Listy dostępu systemu Cisco IOS

1. Obsługa routera Cisco

Konsola zarządzania routera firmy Cisco pracującego pod kontrolą systemu operacyjnego IOS może pracować w **trybie zwykłym** lub **uprzywilejowanym**, sygnalizowanymi różnymi znakami zachęty konsoli routera.

Tryb zwykły: **`ROUTER>`**

Tryb uprzywilejowany: **`ROUTER#`**

Większość opisanych poniżej poleceń, wymaga trybu uprzywilejowanego (ilość poleceń w obu trybach można porównać, wykonując polecenie **`?`**, powodujące wypisanie wszystkich dostępnych poleceń).

Na przejście do trybu uprzywilejowanego pozwala polecenie: **`enable`**. Po jego wydaniu należy wprowadzić odpowiednie hasło.

Tryb uprzywilejowany udostępnia, między innymi, polecenie **`configure`**, które powoduje przejście do **trybu konfiguracji routera**. Na pytanie o sposób konfiguracji odpowiadamy **`terminal`**, lub, jeśli terminal jest wyświetlony jako opcja domyślna (w nawiasach kwadratowych), po prostu naciskając ENTER.

Tryb konfiguracji: **`ROUTER(config)#`**

Tryb ten udostępnia własny zestaw poleceń, dotyczących głównie zamiany ustawień routera.

W obrębie tego trybu można wchodzić do „pod-menu", na przykład w celu zmiany ustawień interfejsu (poleceniem np.: **`interface ethernet 1`** – konfiguracja interfejsu ethernetowego numer 1). Przejście do takiego pod-menu, sygnalizowane jest zmianą znaku zachęty.

Pod-menu konfiguracji interfejsu sieciowego: **`ROUTER(config-if)#`**

Wyjście z pod-menu, do głównego menu konfiguracji, możliwe jest z użyciem polecenia **`exit`**.

Wyjście z trybu konfiguracji do trybu uprzywilejowanego, następuje po wydaniu polecenia **`end`** lub naciśnięciu **Ctrl+Z**.

Wprowadzone w ten sposób zmiany konfiguracji dotyczą, tak zwanej, konfiguracji bieżącej (running-config) i zostaną utracone po restarcie routera.

2. Mechanizm Help systemu IOS

System IOS jest wyposażony w rozbudowany system pomocy. Poniżej przedstawiono podstawowe sposoby jego wykorzystania.

Polecenie:

? – powoduje wypisanie listy wszystkich dostępnych w danym trybie poleceń.

***ciąg_znaków*?** – powoduje wypisanie wszystkich dostępnych poleceń rozpoczynających się od podanego ciągu znaków

***ciag_znaków*<TAB>** – powoduje uzupełnienie ciągu znaków do pełnego polecenia, o ile można to zrobić jednoznacznie

***polecenie* ?** – powoduje podanie opisu następnego argumentu którego wymaga polecenie. Ta możliwość jest szczególnie przydatna, gdyż pozwala nam stworzyć odpowiednie polecenie krok po kroku, dopisując kolejne parametry i wywołując po każdym pomoc dotyczącą następnego. Jeśli router wyświetla na liście możliwości **<cr>** można nakazać wykonanie polecenia, naciskając ENTER.

3. Konfiguracja IP interfejsów sieciowych

Do wyświetlenia aktualnej konfiguracji IP interfejsów sieciowych używamy polecenia:

`show ip interface [`*`interfejs`*`]`

Interfejs podajemy jako parę wartości: <*typ*> <*numer*>. Na przykład: ethernet 2.

Aby zmienić konfigurację interfejsu wchodzimy do trybu konfiguracji, a następnie do pod-menu danego interfejsu sieciowego używając polecenia:
`interface <typ interfejsu> <nr interfejsu>`
Gdzie:

- typ interfejsu – np: ethernet, fddi, serial itp.
- nr interfejsu – numer kolejny interfejsu w obrębie danego typu. Patrz rozdział „Numeracja interfejsów" poniżej.

