ACL – seznamy řízení přístupu

Standardní ACL

ACL (Access Control List, seznam řízení přístupu) je mechanismus filtrování na vrstvě L3, částečně L4. Standardní ACL filtruje podle IP adres, extended ACL umí i podle portů a protokolů.

Každý ACL je identifikován svým číslem, může (nemusí) mít také jméno (to je pak pojmenovaný ACL).

Vyhrazené rozsahy čísel ACL:

1–99 nebo 1300–1399	standardní ACL
100–199 nebo 2000–2699	extended ACL (rozšířené)
zbytek	AppleTalk, IPX, extended IPX,… (nepoužíváme)

Takže můžu vytvořit standardní ACL určený číslem nebo jménem, a podobně rozšířený.

ACL nejdřív vytvoříme, a pak nasadíme na rozhraní a směr (tj. filtrujeme na konkrétním rozhraní, a to v příchozím nebo odchozím směru). Speciálním typem ACL je taky ACL na ochranu VTY linek.

ACL je posloupnost pravidel (taktéž očíslovaných), a paket na daném rozhraní a daném směru musí touto posloupností projít. Mohou nastat tyto situace:

- podmínka v pravidle neodpovídá paketu, tedy se jde na následující pravidlo v ACL,
- v pravidle je určeno, že pokud paket splňuje určitou vlastnost (například IP adresa patří do určité sítě), tak může pokračovat v cestě (permit),
- v pravidle je určeno, že pokud paket splňuje určitou vlastnost, tak má být zahozen (deny),
- paket postupně projde všemi pravidly v ACL a u žádného nedojde ke shodě s podmínkou (tedy vždy nastává první odrážka tohoto seznamu), pak záleží, jaké pravidlo je na konci:
    - deny any … bude zahozen,
    - permit any … projde, může pokračovat.

ACL pravidla obvykle obsahují IP adresy, k nim potřebujeme dopsat masku. Jenže pozor, Cisco u ACL používá wildcard masky, tj. inverzní. Wildcard maska vznikne tak, že v běžné (binární) masce převrátím 0 a 1. Wildcard maska nemusí mít nutně na začátku samé 0 a na konci samé 1, prostě určujeme, že v IP adrese na dané binární pozici buď musí být číslice předepsaná uvedenou adresou, nebo naopak je jedno, jestli v paketu v dané IP adrese je na tom místě 0 nebo 1.

Pokud chci do ACL pravidla uvést konkrétní unicast IPv4 adresu (jednu, žádnou síť), běžná maska by byla 255.255.255.255, ale wildcard maska bude 0.0.0.0. Příklad:

```
172.16.0.12 0.0.0.0
```

Pokud chci určit tuto podsíť: 172.16.0.0 255.255.0.0, bude to:

```
172.16.0.0 0.0.255.255
```

Jestliže v síti 10.0.0.0/8 chci v ACL zachytit právě všechny pakety s IP adresou, kde v druhém oktetu je pevně dané číslo:

```
10.96.0.0 0.0.255.255
```

Případně jsou napevno jen některé bity z toho oktetu:

```
10.96.0.0 0.15.255.255
```

Číslo 15 je binárně 0000 1111, po invertování dostaneme 1111 0000, tedy horní polovina daného oktetu musí být podle předpisu. Číslo 96 je binárně 0110 0000, což znamená, že horní polovina druhého oktetu musí být 0110, druhá polovina může být jakákoliv. Pro které adresy z následujících bude takové pravidlo v ACL platit?

```
10.96.52.4
10.105.0.4
10.128.22.1
10.112.150.32
```

A co když to pomícháme? V pravidle bude uvedeno například toto:

```
10.96.32.0 0.0.15.223
```

Co to bude znamenat? Bude tomuto předpisu odpovídat adresa 10.105.32.8?

Standardní ACL určený číslem vytvoříme takto:

```
access-list 10 permit 10.96.0.0 0.0.255.255        ; zdrojová IP
access-list 10 deny host 10.96.100.84  ; místo wildcard masky 0.0.0.0 uvedeme slovo host
access-list 10 deny any                ; defaultní zakončení, ale hodí se to uvádět
access-list 10 permit any              ; pokud chceme, aby prošlo vše, co došlo sem
```

Možné akce:

permit, deny, remark

Seznam ACL obsahuje jednu nebo více položek řízení přístupu ACE, každá má své vlastní číslo.

Vytvoření pojmenovaného ACL se dvěma položkami ACE (tradičně se název píše velkými písmeny):

```
ip access-list standard NO_ACCESS
      deny host 10.96.100.84
      permit 10.96.0.0 0.0.255.255
      exit
```

Nasazení na rozhraní:

```
interface f0/0
      ip access-group 10 out          ; nasazeno na odchozí provoz
      ip access-group 20 in           ; nasazeno na příchozí provoz
```

Verifikace:

```
sh access-lists
sh access-list 10
sh ip int f0/0
sh run
```

Úkol:

Na webu je předpřipravený soubor 05_ACL-predpripraveno.pka. Stáhněte si ho a otevřete. Projděte si všechna rozhraní (včetně loopbacků) a sítě. Ověřte, jestli na routerech opravdu nejsou žádné vytvořené seznamy ACL. Ověřte, jestli funguje směrování (který směrovací protokol je použit?). Ověřte, jestli jsou počítače navzájem dostupné.

Vytvořte standardní číslovaný ACL (č. 1), který povolí provoz ze sítí 192.168.30.0/24 a 192.168.20.0/24 do sítě 192.168.30.0/24, vše ostatní vedoucí do této sítě zakažte. Nasaďte ACL na vhodném rozhraní. Nezapomeňte, že standardní ACL nasazujeme vždy co nejblíž cíli.

Pomocí příslušných příkazů show zobrazte vytvořený ACL a také jeho nasazení na rozhraní.

Ověřte, jestli ACL opravdu funguje – pro povolené i zakázané sítě. Můžete použít také extended ping.

Dále vytvořte pojmenovaný standardní ACL ACL-CONFIG, který povolí provoz ze sítě 192.168.40.0/24 do sítě 192.168.10.0/24, a dále povolí přístup PC-C (192.168.30.3) do této sítě. Nasaďte na vhodném zařízení a rozhraní.

Opět si prohlédněte vytvořený ACL a také místo, kde je vytvořen.

Ověřte funkčnost ACL na spojeních jak povolených, tak i zakázaných. Prohlédněte si také statistiku přes show access-lists.

Modifikace existujícího standardního ACL

Jsou dvě možnosti, jak pozměnit existující ACL:

- bokem v textovém editoru si vytvořím celý ACL (zkopíruji z konzole, pozměním), původní odstraním (no access list…, no ip access-list…) a během znovuvytváření vkopíruji),
- použiju příkazy pro přidání nových ACE, musím vědět, která čísla ACE jsou v seznamu volná

Pro pojmenovaný ACL:

```
sh access-lists           ; ověřím, která čísla jsou volná
ip access-list standard název
      30 permit adresa inv-maska
      40 deny any
      end
```

ACL zůstal nasazen na rozhraní i po případném smazání či modifikování ACL, takže po modifikaci nemusíme znovu umísťovat na rozhraní.

Upozornění: položka deny any je sice defaultně platná, ale pokud ji do seznamu přímo umístíme, můžeme si zobrazit související statistiku.

Úkol:

Proveďte tuto modifikaci: zařízení ze sítě 209.165.200.224/27 mají mít přístup do 192.168.10.0/24, a dále má být na konec přidána položka deny any.

Otestujte, jestli přidané položky fungují jak mají.

ACL pro ochranu VTY linek

Seznam ACL lze nasadit i na VTY linky. Tím určujeme, odkud bude fungovat přístup do administrace zařízení.

ACL se vytváří úplně stejně jak je výše uvedeno, jen nasazení na linky je trochu jinak:

```
line vty 0 4       ; nebo line vty 0 15, podle skutečného počtu linek
      access-class jméno-nebo-číslo-ACL in
```

Úkol:

Jednoduše zprovozněte přístup přes telnet na routeru R3 (ano, normálně bychom to nedělali, tady to je jen z testovacích důvodů). Ověřte, jestli funguje z PC-A.

Na R3 vytvořte číslovaný ACL s číslem 2, ve kterém povolíte přístup z adresy 192.168.10.3, a dále přístup z adres v rozsahu 192.168.10.4 až .7, přičemž použijte vhodnou inverzní masku pro celý rozsah.

Nasaďte tento ACL na VTY linky na daném routeru.

Ověřte, jestli vytvořený ACL správně funguje. Změňte adresu PC-A na nějakou mimo rozsah povolený v ACL a vyzkoušejte, jestli to projde.

Na R3 si zobrazte statistiku ACL (v příkazu show access-lists) a zkontrolujte výsledek filtrování.

Na R3 nakonfigurujte SSH (přidejte vhodně pojmenovaného uživatele s heslem) a změňte přístup přes VTY na pouze přes SSH. Opět vyzkoušejte.

VTY se dají chránit také seznamy na jednotlivých rozhraních. Jaké výhody však má nasazení rovnou na VTY?