Příprava na maturitu: Seznamy řízení přístupu (ACL)

Seznamy ACL společnosti Cisco se vyznačují jednoduchým nebo více výpisy povolení / odepření. Účelem je filtrování příchozích nebo odchozích paketů na vybraném síťovém rozhraní. Existuje řada typů ACL, které jsou nasazeny na základě požadavků. Na rozhraní Cisco jsou povoleny pouze dva ACL na protokol. To by zahrnovalo například jeden IP ACL aplikovaný příchozí a jeden IP ACL aplikovaný odchozí.

Osvědčené postupy společnosti Cisco pro vytváření a používání seznamů ACL

- Použít standardní ACL poblíž cíle
- Použít rozšířený seznam ACL poblíž zdroje
- Pište ACL s více výpisy od nejkonkrétnějších po nejméně konkrétní.
- Na síťové rozhraní lze použít maximálně čtyři seznamy ACL, IPv4 tam, IPv6 tam, IPv4 zpět a iPv6 zpět.
- Pouze jeden ACL lze použít příchozí nebo odchozí na každé rozhraní a protokol vrstvy 3.

Při vytváření a používání seznamů řízení přístupu (ACL) existují některé doporučené postupy. Správce sítě by měl použít standardní seznam ACL nejblíže k cíli. Standardní příkaz ACL se skládá ze zdrojové adresy IP a masky zástupných znaků zvané wildcard. Existuje společné číslo nebo název, který přiřazuje více příkazů ke stejnému seznamu ACL.

Standardní seznamy ACL jsou staršího typu a velmi obecné. Díky tomu mohou nechtěně filtrovat provoz nesprávně. Doporučuje se použít standardní seznam ACL v blízkosti cíle, aby se zabránilo možnému nadměrnému filtrování. Rozšířený seznam ACL by měl být použit nejblíže ke zdroji. Rozšířené seznamy ACL jsou granulární (specifické) a poskytují více možností filtrování. Zahrnují zdrojovou adresu, cílovou adresu, protokoly a čísla portů. Použití rozšířených ACL nejblíže ke zdroji zabrání přenosu, který by měl být filtrován, v procházení sítí. To šetří šířku pásma a další zpracování vyžadované u každého směrování routeru ze zdrojového do cílového koncového bodu.

Některé seznamy řízení přístupu se skládají z více příkazů. Uspořádání příkazů je klíčem ke zpracování ACL. Router začíná shora (první) a cykluje všemi příkazy, dokud není nalezen odpovídající příkaz. Paket je zrušen, pokud neexistuje žádná shoda. Pořadí všech výpisů ACL od nejkonkrétnějších po nejméně konkrétní. Přiřazení nejméně konkrétních příkazů jako první způsobí, že dojde k falešné shodě. V důsledku toho nikdy nedojde ku shodě v zamýšleném příkazu ACL.

Specifičtější příkaz ACL se vyznačuje zdrojovou a cílovou adresou s kratšími maskami zástupných znaků (více nul). To nakonfiguruje konkrétní podsítě tak, aby odpovídaly. Kromě toho jsou také specifikovány aplikační protokoly nebo čísla portů. První příkaz ACL je konkrétnější než druhý příkaz ACL:

access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.10.64.1 eq 23
access-list 100 deny tcp any any eq 23

Dynamický seznam ACL poskytuje dočasný přístup k síti pro vzdáleného uživatele. Konfigurovaný seznam ACL definuje typ povoleného přístupu a zdrojovou adresu IP. Kromě toho existuje hodnota časového limitu, která omezuje dobu přístupu k síti. Vzdálené přihlášení uživatele je k dispozici s nakonfigurovaným uživatelským jménem a heslem.

