Cisco IOS 8 - ACL - Access Control List

Vložil/a Samuraj [1], 20 Červenec, 2011 - 18:17

- Networks & Protocols [2]
- Security [3]

Další část seriálu o Cisco IOSu je trošku více teoretická a věnuje se tématu Access Control List, tedy ACL. Můžeme říci, že se jedná o řízení nebo identifikaci přístupu k nějakému objektu. Začínám obecnějším popisem a dělením ACL a dále se věnuji rozšířenějším IP ACL a trochu méně používaným MAC ACL. Také článek ukazuje konfiguraci Standard, Extended i Named ACL na Cisco zařízeních a jejich aplikaci na Port nebo L3 interface.

Access Control List

Access Control List (dále jen ACL) je seznam pravidel, která řídí přístup k nějakému objektu. ACL jsou používány v řadě aplikací, často u aktivních síťových prvků, ale třeba také u operačních systémů při řízení přístupu k objektu (souboru). Pokud někdo požaduje přístup k nějakému objektu, tak se nejprve zkontroluje ACL přiřazený k tomuto objektu, zda je tato operace povolena (případně povolena komu).

Cisco ACL

Na aktivních prvcích Cisco jsou ACL vlastností IOSu. Můžeme je používat na několika místech, ale nejčastější použití je pro řízení (omezování) síťového provozu, tedy pro filtrování paketů. Různých typů ACL je celá řada, určité typy ACL se dají aplikovat na různá místa a také jsou zde určité vazby. Takže máme například IP Extended Named ACL. Pokusil jsem se vytvořit trochu méně tradiční, ale pro mne více praktický, seznam typů ACL.

```
    IP ACL – filtruje IPv4 provoz – IP, TCP, UDP, IGMP (multicast), ICMP
        Port ACL – pro fyzický L2 interface (aplikujeme na port), pouze p?ichozí sm?r
            Numbered Standard – ?íslované, pouze zdrojová adresa
            Numbered Extended – ?íslované, zdrojová i cílová adresa a voliteln? port
            Named Standard – pojmenované standard
            Named Extended – pojmenované extended
        Router ACL – pro L3 interface - SVI (switch virtual interfaces – L3 interface
pro VLAN), fyzický L3 interface (port – vznikne pomocí no switchport), L3
EtherChannel (spojení více port?); kontrolují routovaný provoz, odchozí nebo p?ichozí
sm?r
            Standard
            Extended
            Named
        VLAN map – kontroluje všechny pakety (routované i bridgované = switchované),
m?žeme kontrolovat provoz mezi za?ízeními v rámci jedné VLAN. Ne?eší se sm?r
(odchozí, p?ichozí)., aplikuje se na VLANu.
            Standard
            Extended
            Named
    MAC ACL (Ethernet ACL) – non-IP provoz
        Port ACL
            Standard
            Extended
            Named Extended
        VLAN map
```

```
Named Extended
```

Hlavní dělení je tedy podle typu adres, které používáme v pravidlech. Nejčastější jsou IP a MAC ACL, ale také dnes také (zatím méně využívané) IPv6 ACL, která mohou být Port nebo Router a pouze Named. V konfiguraci se používají prefixy místo Wildcard masky. Nebo již skoro nepoužívané IPX ACL.

Další dělení je podle toho, kam dané ACL aplikujeme. Můžeme na L2 interface, L3 interface a nebo speciální VLAN map. Potom již máme vlastní typy ACL, buď standardní, rozšířené nebo pojmenované.

```
V tomto ?lánku se v?nuji obecn? ACL, potom více IP ACL a na záv?r MAC ACL. Co se tý?e aplikace, tak je to sice obecné, ale více zam??eno na Port ACL. Router ACL (více prakticky) se v?nuji v dalším ?lánku Cisco IOS 18 - inter-VLAN routing a ACL - sm?rování mezi VLANy. Specifickým p?ípadem jsou VLAN mapy, o kterých vyjde další ?lánek.
```

ACL slouží hlavně

- jako základní síťová bezpečnost k blokování nebo povolení (routovaného) provozu
- ke kontrole šířky pásma
- Policy Based Routing
- vynucení síťových politik
- identifikaci nebo klasifikaci provozu (pro QoS, NAT, apod.)

