# Listy dostępu

Autor: Dawid Koń  IVFDS L07

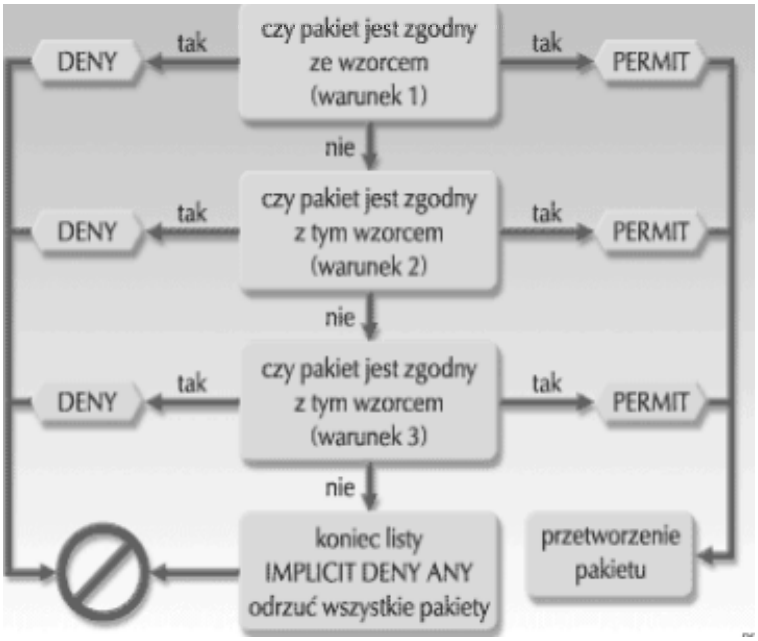
# STRESZCZENIE

W tym projekcie przedstawione zostaną najważniejsze zagadnienia związane z bezpiecznym dostępem do sieci lokalnej poprzez router Cisco. Poruszone zostaną kwestie filtrowania pakietów, ruchu skierowanego do konkretnej aplikacji jak również dystrybucji rozgłoszeń. Główny nacisk położę na konfigurowanie podstawowych i rozszerzonych list dostępu dla sieci opartych na protokole TCP/IP, jak również IPX/SPX.

# SPIS TREŚCI

# 1. LISTY DOSTEPU

Listy dostępu pozwalają na wstępną kontrolę i ograniczenie ruchu w sieci TCP/IP.




**Rys. 1**

## 1.1 Zabezpieczanie sieci poprzez listy dostępu na routerze Cisco

Systemy operacyjne routerów Cisco mogą filtrować ruch poprzez listy dostępu. Jedną z podstawowych metod zabezpieczenia i ograniczenia ruchu w sieci jest filtrowanie pakietów. Określa to, z jakiej sieci źródłowej do jakiej sieci docelowej odbywa się komunikacja, i wskazuje typ pakietów oraz aplikacji występujących na danym połączeniu. Lista dostępu nie jest tożsama z filtrowaniem pakietów przez router. Jest to zestaw kryteriów, według których procesy routera podejmują decyzję, co zrobić z pakietami danego typu. Decyzja ta jest jednoznaczna, i sprowadza się do wyboru między dwoma stanami: zgoda (allow) lub odmowa (deny) na przetworzenie pakietu.[1]

## 1.2 Funkcjonalność list dostępu

Listy dostępu mają zastosowanie w takich elementach konfiguracyjnych routera, jak:

-Opisanie ograniczeń dostępu do routera poprzez wirtualne linie terminalowe, czyli poprzez telnet.

-Ograniczenie zawartości uaktualnień tras wysyłanych przez protokoły routingu dynamicznego. To ograniczenie może również dotyczyć uaktualniania tablicy routingu przez router odbierający ogłoszenia tras. Proces ten nazywany jest również filtrowaniem tablicy routingu.

-Określenie pakietów, spowodujących zainicjowanie dodzwanianego połączenia DDR (Demand Dial Routing) z innym urządzeniem w sieci rozległej.

-Wskazanie ruchu zabezpieczonego , np. uwierzytelniany lub szyfrowany specjalizowanymi procesami w rodzaju protokołu IPSec.

-Ustalenie kolejkowania i priorytetów ruchu na interfejsach routera. Procesy te pozwalają i wskazać kolejność przetwarzania pakietów na poszczególnych interfejsach oraz umożliwiają zrównoważenie ruchu w sieci.

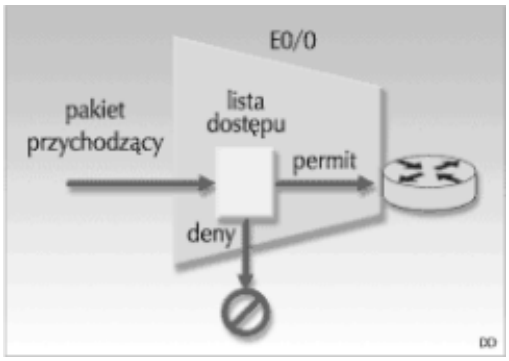
Listy dostępu są więc podstawą do konfiguracji wielu procesów związanych nie tylko z bezpieczeństwem sieci. [2]

## 1.3 Analiza list dostępu

Listy dostępu są zapisem kryteriów dotyczących typu i kierunku ruchu pakietów, ważne jest więc, z jakiej możliwości i w jakiej kolejności założenia te będą brane pod uwagę. Router przetwarza sekwencyjnie następne warunki zapisane na liście dostępu. Przetwarzanie ich jest sekwencyjne - router bada jeden warunek po drugim, konfrontując nagłówek pakietu ze wzorcem zapisanym w liście dostępu. Jeśli są one podobne, to na podstawie informacji w danym wzorcu pakiet jest przesyłany do nastepnego procesu lub odrzucany, w pozostałym razie sprawdzane są kolejne warunki aż do wyczerpania listy. Wykonanie warunku umieszczonego wyżej na liście zamyka proces sprawdzania, warunek ten rozstrzygnie więc o odrzuceniu lub przyjęciu pakietu.