Příklad 1: Classful Wildcard Mask

Následující zástupný znak (wildcard) 0.0.0.255 bude odpovídat pouze v podsíti 192.168.3.0 a nebude odpovídat všem ostatním. To by mohlo být použito s ACL například k povolení nebo zakázání podsítě:

192. 168. 3. 0
11000000.10101000.00000011.00000000
00000000.00000000.00000000.1111111 = 0,0.0.255
192.168.3.0 0.0.0.255 = mat

Masky zástupných znaků ACL

Maska zástupného znaku je technika pro párování konkrétní adresy IP nebo rozsahu adres IP. Filtr seznamů řízení přístupu Cisco (ACL) založený na rozsahu adres IP konfigurovaném pomocí masky zástupných znaků. Maska zástupného znaku je obrácená maska, kde odpovídající adresa IP nebo rozsah je založen na 0 bitech. Další bity jsou nastaveny na 1, protože není nutná shoda. Zástupný znak 0.0.0.0 se používá k přiřazení jedné IP adrese. Maska zástupného znaku pro 255.255.224.0 je 0,0.31.255 (invertovat bity tak, aby nula = 1 a jedna = 0) uvedená v následujícím příkladu.

11111111.11111111.111 00000.00000000 = maska podsítě
00000000.00000000.000 11111.11111111 = maska se zástupnými znaky

Všichni hostitelé a síťová zařízení mají síťová rozhraní, kterým je přiřazena adresa IP. Každá podsíť má řadu hostitelských IP adres, které lze přiřadit k síťovým rozhraním. Zástupné znaky ACL jsou nakonfigurovány k filtrování (povolení / odepření) na základě rozsahu adres. To by mohlo zahrnovat hostitele, podsítě nebo více podsítí.

K dispozici jsou plnětřídní (classfull), tj. co znají jen adresy typu A, B, C s maskami 255.0.0.0, nebo 255.255.0.0 anebo 255.255.255.0) a beztřídní masky (classless, kdy může být maska jakákoliv, kdy levá část jsou jednotky a pravá nuly) podsítě spolu s přidruženými maskami zástupných znaků. Klasické masky zástupných znaků jsou založeny na výchozí masce pro konkrétní třídu adres (A, B, C). Kdykoliv je na třídu adresy použita nestandardní maska zástupného znaku (nebo maska podsítě), je to beztřídní adresování.

Příklad 2: Classful Wildcard Mask

Následující zástupný znak (wildcard) 0.0.0.255 bude odpovídat pouze v podsíti 192.168.3.0 a nebude odpovídat všem ostatním. To by mohlo být použito s ACL například k povolení nebo zakázání podsítě.

192. 168. 3. 0
11000000.10101000.00000011.00000000
00000000,00000000,00000000,1111111 = 0,0.0.255
192.168.3.0 0.0.0.255 = shoda pouze v podsíti 192.168.3.0

Příklad 3: Klasická maska se zástupnými znaky

Následující zástupný znak 0.0.0.255 bude odpovídat pouze v podsíti 200.200.1.0 a nebude odpovídat všem ostatním. To by mohlo být použito s ACL například pro povolení nebo odepření veřejné adresy hostitele nebo podsítě.

200. 200. 1. 0
11001000.11001000,00000001,00000000
00000000,00000000,00000000,1111111 = 0,0.0.255
200.200.1.0 0.0.0.255 = shoda pouze v podsíti 200.200.1.0

Příklad 4: Klasická maska se zástupnými znaky (wildcard)

Následující zástupný znak 0.0.255.255 se bude shodovat ve všech podsítích 172.16.0.0 a nebude odpovídat všem ostatním. To by mohlo být použito s ACL například k povolení nebo zakázání více podsítí.

172. 16. 0. 0
10101100 00010000,00000000,00000000
00000000.00000000.11111111.11111111 = 0,0.255.255
172.16.0.0 0.0.255.255 = shoda pouze v podsíti 172.16.0.0

Příklad 5: Classless Wildcard Mask

Kdykoli použijete nestandardní zástupný znak, který se označuje jako beztřídní (classless) adresování. V tomto příkladu je 192.168.1.0 síťová adresa třídy C. Všechny adresy třídy C mají výchozí masku podsítě 255.255.255.0 (/ 24). Naopak výchozí maska zástupných znaků je pro adresu třídy C 0.0.0.255.