Stručná charakteristika a vlastnosti

- ACL je sekvenční (řazený) seznam pravidel permit (povolit) a deny (zakázat), těmto pravidlům se říká ACE (Access Control Entries).
- ACL můžeme identifikovat číslem nebo jménem (pojmenované ACL).
- Nová pravidla se přidávají vždy na konec seznamu.
- Používá se pravidlo first-fit. Seznam se prochází od začátku ke konci, a pokud dojde ke shodě, tak se dále neprochází.
- Každý neprázdný seznam má na konci defaultní pravidlo, které zakazuje vše (deny any). Prázdný seznam povoluje vše.
- Je dobré umísťovat více specifická pravidla na začátek a obecná (subnety apod) na konec.
- Pokud se v ACL vyhodnotí deny, tak se odešle ICMP host nedosažitelný (unreachable).
- Filtrování (používání ACL) zpomaluje zařízení (stojí výpočetní výkon).
- Odchozí pravidla (outbound filters) neovlivňují provoz, který pochází lokálně z routeru (filtrují pouze procházející provoz).

Pokud chceme upravit nějaké hotové ACL, tak jej (ve většině případů) musíme smazat a vytvořit znovu. Doporučuje se napsat nejprve ACL v textovém editoru a následně zkopírovat do CLI. Případně Cisco Network Assistant má nástroj na úpravu ACL.

Pozn.: Výjimkou jsou pojmenované ACL, kde jsou určité úpravy možné.

- na interfacu můžeme kombinovat IP ACL a MAC ACL, abychom filtrovali veškerý provoz
- také můžeme používat dohromady Port ACL, Router ACL i VLAN map, ale Port ACL má největší prioritu, potom je Router ACL a teprve poslední VLAN map

Wildcard subnet mask

U ACL se Cisco rozhodlo nepoužívat tradiční masky podsítí (subnet mask), ale tzv. wildcard mask. Je to malé zkomplikování, ale nejedená o nic složitého. Pouze je třeba na tuto vlastnost nezapomenout

při konfiguraci, protože by mohlo dojít k řadě problémů. Tato maska se také označuje jako inversní maska (inverse mask), což ji lépe popisuje. Jedná se totiž o opačnou masku k tradiční masce.

Výpočet inversní masky je jednoduchý, vezmeme postupně všechny čtyři oktety masky a spočítáme 255 - oktet. Takže například maska 255.255.255.0 má inverzní verzi 0.0.0.255 nebo k 255.255.192.0 je 0.0.63.255.

Typy ACL

Nejpoužívanější je dělení ACL na dva typy

- **standard ACL** - starší a jednodušší verze ACL s méně možnostmi konfigurace
- **extended ACL** - novější a složitější ACL s více možnostmi

Dále existují různé speciální ACL, které jsou často odvozeny z těchto dvou, jako je dynamic ACL, context-based ACL, reflexive ACL nebo named ACL.

Standard ACL - standardní ACL

- používá čísla 1 - 99 a 1300 - 1999 v rozšířeném módu
- je jednoduché na konfiguraci
- filtruje (dívá se) pouze podle zdrojové adresy a používá se jako odchozí
- používá se pro blokování provozu blízko cíle

SWITCH(config)#access-list číslo {deny|permit} {host|source source-wildcard|any} [log]

Pozn.: Konfigurace standard i extended ACL se provádí stejně, rozlišuje se podle použitého čísla.

Na místě deny|permit můžeme také použít klíčové slovo remark a za něj vložit popis (komentář) daného pravidla.

Volitelný atribut log způsobí, že na konzolu a do logu budou posílány informace o paketech, které splní daná kritéria (dané pravidlo). Hodí se pro ladění, ale pro ostrý provoz příliš zatěžuje zařízení.

