**Définissez les accès utilisateur avec les ACLs (Access control list)**

Après avoir sécurisé l’accès à vos routeurs par des mots de passe, je vous propose cette fois-ci de limiter l’accès à un réseau entier en créant des listes d’accès. Cela vous permettra, par exemple, d’interdire un spammeur connu d'atteindre votre data center. Allez, on commence.

**Ne faites pas entrer de spammeur dans votre data center**

Votre data center est en place et vos clients profitent de vos services comme ils le souhaitent. Ils peuvent vendre leurs produits depuis vos serveurs. Cependant, votre client d’e-commerce s’est fait attaquer et un spammeur utilise son serveur afin d’envoyer des mails à travers le monde entier. En regardant les logs de son serveur, vous avez identifié l’adresse publique du spammeur, il ne vous reste plus qu’à lui interdire d’entrer dans votre data center !

Pour cela, vous allez créer une liste d’accès. Vous vous souvenez, vous en avez créé une lors de la partie sur le NAT ? Vous aviez en fait permis à vos réseaux VLAN d’utiliser le NAT sur l’interface WAN du routeur 1.

Il est temps de vous expliquer cela un peu plus en profondeur.

Une liste d’accès ou access-list en anglais (ACL) est donc un moyen de filtrer certains paquets sur le réseau. Elle se crée en deux parties :

* Premièrement, vous créez l’ACL c’est-à-dire un nom d’ACL autorisant ou interdisant un réseau.
* Deuxièmement, vous l’associez à une interface d’un routeur, en entrée ou en sortie. L’entrée étant en direction du routeur, la sortie en sortant du routeur.

**Faites le bon choix entre interdire la source ou la destination**

Chez CISCO, il existe deux types d’ACL :

1. L’une est appelée standard :
   * Elle prend un numéro de 1 à 99.
   * Elle permet de bloquer (ou d’autoriser) une adresse source, c’est-à-dire dans notre cas, le spammeur.
   * Elle doit se placer le plus près possible de la destination (vous verrez dans quelques lignes pourquoi) dans notre cas sur le routeur 1, le routeur le plus près du serveur attaqué par le spammeur.
2. L’autre est appelée étendue :
   * Elle prend un numéro de 100 à 199.
   * Elle peut bloquer (ou autoriser) soit l’adresse source, soit l’adresse de destination, soit un port ou service (comme SSH ou telnet par exemple).
   * Elle doit être placée le plus proche de la source.

Voyons comment appliquer une ACL standard pour bloquer le spammeur.

**Bloquez le spammeur avec une ACL standard**

Vous avez identifié l’adresse publique du spammeur comme étant 223.0.1.4 (il est donc connecté au routeur 4). Il vous faut donc créer une ACL interdisant cette adresse et ensuite l’appliquer sur l’interface VLAN2 du routeur 1.

Vous allez devoir vous connecter au routeur 1 et entrer cette commande :

routeur1(config)#access-list 1 deny host 223.0.1.4

Une seule ligne suffit.

L’argument  host  vous permet de ne pas spécifier le masque s’il s’agit d’une adresse unique. Voici l’autre façon avec masque :

routeur1(config)#access-list 1 deny 223.0.1.4 0.0.0.0

Souvenez-vous, il s’agit d’un masque inversé. Si vous voulez interdire tout le réseau 223.0.1.0/24, il faudra plutôt procéder comme ceci :

routeur1(config)#access-list 1 deny 223.0.1.0 0.0.0.255

0.0.0.255 en masque inversé correspond à 255.255.255.0 en masque normal.

Il vous faut maintenant appliquer cette liste à l’interface VLAN 2 en sortie du routeur.

routeur1(config)#int GigabitEthernet0/0/0.2

routeur1(config-subif)#ip access-list 1 out

Ici vous appliquez l’ACL 1 en sortie de l’interface VLAN 2.

Regardez dans votre running-config :

routeur1#show running-config interface gi0/0/0.2

Building configuration...

Current configuration : 180 bytes

!

interface GigabitEthernet0/0/0.2

encapsulation dot1Q 2

ip address 192.168.2.254 255.255.255.0

ip access-group 1 out

ip nat inside

ip virtual-reassembly in

no cdp enable

end

En utilisant  sh run interface n°Interface , vous n’affichez que l’interface voulue. Vous voyez ici que l’access-group 1 est bien activé en sortie.

routeur1#sh run | begin access-list 1

access-list 1 deny 223.0.1.4

!

