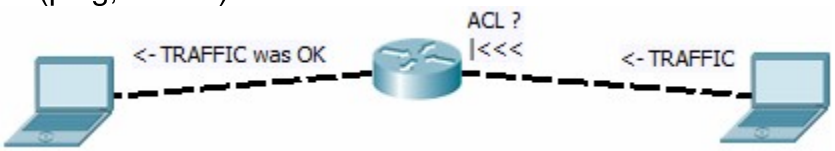
SIECI KOMPUTEROWE – LABORATORIUM 072

Tematyka:
Access Control Lists w ruterach Cisco

Zadanie A: Filtrowanie ruchu datagramów - standardowe listy kontrolne

1. Należy przygotować do pracy ruter Cisco, łącząc go okablowaniem TP (*Twisted Pair*) w układzie PC-ruter-PC. Należy skonfigurować i włączyć stosowne interfejsy rutera – definiując różne bezpośrednio podłączone sieci IP zgodnie z ogólnie znanymi zasadami, np.:
   Router(config)# int fa 0/0
   Router(config-if)#ip address 200.200.200.1 255.255.255.0
   Router(config-if)#no shut
   Router(config-if)#int fa 0/1
   Router(config-if)#ip address 200.200.201.1 255.255.255.0
   Router(config-if)#no shut
   Interfejsy IP stacji PC także należy odpowiednio skonfigurować
   Uwaga: W każdej ze stacji PC należy zdefiniować adres IP domyślnej bramki, jako adres interfejsu IP rutera po tej jego stronie, gdzie znajduje się wspomniana stacja.
   Należy sprawdzić, czy w ruterze zostało uruchomione rutowanie IP i ewentualnie uruchomić je:
   Router(config)#ip routing
   Po skonfigurowaniu instalacji należy sprawdzić sprawność komunikacji pomiędzy stacjami PC (ping, tracert).



2. Bieżąca seria doświadczeń będzie polegała na eksperymentalnym blokowaniu wybranego ruchu sieciowego pomiędzy dwoma stacjami PC za pomocą *List kontroli dostępu* (*ACL – Access Controll Lists*) definiowanych w ruterze. Listy te są numerowane wartościami identyfikatorów. Tak zwane *standardowe* listy posiadają identyfikatory z przedziału 1-99 (czyli wartość samego identyfikatora w momencie definiowania wpisów listy określa jej rodzaj). Listy te są uproszczone i pozwalają na blokowanie ruchu dotyczącego specyficznych adresów IP lub ich grup bez możliwości rozróżniania osobno cech nadawcy od odbiorcy.
   Zakres adresów (lub pojedynczy adres) można specyfikować na trzy sposoby, przykładowo:
   - *any* - wszystkie adresy, dowolny host
   - *10.10.10.0 0.0.0.255* - sieć z maską
   - *host 10.10.10.1* - konkretny, jeden host

3. Tworzenie listy dostępu, np.:
   Router(config)#access-list 90 deny any
   gdzie *90* to ID nowej listy, *deny* to zakaz- możliwe są jeszcze wartości *permit* (zezwolenie) i *remark* (komentarz listy).
4. Zapisane listy można sprawdzić komendą:
   Router#show access-lists
   Przy uzupełnianiu listy zabraniającej operacji na szczególnych IP należy pamiętać o dodaniu zapisu zezwalającego na pozostały ruch, np.:
   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
5. Przypisanie listy do interfejsu, np.:
   Router(config)#int fe 0/0
   Router(config-if)#ip access-group 90 in
   gdzie *in* oznacza filtr dla pakietów wchodzących przez interfejs, analogicznie *out* - dla wychodzących.
   Sprawdzenie przypisania ACL do interfejsów:
   Router#show run
6. Usuwanie całej listy:
   Router(config)#no ip access-list standard 90
   Usuwanie przypisania do interfejsu:
   Router(config-if)#no ip access-group 90 in
   Należy pamiętać, że struktury access-lists nie są wykorzystywane jedynie do regulowania ruchu przez interfejsy, lecz w wielu innych mechanizmach.
   Uwaga: do określania grup hostów w access-lists stosowane są maski zapisywane w **inwersji bitowej**, więc na przykład reguła:
   Router(config)#access-list 70 deny 10.10.10.0 0.0.0.255
   odnosi się do puli adresów 10.10.10.0 - 10.10.10.255 (0 w masce oznacza polecenie sprawdzenia odpowiadającego mu bitu w adresie, 1 – zignorowania)
7. Reguły zapisane w listach dostępu posiadają numery sekwencji, gwarantujące porządek sprawdzania (sprawdzanie odbywa się zgodnie z rosnącymi wartościami numerów sekwencji). Numery widoczne są przy wypisywaniu list. Aby przebudować numerację należy posłużyć się komendą, np.:
   Router(config)#ip access-list resequence 60 20 10
   gdzie 60 to numer listy, 20 to nowy początek numeracji dla numerów sekwencji, 10 to kolejny przyrost.
8. W ogólnym trybie *config* możliwe jest tworzenie list oraz dodawanie do nich reguł bez wywierania wpływu na numery sekwencji (przydzielane są automatycznie jako rosnące wartości: 10,20,30,...itd.). W związku z tym dokonywanie wpisów musi odbywać się z poszanowaniem porządku „od szczegółu do ogółu”. Użycie innego porządku (np. poprzez dodanie reguły dla sieci, a później dla hosta) spowoduje błąd. W efekcie lista nie będzie zawierała reguł, które sprawdzane wcześniej pokryją inne, bardziej szczegółowe. Aby możliwe było posługiwanie się wybranymi numerami sekwencji przy definiowaniu wpisów trzeba przejść do trybu edycji listy (ACL), np.:
   Router(config)#ip access-list standard 70
   Router(config-std-nacl)#26 deny host 10.10.10.1
   gdzie *26* to numer sekwencji, pod jakim reguła zostanie umieszczona na liście numer *70*. Tu jednak także nie można doprowadzić do sytuacji, w której reguła o