Příklad:

Následující ACL s číslem 5 povoluje přístup subnetu 10.5.1.0/24 mimo adresy 10.5.1.10, všechny ostatní adresy jsou zakázány.

```
SWITCH(config)#access-list 5 deny host 10.5.1.10
SWITCH(config)#access-list 5 permit 10.5.1.10 0.0.0.255
SWITCH(config)#access-list 5 deny any
```

Pozn.: Poslední pravidlo je defaultní a nevkládá se.

Extended ACL - rozšířené ACL

- používá čísla 100 - 199 a 2000 - 2699 v rozšířeném módu
- dívá se na IP adresu zdroje i cíle
- kontroluje řadu položek v hlavičce vrstvy 3 a 4 (protokol, port apod.)
- může blokovat provoz kdekoliv (nejlépe blízko zdroje)

Pozn.: Další číselné rozsahy se používají pro ostatní typy ACL, jako IPX, AppleTalk, XNS, apod.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Extended ACL může kontrolovat tyto parametry

- **Ve 3. vrstvě** ISO/OSI, tedy v IP hlavičce kontroluje: IP adresy, protokol, údaje z ToS (Type of Service - prioritu 802.1q a službu).
- **Ve 4. vrstvě** kontroluje v TCP hlavičce: porty a protokoly, v UDP hlavičce: porty, v ICMP hlavičce typ zprávy.

Pozn.: Při používání údajů ze 4. vrstvy (tedy portů) je třeba uvažovat fragmentovaný provoz, protože při fragmentaci pouze první paket obsahuje údaje ze 4. vrstvy. Můžeme využít klíčové slovo fragments v pravidle.

SWITCH(config)#access-list číslo {deny|permit} protokol {host|source source-wildcard|any} [port] {host| destination destination-wildcard|any} [port]

Výše uvedený zápis extended ACL je pouze zjednodušený, je zde možno použít řadu dalších parametrů a vytvořit třeba dynamický ACL či omezit časově platnost ACL.

Jako protokol je možno použít IP, TCP, ICMP, UDP nebo i řadu dalších. Podle zvoleného protokolu se mění i parametry, které můžeme v ACL použít, například port je možno použít jen u TCP a UDP.

Pozn.: Pokud chceme filtrovat všechny protokoly, tak použijeme IP, ostatní patří pod něj.

Omezení na port se zadává pomocí operátoru, můžeme použít operátory eq (rovná se), neq (nerovná), gt (větší než), lt (menší než) a range (rozsah). Operátor s portem se zadává za zdrojovou adresu nebo za cílovou adresu a port se pak aplikuje u zdroje nebo cíle.

Je třeba si dobře promyslet, kam umístit kontrolu portu (zda ke zdroji nebo k cíli), podle toho, zda aplikujeme ACL jako vstupní nebo výstupní (je popsáno dále). Následující příklad ukazuje dvě možnosti.

```
SWITCH(config)#access-list 105 permit tcp 10.1.0.0 0.0.0.255 any eq www
SWITCH(config)#access-list 105 permit tcp 10.1.0.0 0.0.0.255 eq www any
```

Příklad:

ACL číslo 105 povoluje přístup na server 10.5.1.10 odkudkoliv, ale pouze na port 80 (tedy http) a ping.

```
SWITCH(config)#access-list 105 permit tcp any host 10.5.1.10 eq 80
SWITCH(config)#access-list 105 permit icmp any any echo
SWITCH(config)#access-list 105 permit icmp any any echo-reply
SWITCH(config)#access-list 105 deny ip any any
```

Pozn.: Poslední pravidlo je defaultní a nevkládá se.