## 1.4 Zasady budowania list dostępu

W każdej liście dostępu występuje ostateczny warunek odrzucający wszystkie pakiety. Sekwencja zapisów w listach dostępu ma zasadnicze znaczenie, możemy jednym wpisem zablokować wszystkie pakiety. Jeżeli pakiet nie spełni żadnego z zadeklarowanych warunków, to zostanie odrzucony - reguła ta nazwana jest implicit deny any (niejawne odrzucenie wszystkiego). Przy budowie listy dostępu trzeba mieć na uwadze dwa elementy: kolejność kryteriów oraz warunek ostateczny odrzucający wszystkie pakiety. Zarządzanie ruchem dotyczy zazwyczaj konkretnego interfejsu routera (przyłączonego do sieci lokalnej lub rozległej) i kierunku ruchu - ważne jest więc, z którym interfejsem routera skojarzymy listę dostępu oraz czy filtrowanie ma działać na wejściu czy na wyjściu interfejsu. Jeżeli lista dostępu została zadeklarowana na wejściu, to konfiguracja interfejsu "wejściowego" sprawdzana jest przed przystąpieniem do jakiegokolwiek przetwarzania. Natomiast jeżeli lista dostępu została przypisana do wyjścia przez dany interfejs, to pakiet zostanie przetworzony zgodnie z następującą kolejnością : router sprawdzi w tablicy routingu, przez który interfejs należy dany pakiet skierować - jeżeli do interfejsu nie została przypisana lista dostępu, pakiet umieszczany jest w buforze tego interfejsu; jeżeli zaś taka lista istnieje, to pakiet jest poddawany sprawdzeniu.




**Rys. 2**

Gdy pakiet nie może być przesłany do miejsca docelowegp, router wysyła do nadawcy komunikat ICMP Destination net unreachable.

Router uzywasię bardzo specyficznych oznaczeń hostów i sieci za pomocą tzw. maski wzorca. Ważnym detalem przy budowie list dostępu jest sposób adresowania używany przy opisywaniu kryteriów. Jest to zapis maski, w którym bit ustawiony na 0 porównuje odpowiadający mu bit w analizowanym pakiecie z adresem umieszczonym w warunku, natomiast przy bicie ustawionym na 1 dany bit w pakiecie nie jest sprawdzany ze wzorcem. [2]

Na przykład pakiet kierowany do konkretnego hosta o adresie IP 111.111.1.100. Wtedy maska wzorca w liście dostępu miałaby wartość 0.0.0.0, a opis hosta w warunku listy dostępu miałby postać 111.111.1.100 0.0.0.0. Zaś dowolny adres w podsieci 111.111.1.0 możemy opisać jako 111.111.1.0 0.0.0.255, co oznacza, że tylko bity ostatniego bajtu adresu w pakietach IP nie będą sprawdzane ze wzorcem. Każdego adresata w sieci IP można wytypować, posługując się zapisem 0.0.0.0 255.255.255.255, gdzie wynika, że nie interesuje nas żaden z 32 bitów adresu IP pakietów analizowanych przez router. Kiedy stosujemy podsieci, wyliczamy, ile bitów można pomijać przy porównywaniu ze wzorcem, a ile dokładnie musi być. Wyobraźmy sobie, iż chcemy objąć naszym warunkiem każdego adresata w podsieci 191.161.1.64/27 - podsieć ta jest utworzona na 3 bitach ostatniego bajtu i to one wyróżniają hosty z danej podsieci. Maska wzorca musi więc powodować sprawdzenie pierwszych trzech bitów ostatniego bajtu w nadesłanych pakietach IP, a pozostałe 5 bitów może być jakiekolwiek:

zapis podsieci 191.161.1.64/27
ostatni oktet - zgodnie z maską podsieci 0 1 0 0 0 0 0 0
maska wzorca - ostatni oktet 0 0 0 1 1 1 1 1 = 31
zapis adresu podsieci w liście dostępu 191.161.1.64 0.0.0.31

Coraz to dla ułatwienia zapisu założeń list dostępu używane są tzw. schowane maski wzorca, które pozwalają na ukazanie dowolnego adresu lub konkretnego adresata (**host**). Na przykład host o adresie 151.158.1.100 można wskazać zapisem **151.158.1.100 0.0.0.0** lub też: host **151.158.1.100.**

Listy dostępu identyfikowane są poprzez niepowtarzalny numer, który znamionuje je w zupełnej konfiguracji routera. Wskazuje on listę dostępu, jej typ oraz protokół, którego ona obejmuje. Numery te są z góry ustalone, i posługiwanie się nimi zależy jaki ruch chcemy filtrować. Obszar list dostępu jest inny w zależności od wersji systemu operacyjnego routera. [1]

Np w modelu 2600 jest taki, jak w tabelce.

**Tabela 1.**

| Typ list dostępu | Zakres numerów |
|---|---|
| IP Standard | 1 - 99 |
| IP Rozszerzona | 100 - 199 |
| Określana na podstawie kodu protokołu | 200 - 299 |
| DECnet | 300 - 399 |
| XNS Standard | 400 - 499 |
| XNS Rozszerzona | 500 - 599 |
| AppleTalk | 600 - 699 |
| MAC Address | 700 - 799 |
| IPX Standard | 800 - 899 |
| IPX Rozszerzona | 900 - 999 |
| IPX SAP | 1000 - 1099 |
| MAC Address Rozszerzona | 1100 - 1199 |

## 1.5 Standardowe listy dostępu i ich konfiguracja

Standardowe Listy jest prosto skonfigurować, nie mają jednak wielu sposobności zaawansowanej analizy pakietów. konfigurując warunki jedynym warunkiem wyboru pakietu jest adres nadawcy źródłowy.

