Wprowadzenie do list dostępu w routerach Cisco

Filtrowanie ruchu sieciowego

Filtrowanie ruchu sieciowego pozwala na kontrolowanie co dzieje się w poszczególnych segmentach sieci. Jest to proces analizujący zawartość pakietów w celu podjęcia decyzji czy pakiet ma być dopuszczony do pewnej strefy sieci czy też zablokowany.

Filtrowanie pakietów może odbywać się na podstawie:

• Adresu źródłowego IP
• Adresu docelowego IP
• Adresów MAC
• Protokołów
• Typu aplikacji

Filtrowanie ruchu pozwala także podwyższyć wydajność sieci. Za pomocą blokowania niechcianego ruchu najbliżej źródła, nie pozwala na generowanie niepożądanych pakietów w całej sieci.

Jedną z metod używaną przez routery do filtrowania pakietów jest ACL (access control lists) zarówno do zarządzania ruchem wchodzącym jak i wychodzącym z sieci.

ACL używa się do wielu zastosowań np.:
• Określania wewnętrznych hostów dla NAT
• Identyfikowania ruchu dla zaawansowanych celów np. QoS
• Ograniczenia rozmiaru tablic routingu
• Ograniczenia liczby komunikatów serwisowych
• Kontrolowania dostępu wirtualnych terminali do routerów

Problemy

Potencjalne problemy mogące wystąpić przy używaniu ACL to:

• Dodatkowy czas procesora w routerze w celu sprawdzenia wszystkich pakietów.
• Źle zaprojektowane listy ACL zwiększają czas pracy routera i mogą spowodować niższą wydajność sieci.
• Źle umiejscowione listy ACL mogą zablokować ruch, który powinien być przepuszczony oraz zezwolenie na ruch który powinien być blokowany.

ACL (access lista, lista dostępu) jest to uporządkowany zestaw instrukcji akceptujących ***(permit)*** lub odrzucających ***(deny)*** pakiety przekazywane przez interfejs zgodnie z kryteriami określonymi przez parametry listy dostępu i zawartością pakietów.

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

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

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**.

Na końcu każdej access-listy jest niejawny (domyślny) wpis deny any any

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:

- **listy standardowe** - posiadają numery od 1-99
- **listy rozszerzone** - posiadają numery od 100 - 199.

W przypadku **list nazwanych**, typ listy podawany jest jawnie w poleceniu nakazującym jej utworzenie.

Ważna jest kolejność zapisywania poleceń. ACL są wykonywane od góry do dołu.

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.

Standardowa lista ACL jest ograniczona pod względem funkcjonalnym, gdyż umożliwia filtrowanie ruchu tylko w oparciu o adres źródła.

Dla protokołu IP numery ACL standardowych są w zakresie od 1 do 99.

```
access-list <nr listy 1-99> {permit | deny} <źródłowy adres IP>
<maska blankietowa>
```

Dla tego ACL adres źródłowy jest adresem IP komputera lub grupy komputerów, przy czym do polecenia access-list stosujemy ***wildcard mask*** (inaczej maska dopasowania lub blankietowa), która jest odwrotnością maski podsieci.

Np. chcąc zablokować podsieć 10.1.1.0 **255.255.255.0** wpiszemy następujące polecenie:

```
router# access-list 1 deny 10.1.1.0 0.0.0.255
```

gdyż: 255.255.255.255
- 255.255.255.000

000.000.000.255

Słowa kluczowe:
permit /deny - pakiety mogą być przekazywane przez interfejs / są filtrowane
log - umieszczenie tego słowa kluczowego na liście dostępu powoduje rejestrowanie w dziennikach pakietów zgodnych z instrukcjami permit i deny listy dostępu. ACL zawierające słowo kluczowe log są również nazywane *listami dostępu z obsługą dzienników*.

skróty, którymi można się posłużyć podczas wpisywania reguł:

- ***host*** **<adres IP>** => **<adres IP> 0.0.0.0**

np. chcemy akceptować pakiety z adresu źródłowego 172.19.1.100

```
router# access-list 2 permit 172.19.1.100 0.0.0.0
```

lub

```
router# access-list 2 permit host 172.19.1.100
```

- ***any*** => **0.0.0.0 255.255.255.255**

np. chcemy odrzucić pakiety z adresu źródłowego 172.20.100.1, ale wszystkie pakiety z innych adresów źródłowych chcemy akceptować.

```
router# access-list 1 deny host 172.20.100.1
router# access-list 1 permit 0.0.0.0 255.255.255.255
```

lub

```
router# access-list 1 deny host 172.20.100.1
router# access-list 1 permit any
```

ta druga linijka jest konieczna, gdyż domyślnie ACL kończą się deny any

Rozszerzona lista ACL oferuje dodatkowe funkcje i pozwala filtrować pakiety na podstawie adresu źródłowego, jak i docelowego. Wykorzystują protokoły oraz numery portów.
Dla protokołu IP numery ACL rozszerzonej są w zakresie od 100 do 199.

Format rozszerzonej ACL

access-list <nr listy 100-199> <deny | permit> <protokół> <źródłowy adres IP> <wilcard mask> <docelowy adres ip> <wilcard mask> <operator> <port lub usługa> [established]

- **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 192.168.1.1 any established - nakazuje przepuszczać ruch należący do już zestawionych połączeń TCP pomiędzy adresem 192.168.1.1 a wszystkimi innymi

- **operator** - używamy wtedy, gdy chcemy określić jakiego zbioru portów dotyczy reguła:
  - **eq <port>** - nr portu równy parametrowi <port>
  - **range <port1> <port2>** - nr portu zawarty w przedziale od <port1> do <port2> włącznie
  - **neq <port>** - nr portu różny od parametru <port>

Słowa kluczowe zaznaczone kolorem zawsze muszą wystąpić !

Protokoły:

Standardowo wykorzystujemy 4 protokoły:

ip, tcp, udp, icmp

Ale mogą wystąpić jeszcze inne, m.in.

ahp - authentication header protocol
eigrp - Cisco's EIGRP routing protocol
esp - encapsulation security payload
gre - Cisco's GRE tunneling
ospf - OSPF routing protocol

Protokół IP uwzględnia protokoły ICMP, TCP i UDP, dlatego bardziej specyficzne wpisy należy umieszczać na liście przed wpisami ogólnymi, aby kolejne instrukcje nie negowały poprzednich instrukcji znajdujących się na danej liście dostępu.

Porty i usługi używane przy konfiguracji (słowa kluczowe)

możemy używać zarówno numery portów jak i nazwy

Protokół	Numer portu	Nazwa
TCP	20	ftp-data
TCP	21	ftp
TCP	22	ssh
TCP	23	telnet
TCP	25	smtp
TCP	80	www
UDP	53	dns
UDP	69	tftp
UDP	161	snmp
TCP	443	https (ssl)
UDP	520	rip

ACL nazywane

Lista ACL zamiast numeru może posiadać nazwę.

Konfiguracja takiej ACL wygląda następująco:

```
router# conf t
router(config)# ip access-list <standard | extended> nazwa
router(config-std-nacl)#<permit | deny> <protokół>
<źródłowy host lub sieć> <wildcard> <docelowy host lub sieć>
<wildcard> <operator> <port>
```

Przypisanie listy do interfejsu

Stworzoną listę ACL należy przypisać do interfejsu 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.

```
router# conf t
router(config)# interface {fa | se} <nr interfejsu>
router(config-if)#ip access-group <nr listy lub nazwa> {in | out}
```

{in | out} - decydujemy czy ACL ma być używane do filtracji wyłącznie ruchu odbieranego (in) czy też wyłącznie wysyłanego (out) przez dany interfejs.

Przypisanie listy ACL do interfejsu likwidujemy wpisując:

```
no ip access-group <nr listy lub nazwa>
```

Rozmieszczenie list dostępu

Standardowe listy dostępu powinny być umieszczane w pobliżu punktu docelowego.
Listy tego typu wykorzystują wyłącznie adresy źródłowe, dlatego umieszczenie listy zbyt blisko punktu źródłowego może spowodować zablokowanie przepływu pakietów do innych portów.

Rozszerzone listy dostępu powinny być umieszczane w pobliżu filtrowanego źródła.
W tej konfiguracji można utworzyć filtry, które nie muszą wpływać na przepływ danych przez inne interfejsy.