# Stosowanie List ACL na Urządzeniach Cisco

## Wstęp

Access Control Lists (ACL) są zestawem reguł stosowanych w urządzeniach sieciowych Cisco, które kontrolują ruch sieciowy przechodzący przez te urządzenia. Głównym celem stosowania ACL jest zwiększenie bezpieczeństwa sieci poprzez filtrowanie ruchu na podstawie adresów IP, protokołów i innych kryteriów. ACL pozwalają na dokładne definiowanie, które pakiety są dozwolone, a które mają zostać odrzucone.

## Konstrukcja List ACL Standardowych

Standardowe listy ACL są podstawowymi listami kontroli dostępu, które filtrują ruch wyłącznie na podstawie adresów IP źródłowych. Nie oferują możliwości filtrowania na podstawie portów lub protokołów. Standardowe listy ACL stosuje się głównie do kontroli dostępu do zasobów sieciowych na podstawie adresu źródłowego.

Przykład konfiguracji standardowej listy ACL na urządzeniu Cisco:

```
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any
```

## Konstrukcja List ACL Rozszerzonych

Rozszerzone listy ACL pozwalają na bardziej szczegółowe filtrowanie ruchu sieciowego. Oferują możliwość filtrowania na podstawie adresów IP źródłowych i docelowych, a także na podstawie protokołów, takich jak TCP, UDP czy ICMP, oraz numerów portów. Dzięki temu, są bardziej elastyczne i stosowane tam, gdzie wymagana jest większa kontrola nad ruchem sieciowym.

Przykład konfiguracji rozszerzonej listy ACL na urządzeniu Cisco:

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 100 deny ip any any
```

## Konstrukcja List Nazwanych ACL

Nazwane listy ACL pozwalają na przypisanie nazwy do listy ACL, co ułatwia zarządzanie, szczególnie w większych konfiguracjach. Mogą być standardowe lub rozszerzone, a ich definicja jest bardziej elastyczna niż w przypadku list numerowanych. Listy nazwane umożliwiają również edycję poszczególnych reguł w ramach listy, co nie jest możliwe przy użyciu list numerowanych.

Przykład konfiguracji nazwanej listy ACL na urządzeniu Cisco:

```
ip access-list extended MyACL
 permit tcp 192.168.1.0 0.0.0.255 any eq 80
 deny ip any any
```

### Przypisanie Listy ACL do Interfejsu

Aby lista ACL mogła działać, musi zostać przypisana do interfejsu na urządzeniu sieciowym. Przypisanie odbywa się dla ruchu przychodzącego (inbound) lub wychodzącego (outbound). Komenda używana do przypisania ACL różni się w zależności od kierunku ruchu oraz interfejsu, do którego jest przypisywana.

Przykład przypisania listy ACL do interfejsu:

```
interface GigabitEthernet0/1
 ip access-group 100 in
```

## Przykłady List ACL na Urządzeniach Cisco

Poniżej znajdują się różne przykłady konfiguracji list ACL na urządzeniach Cisco. Każdy przykład jest opisany szczegółowo, aby ułatwić zrozumienie zastosowania oraz efektu poszczególnych reguł na ruch sieciowy.

### Przykład 1: Prosta Lista Standardowa

Lista ACL 15 pozwalająca na dostęp tylko dla ruchu z sieci 192.168.10.0/24. Wszystkie inne adresy IP są blokowane. Jest to przykład prostej listy standardowej filtrującej ruch wyłącznie na podstawie adresów IP źródłowych.

```
access-list 15 permit 192.168.10.0 0.0.0.255
access-list 15 deny any
```

### Przykład 2: Lista Rozszerzona dla Ruchu HTTP

Lista rozszerzona 105, która pozwala na ruch HTTP (port 80) z sieci 10.1.1.0/24 do dowolnych adresów IP w sieci, jednocześnie blokując wszystkie inne pakiety z tej sieci. To przykład bardziej szczegółowej listy ACL, która filtruje ruch na podstawie portów i protokołów.

```
access-list 105 permit tcp 10.1.1.0 0.0.0.255 any eq 80
access-list 105 deny ip any any
```

### Przykład 3: Nazwana Lista ACL dla SSH

Nazwana lista ACL o nazwie 'AllowSSH', która pozwala na ruch SSH (port 22) do routera tylko z sieci 172.16.0.0/16. Wszystkie inne połączenia na ten port są blokowane. Lista ACL pozwala na wyodrębnienie specyficznych połączeń dla zarządzania siecią.

```
ip access-list extended AllowSSH
 permit tcp 172.16.0.0 0.0.255.255 any eq 22
 deny ip any any
```

### Przykład 4: Lista ACL z Wieloma Regułami

Rozszerzona lista ACL 110, która pozwala na ruch ICMP (ping) oraz HTTP z sieci 192.168.20.0/24 do dowolnych adresów, jednocześnie blokując wszystkie inne połączenia. Ta konfiguracja zawiera wiele reguł w jednej liście ACL, co pozwala na bardziej złożone filtrowanie ruchu.

```
access-list 110 permit icmp 192.168.20.0 0.0.0.255 any
access-list 110 permit tcp 192.168.20.0 0.0.0.255 any eq 80
access-list 110 deny ip any any
```