

Wykorzystaj : CCNA_cw_15_ACL_01.pkt

ACL Zadania podstawowe

Zadanie 1: Blokowanie ruchu HTTP między Warszawą a Opolem

Stwórz ACL, która zablokuje ruch http,HTTPS (port 80,443) z sieci Warszawa (172.16.8.0/22) do sieci Opole (172.16.12.0/23).

Zadanie 2: Ustal priorytety ruchu tylko dla sieci Katowice

Stwórz ACL, która umożliwi ruch tylko na portach 80 (HTTP), 443 (HTTPS) i 22 (SSH) z sieci Katowice (172.16.14.0/23) do wszystkich sieci. Wszystkie inne rodzaje ruchu z tej sieci powinny być zablokowane.

Zadanie 3: Ograniczenie dostępu do Katowic

Stwórz ACL, która zablokuje dostęp do sieci Katowice (172.16.14.0/23) z wyjątkiem komputerów z sieci Opole (172.16.12.0/23).

Zadanie 4: Ochrona przed atakami w sieci Katowice

Stwórz ACL, która zablokuje ruch ICMP (ping) do sieci Katowice (172.16.14.0/23), aby uchronić sieć przed potencjalnymi atakami.

Zadanie 5: Dostęp do zarządzania routerami

Stwórz ACL, która ograniczy zdalny dostęp do zarządzania routerami tylko do hostów w sieci Warszawa (172.16.8.0/22).

Rozwiązania Zadania podstawowe, listy numerowane

Zadanie 1: Blokowanie ruchu HTTP, HTTPS między Warszawą a Opole

```
no access-list 110
access-list 110 deny tcp 172.16.8.0 0.0.3.255 172.16.12.0 0.0.1.255 eq 80
access-list 110 deny tcp 172.16.8.0 0.0.3.255 172.16.12.0 0.0.1.255 eq 443
access-list 110 permit ip any any

interface g0/0
ip access-group 110 in
```

Zadanie 2: Ustal priorytety ruchu tylko dla sieci Katowice

```
no access-list 110
access-list 111 permit tcp 172.16.14.0 0.0.1.255 any eq 80
access-list 111 permit tcp 172.16.14.0 0.0.1.255 any eq 443
access-list 111 permit tcp 172.16.14.0 0.0.1.255 any eq 22
access-list 111 deny ip 172.16.14.0 0.0.1.255 any
access-list 111 permit ip any any

interface g0/0
ip access-group 111 in
```

Zadanie 3: Ograniczenie dostępu do Katowic

```
no access-list 112
access-list 112 permit ip 172.16.12.0 0.0.1.255 172.16.14.0 0.0.1.255
access-list 112 deny ip any 172.16.14.0 0.0.1.255
access-list 112 permit ip any any
interface g0/0
ip access-group 112 out
```

Zadanie 4: Ochrona przed atakami w sieci Katowice

```
no access-list 113
access-list 113 deny icmp any 172.16.14.0 0.0.1.255
access-list 113 permit ip any any
interface g0/0
ip access-group 113 out
```

Zadanie 5: Dostęp do zarządzania routerami

```
access-list 115 permit ip 172.16.8.0 0.0.3.255 any
access-list 115 deny ip any any
line vty 0 15
access-class 115 in
```



```
no ip access-list extended WARSAW_OPOLE
ip access-list extended WARSAW_OPOLE
  deny tcp 172.16.8.0 0.0.3.255 172.16.12.0 0.0.1.255 eq 80
  deny tcp 172.16.8.0 0.0.3.255 172.16.12.0 0.0.1.255 eq 443
  permit ip any any
```

```
interface g0/0
ip access-group WARSAW_OPOLE in
```

```
no ip access-list extended KATOWICE_PRIORITY
ip access-list extended KATOWICE_PRIORITY
  permit tcp 172.16.14.0 0.0.1.255 any eq 80
  permit tcp 172.16.14.0 0.0.1.255 any eq 443
  permit tcp 172.16.14.0 0.0.1.255 any eq 22
  deny ip 172.16.14.0 0.0.1.255 any
  permit ip any any
```

```
interface g0/0
ip access-group KATOWICE_PRIORITY in
```

```
no ip access-list extended ACCESS_TO_KATOWICE
ip access-list extended ACCESS_TO_KATOWICE
  permit ip 172.16.12.0 0.0.1.255 172.16.14.0 0.0.1.255
  deny ip any 172.16.14.0 0.0.1.255
  permit ip any any
```

```
interface g0/0
ip access-group ACCESS_TO_KATOWICE out
```

```
no ip access-list extended KATOWICE_PROTECTION
ip access-list extended KATOWICE_PROTECTION
  deny icmp any 172.16.14.0 0.0.1.255
  permit ip any any
```

```
interface g0/0
ip access-group KATOWICE_PROTECTION out
```

```
no ip access-list standard ROUTER_MANAGEMENT
ip access-list standard ROUTER_MANAGEMENT
  permit ip 172.16.8.0 0.0.3.255 any
  deny ip any any
```

```
line vty 0 15
access-class ROUTER_MANAGEMENT in
```

Zadanie 6: Ograniczenie dostępu do Internetu

Stwórz ACL, która zablokuje dostęp do Internetu dla sieci Katowice (172.16.14.0/23), ale nadal pozwoli na ruch wewnętrzny.

Zadanie 7: Filtracja zawartości

Stwórz ACL, która zablokuje dostęp do sieci o adresie IP 8.8.8.8 tylko dla sieci Warszawa (172.16.8.0/22).

Zadanie 9: Ograniczenie dostępu do Internetu

```
access-list 117 deny ip 172.16.14.0 0.0.1.255 any
access-list 117 permit ip any any
```

```
interface [Interfejs_router_Opole_g0/0]
ip access-group 117 in/out
```

Zadanie 10: Filtracja zawartości

```
access-list 118 deny ip 172.16.8.0 0.0.3.255 host 8.8.8.8
access-list 118 permit ip any any
```

```
interface [Interfejs_router_Warszawa_g0/0]
ip access-group 118 in/out
```