Extended ACL a domény

Extended ACL

Jak funguje extended ACL

Rozšířené seznamy řízení přístupu dokážou filtrovat podle více kritérií než jen zdrojové IP adresy: zdrojová a cílová IP, protokol, port. Jinými slovy: filtruje se podle různých informací v L3 a L4 záhlaví.

Na rozdíl od standardních ACL je umísťujeme co nejblíž zdroji, aby zakazovaný provoz co nejméně zatěžoval síť.

Vytvoření ACE číslovaného rozšířeného ACL:

```
access-list 105 permit protokol zdrojova-ip cilova-ip eq port
access-list 105 permit protokol zdroj-ip eq zdroj-port cil-ip eq cil-port
access-list 105 permit protokol zdrojova-ip cilova-ip established
```

Místo adresy můžeme uvést `any`, pokud tento parametr nemá být rozlišován. Možnosti pro protokol zjistíme otazníkem (tcp, udp, icmp, smtp, ftp, ftp-data,…). Porty mohou být zadány číslem nebo jménem (např. http 80, https 443 – možnosti opět zjistíme otazníkem).

Na konci se předpokládá `deny ip any any`, nicméně může být praktické uvést explicitně.

Vytvoření pojmenovaného rozšířeného ACL:

```
ip access-list extended jmeno
       permit tcp……
       exit
```

Pokud na konec ACL připíšeme klíčové slovo `established`, vyhodnotí se shoda jen tehdy, pokud má příslušný TCP segment nastavený bit ACK nebo RST, které nebývají u prvního TCP segmentu v handshaku (u protokolu UDP nemá smysl, tam se handshake nekoná). Takže pokud chceme ztížit hackerům pokusy o navázání spojení do naší části sítě, ve které nemáme žádné servery, můžeme nastavit:

```
permit tcp any adresa.chráněné.sítě eq 80 established
```

a zbytek provozu zakážeme, tento ACL nastavíme na vstupním rozhraní z „nebezpečné“ sítě nebo výstupním do „chráněné“ sítě. Důsledkem je, že zde konkrétně lze navázat spojení na webové servery z chráněné sítě ven, ale nikoliv dovnitř.

Jako první ACE do sítě bez serverů bývá velmi často tato položka:

```
permit tcp any any established
```

Což znamená, že provoz, který byl navázán z vnitřní sítě ven, projde rychle a bez problémů, a až další bude podrobněji filtrováno. Pozor na UDP provoz, pokud bychom ho nepovolili některým dalším pravidlem, nefungoval by mnohý multimediální provoz.

Defaultní „zákaz ostatního“ může být explicitně uveden takto:

```
deny ip any any
```

Znamená to, že veškerý IP provoz (tedy to, v čem jsou zapouzdřeny všechny TCP a UDP segmenty) bude zakázán. Zamyslete se: co projde?

Příklad

na webu si najděte předpřipravený příklad 06_ExtendedACL-predpripraveno.pkt. Jsou tam tři routery, dva switche, jeden server a dva počítače. Projděte si jejich nastavení, zjistěte, kde je zprovozněn přístup přes SSH.

Nastavte v síti ACL takto:

- Půjde o pojmenovaný extended ACL s názvem WEB_ACCESS.
- Počítač s adresou 10.10.0.11 může přes SSH přistupovat k routeru R2.
- Webový provoz ze sítě 10.10.0.0/16 může kamkoliv.

Vyzkoušejte na počítači s adresou 10.10.0.11 ping na druhý počítač (10.20.0.11). Bude to fungovat? Dále ve webovém prohlížeči na tomtéž počítači zobrazte web 192.168.0.11. Funguje?

Vyzkoušejte na tomtéž počítači přístup přes SSH k routerům R1 a R2. Který z nich funguje? Jsou to tyto příkazy:

```
ssh –l admin 10.40.0.2
ssh –l admin 10.10.0.1
```

Na routeru ISP vytvořte loopback lo0 s IP adresou 209.165.200.225/27 (tj. maska 255.255.255.224). To bude simulace našeho poskytovatele internetu. Zakažte veškerý telnet provoz ve směru z internetu.

Filtrace ICMP paketů

Pro protokol ICMP existuje několik „portů“ (i když zde samozřejmě o porty nejde, ale spíše o typy ICMP):

- unreachable
- time-exceeded
- echo
- echo-reply
- parameter-problem
- source-quench

Poslední dva uvedené typy jsou důležité například při zjišťování MTU na cestě.

Pokud tedy chceme povolit všechny kromě echo, můžeme je buď vyjmenovat v jednotlivých ACE, nebo to může být třeba takto:

```
deny icmp any any echo
permit icmp any any
… další, co chceme povolit či zakázat
```

Pokud máme obavy z DoS útoku zneužitím ICMP echo, můžeme místo zákazu nastavit limit (nejde v Packet Traceru). Nastavuje se vždy na rozhraní (na každém rozhraní to můžeme mít jinak, jak co se týče ACL, tak i tohoto limitu). Je to příkaz rate-limit, takže:

```
interface g0/1
        rate-limit input access-group ozn_ACL bps bpsnormal bpsmax conform-action transmit exceed-action drop
```

To znamená, že ACL nasadím na rozhraní s tím, že pokud je provoz uvedený v ACL do limitu, tak projde, ale pokud už je nad limit, bude zahozen. Za označením ACL jsou tři čísla (mohou být stejná) – je to provoz v bitech za sekundu.