Povolení či odepření (permit nebo deny) rozsahu adres hostitele ve 4. oktetu vyžaduje beztřídní masku zástupných znaků (neřídí se standardem pro adresu A, B nebo C, kdy pro adresu A zabere síť přesně 8 znaků, u B přesně 16 znaků a u C přesně 24 znaků). V tomto příkladu bude zástupný znak 0.0.0.15 odpovídat v rozsahu adres hostitele od 192.168.1.1 do 192.168.1.14. a neodpovídá na všechno ostatní. Jedná se o první čtyři bity 4. oktetu, které přidávají až 14 hostitelských adres. Síťovou a broacast adresu nelze přiřadit síťovému rozhraní. To by mohlo být použito s ACL například k povolení nebo zakázání pouze konkrétních adres hostitele.

192. 168. 1. 0
11000000.10101000.00000001,0000 0000
00000000.00000000.00000000.0000 1111 = 0,0.0.15
192.168.1.0 0.0.0.15 = shoda 192.168.1.1/28 -> 192.168.1.14/28

Příklad 6: Classless Wildcard Mask

Následující maska zástupného znaku 0.0.0.3 se bude shodovat v rozsahu adres hostitele od 192.168.4.1 - 192.168.4.2 a nebude odpovídat všem ostatním. Jedná se o první dva bity 4. oktetu, které přidávají až 2 adresy hostitele; adresu sítě a broadcast adresu nelze přiřadit síťovému rozhraní. To by mohlo být použito například k povolení nebo zákazu konkrétních adres hostitele na připojení WAN point-to-point.

192. 168. 4. 0
11000000.10101000.00000100.000000 00
00000000,00000000,00000000,000000 11 = 0,0.0.3
192.168.4.0 0.0.0.3 = shoda 192.168.4.1/30 a 192.168.4.2/30

Příklad 7: Classless Wildcard Mask

Správce sítě musí nakonfigurovat seznam ACL, který povoluje provoz pouze z rozsahu hostitele 172.16.1.32/24 až 172.16.1.39/24. Co je to maska ACL a zástupných znaků, která by toho dosáhla?

Odpověď

Následující maska zástupného znaku 0.0.0.7 bude odpovídat v rozsahu adres hostitele od 172.16.1.33 do 172.16.1.38 a nebude odpovídat ve všech ostatních. Jedná se o první tři bity 4. oktetu, které přidávají až 6 hostitelských adres. Síťovou adresu a vysílací adresu nelze přiřadit síťovému rozhraní. To by mohlo být použito například k povolení nebo zakázání konkrétních adres hostitele v podsíti.

172. 16. 1. 32
10101100 00010000,00000001,00100 000
00000000,00000000,00000000,00000 111 = 0,0.0.7
172.16.1.0 0.0.0.7 = shoda 172.16.1.33/29 -> 172.16.1.38/29

Následující standardní seznam ACL povolí provoz z rozsahu IP adres hostitele 172.16.1.33/29 až 172.16.1.38/29. Chcete-li vypočítat masku podsítě (0.0.0.7 = 255.255.255.248 (/ 29), nebo spočítat všechny nuly), převraťte masku zástupného znaku.

access-list 10 permit ip 172.16.1.32 0.0.0.7

Standardní pojmenovaný seznam ACL

To je seznam ACL, který je konfigurován jménem (v tomto případě internet) místo čísla. Má stejná pravidla jako standardní očíslované ACL. Následující seznam ACL s názvem internet odepře veškerý provoz ze všech hostitelů v podsíti 192.168.1.0/24. Kromě toho bude protokolovat všechny pakety, které byly zamítnuty.

```
ip access-list internet log
deny 192.168.1.0 0.0.0.255
permit any
```