Named ACL - pojmenované ACL

- můžeme jej použít pro standard i extended ACL
- umožňuje upravovat či mazat jednotlivá pravidla v ACL
- jména se lépe pamatují
- můžeme použít "neomezený" počet pojmenovaných ACL
- jako jméno můžeme použít i číslo, ale to musí patřit do správného rozsahu

Pozn.: Přestože mají pojmenované ACL určité výhody, tak Cisco v některých materiálech doporučuje spíše používat běžné ACL. Pojmenovaná ACL nejdou použít úplně všude, já však s nimi v praxi neměl problém.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Pojmenované ACL se vytváří jiným způsobem. Nejprve vytvoříme ACL a zároveň se přepneme do konfiguračního ACL módu.

```
SWITCH(config)#ip access-list {standard|extended} jmeno
```

Dále zadáváme jednotlivá pravidla dle typu ACL a se stejnými možnostmi jako u číslovaných ACL. Číslo řádku (na začátku příkazu) je nepovinné.

```
SWITCH(config-ext-nacl)#[?ísło ?ádku] permit|deny ...
```

Pokud si zobrazíme ACL, tak uvidíme, že jednotlivé řádky jsou číslovány. Pomocí těchto čísel můžeme pravidla mazat a nová pravidla můžeme vkládat na určité místo.

Pozn.: Automatická čísla řádku se vytvářejí po desítkách (první pravidlo 10, pak 20, 30 ...) a řádky se číslují i u nepojmenovaných ACL. Pokud zadáváme vlastní čísla, tak ty se použijí a vidíme je při zobrazení ACL. Pokud se však podíváme do running-config, tak zde tato čísla nejsou a po restartu switche se automaticky přečíslují.

Příklad:

```
SWITCH(config)#ip access-list extended jmeno
SWITCH(config-ext-nacl)#deny ip 192.168.190.100 0.0.0.1 host 192.168.190.200
SWITCH(config-ext-nacl)#permit ip any any
```

Malé rady

- klíčové slovo host - místo 10.0.5.2 0.0.0.0 můžeme použít host 10.0.5.2
- klíčové slovo any - místo 0.0.0.0 255.255.255.255 dáme any
- Nelze editovat nebo měnit pořadí v běžných ACL, pravidla se přidávají na konec. Pokud chceme něco změnit, tak musíme celé ACL smazat a znovu vytvořit.
- Při odstranění ACL se může stát, že pokud je stále aplikováno na interface, tak se nahradí defaultním zákazem všeho. Správně by však při neexistenci ACL mělo procházet vše.

Konfigurace ACL

Konfigurace ACL se provádí ve dvou krocích

- vytvoření ACL - nejprve vytvoříme pravidla podle typu ACL, viz. předchozí odstavce
- aplikace ACL na rozhranní - následně musíme toto ACL přiřadit k nějakému objektu, v tomto případě interfacu, to se provádí vždy stejně

Aplikace ACL

Tím, že aplikujeme ACL na interface, tak řídíme přístup paketů k tomuto interfacu. ACL (v rozsahu popisovaném v tomto článku) můžeme aplikovat na nějaké rozhranní, kterým může být port, sériová linka, VLAN, apod.

Můžeme aplikovat pouze jedno ACL pro interface, směr a protokol. Protokolem je myšleno IP, IPX, Apple Talk apod. Takže například pro jeden port v TCP/IP síti můžeme aplikovat maximálně dvě ACL (jedno vstupní - inbound a jedno výstupní - outbound).

Při umisťování ACL je třeba dobře rozmýšlet, aby bylo umístění efektivní. Pokud to jde, tak je dobré volit co nejblíže zdroji, aby nebyla zatěžována síť. Můžeme však umísťovat ACL pouze na zařízení, která kontrolujeme, takže často je třeba nastavit ACL blízko cíle.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Aplikace ACL je jednoduchá. Přepneme se na daný interface a pomocí příkazu ip access-group nastavíme ACL určitého čísla nebo jména, spolu s určením směru.

SWITCH(config-if)#ip access-group {číslo|jméno ACL} {in|out}

Pozn.: Na dotaz jednoho čtenáře jsem se dočetl, že směr out není podporovaný na L2 interfacech (tzn. portech), ale pouze na L3 (typicky VLAN a routovaný port). A to se týká pouze L3 (C3750) a vyšších switchů, L2 switch (C2960) má pouze in ACL. Takže směr out využijeme pouze na routerech a L3 switchích. Pokud nám jde o port ACL a switch, tak musíme daný port převést na routovaný, pomocí no switchport a nastavení IP adresy.

