Configuration des filtres ACL

L'exemple présenté dans cette tâche montre comment bloquer le trafic IP en provenance d'un hôte ayant pour adresse IP 12.0.0.100. Voir la section Basic SEFOS Topology pour connaître la topologie de cette tâche.

Le type de filtre peut être étendu ou standard. Les filtres standard filtrent le trafic en fonction de l'adresse IP source et de l'adresse IP de destination. Les filtres étendus peuvent également indiquer l'ID de protocole, les numéros de port TCP/UDP, les valeurs DSCP et l'étiquette de flux. Dans cet exemple, les paquets IP ayant pour adresse source 12.0.0.100 sont filtrés.

Les filtres ACL filtrent les paquets sur le matériel en fonction de certains critères de filtrage configurés ou programmés dans le commutateur. Le commutateur examine chaque paquet pour déterminer s'il doit être bloqué ou transféré en fonction des listes d'accès configurées. Saisissez les commandes suivantes sur le commutateur SEFOS-1.

1. **vous connecter à SEFOS ;**

   Voir la section Connect to SEFOS.

2. **Configurez l'adresse IP du commutateur sur 12.0.0.1.**

```
SEFOS-1# configure terminal
SEFOS-1(config)# interface vlan 1
SEFOS-1(config-if)# shutdown
SEFOS-1(config-if)# ip address 12.0.0.1  255.0.0.0
SEFOS-1(config-if)# no shutdown
SEFOS-1(config-if)# exit
SEFOS-1(config)# interface xl-ethernet 0/25
 SEFOS-1(config-if)# no shutdown
 SEFOS-1(config-if)# exit
 SEFOS-1(config)# interface xl-ethernet 0/26
 SEFOS-1(config-if)# no shutdown
 SEFOS-1(config-if)# exit
```

15. **Créez un filtre IP avec l'ID 11.**

```
 SEFOS-1(config)# ip access-list extended 11
```

17. **Interdisez le trafic IP en provenance de l'hôte 12.0.0.100 vers un réseau ou un hôte.**

```
 SEFOS-1(config-ext-nacl)# deny ip host 12.0.0.100 any
 SEFOS-1(config-ext-nacl)# end
```

20. **Envoyez une commande `ping` de l'hôte A vers l'hôte B.**

```
 # ping 12.0.0.17
 12.0.0.17 is alive
```

23. **Appliquez le filtre IP 11 au port 25.**

```
 SEFOS-1(config)# interface xl-ethernet 0/25
 SEFOS-1(config-if)# ip access-group 11 in
 SEFOS-1(config-if)# exit
 SEFOS-1(config)# vlan 1
 SEFOS-1(config-vlan)# ports xl-ethernet 0/25 xl-ethernet
 0/26 untagged xl-ethernet 0/25 xl-ethernet 0/26
```

Remarque - Vous risquez de voir s'afficher le message suivant si les ports 25 et 26 se trouvent déjà dans VLAN 1. Si vous voyez ce message, vous pouvez l'ignorer.

```
% Member Ports cannot be added/deleted on Default VLAN
SEFOS-1(config-vlan)# end
```

30. **Affichez les détails de configuration.**

```
SEFOS-1# show access-lists
...
IP address Type                    : IPV4
...
In Port List                       : X10/25
...
Filter Action                      : Deny
Status                             : Active
```

39. **Envoyez le trafic de transfert de l'hôte A vers l'hôte B en utilisant la même procédure que celle indiquée pour la commande `ping` entre l'hôte A et l'hôte B à l'Step 5.**

    Les paquets envoyés à partir de l'hôte A ne sont pas transférés vers le port 26 car l'action de filtrage est définie sur deny. L'envoi de la commande `ping` vers 12.0.0.17 à partir de l'hôte A échoue sans réponse de 12.0.0.17.

40. **Supprimez le filtre IP du port 25.**

```
SEFOS-1# configure terminal
SEFOS-1(config)# interface xl-ethernet 0/25
SEFOS-1(config-if)# no ip access-group 11 in
SEFOS-1(config-if)# end
SEFOS-1# show access-lists
...
Status                             : InActive
```

48. **Envoyez le trafic de transfert de l'hôte A vers l'hôte B en utilisant la même procédure que celle indiquée pour la commande `ping` entre l'hôte A et l'hôte B à l'Step 5.**

    L'hôte B répond à la commande `ping`. Les paquets envoyés à partir de l'hôte A sont transférés vers le port 26. Les deux commandes consécutives `ping` suivantes montrent que l'action de filtrage deny définie dans la liste de contrôle d'accès a été appliquée à un port et supprimée d'un autre port.

```
# ping 12.0.0.17
no answer from 12.0.0.17
# ping 12.0.0.17
12.0.0.17 is alive
```