Viz https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_classn/configuration/15-mt/qos-classn-15-mt-book/qos-classn-car.html, https://www.networkcomputing.com/network-security/protecting-cisco-router-ping-flooding

Příklad

Na routeru R2 vytvořte ACL (číslovaný s číslem 102), který bude filtrovat provoz přicházející od ISP, a to takto:

- povolte veškerý TCP provoz, který byl navázán z vnitřních sítí,
- povolte ICMP echo reply a další ICMP provoz zjišťující chyby (vyjmenujte v jednotlivých ACE),
- zakažte veškerý ostatní IP provoz.

Otestujte ping vedoucí z a do chráněné sítě, pak si vypište statistiky.

Pár doporučení k ACL

Nejdřív obecně k ACL: různá zařízení obvykle podporují pojmenované i číslované seznamy, ale nemusí to být pravidlem. Výjimečně můžeme narazit na zařízení (ani ne tak router, jako spíše hardwarový firewall), kde něco z toho „nejde“.

V příkladech (nejen zde) vidíme obvykle IP adresy, ale ve skutečnosti mohou být použity i jmenné adresy. Například:

```
access-list 104 permit tcp any host web.domena.cz eq www
```

Zařízení, na kterém něco takového použijeme, však musí být schopno toto jméno přeložit.

V ACL existují určitá doporučení ohledně řazení položek ACE:

- bereme v úvahu, že se ACE v seznamu zpracovávají shora dolů, tedy nejdřív mají být specifičtější položky a až potom obecnější,
- obvykle bývají nejdřív položky typu permit, ale záleží na podmnožinách/nadmnožinách sítí: můžeme třeba chtít, aby pro některá zařízení dané sítě platilo určité nastavení, ale pro zbytek sítě jiné nastavení, což se v pořadí položek musí odrazit (bez ohledu na to, co je permit a co deny),
- pokud se to „nebije“ s předchozím bodem, umísťujeme dřív to, co bude častěji používáno.

Co s druhým bodem, jak zjistíme typickou frekvenci používání konkrétních ACE v pravidle? Jednoduše tak, že položky ACE nejdřív nasadíme podle odhadu, ale po určité době používání si zobrazíme statistiku pomocí show access-list. U každé ACE bude uveden počet „zásahů“, podle toho přeuspořádáme.

Proč je vlastně druhý bod důležitý? Protože tak zlepšujeme průchodnost (propustnost) filtrování, a taky šetříme výpočetní zdroje daného zařízení.

Je jedno úplně nejdůležitější pravidlo: přehlednost. Pokud aplikace výše uvedených pravidel snižuje přehlednost, u seznamu s několika položkami to nevadí, ale u seznamu s desítkami či stovkami položek to už může vadit velmi podstatně.

Některá zařízení umožňují vytvářet *skupiny* (sítí, rozsahů portů, protokolů), obvykle jen u extended ACLs a jen pro IPv4 adresy. Pokud zjistíme, že na daném zařízení to lze (tedy je podporován příkaz `object-group` v globálním konfiguračním módu), může nám to hodně pomoci při zvýšení přehlednosti ACE v seznamu. Má to své výhody (zpřehlednění ACL), ale i nevýhody: navyšuje se výpočetní náročnost práce se seznamem a zabírá to více paměti v NVRAM.

Práce se skupinami v ACL:

https://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/sec-object-group-acl.html

Dalším „vylepšením“ jsou *Turbo ACL* (čte se údajně jako turbo-ackle). Jsou to kompilované ACL, tedy přeložené do strojového kódu (běžné ACL jsou vlastně obdobou interpretovaných programů v textové podobě), čímž se urychluje práce s nimi. Zapnutí Turbo ACL znamená, že všechny definované ACL budou zkompilovány, přičemž se dá i ovlivnit množství paměti pro ně vyhrazené.

```
access-list compiled
show access-lists compiled
```

Jmenný překlad přímo na routeru

Můžeme si přímo na routeru rozjet místní překlad názvů. Například:

```
ip host webserver 192.168.25.4
```

Pak můžeme v různých příkazech (nejen v pingu) místo IP adresy používat tuto jmennou adresu. Ovšem tato vazba bude viditelná opravdu jen lokálně na tomto zařízení.

Můžu také nastavit adresu jmenného serveru:

```
ip name-server ip.adresa
```

Pokud jsme si hráli s ACL, je třeba povolit UDP provoz na portu 53 (tedy „domain“):

```
access-list 105 permit udp any any eq domain
access-list 105 permit udp any eq domain any
```

Z bezpečnostních důvodů se naopak často zakazuje DNS překlad:

```
no ip domain-lookup
```

Příklad:

Pokud si vytvoříme název pro některý server a pak zakážeme domain lookup, bude fungovat ping na vytvořený název?