W pod-menu mamy możliwość użycia następujących poleceń:
`ip address <adres IP> <maska>` - aby zmienić adres IP oraz maskę IP,
`shutdown` – aby wyłączyć interfejs,
`no shutdown` – aby włączyć interfejs.
Po dokonaniu zmian wychodzimy z trybu konfiguracyjnego.

3.1. Numeracja interfejsów routerów Cisco 4000

Interfejsy routerów Cisco 4000 numerowane są od 0, oddzielnie dla każdego z typów, np.: ethernet, fddi, serial… W obrębie jednego typu, niższe numery mają moduły zlokalizowane z prawej strony routera.
W obrębie jednego modułu interfejsy opisane są numerami wskazującymi na kolejność ich liczenia.
Na przykład jeśli nasz router ma 2 moduły Ethernetowe i jeden moduł FDDI to:
Ethernet 0 – port 0 (dolny) z prawego modułu Ethernet,
Ethernet 1 – port 1 (górny) z prawego modułu Ethernet,
Ethernet 2 – port 0 (dolny) z lewego modułu Ethernet,
Ethernet 3 – port 1 (górny) z lewego modułu Ethernet,
Fddi 0 – jedyny port FDDI.

---

4. Listy ACL

Aby skorzystać z mechanizmów filtrowania ruchu, opartych na listach dostępu (Access Control Lists – ACLs), należy:

- stworzyć listę ACL, dodając do niej reguły,
- przypisać listę ACL do interfejsu.

Lista będzie wykorzystywana wyłącznie do filtrowania ruchu wymienianego z użyciem interfejsów (można ją przypisać do więcej niż jednego) do których jest przypisana.

Router będzie, dla każdego pakietu przechodzącego przez interfejs, przeszukiwał nakazaną listę ACL do czasu napotkania pierwszej pasującej reguły. Jeśli znajdzie pasującą regułę, wykona zawarte w niej polecenie (**permit** lub **deny**) i zakończy przeszukiwanie listy. Jeśli żadna pasująca reguła nie zostanie odnaleziona, wobec pakietu zostanie zastosowanie działanie **deny**.
Z powyższego względu przypisywanie więcej niż jednej listy dla tego samego interfejsu i kierunku transmisji (patrz 4.5) nie ma sensu – już pierwsza z nich kończy się domyślną regułą **deny**, kończącą przetwarzanie reguł.

Listy mogą być identyfikowane przez numery lub nazwy. Jednak nie wszystkie wersje systemu Cisco IOS obsługują listy nazwane. Listy identyfikowane numerami dostępne są we wszystkich wersjach systemu.
W przypadku list identyfikowanych numerami, przedział, do którego należy numer identyfikujący listę decyduje też o typie listy – np. listy proste posiadają numery od 1-99. W przypadku list nazwanych, typ listy podawany jest jawnie w poleceniu nakazującym jej utworzenie.

W przypadku list identyfikowanych numerami, lista do której chcemy dodać regułę nie musi być „tworzona" w jawny sposób – stanie się to automatycznie po dopisaniu do niej pierwszej reguły. Reguły dopisywane poleceniem **access-list** dodawane są na końcu danej listy ACL.
Nie ma możliwości edycji bądź usunięcia wybranej reguły z listy ACL. W takim przypadku należy usunąć całą listę poleceniem **no access-list** ***<nazwa lub nr listy>*** i stworzyć ją ponownie wprowadzając pożądane reguły.

Listy nazwane są natomiast tworzone specjalnym poleceniem, które powoduje wejście do pod-menu konfiguracyjnego, pozwalającego na dodawanie reguł do listy (patrz 4.3).