Avec la commande begin juste après le pipe, vous pouvez commencer l’affichage après access-list Vous voyez ici que l’access-list 1 que vous avez créé est bien présente.

Vérifions le fonctionnement. Depuis le routeur 4 qui a l’interface 223.0.1.4 vous ne devriez pas pouvoir pinguer le VLAN2.

routeur4#ping 223.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 223.0.0.1, timeout is 2 seconds:

.UUUU

Success rate is 0 percent (0/5)

Parfait ! Mais n’oubliez pas de vérifier que les autres le peuvent, la règle ne doit interdire que l’adresse 223.0.1.4.

routeur2#ping 223.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 223.0.0.1, timeout is 2 seconds:

UUUUU

Success rate is 0 percent (0/5)

Résultat : depuis le routeur 2, il est aussi impossible de pinger le VLAN2 (avec l’adresse 223.0.0.1 qui redirige vers le serveur). Et ce n’est pas ce que nous voulons !

Mais pourquoi l’accès au VLAN2 est bloqué pour tous les routeurs si nous n’avons interdit qu’un seul host ?

Lorsque l’on crée une ACL, une règle implicite, qui interdit tout, se crée à la fin de nos règles. Cela se présente comme cela :

access-list 1 deny 223.0.1.4

access-list 1 deny any

Cette ligne n'apparaît certes pas dans votre configuration, mais c’est comme si elle y était.

Pour éviter que cette règle ne soit appliquée, on ajoute une règle qui autorise tout le monde juste après la première règle.

access-list 1 deny   223.0.1.4

access-list 1 permit any

Essayez de nouveau avec le routeur 4 puis le routeur 2... le routeur 4 est bloqué alors que le routeur 2 peut bien pinger.

Parfait ! Le serveur de votre client n’est plus utilisé par le pirate, mais vous vous rendez compte qu’une autre adresse IP (223.0.2.3) attaque de nouveau la même victime. Vous décidez donc de l’ajouter à votre liste.

routeur1(config)#access-list 1 deny host 223.0.2.3

% Access rule can't be configured at higher sequence num as it is part of the existing rule at sequence num 20

Le routeur ne veut pas, mais pourquoi ?

Votre routeur lit ces règles de haut en bas, de la première à la dernière. Lorsqu’un paquet passe par l’interface VLAN 2, le routeur lit comme ceci :

* Est-ce que mon paquet a pour source 223.0.1.4 ?
  + Si oui, il l’interdit.
  + Sinon il passe à la ligne suivante.
* Est-ce que mon paquet fait partie de toutes les autres adresses ?
  + Si oui, il le laisse passer et cette ligne est forcément vraie puisqu’elle regroupe toutes les adresses.

Donc lorsque vous tentez de bloquer une adresse après cette ligne, le routeur (il est sympa) vous dit que votre règle ne sera jamais lue étant donné que juste au-dessus une règle prend déjà en compte l’adresse 223.0.2.3 !

La solution est donc de placer votre règle concernant l’adresse 223.0.2.3 au-dessus de votre règle globale. Ce sera d’ailleurs bien souvent ce que vous devrez faire, placer les règles les plus précises en premières et les règles les plus globales en dernières.

routeur1(config)#no access-list 1

Vous supprimez l’ACL.

routeur1(config)#access-list 1 deny host 223.0.1.4

routeur1(config)#access-list 1 deny host 223.0.2.3

routeur1(config)#access-list 1 permit any

**Placez votre règle au bon endroit sur le réseau**

Vous avez vu plus haut que les règles standards devaient se trouver le plus près possible de la destination.

Mais pourquoi ?

Si je place ma règle au niveau du routeur 4, le réseau du spammeur n’aura plus accès à aucun réseau ! Vous allez me dire que c’est tant pis pour lui. Mais si votre règle ne concernait pas un pirate mais juste une règle de sécurité, comme l’interdiction pour certaines personnes de se connecter au serveur de l’administrateur, ces personnes se verraient interdites de naviguer sur le NET alors que votre règle ne concernait, à la base, que votre poste.

À l’inverse, lorsque l’on spécifie une adresse de destination avec les ACL étendues, il vaut mieux les placer au plus proche de la source. Si vous les placez au niveau de la destination, il vous faudrait placer cette règle sur plusieurs routeurs.

Et si vous deviez bloquer l’accès à un réseau mais que celui-ci était joignable par deux routeurs, que feriez-vous ? Eh bien, vous devrez placer votre règle deux fois.

Regardons maintenant comment créer une ACL étendue.

