**ZADANIE A: Filtrowanie ruchu datagramów - standardowe listy kotrolne**

NUMER INSTRUKCJI   
(WEDŁUG LAB ROADMAP)

**072**

|  |
| --- |
| Tworzenie listy dostępu:  Router(config)#access-list 90 deny any (90 to ID nowej listy)  Sprawdzenie zapisanych list:  Router#show access-lists  Przy uzupełnianiu listy zabraniającej operacji na szczególnych IP dodajemyzapis zezwalający na pozostały ruch:  Router(config)#access-list 70 deny host 10.10.10.1  Router(config)#access-list 70 permit any  Router(config)#access-list 70 remark To jest lista usuwająca 10.10.10.1  Przypisanie listy do interfejsu :  Router(config)#int fe 0/0  Router(config-if)#ip access-group 90 in  Usuwanie całej listy:  Router(config)#no ip access-list standard 90  Usuwanie przypisania do interfejsu:  Router(config-if)#no ip access-group 90 in  Aby przejść do trybu edycji listy (ACL):  Router(config)#ip access-list standard 90  Router(config-std-nacl)#26 deny host 10.10.10.1 |

1. **Standardowe** listy dostępu (access-lists) posiadają identyfikatory z przedziału **1-99**
2. Do określania grup hostów w access-lists stosowane są maski zapisywane w **inwersji bitowej**
3. Reguły zapisane w listach dostępu posiadają **numery** **sekwencji**, gwarantujące porządek sprawdzania. Aby przebudować numerację:

Router(config)#ip access-list resequence 60 20 10

(60 to numer listy, 20 to nowy początek numeracji dla numerów sekwencji, 10 to kolejny przyrost)

1. Zakres adresów można określić na trzy sposoby: **wszystkie adresy dowolny host, 1 konkretny host, sieć z maską.**

* any - wszystkie adresy, dowolny host
* 10.10.10.0 0.0.0.255 - sieć z maską
* host 10.10.10.1 - konkretny, jeden host

W ogólnym trybie **config** dokonywanie wpisów musi odbywać się z poszanowaniem porządku **„od szczegółu do ogółu”.**

**ZADANIE B: Filtrowanie pakietów - listy rozszerzone**

|  |
| --- |
| Tworzenie przykładowej listy dostępu:  Router(config)#access-list 190 deny tcp any 10.10.10.0 0.0.0.255 eq 23 (tcp - IP protokołu, any - dowolne źródło, 10.10.10.0 0.0.0.255 - dowolny host docelowego w sieci 10.10.10.0/24, eq 23 - dalsze cechy z nim związane)  Zapisane listy można sprawdzić komendą:  Router#show access-lists  Zezwolenie na pozostały ruch w IP (którego nie zamierzamy blokować):  Router(config)#access-list 190 allow ip any any  Przypisanie listy do interfejsu.:  Router(config)#int fa 0/0  Router(config-if)#ip access-group 190 in (in oznacza filtr dla pakietów wchodzących przez interfejs, out - dla wychodzących. )  Po sprawdzeniu funkcjonowania blokady należy usunąć przypisanie:  Router(config-if)#no ip access-group 190 in |

1. Listy rozszerzone są rejestrowane w przedziale **100 – 199**
2. Definiowanie adresów IP tak samo jak w przypadku list standardowych.

Pozwalają na wyszczególnienie osobno cech puli IP odbiorcy i nadawcy, a także kilku popularnych protokołów nad IP, których datagramy są przedmiotem transmisji. Ponadto - w przypadku TCP i UDP - numerów/zakresów portów dla tych protokołów (nie obowiązkowo). W przypadku niektórych usług nad UDP czy TCP można się posłużyć ich nazwami zamiast numerami portów (np. telnet, SNMP, ISAKMP, FTP, WWW itp.).

Tak samo też użytkowane są słowa **deny/permit/remark**. Gdy z puli protokołów wybierzemy po prostu IP - rezygnujemy z dodatkowego filtrowania protokołów nad IP (określamy wtedy tylko filtry IP dla source lub destination).

**ZADANIE C:** **Filtrowanie pakietów - listy nazwane (named lists)**

|  |
| --- |
| Utworzenie standardowej nazwanej listy dostępu:  Router(config)#IP access-list standard moja\_lista  Router(config-std-nacl)#deny 10.10.10.1 0.0.0.0  Router(config-std-nacl)#permit 10.10.10.2 0.0.0.0  Utworzenie rozszerzonej nazwanej listy dostępu:  Router(config)#IP access-list extended moja\_lista2  Router(config-ext-nacl)#deny TCP 10.10.10.1 0.0.0.0 20.10.10.1 0.0.0.0 eq www  Przypisanie listy do wybranego interfejsu:  Router(config-line)#access-group moja\_lista2 in  Sprawdzenie zdefiniowanych list:  Router#sh access-lists  Po sprawdzeniu funkcjonowania list należy je usunąć. |