Standardową listę dostępu sporządzimy komendą trybu konfiguracyjego:

```
C2800(config)#access-list numer_listy_dostępu {permit|deny}
                          adres_źródłowy_pakietu maska_wzorca log
```

Jakikolwiek następny warunek, który chcemy dopisać do listy dostępu musi obejmować ten sam numer listy, ważna jest kolejność warunków podawanych komendą **access-list**, gdyż w takiej hierarchii będą one analizowane. W standardowej liście dostępu jedynie numer listy pozwala wskazać routerowi, które pakiety nas interesują. Lista ta nie odróżnia ruchu związanego z protokołem TCP czy UDP, nie wspominając już o typach aplikacji. Opcja **log** sprawi wysłanie komunikatu dla każdego pakietu dopasowanego do wzorca, używanie z niej nie jest obowiązkowe podczas normalnej pracy routera ze względu na duże obciążenie procesora. Numer listy dostępu to wartość z przedziału od 1 do 99 (dla IP), natomiast adres źródłowy pakietu w połączeniu z maską wzorca jest zapisem adresu hosta lub sieci nadawcy. Listę dostępu przypisujemy do wybranego interfejsu rozkazem trybu konfiguracji interfejsu:

```
C2800(config-if)#ip access-group numer_listy_dostępu {in|out}
```

Rozkaz ten wiąże się z filtrowaniem pakietów na poziomie danego interfejsu i jest jednym z wariantów wykorzystania list dostępu. Pomijając podanie numeru listy, którą chcemy skojarzyć z danym interfejsem, definiujemy tryb, w jakim lista ma być analizowana: na wejściu  czy na wyjściu pakietu z interfejsu .

Sprawdźmy konfigurację listy standardowej analizując przykład routera z dostępem do dwóch sieci lokalnych i sieci rozległej. Zabroniamy komputerowi o adresie 111.117.1.100 korzystania z sieci rozległej (np. z Internetu), lecz nie chcemy blokować mu dostępu do serwera znajdującego się w innej lokalnej sieci.

Lista standardowa obejmuje jedynie adres nadawcy pakietu, więc nie możemy przypisać takiej listy do konfiguracji interfejsu E0, ponieważ to zablokowałoby nie tylko dostęp do zasobów sieci rozległej, lecz również do sieci lokalnej 111.118.1.0 - na tym poziomie router wie, od kogo jest pakiet, ale nie wie, do kogo jest kierowany. W tym przypadku naszą listę dostępu najlepiej jest przypisać do wyjścia (out) interfejsu S0, czyli do granicy sieci lokalnych. W trybie konfiguracji wydajemy komende:

```
C2800(config)#access-list 1 deny 111.117.1.100 0.0.0.0
```

lub w postaci skróconej:

```
C2800(config)#access-list 1 deny host 111.117.1.100
```

Zakończając tak listę spowodowałoby to, że ani jeden komputer z obu sieci lokalnych nie mógłby korzystać z Internetu, gdyż wszelka lista zawiera *niejawny warunek odrzucający wszystko* (**deny any**). Konieczne są dodatkowe założenia:

```
C2800(config)#access-list 1 permit 111.117.1.0 0.0.0.255
C2800(config)#access-list 1 permit 111.118.1.0 0.0.0.255
```

lub skótowo:

```
C2800(config)#access-list 1 permit any
```

Pierwszy warunek określa adres hosta (111.117.1.100) i zabrania mu dostępu; ponieważ wszystkie pozostałe hosty nie spełniają tego warunku, będą podlegać regule zezwalającej na wejście. Przygotowaną listę możemy przypisać do interfejsu S0:

```
C2800(config-if)ip access-group 1 out
```

W konfiguracji routera C2800 zobaczymy:

```
!
Interface Serial 0
ip address 212.1.1.1 255.255.255.0
ip access-group 1 out
!
access-list 1 deny host 111.117.1.100
access-list 1 permit 111.117.1.0 0.0.0.255
access-list 1 permit 111.118.1.0 0.0.0.255
```

Modyfikując powyższy przykład : chcemy dać dostęp do Internetu tylko komputerom z sieci 111.118.1.0, a komputerom z sieci 111.117.1.0 umożliwiamy usługe (np. FTP) serwera o adresie 111.118.1.254.

```
c2800(config)#access-list 1
  permit 111.118.1.0 0.0.0.255
c2800(config)#access-list 2
  permit host 111.118.1.254
c2800(config)#interface S0
c2800(config-if)#ip access-group 1 out
c2800(config-if)#interface E0
c2800(config-if)#ip access-group 2 out
```

W sieci 111.117.1.0 - nie możemy w liście standardowej podać adresu docelowego (111.118.1.254), musimy prześledzić drogę pakietów IP. Lista dostępu 1 pozwala na dostęp tylko nadawcom z sieci 111.118.1.0. Gdy dowolny host z sieci 111.117.1.0 wyśle pakiet na adres 111.118.1.254, to router przy takiej konfiguracji nie ma podstaw, aby ten pakiet odrzucić. Co więcej, gdy pakiet z sieci 111.117.1.0 przesyłany jest na dowolny adres w sieci 111.118.1.0, router nie ma prawa zareagować. Ale gdy po otrzymaniu takiego pakietu odbiorca próbuje odesłać go do pierwotnego nadawcy (do sieci 111.117.1.0), router wstrzyma transmisję wszystkich pakietów zwrotnych do momentu, gdy nadawcą (odpowiadającym) będzie serwer o adresie 111.118.1.254, ponieważ reguła skojarzona z interfejsem E0 pozwala na wysłanie tylko takiego pakietu przez ten interfejs. Zwróćmy uwagę na to, że filtrowanie to zostało zrealizowane poprzez utworzenie dwóch niezależnych, standardowych list dostępu.

