ASA

Quelques informations pour comprendre et configurer un CISCO ASA

Principe de l'ASA :

L'ASA possède plusieurs interfaces qui devront être nommées et adressé. Ces même interfaces possède un security level. Grâce au security level une interface avec un nombre inférieur à une autre interface ne pourra pas communiquer avec celle-ci, cependant une interface avec un nombre supérieur à une autre interface pourra communiquer avec elle.

L'ASA fonctionne avec des ACL Une ACL est une règle qui nous permettra d'autoriser ou d'interdire une ip ou un protocole sur un réseau.

Ces ACL fonctionnent avec des access group qui se chargeront d'appliquer un groupe d'ACL portant le même nom sur une interface choisit de l'ASA.

Connexion à l'interface graphique:

Port Management Il existe sur notre firewall asa un port management qui nous permettra de configurer l'asa via une interface graphique. Pour cela il faut impérativement que la machine qui voudra accéder à l'interface graphique soit sous java 6 en 32 bits (Cette version est disponible sur le nas dans: PARTAGE_OUTILS/Reseau/ASA5520) Ensuite Il vous faudra configurer l'interface management pour lui attribuer une ip.

```
#en
#conf t
#http server enable
#http "ip et masque du réseau du port management" inside
#no snmp-server location
#no snmp-server contact
#snmp-server enable traps snmp authentication linkup linkdown coldstar
#telnet timeout 5
```

<html> On connecte un pc dans le même réseau que le port management sur le port management dans un navigateur on tape https:*"ip du port management"/admin puis on télécharge l'ASDM ensuite on se connecte sur l'asa via le logiciel téléchargé </html> ===== Copier configuration en TFTP ===== <code lscript> copy running-config tftp </code> ===== Importer Configuration depuis TFTP ===== <code lscript> copy tftp start </code> ===== Activation du SSH ===== <code lscript> #username "nom de l'utilisateur" password "le mot de passe voulu" #aaa authentification ssh console #ssh "ip réseau ou machine qui se connectera en ssh " "masque IP réseau ou masque 255.255.255.255" "nom d'interface sur laquelle le ssh se #connectera" #ssh timeout 60 </code> —- ==== Configuration de l'ASA en CLI: ==== == Pour configurer l'ASA il faut en premier configurer les interfaces: == <code lscript> #en #conf t #interface gigabitEthernet "n°int"* Maintenant que nous avons sélectionné l'interface nous allons la configurer #ip address XXX.XXX.XXX.XXX

255.XXX.XXX.XXX #nameif “Nom souhaité de l'interface” #security-level “N°0-100” </code>

Creation ACL

```
#access-list “nom de l’access-list” “deny (pour refuser)/permit (pour autoriser) “  “on choisi le fonctionnement de l’acl” “on choisit sur qui on agit” “on choisit la destination de la régle ”
//exemple d'ACL concrète plus bas.
```

Creation Access-Group

```
#access-group "nom des ACL crée" "in ou out" interface "nameif de l'interface"
                              //in ou out indique si le traffic rentre ou sort de l'interface choisi à la fin de l'access-group
```

Exemple :

ICI nous allons autoriser le PING dans tous le réseau sauf de l'exterieur vers l'interne, et on va seulement autoriser le Serveur WEB à accéder au ServeuBDD

Voici la configuration complète:

```
#en
#conf t
//configuration interface 1/2 DMZ
#interface GigabitEthernet1/2
#ip address 192.168.10.1 255.255.255.0
#nameif DMZ
#security-level 50
#ex
//configuration interface 1/1 Externe
#int GigabitEthernet 1/1
#ip address 192.168.1.1 255.255.255.0
#nameif externe
#security-level 0
//configuration interface 1/3 Interne
#ex
#int gigabitEthernet 1/3
#ip address 192.168.20.1 255.255.255.0
#nameif interne
#security-level 100
#ex
```

```
//maintenant on va configurer les ACL pour autoriser le PING
#access-list PING permit icmp any any
#access-list PING deny icmp any 192.168.20.0 255.255.255.0
//les access-list pour le ping sont crée maintenant on va les appliquer sur les interface avec les access-group
#access-group PING in interface externe
//Désormais les ping ne peuvent plus circuler de l'extérieur vers interne
//Création des ACL pour le serveur WEB et sa base de donnée
#access-list HTTP permit tcp host 192.168.20.250 eq www host 192.168.10.12
#access-list HTTP deny tcp host 192.168.20.250 eq www any
#access-group HTTP in interface interne
#access-group HTTP out interface interne
```

— *wikisio 2021/02/19 12:07* Clément GROULT Jules CATHERINE