Cisco: Reflexive ACL

Introduction

Reflexive ACLs (Dynamic Reflexive Access Lists) is an extension to ACLs in Cisco IOS that allows traffic to be filtered **based on sessions initiated from within the network**. They are particularly useful for controlling traffic **incoming** in networks where only **responses to outgoing calls** should be allowed.

This works similarly to the principle of **stateful firewall**: only packets belonging to previously initiated TCP/UDP sessions are allowed to pass in the return direction.

Main features

- Works only for session-based protocols: **TCP** i **UDP**.
- Creates temporary dynamic ACL entries based on outgoing connections.
- Deleted automatically when the session ends.
- Configuration based on classic ACLs of type **extended**.

Example of topology

Private network: `192.168.1.0/24` Cisco router with external interface `GigabitEthernet0/0`. Public network (e.g. Internet): `0.0.0.0/0`

Configuration of Reflexive ACL

1. create ACL with dynamic entry

```
ip access-list extended OUTBOUND
 permit tcp 192.168.1.0 0.0.0.255 any reflect ALLOW_OUT
 permit udp 192.168.1.0 0.0.0.255 any reflect ALLOW_OUT
```

* `reflect ALLOW_OUT` - creates a dynamic entry with this name for each outgoing connection.

2. ACL list for incoming traffic

```
ip access-list extended INBOUND
 evaluate ALLOW_OUT
```

* `evaluate` - checks the dynamic entries created by the OUTBOUND ACL.

Assigning ACLs to interfaces.

Assume:

- `GigabitEthernet0/0` is. **external interface**
- `GigabitEthernet0/1` is the **internal interface**

```
interface GigabitEthernet0/1
 ip access-group OUTBOUND out

interface GigabitEthernet0/0
 ip access-group INBOUND in
```

Performance check

Check the dynamic ACL entries created:

```
show ip access-lists
```

View information about dynamic sessions:

```
show ip access-list cache
```

Recommendations and comments

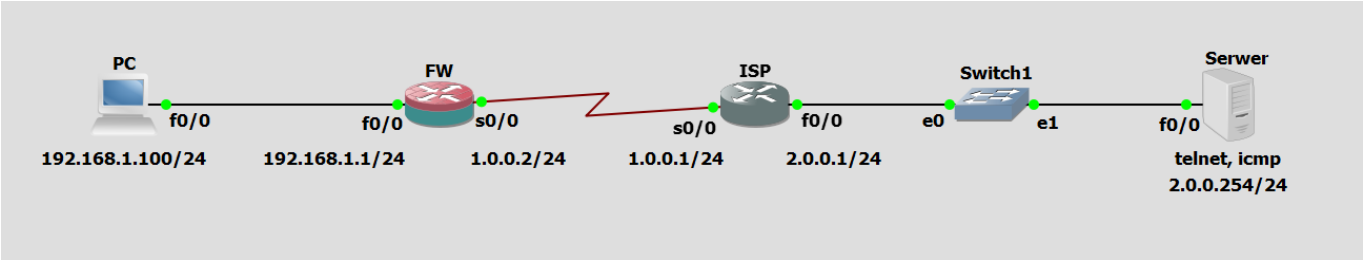
- Reflexive ACLs do not support ICMP (e.g. `ping`).
- Other ACL rules should be added for management protocols (e.g. `permit tcp any host <router-ip> eq 22` for SSH).
- With heavy traffic, it can be a load on the CPU.
- You can limit the existence time of dynamic entries with:

```
ip reflexive-list timeout 300
```

Summary

Reflexive ACLs are a simple way to protect your internal network from unauthorised inbound traffic, while maintaining functionality for outbound traffic. Ideal in scenarios where a full-fledged firewall is not available or required.

Example



FW configuration:

```
FW#show running-config
Building configuration...

Current configuration : 1481 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group wejscie in
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 1.0.0.2 255.255.255.0
 ip access-group wyjscie out
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 1.0.0.1
!
!
no ip http server
no ip http secure-server
!
ip access-list extended wejscie
 evaluate ok
ip access-list extended wyjscie
 permit ip any any reflect ok
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```