**Interdisez l’accès au routeur via SSH depuis certaines adresses**

C’est une des fonctions des ACL étendues, elles peuvent non seulement spécifier l’adresse source et l’adresse de destination mais aussi le port et donc le protocole utilisé. Cela vous permet par exemple de n’autoriser l’accès en administration au routeur (via SSH) qu’à certaines adresses, par exemple, seules les adresses utilisées par l’administrateur. C’est ce que vous allez faire. Sachant que l’adresse 223.0.1.4 est potentiellement utilisée par un pirate, vous allez lui interdire l’accès à SSH vers vos routeurs, mais pas au reste. Il aura ainsi accès à HTTP par exemple et pourra même pinguer vos routeurs.

Ce type de règle vous permettra aussi de n’ouvrir l’accès aux utilisateurs de vos réseaux que de HTTP et non pas FTP qui peut être dangereux.

Nous avons dit que ces ACL se placent le plus près de la source, alors connectez-vous au routeur 4.

Vous interdisez à l’adresse 223.0.1.4 de se connecter en SSH vers toutes les adresses du réseau.

routeur4(config)#access-list 100 deny tcp  host

223.0.1.4 any eq 22

Puis vous autorisez tout le reste.

routeur4(config)#access-list 100 permit ip any any

Enfin, n’oubliez pas de l’appliquer à votre interface.

routeur4(config)#interface gi0/1

routeur4(config-if)#ip access-group 100 in

Et comme toujours, faites des tests ! Depuis le routeur 4, il est maintenant impossible de vous connecter en SSH au routeur 1. Par contre, vous êtes en mesure de le pinger.

Je pensais qu’on allait mieux comprendre la règle NAT écrite dans le chapitre sur le NAT ?

En effet, la règle que vous avez créée pour le NAT ne ressemble a priori pas à ce que vous venez de faire. C’est qu’il existe une autre façon de créer ces deux types d’ACL. "Comment" me direz-vous ? En donnant un nom à la règle au lieu d’un numéro.

Regardez de nouveau votre règle NAT.

routeur1(config)#ip access-list standard NAT\_INTERNET\_VLAN2

routeur1(config-std-nacl)#permit 192.168.2.0 0.0.0.255

Elle se décompose cette fois-ci en deux lignes, mais l’information est la même. Vous voyez qu’il s’agit bien d’une ACL avec le mot  access-list  et qu’elle est  standard  . Vous voyez aussi qu’elle autorise le réseau 192.168.2.0/24 à passer.

Regardez comment faire vos règles étendues avec un nom, ce qui vous permet de mieux comprendre les règles que vous avez créées.

routeur4(config)#ip access-list extended interdiction\_SSH

routeur4(config-ext-nacl)#deny tcp host 223.0.1.4 any eq 22

routeur4(config-ext-nacl)#permit ip any any

Il suffit ensuite d’appliquer le nom de l’ACL à l’interface.

Votre réseau est de plus en plus sûr ce qui vous rend de plus en plus fiable auprès de vos clients. Vous allez découvrir dans le prochain et dernier chapitre de ce cours, le serveur RADIUS qui vous permettra de centraliser les données de vos utilisateurs et ainsi vous faciliter la vie quant à la sécurité de votre réseau.

**En résumé**

* Les ACL vous permettent de créer des règles autorisant ou interdisant l'accès à un réseau.
* Il existe deux types d’ACL :
  + Les standards qui permettent de configurer la source et doivent être placés au plus près de la destination.
  + Les étendues qui permettent de renseigner la source, la destination ainsi que le port et doivent être placées au plus près de la source.
* Les ACL peuvent soit autoriser soit interdire un réseau.
* Une fois créée L’ACL doit être associée à une interface.
* Les règles des ACL se lisent de haut en bas, l’ordre a donc une importance.
* Les règles les plus précises doivent être placées en haut et les plus générales en bas.
* Pour créer une ACL standard, il faut entrer la commande :
  + routeur(config)#access-list n°1-99 deny/permit réseau masqueInversé
* Pour créer une ACL étendue, il faut entrer la commande :
  + routeur(config)#access-list n°100-199 deny/permit protocole réseauSource masqueInversé réseau Destination masqueInversé n°port
* Ces deux types d’ACL peuvent être renseignés par un nom au lieu d’utiliser un numéro :
  + routeur(config)#ip access-list standard/extended Nom
  + routeur(config-ext-nacl)#deny/permit protocol réseauSource masqueInversé réseau Destination masqueInversé n°port