de filtrage correspondant au cahier des charges :

- R1 acces-list 100 (paramètres)

contraintes R2 acces-list 100

R3 acces-list 100

* ***Les ACL standard***

Ces ACL assurent le filtrage sur la base de l’@IP source et du masque uniquement.

Ces ACL sont identifié par un n° de 1 à 99.

Exemple : Interdire le trafic entre 2 sous réseaux.(du réseau 192.168.1.0/24 vers réseau 192.168.2.0/26)

Autoriser le serveur DHCP a communiqué

Access-list 10 permit host 192.168.1.250

Access- list 10 deny 192.168.1.0 0.0.0.255

Synthaxe :

* Access-list 10 permit host 192.168.1.250
* Access- list 10 deny 192.168.1.0 0.0.0.255
* int fa 0/0
* Ip access-group 10 out
* ***Les ACL étendues***

Ces ACL permettent de filtrer un trafic sur la base des informations suivantes :

* Protocole réseau
* Adresse IP SRC/Masque
* Adresse IP dest/Masque
* Les protocoles de transport (TCP ou UDP) + état
* Les Protocoles de communication (www,ftp,mail,boot p s ou boot pc…)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| N° | Interface | @IP S/masque | @IP dest/ masque | Proto | Action |
| 1 (C5) | I3 in | Any | 192.168.2.0/  0.0.0.15 | IP | permit |
| 2 (C2,C1) | I3in | Any | 192.168.1.0  0.0.0.31 | ICMP/réponse | permit |
| 3 | I1 in | Any | Any | TCP/établit | permit |

http requete http réponse 192.168.1.36

FW

192.168.1.36 Internet

INTERNE

I1 I I 3

I2

DMZ 192.168.2.0/28

C1 => Les postes du réseau informatique (192.168.1.0/27) peuvent emmetre le ping (réponse OK) vers tous le réseau et vers l’internet .

C2 => les internautes ne peuvent pas pinguer le réseau interne (192.168.1.0/24)et la DMZ

C3=>les internautes ne peuvent pas communiquer avec le réseau interne

C4=>L e réseau interne à accès à Internet

C5=> Les internautes peuvent acceder à la DMZ 192.168.2.0/28

***Commande cisco : Access-list 100 permit icmp any @IP+mask echo reply***