Konfigurując listy dostępu trzeba pamiętać, że wszelki nowy warunek dopisywany jest na końcu listy. Jednocześnie w trakcie próby usunięcia określonego warunku (np. poleceniem **no ip access-list 1 permit 111.118.1.254**) usunięta zostanie cała lista, komenda **ip access-group** będzie w konfiguracji interfejsu. Co prawda brak w konfiguracji listy o podanym numerze nie skutkuje podjęciem jakiegokolwiek działania w wyniku polecenia **ip access-group**, lecz pojawienie się listy o tym numerze spowoduje natychmiastowe filtrowanie pakietów zgodnie z nowymi warunkami.

Praktycznym rozwiązaniem jest zapis konfiguracji na serwerze TFTP i edycja pliku w celu uzyskania założonego efektu. Trzeba pamiętać o tym, iż zmiana kolejności w warunkach listy dostępu w pliku konfiguracyjnym nie będzie uwzględniona przy wczytaniu jej do routera. Gdy chcemy zachować listę dostępu z nową kolejnością wa-

runków,trzeba dopisać na początku listy nowy wiersz **no access-list**, podając numer naszej listy, wówczas router podczas interpretacji skryptu usunie istniejącą listę i utworzy ją w podanej kolejności warunków na nowo.[2]

## 1.6 Rozszerzone listy dostępu

Potencjalności list standardowych są ograniczone i wprowadzenie powoduje nadmiarowość ruchu w sieci. Listy rozszerzone dają zwiększone możliwości wyboru ruchu, który chcemy filtrować. Dzięki stosowaniu maski wzorca wskazujemy konkretny adres nadawcy i odbiorcy, całą sieć, podsieć nadawców wszystkich potencjalnych nadawców i odbiorców. W stosunku do list standardowych jest sposobność określenia protokołu, którego dotyczyć ma warunek. W listach standardowych numer listy informował router, że chodzi nam o cały ruch TCP/IP, a w listach rozszerzonych dla stosu TCP/IP (numery od 100 do 199) istnieje możliwość wskazania zarówno protokołu IP jako podstawy do kontroli ruchu, jak również protokołu TCP, UDP, ICMP, IGMP, IGRP, OSPF i wielu innych, w zależności od systemu operacyjnego routera. Konfigurując listy dla protokołów TCP bądź UDP możemy też wybrać numery portów - kierowane do nich pakiety zostaną poddane filtrowaniu. Konstrukcja warunków dla listy rozszerzonej musi być wykonywana rozważniej i precyzyjniej. [1]

## 1.7 Konfigurowanie rozszerzonych list dostępu

Rozszerzoną Listę tworzymy komendą:

```
C2800(config)#access-list numer_listy {permit|deny}
  protokół adres_źródłowy [operator port]
  adres_docelowy [operator port] [established] [log]
```

Opcję established stosuje sie dla protokołu TCP i odnosi się do segmentów, w których został ustawiony bit synchronizacji (SYN) podczas zestawiania sesji TCP. Adres źródłowy i adres docelowy konstruowany jest tak, jak w listach standardowych (adres hosta lub sieci i maska wzorca), potrafimy korzystać ze słów kluczowych **host** i **any**. Komenda access-list zależy od protokołu, którego dotyczy dany warunek. W protokołach warstwy transportowej (TCP czy UDP) możemy posłużyć się operatorem pozwalającym na przedstawienie portów: Lt - mniejsze od, Gt - większe od, Eq - równe, Neq - różne od.

Przykładowy układ złożonym z routera C2800, dwóch segmentów sieci lokalnej i sieci rozległej. Celem jest zablokowanie dostępu do usług FTP i telnet na serwerze 111.118.1.254 wszystkim klientom. Nie chcemy jednak ograniczać ruchu pomiędzy sieciami lokalnymi a siecią rozległą. Zarówno telnet (port 23), jak i FTP (port 20,21) korzystają z protokołu TCP, więc to jego będzie dotyczyć lista dostępu poniżej:

```
C2800(config)#access-list 101 deny
  tcp any host 111.118.1.254 eq 23
C2800(config)#access-list 101 deny
  tcp any host 111.118.1.254 eq 21
```

Operatora **eq** (równy), deklaruje, że chcemy odrzucić wszystkie segmenty TCP od dowolnego nadawcy (any) kierowane na adres serwera (host 111.118.1.254), związane z portem TCP numer 23 i 21. Praca FTP używa dwóch portów TCP: 20 - do przesyłania danych i 21 - do zestawienia sesji FTP, wystarczy więc zablokować port 21. Tak zbudowana lista zablokuje dostęp nie tylko do usług FTP i telnet, ale również do wszystkich hostów i serwera w sieci 111.118.1.0 (listy rozszerzone zawierają niejawny warunek **deny any any**), trzeba dopisać warunek zezwalający na komunikację z siecią 111.118.1.0:

```
C2800(config)#access-list 101 permit ip any any
```

