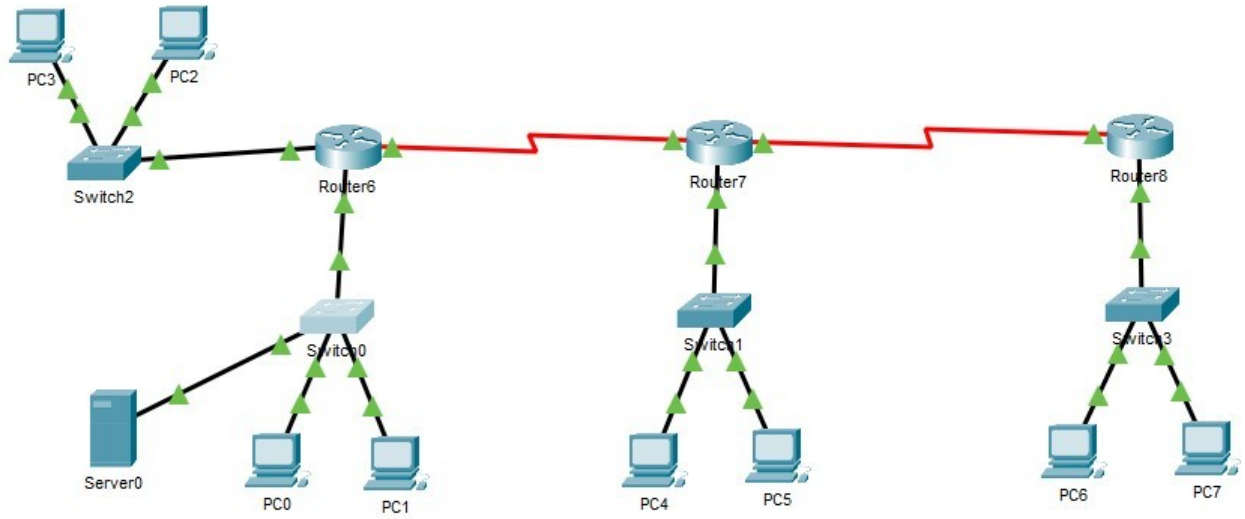
Bezpieczeństwo sieci komputerowych
Temat: VPN

Data: 07/06/2022
Ewa Namysł
Informatyka stosowana, III rok

1. Opis i cel zadania:

Celem zadania jest ustawienie zapory na routerze. Zapora ma blokować ruch na porcie 80 oraz 443 (HTTP, HTTPS), blokować wybrany komputera w sieci na wszystkich portach oraz blokować cały ruch z jednej podsieci.

Wykorzystaną topologię przedstawiono poniżej:



2. Blokowanie HTTP/HTTPS

Strona dostępna jest pod adresem serwera (192.168.50.4). Tworzymy ACL:

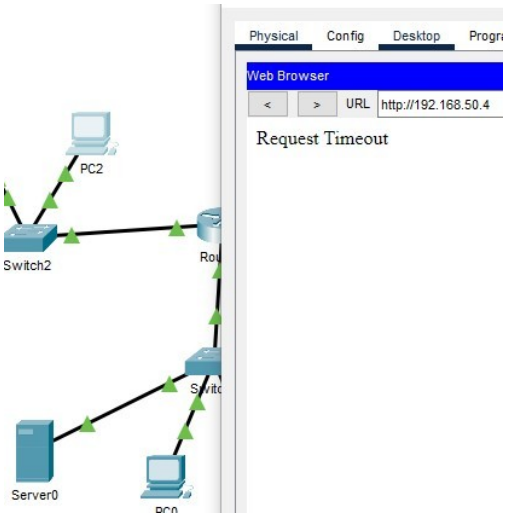
access-list 101 deny tcp any any eq 80
access-list 101 deny tcp any any eq 443

Przypisujemy listę do wybranego interfejsu:

ip access-group 101 in

Teraz strona dostępna jest tylko w jej sieci:

Poza nią jest nieosiągalna:



3. Blokowanie wybranego komputera:

Do zablokowania wybrany został komputer PC1 o adresie 192.168.50.3. Wpisujemy:

access-list 101 deny ip host 192.168.50.3 any

Po przypisaniu do interfejsu, komunikacja z komputerem PC0 o adresie 192.168.50.3 jest możliwe, lecz komunikacja z PC1 jest uniemożliwiona:

Fire	Last Status	Source	Destination	Type
	Successful	PC2	PC0	ICMP
	Failed	PC2	PC1	ICMP

4. Blokowanie sieci:

Blokujemy sieć 205.7.5.0, wpisujemy:

access-list 101 deny ip 205.7.5.0 0.0.0.255 any

Po wprowadzeniu i przypisaniu sieć będzie izolowana.

5. Sprawdzanie ACL i usuwanie:

Aby zobaczyć access-listy na routerze wpisujemy:

show access-lists

Żeby usunąć ACL, usuwamy ją najpierw z interfejsu:

no ip access-group 100 in
lub/i
no ip access-group 100 out

A następnie w trybie konfiguracyjnym wpisujemy:

no access-list 100