Stworzoną listę ACL należy przypisać do interfejsu opisanym poniżej poleceniem **access-group**. Z chwilą przypisania zacznie być ona uwzględniana przy przetwarzaniu pakietów. Przypisanie nieistniejącej listy ACL lub skasowanie poleceniem **no access-list** listy ACL przypisanej aktualnie do interfejsu, spowoduje przekazywanie przez ten interfejs dowolnego ruchu, do czasu ponownego stworzenia tej listy ACL.
Należy zwrócić uwagę, że listę można przypisać do interfejsu dla określonego kierunku przepływu ruchu (**in** i/lub **out** – patrz 4.5). W takim przypadku list będzie wykorzystywana do wyłącznie do filtracji ruchu przepływającego przez interfejs w określonym kierunku: **out** – ruchu wysyłanego przez router z użyciem danego interfejsu, **in** – ruchu otrzymywanego przez router za pośrednictwem danego interfejsu.

4.1. Wyświetlanie stworzonych list ACL i statystyk

`show access-list [<nazwa lub nr listy>]`
Jeśli podamy to polecenie bez parametru, to spowoduje to wyświetlenie zawartości wszystkich (podstawowych i rozszerzonych) list ACL danego routera.
Podanie parametru **<nazwa lub nr listy>** spowoduje wyświetlenie tylko listy ACL o podanej nazwie lub numerze.
W wyświetlanej przez polecenie tabeli, w nawiasach podawana jest liczba pakietów przetworzonych z użyciem danej reguły, co może okazać się przydatne dla celów diagnostyki i usuwania błędów.

4.2. Listy identyfikowane numerami

4.2.1. Listy podstawowe

`access-list <nr listy 1-99> {permit | deny} <źródłowy adres IP> [maska wzorca]`
gdzie:

- **<nr listy>** - numer listy ACL którą modyfikujemy. Listy podstawowe IP mają numery 1-99.
- **{permit | deny}** – decyzja czy dany pakiet przepuścić (permit) czy odrzucić (deny).
- **<źródłowy adres IP>** - adres IP który zostanie porównany z adresem źródłowym zawartym w nagłówku pakietu,
- **opcjonalnie: <maska wzorca>** – określa które bity adresu są porównywane. Jeśli dany bit jest ustawiony na 0 to jest on porównywany i musi być zgodny z ustawionym w parametrze *<adres IP>*. Jeśli bit maski wzorca ma wartość 1 to jego wartość nie jest brana pod uwagę przy porównywaniu. Np: 0.0.255.255 oznacz, że porównywane są 2 pierwsze bajty.
  Brak parametru oznacza przyjęcie maski 0.0.0.0 czyli adresu konkretnego hosta.

Przykłady:
`access-list 1 permit 192.168.1.1` – powoduje dopisanie do listy ACL nr 1 nowej reguły, nakazującej przepuszczenie ruchu z urządzenia o adresie 192.168.1.1
`access-list 1 permit 192.168.1.0 0.0.0.255` – powoduje dopisanie do listy ACL nr 1 nowej reguły, nakazującej przepuszczenie ruchu z urządzeń o adresach rozpoczynających się od 192.168.1, czyli od 192.168.1.0 do 192.168.1.254.
`access-list 1 deny 0.0.0.0 255.255.255.255` – powoduje dopisanie do listy ACL nr 1 nowej reguły, nakazującej zablokowanie ruchu ze urządzeń o dowolnym (każdym) adresie IP.

4.2.2. Listy rozszerzone

access-list *<nr listy 100-199>* {permit | deny} *<protokół>*
<definicja punktu źródłowego>
<definicja punktu docelowego>
[established] [log]
gdzie:

- **<nr listy>** - numer listy ACL którą modyfikujemy. Listy rozszerzone IP mają numery 100-199.
- **{permit | deny}** – decyzja czy dany pakiet przepuścić (permit) czy odrzucić (deny).
- **<protokół>** - protokół którego dotyczy dana reguła. Możliwe wartości: ***ip, tcp, udp, icmp,*** lub ***numer protokołu ip.***
- **<definicja punktu źródłowego>** i **<definicja punktu docelowego>** Definiowane w ten sam sposób mają następującą składnię:
  <adres IP> <maska wzorca> **[{eq|neq|gt|ln|range}** ***<port(y)>*****]**
  gdzie:
  - **<adres IP>** - jak w przypadku list prostych,
  - **<maska wzorca>** – jak w przypadku list prostych.
  - **{eq | neq| gt | ln | range} <port(y)>** - określa jakiego zbioru portów dotyczy reguła.
    - eq <port> – nr portu równy parametrowi <port>
    - neq <port> - nr portu różny od parametru <port>
    - gt <port> – nr portu większy od parametru <port>
    - ln <port> – nr portu mniejszy od parametru <port>
    - range <port1> <port2> – nr portu zawarty w przedziale od <port1> do <port2> (włącznie).
- **opcjonalnie: established** – opcja dostępna tylko dla protokołu TCP. Powoduje, że reguła dotyczy wszystkich pakietów już zestawionego połączenia TCP, niezależnie od portu docelowego i źródłowego (których nie podajemy). Np.: **access-list 101 permit tcp host 192.168.1.1 any established** – nakazuje przepuszczać ruch należący do już zestawionych połączeń TCP pomiędzy adresem 192.168.1.1 a wszystkimi innymi.
- **opcjonalnie: log** – powoduje rejestrowanie pasujących do reguły pakietów w logu systemowym.

Przykłady:
access-list 100 permit tcp 10.1.1.1 0.0.0.0 gr 1023 0.0.0.0 255.255.255.255 eq 436
Powoduje dopisanie do listy nr 100, reguły przepuszczającej ruch TCP z adresu 10.1.1.1, z portów źródłowych większych od 1023, skierowany do dowolnych docelowych adresów IP na port 436.

access-list 100 permit udp 10.15.1.1 eq 123 192.168.5.0 0.0.0.255 range 1024 2048
Powoduje dopisanie do listy nr 100, reguły przepuszczającej ruch UDP z adresu 10.15.1.1, z portu 123, do docelowych adresów IP rozpoczynających się sekwencją 192.168.5 na porty od 1024 do 2048.

access-list 100 deny icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 log
Powoduje dopisanie do listy nr 100, reguły blokującej ruch ICMP z dowolnego źródłowego adresu IP do dowolnego docelowego adresu IP i zapisywanie informacji o takich pakietach w logu systemowym.

4.3. Listy nazwane (nieobsługiwane w routerach serii Cisco 4000)

W celu utworzenia nazwanej listy ACL używamy polecenia trybu konfiguracyjnego:
ip access-list {standard | extended} <nazwa listy>
Jak widać, jawnie podejmujemy tu decyzję czy lista ma być podstawowa (standard) czy rozszerzona (extended), jako że nie posiada ona numeru, który w przypadku list numerowanych określa typ listy.

Po wykonaniu tego polecenia, router przechodzi do pod-menu pozwalającego na dodawanie reguł do listy, co sygnalizowane jest zmianą znaku zachęty na `(config-std-nacl)` lub `(config-ext-nacl)` w zależności czy tworzymy listę podstawową czy rozszerzoną.
Reguły dopisujemy posługując się składnią opisaną już w 4.2.1 (listy proste) i 4.2.2 (listy rozszerzone), pomijając jednakże polecenie „access-list" i numer listy. Dodawanie reguł kończymy poleceniem **`exit`**, co powoduje powrót do trybu konfiguracyjnego.

Przykład:

```
ROUTER(config)# ip access-list standard lista_testowa
ROUTER(config-std-nacl)# permit 192.168.1.0 0.0.0.255
ROUTER(config-std-nacl)# permit 10.10.0.1 0.0.0.0
ROUTER(config-std-nacl)# exit
```

Aby dodać reguł do już istniejącej listy ponownie używamy tego samego polecenia, co przy jej tworzeniu, podane następnie (w pod-menu) reguły zostaną dopisane na końcu istniejącej listy.

4.4. Usuwanie list ACL

Listy ACL usuwamy poleceniem:

no access-list *<nazwa lub nr listy>*

Usunięcie listy ACL nie powoduje likwidacji przypisania listy do interfejsu. Interfejs z przypisaną nieistniejącą listą przenosi dowolny ruch sieciowy.

4.5. Przypisanie listy do interfejsu

W trybie konfiguracyjnym wchodzimy do menu konfiguracyjnego określonego interfejsu z użyciem polecenia:

interface {ethernet | fastethernet| gigabitethernet | fddi } <nr interfejsu>

po czym przypisujemy daną listę do interfejsu poleceniem:

ip access-group *<nazwa lub nr listy>* [in | out]

gdzie:

- <nazwa lub nr listy> – numer lub nazwa, stworzonej wcześniej, listy ACL, którą chcemy przypisać do interfejsu.
- **[in | out] – opcjonalnie decydujemy, czy lista ACL ma być używana do filtracji wyłącznie ruchu odbieranego (in) czy też wyłącznie wysyłanego (out) przez dany interfejs.**
  Przypisanie listy do interfejsu nie precyzując kierunku (ani in ani out), powoduje użycie jej do filtracji ruchu dla OBU kierunków.

4.6. Likwidacja przypisania listy do interfejsu

Przypisanie listy ACL do interfejsu likwidujemy z menu konfiguracyjnego danego interfejsu, z użyciem polecenia trybu konfiguracyjnego:

no ip access-group <nazwa lub nr listy > [in | out]

Likwiduje to przypisanie określonej listy do interfejsu.

Polecenie **no ip access-group in** likwiduje wszystkie przypisania filtrujące ruch odbierany na interfejsie, a **no ip access-group out** – wszystkie przypisania filtrujące ruch wysyłany przez interfejs. Polecenie **no ip access-group** likwiduje wszystkie przypisania list ACL do interfejsu.

4.7. Logowanie użycia list ACL

Jak zaznaczono w 4.2.1 i 4.2.2, reguły list ACL mogą zwierać element **log**, nakazujący wygenerowanie komunikatu, gdy dana reguła zostanie użyta.

Komunikaty te mogą być kierowane do różnych lokalizacji, lecz domyślnie trafiają do logu systemowego oraz wypisywane są z użyciem konsoli szeregowej (lecz nie są widoczne w sesjach telnet).

Ponadto, ze względów wydajnościowych, komunikaty nie są wypisywane natychmiast, lecz podlegają grupowaniu – tzn. router gromadzi komunikaty oczekując aż zbierze ich określoną liczbę, a następnie wypisuje je, zastępując np. 10 komunikatów o użyciu danej reguły jednym, zawierającym informację, że reguły użyto dla 10 pakietów:

```
*May 1 23:02:27.187: %SEC-6-IPACCESSLOGP: list lista_testowa permitted
tcp 192.168.1.3(1026) -> 192.168.2.1(80), 10 packets
```

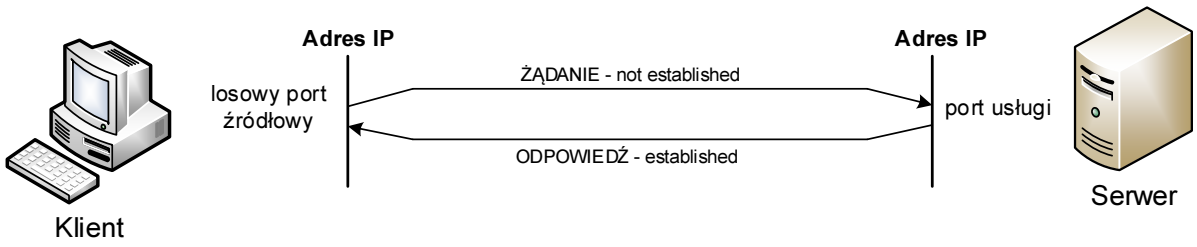
Aby zmienić liczbę komunikatów w grupie, należy użyć polecenia trybu konfiguracyjnego:
`ip access-list log-update threshold <liczba komunikatów>`
Jeśli chcielibyśmy, aby komunikaty o użyciu reguł ACL nie były grupowane, lecz wypisywane natychmiast, należy ustawić liczbę komunikatów na 1.

4.8. Inne uwagi dotyczące składni poleceń routera

Przy podawaniu adresów IP i masek w regułach list ACL, można posłużyć się następującymi skrótami:
`any = 0.0.0.0 255.255.255.255`
`host <adres IP> = <adres IP> 0.0.0.0`
Przykładowo pozwoli to na zapisanie, wyżej przytoczonych przykładów reguł z rozszerzonej listy ACL w postaci:
Przykład 1:
access-list 100 permit tcp 10.1.1.1 0.0.0.0 gr 1023 0.0.0.0 255.255.255.255 eq 436
access-list 100 permit tcp host 10.1.1.1 gr 1023 any eq 436
Przykład 2:
access-list 100 deny 47 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 log
access-list 100 deny 47 any any log

4.9. Ogólny uwagi na temat komunikacji IP w modelu klient-serwer

Należy pamiętać, iż aby klienta danej usługi oferowanej przez serwer mógł z niej skorzystać, w ogromnej większości przypadków konieczna jest łączność 2 kierunkowa – klient wysyła żądanie do serwera, a ten odpowiada wysyłając żądaną treść.
Klient wysyła pakiet(y) z żądaniem ze swojego adresu IP oraz losowo wybranego portu źródłowego (domyślnie >= 1024) na adres IP serwera i port, na którym serwer udostępnia daną usługę.
Serwer odpowiada z adresu IP i portu, na który otrzymał żądanie, wysyłając odpowiedź na adres IP i port, które były źródłowymi w otrzymanym żądaniu – czyli na adres IP klienta i wybrany wcześniej przez klienta (przy wysyłaniu żądania) port źródłowy.



O ile w przypadku żądania nie ma problemu z jednoznacznym ustaleniem reguły, która pozwoli na przepuszczenie go przez router (gdyż port docelowy jest jasno określony), to z analogiczną regułą pozwalającą na przepuszczenie odpowiedzi pojawiają się problemy, gdyż portem docelowym jest tu losowy port wybrany wcześniej przez klienta.
W przypadku ruchu UDP stanowi to poważny problem, lecz w przypadku TCP możemy wykorzystać fakt istnienia w tym protokole tzw. połączeń. Klient, wysyłając pierwszy pakiet do serwera inicjuje pomiędzy nimi połączenie, a kolejne pakiety wymieniane pomiędzy klientem a serwerem (w obu kierunkach) uznaje się za należące do tego połączenia.
Możemy zatem, wykorzystując opisany w 4.2.2 parametr **`established`**, ograniczyć przepuszczane pakiety wyłącznie do tych, które są częścią istniejącego już połączenia.
Należy tu podkreślić, iż parametr established powoduje dalsze zawężenie działania reguły, tzn.:

- **access-list 101 permit tcp host 192.168.1.1 any** – nakazuje przepuszczać wszystkie pakiety TCP z adresu 192.168.1.1, do dowolnego innego.

- **access-list 101 permit tcp host 192.168.1.1 any established** – nakazuje przepuszczać pakiety TCP z adresu 192.168.1.1, do dowolnego innego, lecz jedynie wtedy, kiedy należą do już zestawionego połączenia.

4.10. Inne przydatne polecenia routera

`ping <adres>` – wysyła, z routera, ping pod podany adres
`show running-config` – powoduje wyświetlenie skryptu konfiguracji routera, zawierającego jego obecnie aktywne ustawienia (running-config). W skrócie **`show run`**.

4.11. Lista portów wybranych usług IP

Port	Protokół	Usługa
7	TCP/UDP	Echo
13	TCP/UDP	Daytime
17	TCP/UDP	Quote of the day (qotd)
19	TCP/UDP	Chargen
23	TCP	Telnet