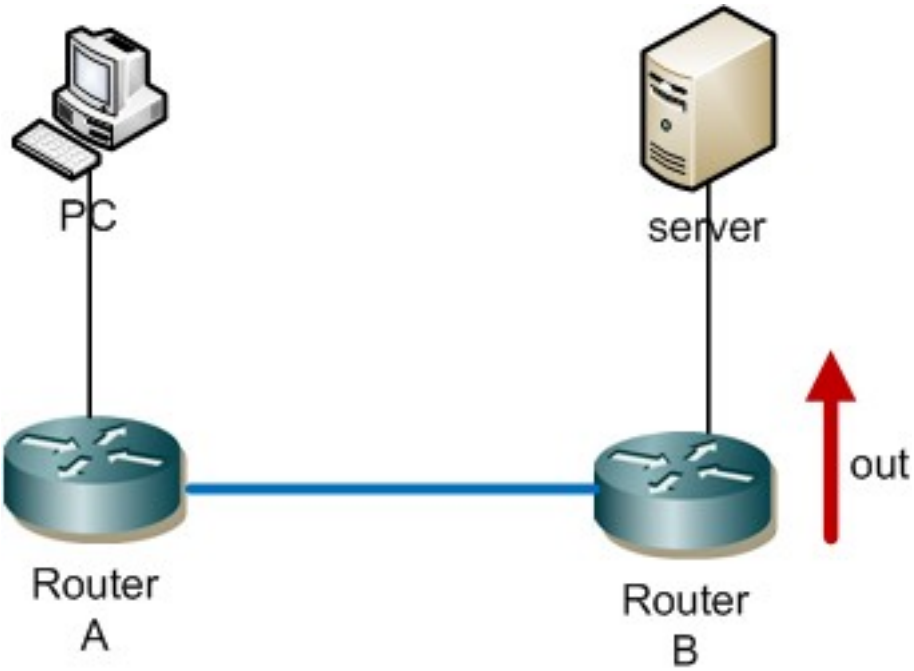
Příklad:

```
SWITCH(config)#interface serial0
SWITCH(config-if)#ip access-group 5 in
```

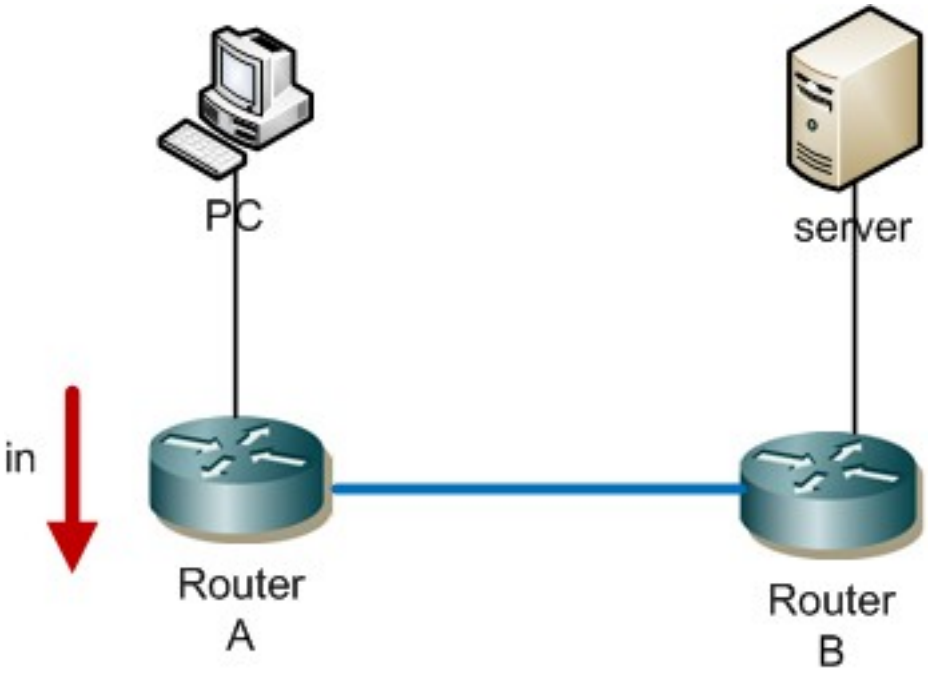
Určení směru

Určení směru, v kterém má ACL působit není složité. Je třeba se podívat na switch, kde jej aplikujeme a rozhodnout, zda chceme omezit pakety, které z něj odchází (out) nebo hned na vstupu, ty které přichází (in).