niższym numerze sekwencji (sprawdzana wcześniej) pokryje swoją ogólnością inną, o wyższym numerze sekwencji.
Gdy chcemy skasować wpis o wybranym numerze sekwencji, piszemy np.:
Router(config-std-nacl)#no 26
Tryb konfigurowania wpisów ACL z typowaniem numeru sekwencji może być także używany wobec innych typów list, omawianych w następnych punktach.
Przetestuj poprawność funkcjonowania filtrów ACL dla wybranego ruchu pomiędzy stacjami PC (po zdefiniowaniu i przypisaniu listy do interfejsu) spowoduj testowe wysłanie takiego ruchu.
W raporcie generowanym przez komendy typu:
Router#show access-list interface fa 0/0 in
Router#show access-list 70
zwróć uwagę na liczby dopasowań (*matches*) datagramów do poszczególnych wpisów list ACL.
Kasowanie liczników dopasowań:
Router#clear access-list counters

Zadanie B: Filtrowanie ruchu datagramów - listy rozszerzone

1. Używając konfiguracji z zadania A należy przygotować listy rozszerzone. Są one rejestrowane w przedziale identyfikatorów 100 -199. Pozwalają na wyszczególnienie osobno zakresu adresów IP odbiorcy i nadawcy, odfiltrowanie rodzajów użytych nad IP protokołów, których datagramy są przedmiotem transmisji, czy innych cech tych datagramów. W przypadku TCP i UDP możliwe jest nawet identyfikowanie numerów/zakresów portów dla tych protokołów. CLI rutera umożliwia tu też posługiwanie się nazwami protokołów skojarzonych domyślnie z tymi numerami portów (np. telnet, SNMP, ISAKMP, FTP, WWW itp.). Zasada definiowania zakresów adresów IP podlegających filtrowaniu jest analogiczna jak w przypadku list prostych: użytkowane są słowa *deny/permit/remark*. Gdy z puli protokołów wybierzemy po prostu protokół IP - rezygnujemy z dodatkowego typowania ewentualnych protokołów nad IP (określamy wtedy tylko filtry dla adresów IP source lub destination).
2. Przykładowej tworzenia rozszerzonej listy dostępu:
   Router(config)#access-list 190 deny tcp any 10.10.10.0 0.0.0.255 eq 23
   gdzie *tcp* to identyfikator protokołu nad IP*, any* oznacza dowolny źródłowy adres IP, *10.10.10.0 0.0.0.255* oznacza dowolnego hosta docelowego w sieci *10.10.10.0/24*, natomiast *eq 23* oznacza dalsze ograniczenia związane z protokołem TCP (w tym przypadku*:* port docelowy TCP=23 czyli telnet)
3. Inne przykładowe możliwości formułowania filtrów:
   Router(config)#access-list 190 deny tcp any eq 23 any eq 40
   Router(config)#access-list 190 deny tcp 10.1.1.1 0.0.0.1 eq 23
   200.200.200.1 0.0.0.1 eq 100
   Router(config)#access-list 190 deny tcp host 10.10.10.1 any
   Router(config)#access-list 190 deny ip any 10.10.10.0 0.0.0.255
   Router(config)#access-list 190 deny icmp host 10.10.10.1 any
   Router(config)#access-list 190 deny tcp host 10.10.10.1 any
   Router(config)#access-list 190 deny udp any 10.10.10.0 0.0.0.255 eq tftp
   Zarejestrowane listy można sprawdzić komendą:

Router#show access-lists

4. Jak poprzednio - przy uzupełnianiu listy wybiórczo blokującej określony ruch należy pamiętać o jej zakończeniu zezwoleniem na przesłanie pozostałego ruchu (którego nie zamierzamy blokować):
   Router(config)#access-list 190 permit ip any any
5. Przypisanie listy do interfejsu – analogicznie jak poprzednio, np.:
   Router(config)#int fa 0/0
   Router(config-if)#ip access-group 190 in
   gdzie *in* oznacza filtr dla pakietów wchodzących przez interfejs, *out* - dla wychodzących.
6. Po sprawdzeniu poprawności funkcjonowania ustanowionej wybranej blokady ruchu należy usunąć przypisanie:
   Router(config-if)#no ip access-group 190 in

Zadanie C: Filtrowanie pakietów - listy nazwane (named lists)

1. Listy nazwane identyfikujemy łańcuchem zamiast liczby.
2. Utwórz standardową nazwaną listę dostępu, np.:
   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
   Router(config-std-nacl)#exit
3. Utwórz rozszerzoną nazwaną listę dostępu, np.:
   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
   Router(config-ext-nacl)#exit
4. Przypisz listy do wybranego interfejsu, np.:
   Router(config-if)#access-group moja_lista2 in
5. Sprawdź treść zdefiniowanych list
   Router#sh access-lists
6. Po sprawdzeniu poprawności funkcjonowania list należy je usunąć.