Jko protokół został IP, zezwalając na obsługę pakietów między dowolnymi hostami źródłowymi i docelowymi. Protokół IP pozwala na objęcie warunkiem wszystkich protokołów, które stosują pakiety IP, a więc całego ruchu w sieci TCP/IP. To często stosowane rozwiązanie, którym należy posługiwać się bardzo rozważnie. Po utworzeniu listy dostępu, w konfiguracji interfejsu E0/1 wydajemy polecenie włączające proces filtrowania pakietów na wyjściu zgodnie z kryteriami listy rozszerzonej 101:

```
C2800(config-if)#ip access-group 101 out
```

Zablokujmy teraz dostęp z sieci rozległej do zasobów sieci lokalnych z wyjątkiem usług DNS, WWW i FTP zlokalizowanych na serwerze 111.118.1.254. Dodatkowym wymogiem jest to, aby klienci z sieci lokalnej 111.117.1.0 mogli korzystać ze wszystkich zasobów sieci 111.116.1.0 oprócz serwera 111.116.1.254, który jest przeznaczony dla użytkowników sieci rozległej:

```
C2800(config)#access-list 111 permit
  tcp any host 111.116.1.254 eq www
C2800(config)#access-list 111 permit
  tcp any host 111.116.1.254 eq ftp
C2800(config)#access-list 111 permit
  tcp any host 111.116.1.254 eq ftp-data
C2800(config)#access-list 111 permit
  tcp any host 111.116.1.254 eq domain
C2800(config)#access-list 111 permit udp any host 111.116.1.254 eq domain
C2800(config)#access-list 112 deny ip 111.117.1.0 0.0.0.255 host 111.116.1.254
C2800(config)#access-list 112 permit ip any any
C2800(config)#interface S0/0
C2800(config-if)#ip access-group 111 in
C2800(config)interface E0/0
C2800(config-if)#ip access-group 112 in
```

Struktura listy 111, zezwalająca na dostęp tylko do wybranych usług - ich nazwy podane są po operatorze **eq** zamiast numerów portów (listę z numerami dobrze znanych portów można wyświetlić, wywołując system pomocy). W przypadku usługi DNS (**domain**) podaliśmy dwa numery portów: 53 dla TCP i 53 dla UDP. Ukryty warunek **deny any any** powinien skutecznie zablokować pozostałą komunikację. jeśli listą 111 posłużymy się podczas filtrowania pakietów wejściowych dla interfejsu S0/0, to można zabezpieczyć dostęp nie tylko do sieci lokalnej, w której znajduje się serwer, ale też do sieci 111.117.1.0, co było naszym celem. Lista 112 została tak skonstruowana, że można ją wykorzystać w konfiguracji interfejsu zarówno E0/0, jak i E0/1. Praktyczniej jest jednak podać ją na wejściu interfejsu E0/0, wówczas pakiet będzie jedynie sprawdzany z listą dostępu, bez angażowania routera w proces przeglądania tablicy routingu.

Listy dostępu wyswietlamy poleceniem **show access-lists** (wszystkie protokoły) lub **show ip access-lists** (tylko listy związane z protokołem TCP/IP):

```
c2800#sh ip access-lists

Extended IP access list 111

permit tcp any host 111.116.1.254 eq www (127 matches)

permit tcp any host 111.116.1.254 eq ftp (9 matches)

permit tcp any host 111.116.1.254 eq ftp-data (9 matches)

permit tcp any host 111.116.1.254 eq domain (33 matches)

permit udp any host 111.116.1.254 eq domain

Extended IP access list 112

  deny ip 111.117.1.0 0.0.0.255 host 111.116.1.254

  permit ip any any (831 matches)
```

Wszelki przypadek zgodności przetworzonego pakietu z warunkiem opisanym w liście dostępu jest rejestrowany - na przykład 127 pakietów zostało skierowanych do usługi WWW na serwerze 111.116.1.254 od momentu założenia filtru. Po wyłączeniu filtrowania liczniki te nie są zerowane, przed ponownym włączeniem filtrowania ruchu można wyzerować je wszystkie poleceniem **clear access-list counters** lub wpisać po słowie counters numer wybranej listy. Polecenie **show ip interfaces** pozwala sprawdzić, czy filtrowanie jest włączone.[1]

Wykorzystywanie właściwości protokołów i usług sieciowych w celu dodatkowego obciążenia systemu operacyjnego i w rezultacie spowolnienia, a nawet zawieszenia jego pracy Jednym z najczęściej spotykanych ataków na sieć jest - przykładem jest rozpoczynanie w krótkim okresie czasu wielu sesji TCP. Rozszerzone listy dostępu umożliwiają zabezpieczenie sieci przed tą "pozorną komunikacją". Prześledźmy to na prostym przykładzie. Chcemy, by router zezwolił jedynie na przesyłanie wiadomości do serwera pocztowego, zabezpieczając przy tym sieć lokalną przed nawiązywaniem jakichkolwiek sesji TCP z zewnątrz. Procedura nawiązywania sesji TCP (three-way handshake - potrójne podanie ręki) rozpoczyna się od ustawienia przez nadawcę pakietu bitu synchronizacji (SYN) rozpoczynającego sesję, następnie odbiorca potwierdza otrzymanie pakietu (bit ACK) oraz inicjuje zestawienie sesji (bit SYN), a w ostatniej fazie nadawca odsyła potwierdzenie, ustawiając bit ACK. Cała sekwencja polega więc w skrócie na ustawianiu na przemian bitów SYN- >ACK. Nakazując filtrowanie nagłówka TCP z ustawionym tylko bitem SYN możemy zabezpieczyć się przed próbą zestawienia sesji z zewnątrz i pozwolić jedynie na obsługę sesji już ustanowionych (opcja **established**):

```
C2800(config)#access-list 105 permit

  tcp any host 111.116.1.254 eq smtp

C2800(config)#access-list 105 permit

  tcp any any established

C2800(config)#access-list 105 deny tcp any any

C2800(config)#access-list 105 permit ip any any

C2800(config)#interface S0/0

C2800(config-if)#ip access-group 105 in
```

Konfiguracja taka nie blokuje sesji zestawianych z sieci wewnętrznej, bowiem komputery będą otrzymywać ustawiony bit SYN w nagłówku TCP, lecz łącznie z bitem ACK, czyli poświadczeniem. Operatory list rozszerzonych są na tyle elastyczne, iż pozwalają na filtrowanie nie tylko bitu SYN, ale również pozostałych znaczników (bitów flago-

wych) nagłówka TCP (URG, PSH czy FIN), zakresu portów (opcja **range** - np. **range 1 1024**) oraz pól nagłówków protokołu IP (np. TOS - Type of Service czy znaczników fragmentacji)

Pomijając protokoły IP, TCP i UDP bardzo często w praktyce stosowane jest filtrowanie innych protokołów, takich jak ICMP czy IGMP. Na przykład, lista rozszerzona dla protokołu ICMP ma składnię:

```
C2800(config)#access-list numer_listy {permit|deny} icmp adres_źródłowy
  adres_docelowy [typ_icmp [kod_icmp] | komunikat_icmp]
```

Chąc zablokować wysyłanie odpowiedzi do programu ping musimy wskazać odpowiedni typ komunikatu ICMP, wpisując jego numer (w tym wypadku 0) lub nazwę (echo-reply):

```
C2800(config)#access-list 133 deny icmp any any echo-reply
```

Jedną komendą możemy zablokować grupę komunikatów, np. posługując się nazwą **unreachable** zatrzymujemy wszystkie komunikaty związane z osiągalnością adresata - temu ograniczeniu nie będą podlegać pakiety generowane przez router, na którym została utworzona lista dostępu.

Pewnym ułatwieniem jest posługiwanie się nazwami zamiast uciążliwego numerowania list jest, należy jednak pamiętać, że nie każdy system operacyjny na to pozwala (tylko od wersji 11.2). Po wpisaniu w trybie konfiguracji polecenia:

```
C2800(config)#ip access-list {standard | extended} nazwa_listy_dostępu
```

tworzona jest nowa nazwana lista dostępu, dla której kryteria definiowane są w kontekście routera:

**c2800(config-ext-nacl)**.

Utworzenie listy do_sieci1, blokującej dostęp do usługi telnet na dowolnym serwerze w naszej sieci, można zawrzeć w kilku poleceniach:

```
C2800(config)#ip access-list extended do_sieci1
C2800(config-ext-nacl)#deny tcp any any eq 23
C2800(config-ext-nacl)#permit ip any any
c2800(config-ext-nacl)#interface S0/0
C2800(config-if)#ip access-group do_sieci1 in
```

Taki sposób opisu list dostępu jest z pewnością czytelniejszy i łatwiejszy do znalezienia, kiedy trzeba powrócić do konfiguracji po długim okresie czasu.[2]

## 1.8 Zasady tworzenia list dostępu

- W przypadku użytkowania ze standardowych list dostępu należy rozmieścić je jak najbliżej miejsca przeznaczenia pakietów.

- Nowe warunki dopisywane są do już istniejących, na końcu listy dostępu.

- Warunki bardziej szczegółowe należy umieszczać w miarę możliwości na początku listy.

- Filtrowaniu podlega jedynie ruch przechodzący przez router, a nie ten, którego inicjatorem jest router.

- Krańcowym warunkiem jest niejawne odrzucenie wszystkich pakietów i taka operacja będzie wykonywana, jeżeli pakiet nie będzie pasował do żadnego warunku.

- W interfejsu routera można przypisać tylko jedną listę związaną z danym protokołem.

- Warunki można selektywnie usuwać tylko z list nazwanych (obsługiwanych od systemu 11.2) lub wprowadzając modyfikacje poprzez skrypt konfiguracyjny.

- Komenda ip access-group bez istniejącej w trybie konfiguracji listy dostępu nie filtruje żadnego ruchu.

- Podczas korzystania z rozszerzonych list dostępu należy umieszczać je jak najbliżej miejsca nadawcy pakietów.

## 1.9 Listy dostępu dla protokołu IPX

Protokół IPX pozwala na podłączenie kilku logicznych sieci do jednego interfejsu fizycznego, pod warunkiem że dla każdej z sieci określimy inny typ kapsułkowania protokołu warstwy drugiej modelu OSI. Bardzo ważnym elementem w konfiguracji sieci IPX jest, aby wszystkie urządzenia działające w sieci o tym samym numerze korzystały z tego samego typu kapsułkowania ramek .

IPX to zapisana szesnastkowo 80-bitowa wartość: 32-bitowy numer sieci i 48-bitowy numer węzła. IPX jest bezpołączeniowym protokołem warstwy sieci, z charakterystycznym sposobem adresowania urządzeń. Adres Numer sieci, definiowany dla routerów, pozwala na określenie urządzeń, które mogą się bezpośrednio między sobą komunikować. Numerem węzła jest adres fizyczny MAC karty sieciowej urządzenia, a w przypadku interfejsów Serial może być nadany przez administratora routera. Przykładowo, router o adresie MAC 0010.0c56.de33 z interfejsem lokalnym pracującym w sieci IPX o numerze **1a2c** ma adres IPX w postaci **1a2c.0010.0c56.de33**.

Serwery plików w sieci NetWare wirtualny identyfikator nazywany wewnętrznym numerem sieci, wykorzystywany podczas ogłaszania usług NetWare w sieci lokalnej i rejestrowany przez routery w tablicy routingu RIT (Route Information Table). Drugą formą zbierania informacji o sieci IPX przez router jest tworzenie tablicy usług (Service Information Table) ogłaszanych w segmencie sieci lokalnej przez serwery NetWare.

Serwery NetWare posługują się protokołem SAP do ogłaszania typu i adresu usługi. Każda usługa rozgłaszana protokołem SAP ma swój jednoznaczny, szesnastkowy identyfikator, na przykład serwer plików - 4, serwer wydruku - 7, a usługa katalogowa - 278. Dzięki temu zarówno klient, jak i serwer potrafią jednoznacznie określić typ usługi, jaki ich interesuje. Na podstawie rozsyłanych co 60 sekund rozgłoszeń SAP router tworzy tablicę usług SAP dostępnych w jego lokalnym segmencie sieci i przesyła tę informację do innych urządzeń. Router może również

uczestniczyć w procesie poszukiwania serwera dla klientów w sieci NetWare. Stacja klienta, rozpoczynając pracę w sieci, rozgłasza zapytanie GNS (Get Nearest Server) w celu odnalezienia serwera i zalogowania się do sieci NetWare. Jeżeli router wie, że w danym segmencie sieci pracuje serwer (router odbiera ogłoszenia SAP, co można sprawdzić poleceniem **show ipx servers**), nie będzie na to zapytanie odpowiadał. W przeciwnym wypadku router potrafi odpowiedzieć klientowi na zapytanie GNS na podstawie tablicy SAP.[4]

## 1.10 Filtrowanie ruchu w sieciach bazujących na protokole IPX

Dla protokołu IPX można wskazać nie tylko host lub sieć źródłową, dla której jest wykonywane filtrowanie, lecz również sieć lub urządzenie, do którego kierowane są pakiety:

```
C2800(config)#access-list numer_listy_dostępu {permit | deny}
  numer_sieci_źródłowej [. Numer_węzła] [maska_wzorca_numeru_węzła]
  [numer_sieci_docelowej] [. Numer_węzła] [maska_wzorca_numeru_węzła]
```

Zgodnie z przyjętą konwencją numery list standardowych dla protokołu IPX są zawarte w przedziale 800 - 899. Podobnie jak dla protokołu IP mamy możliwość wskazania zakresu adresów poprzez maskę wzorca. Notacja adresów IPX jest zapisem w postaci szesnastkowej, czyli zapis F w masce oznacza wartość 1 ustawioną na czterech kolejnych bitach.

Naszym celem jest zablokowanie dostępu do sieci 1a dla komputerów pracujących w sieci 1b:

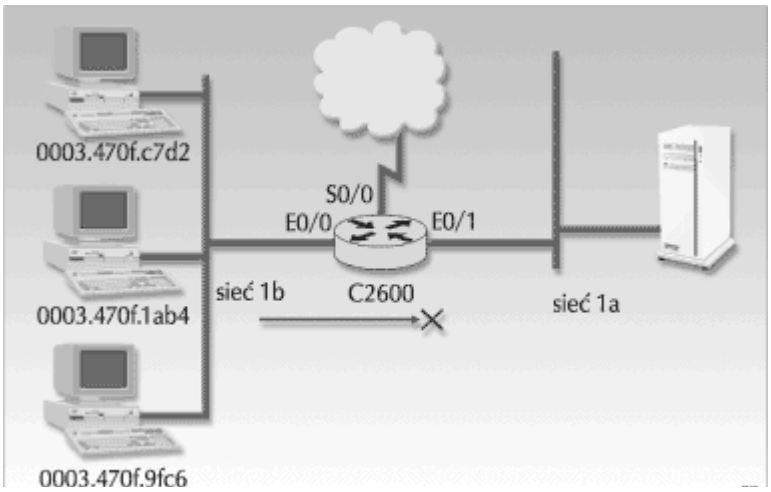
```
C2800(config)access-list 801 deny 1b 1a
C2800(config)access-list 801 permit -1 -1
C2800(config)interface ethernet 0/0
C2800(config-if)ipx access-group 801 in
```

W konfiguracji routera warunek any zapisany zostanie jako **access-list 801 permit FFFFFFFF FFFFFFFF**. Pierwszy warunek listy moglibyśmy zapisać precyzyjniej, określając jako nadawcę grupę komputerów w sieci 1b:

```
c2800(config)access-list 810 deny 1b.0003.470f.0000 0000.0000.ffff
```

Utworzona wcześniej lista dostępu została przypisana do interfejsu E0/0 za pomocą polecenia **ipx access-group**, powodując filtrowanie pakietów już na wejściu danego interfejsu. Lista standardowa jest rozwiązaniem mało elastycznym, ponieważ blokuje cały ruch IPX związany z adresem źródłowym i docelowym, bez możliwości wskazania konkretnych usług w sieci NetWare. Rozszerzone listy dostępu dla protokołu IPX konfigurujemy komendą:

```
c2800(config)#access-list numer_listy_dostępu {permit | deny}
  protokół numer_sieci_źródłowej [. Adres_źródłowy] [maska_wzorca] [numer_gniazda]
  [numer_sieci_docelowej] [. Adres_źródłowy] [maska_wzorca] [numer_gniazda]
```




**Rys. 3**

Przy wykonywaniu listy rozszerzonej trzeba pamiętać, iż numer listy musi być z przedziału 900 - 999. Przy przedstawieniu protokołu możemy się posłużyć identyfikatorem jego typu, jego nazwą (ncp, rip, netbios, sap, spx) lub słowem kluczowym **any** (oznaczającym wszystkie protokoły). Numer gniazda (socket) to identyfikator usługi będący odpowiednikiem numeru portu TCP lub UDP z tą jednak zasadniczą różnicą, że kilka usług może korzystać z tego samego numeru gniazda. Numery gniazd przypisywane są dynamicznie: stacjom klienckim w zakresie 4000-7FFF, a aplikacjom pracującym na serwerach - 8000-FFFF. W tych okolicznościach należy bardzo ostrożnie korzystać z numerów gniazd podczas filtrowania ruchu w sieci IPX, a w wielu przypadkach, gdy nie zależy nam na tak dokładnym badaniu ruchu klient-serwer, jest to wręcz niepotrzebne. Największą zaletą list rozszerzonych jest możliwość zastosowania maski wzorca do wskazania numerów sieci, na przykład listę dostępu uniemożliwiającą korzystanie z zasobów dwóch konkretnych serwerów o wewnętrznych numerach sieci 1000 i 1001 można utworzyć poleceniem:

```
C2800(config)access-list 901 deny any 00001000 0000000F
```

Zapis maski wzorca na siedmiu pierwszych pozycjach adresu sieci wymaga dokładnego odwzorowania z podanym adresem, czyli od lewej 0000100, natomiast na ostatniej pozycji adresu (zapisanej szesnastkowo) zezwala na dowolną wartość. Gdyby jednak okazało się, że podany przez nas warunek jest zbyt ogólny, możemy wskazać dwie konkretne sieci 1000 i 1001, zapisując wcześniejszy warunek w postaci:

```
C2800(config)access-list 901 deny any 00001000 00000001
```

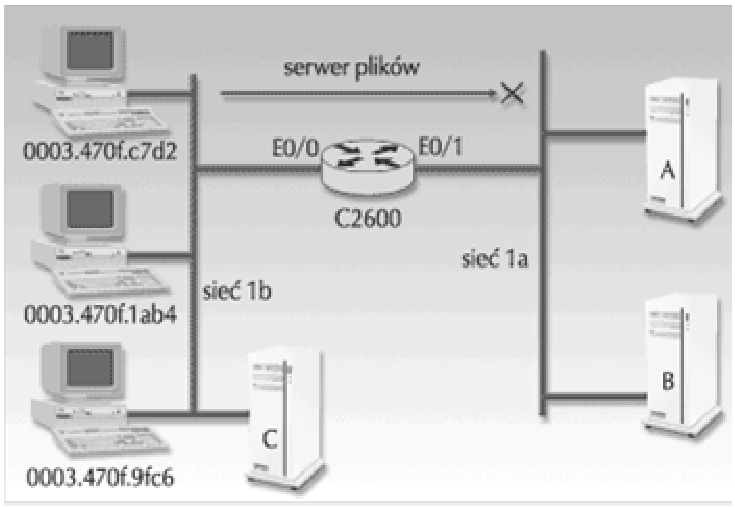
Prostsza metoda filtrowania dostępu do usług w sieci NetWare:

Zadania rozgłaszane są protokołem SAP, a routery Cisco aktywnie w tym uczestniczą: przesyłają informacje w postaci tablicy usług (SIT), lecz nie przekazują samych rozgłoszeń odbieranych na swoich interfejsach. Kolejną kategorią list dostępu są więc listy związane z filtrowaniem ogłoszeń usług. Listy dostępu o numerach od 1000 do 1099 przeznaczone są dla protokołu IPX SAP i na ich podstawie możemy filtrować publikowane w sieci usługi:

```
C2800(config)#access-list numer_listy_dostępu {permit | deny}
  numer_sieci [. Numer_węzła] [maska_wzorca_dla_sieci
  maska_wzorca_dla_węzła] [typ_usługi [nazwa_serwera]]
```

Proces filtrowania konfiguruje się za pomocą dwóch poleceń:

```
C2800(config-if)#ipx input-sap-filter numer_listy_dostępu
C2800(config-if)#ipx output-sap-filter numer_listy_dostępu
```




**Rys.4**

Gdy w konfiguracji interfejsu pojawi się komenda **ipx input-sap-filter**, to tablica usług (SIT) przechowywana na routerze będzie zmodyfikowana zgodnie z podaną listą dostępu, a zmiany dotyczyć będą tylko usług ogłoszonych przez konfigurowany interfejs. Polecenie **ipx output-sap-filter router** będzie przesyłało przez konfigurowany interfejs taką tablicę usług, która jest zgodna z podaną listą dostępu.

Zablokowanie możliwości korzystania w sieci 1b z usług drukowania serwera A:

```
C2800(config)access-list 1001
  deny 1a.0010.72c4.19f2 7
C2800(config)access-list 1001 permit -1
C2800(config)interface E0/1
C2800(config-if)ipx input-sap-filter 1001
```

W tablicy zadań SIT routera rozgłoszenie SAP wysyłane poprzez serwer A będzie opublikowane z pominięciem usługi drukowania (kod 7). Router jest pośrednikiem między dwoma sieciami IPX w ogłaszaniu usług, jeśliby więc nie wyda on informacji o usłudze drukowania, to nie dowie się o niej nikt w sieci 1b. Proces filtrowania usług SAP jest praktycznym mechanizmem umożliwiającym optymalizację ruchu rozgłoszeniowego usług sieci NetWare, a także redukowanie stopnia ich osiągalności. Wyjątkowo niezbędny jest w rozbudowanych sieciach wielosegmentowych.[3]

# LITERATURA

[1] PCkurier 19/2001

[2] Waldemar Pierścionek „Listy dostępu”

[3] Strona internetowa Cisco

[4] Inne strony internetowe oraz artykuły z czasopism