Standard ACL se umisťuje blízko cíle a měl by tedy být vždy odchozí - out. Na následujícím obrázku omezujeme provoz, který přichází na server.
Standard ACL směr



Extended ACL se většinou snažíme umístit co nejblíže ke zdroji a v tom případě je filtr vstupní - in.
Extended ACL směr



Kontrola ACL

Pár show příkazů pro kontrolu ACL.

```
SWITCH#show ip interface       // zobrazí info interface a je zde vid?t, pokud je aplikován ACL
SWITCH#show access-lists       // seznam ACL (IP i MAC) s pravidly
SWITCH#show ip access-lists    // seznam IP ACL
SWITCH#show running-config     // v b?žící konfiguraci jsou take vid?t ACL i jejich aplikace
```

Další metodou pro ladění ACL je využití logování. Ke každému pravidlu můžeme na konec přidat klíčové slovo log a pak jsou logovány všechny pakety, které splní toto pravidlo.

Například pokud chceme vidět komunikaci, která není zachycena žádným pravidlem v ACL a je tedy zakázána, můžeme na konec přidat pravidlo

SWITCH(config)#access-list 5 deny any log

ACL pro VTY

Mimo fyzických interfaců (jako jsou porty) máme také virtuální, např. Virtual Terminal (VTY, kam můžeme přistupovat přes telnet či ssh). Na VTY bychom měli aplikovat pouze jedno ACL, i když se vytváří více spojení pro více uživatelů (protože je nemůžeme rozlišovat - nevíme, přes které se uživatel připojí).

ACL pro VTY se vytvářejí stejně, ale aplikace se provádí pomocí příkazu access-class.

```
SWITCH(config)#line vty 0 4
SWITCH(config-line)#access-class 2 in
```

Named Extended MAC ACL - pojmenované rozšířené MAC ACL

Stejně jako IP ACL můžeme vytvářet MAC ACL, které filtrují komunikaci pomocí MAC adres a používají se na interfacy druhé vrstvy (dle OSI modelu). Konfigurace a použití je obdobné.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Pozn.: Můžeme použít buď číslované standardní MAC ACL (čísla 700 - 799), číslované rozšířené MAC ACL (čísla 1100 - 1199) nebo pojmenované rozšířené MAC ACL. Na řadě switchů je ale k dispozici pouze pojmenované rozšířené MAC ACL.

SWITCH(config)#mac access-list extended jmeno

Tím přejdeme do extended MAC access-list konfiguračního módu, kde definujeme jednotlivá pravidla.

SWITCH(config-ext-macl)#[číslo řádku] {deny|permit} {host source MAC|source MAC mask|any} {host destination MAC|destination MAC mask|any}

Pozn.: Výše uvedené pravidlo může obsahovat i řadu volitelných parametrů, které určují například EtherType nebo COS.

Příklad:
```
SWITCH(config)#mac access-list extended test
SWITCH(config-ext-macl)#permit host 0000.1111.2222 any
SWITCH(config-ext-macl)#deny any any
```

MAC ACL se aplikuje na interface 2. vrstvy a můžeme aplikovat pouze jeden MAC ACL na interface. Aplikace může být pouze na vstupu (in). Pro aplikaci slouží příkaz:

SWITCH(config-if)#mac access-group jméno-ACL in

Pro zobrazení aplikace MAC ACL na porty můžeme použít příkaz:

SWITCH#show mac access-group

URL článku: https://security-portal.cz/clanky/cisco-ios-8-acl-access-control-list

Odkazy:
[1] https://security-portal.cz/users/samuraj
[2] https://security-portal.cz/category/tagy/networks-protocols
[3] https://security-portal.cz/category/tagy/security

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn