Cisco: Reflexive ACL

Wprowadzenie

Reflexive ACL (Dynamiczne listy dostępu zwrotnego) to rozszerzenie list ACL w Cisco IOS, które umożliwia filtrowanie ruchu **na podstawie sesji inicjowanych z wnętrza sieci**. Są one szczególnie przydatne do kontroli ruchu **przychodzącego** w sieciach, gdzie tylko **odpowiedzi na połączenia wychodzące** powinny być dozwolone.

Działa to podobnie do zasady działania **stateful firewall**: tylko pakiety należące do wcześniej zainicjowanych sesji TCP/UDP są przepuszczane w kierunku powrotnym.

Główne cechy

- Działa tylko dla protokołów opartych na sesjach: **TCP** i **UDP**.
- Tworzy tymczasowe, dynamiczne wpisy ACL na podstawie połączeń wychodzących.
- Usuwane automatycznie po zakończeniu sesji.
- Konfiguracja oparta na klasycznych ACL typu **extended**.

Przykład topologii

Sieć prywatna: `192.168.1.0/24` Router Cisco z interfejsem zewnętrznym `GigabitEthernet0/0` Sieć publiczna (np. Internet): `0.0.0.0/0`

Konfiguracja Reflexive ACL

1. Utworzenie listy ACL z dynamicznym wpisem

```
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` – tworzy dynamiczny wpis o tej nazwie dla każdego połączenia wychodzącego.

2. Lista ACL dla ruchu przychodzącego

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

* `evaluate` – sprawdza dynamiczne wpisy utworzone przez ACL OUTBOUND.

3. Przypisanie ACL do interfejsów

Załóżmy:

- `GigabitEthernet0/0` to **interfejs zewnętrzny**
- `GigabitEthernet0/1` to **interfejs wewnętrzny**

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

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

Sprawdzanie działania

Sprawdź utworzone dynamiczne wpisy ACL:

```
show ip access-lists
```

Wyświetl informacje o dynamicznych sesjach:

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

Zalecenia i uwagi

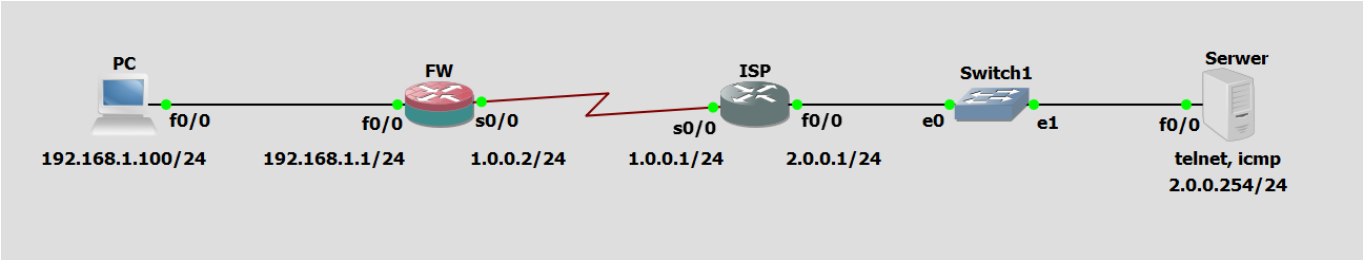
- Reflexive ACL nie obsługują ICMP (np. `ping`).
- Należy dodać inne reguły ACL dla protokołów zarządzających (np. `permit tcp any host <router-ip> eq 22` dla SSH).
- Przy intensywnym ruchu może być obciążeniem CPU.
- Można ograniczyć czas istnienia dynamicznych wpisów za pomocą:

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

Podsumowanie

Reflexive ACL to prosty sposób na ochronę sieci wewnętrznej przed nieautoryzowanym ruchem przychodzącym, przy jednoczesnym zachowaniu funkcjonalności dla ruchu wychodzącego. Idealne w scenariuszach, gdzie nie jest dostępny lub wymagany pełnoprawny firewall.

Przykład



Konfiguracja FW:

```
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
```