Listy ACL na urządzeniach Cisco

Access Control List (ACL) to mechanizm filtracji ruchu sieciowego na urządzeniach Cisco, który pozwala na kontrolowanie dostępu do sieci. Listy ACL mogą być używane do filtrowania pakietów, zabezpieczania dostępu do zasobów i egzekwowania polityki bezpieczeństwa.

Rodzaje list ACL

Na urządzeniach Cisco dostępne są następujące typy list ACL:

1. **ACL standardowe (podstawowe)** – filtrują ruch na podstawie adresu źródłowego IP.
2. **ACL rozszerzone** – filtrują ruch na podstawie adresu źródłowego, docelowego, protokołu oraz portów.
3. **ACL numerowane** – identyfikowane za pomocą numerów.
4. **ACL nazwane** – identyfikowane za pomocą nazw, co ułatwia zarządzanie.

---

1. ACL Standardowe (podstawowe)

Standardowe listy ACL filtrują pakiety na podstawie adresu źródłowego IP. Mogą tylko pozwalać lub blokować ruch bez uwzględnienia portów czy protokołów.

Zakres numeracji: 1 – 99 oraz 1300 – 1999 (rozszerzony zakres)

Przykład konfiguracji ACL standardowej:

Blokowanie dostępu do sieci 192.168.1.0/24 dla hosta 10.0.0.1:

```
Router(config)# access-list 10 deny 10.0.0.1
Router(config)# access-list 10 permit any
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip access-group 10 in
```

---

2. ACL Rozszerzone

ACL rozszerzone umożliwiają filtrowanie ruchu na podstawie:

- adresów źródłowych i docelowych,
- protokołów (TCP, UDP, ICMP itp.),
- numerów portów.

Zakres numeracji: 100 – 199 oraz 2000 – 2699 (rozszerzony zakres)

Przykład konfiguracji ACL rozszerzonej:

Blokowanie dostępu z sieci 192.168.1.0/24 do serwera 10.0.0.100 na porcie HTTP (80):

```
Router(config)# access-list 110 deny tcp 192.168.1.0 0.0.0.255 host
10.0.0.100 eq 80
Router(config)# access-list 110 permit ip any any
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip access-group 110 in
```

---

3. ACL Numerowane

Numerowane listy ACL to tradycyjny sposób tworzenia reguł ACL, w którym każda lista jest identyfikowana przez unikalny numer.

Przykład konfiguracji numerowanej ACL:

Blokowanie dostępu SSH (port 22) do routera z sieci 192.168.50.0/24:

```
Router(config)# access-list 120 deny tcp 192.168.50.0 0.0.0.255 any eq 22
Router(config)# access-list 120 permit ip any any
Router(config)# interface GigabitEthernet0/2
Router(config-if)# ip access-group 120 in
```

---

4. ACL Nazwane

ACL nazwane są bardziej elastyczne i łatwiejsze do zarządzania niż ACL numerowane, ponieważ używają czytelnych nazw zamiast numerów.

Przykład konfiguracji ACL nazwanej:

Blokowanie dostępu do sieci 192.168.100.0/24 z dowolnej sieci:

```
Router(config)# ip access-list extended BLOCK_NET
Router(config-ext-nacl)# deny ip any 192.168.100.0 0.0.0.255
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
Router(config)# interface GigabitEthernet0/3
Router(config-if)# ip access-group BLOCK_NET in
```

Dobre praktyki w konfiguracji ACL

1. **Pamiętaj o domyślnej regule „deny all”** – jeśli nie dodasz reguły permit, wszystko zostanie domyślnie zablokowane.
2. **Umieszczaj najbardziej specyficzne reguły na początku listy** – ACL są przetwarzane w kolejności.
3. **Unikaj stosowania ACL na interfejsach zarządzania** – może to prowadzić do blokady dostępu administracyjnego.
4. **Używaj ACL nazwanych zamiast numerowanych** – są bardziej przejrzyste i łatwiejsze w modyfikacji.

5. **Monitoruj ruch i testuj reguły** – używaj show access-lists oraz debug ip packet do weryfikacji działania ACL.

Podsumowanie

Listy ACL na urządzeniach Cisco są kluczowym narzędziem do zarządzania dostępem i zabezpieczania sieci. Wybór odpowiedniego typu ACL zależy od poziomu kontroli, jaki chcemy uzyskać:

- ACL **standardowe** pozwalają tylko na filtrację po adresie źródłowym,
- ACL **rozszerzone** oferują większą kontrolę (adresy źródłowe i docelowe, protokoły, porty),
- ACL **numerowane** są starszą metodą, wymagającą numeru listy,
- ACL **nazwane** są bardziej czytelne i elastyczne.

Znajomość i umiejętne stosowanie ACL jest kluczowe dla administratorów sieci, aby zapewnić bezpieczeństwo i kontrolę dostępu w infrastrukturze Cisco.