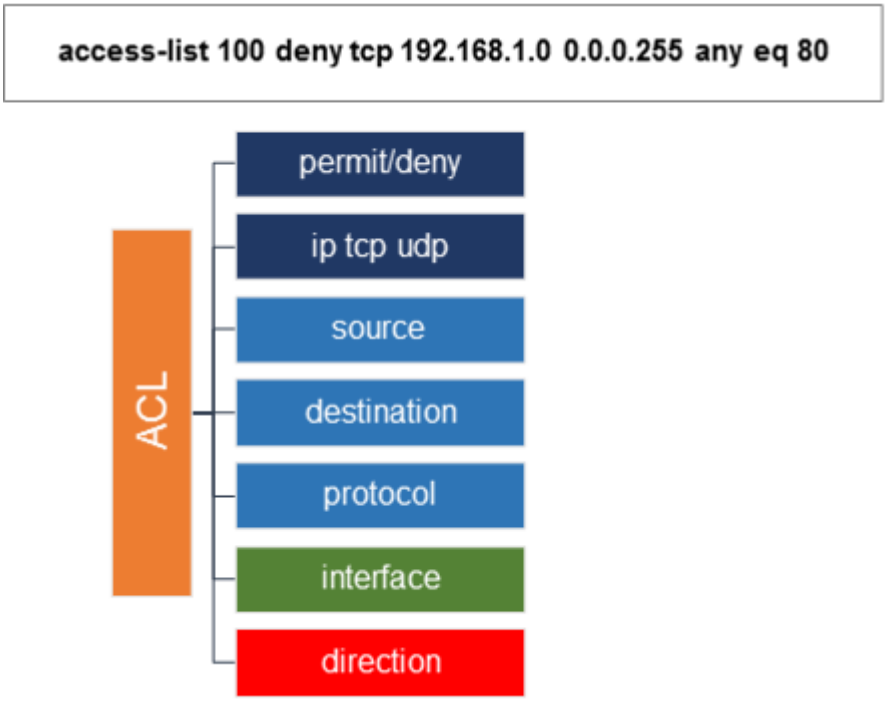
Pojmenované seznamy ACL umožňují dynamické přidávání nebo mazání příkazů ACL, aniž byste museli mazat a přepisovat všechny řádky. Samozřejmě je také vyžadováno menší využití CPU. Snadněji se spravují a řeší problémů se sítí. Slovo **log** znamení, že se bude použití pravidel zaznamenávat.

Rozšířený očíslovaný seznam ACL

Rozsah čísel je od 100 do 199 a od 2000 do 2699. Podporuje více příkazů pro permit a deny se zdrojovou a / nebo cílovou IP adresou. Kromě toho můžete filtrovat podle protokolu IP, TCP nebo UDP založeného na aplikaci nebo čísla portu.

Existuje implicitní skryté odmítnutí **deny any any** přidané na konec libovolného seznamu ACL. Proto musíte jako poslední dát do seznamu ACL povolení **permit ip any any**. To účinně povoluje všechny pakety, které neodpovídají žádnému předchozímu ACL. Některé seznamy ACL se skládají pouze z příkazů **deny**, takže bez posledního **permit ip any any** by byly všechny pakety zahozeny.

Příklad 8 Extended ACL



Příklad 9: Extended ACL

Následující příkaz povoluje http provoz z hostu (počítače) o adrese 10.1.1.1 k hostu s adresou 10.1.2.1.

access-list 100 permit tcp host 10.1.1.1 host 10.1.2.1 eq 80

Příkaz seznamu řízení přístupu (ACL) čte zleva doprava jako - povolte veškerý přenos tcp ze zdrojového hostitele pouze do cílového hostitele, který je http (80). TCP odkazuje na aplikace založené na TCP. Klíčové slovo UDP se používá pro aplikace založené na UDP, například SNMP.

Příklad 10: Extended ACL

Jaký je efekt použití následujícího seznamu ACL?

access-list 100 deny ip host 192.168.1.1 host 192.168.3.1
access-list 100 permit ip any any

První příkaz popírá veškerý (all) provoz aplikace z hostitele-1 (192.168.1.1) na webový server (hostitele 192.168.3.1). Klíčové slovo **ip** odkazuje na vrstvu 3 a ovlivňuje všechny protokoly a aplikace ve vrstvě 3 a vyšší. Poslední příkaz je vyžadován k povolení veškerého jiného provozu, který se neshoduje

Příklad 11: Extended ACL

Jaký je účinek použití následujícího seznamu ACL?

access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq telnet
access-list 100 permit ip any any

První příkaz povoluje provoz Telnetu ze všech hostitelů přiřazených k podsíti podsítě 192.168.1.0/24. Klíčové slovo **tcp** je vrstva 4 a ovlivňuje všechny protokoly a aplikace na vrstvě 4 a vyšší. Konfigurace **permit tcp** umožňuje specifikovanou aplikaci TCP (Telnet). Libovolné klíčové slovo umožňuje relace Telnetu libovolnému cílovému hostiteli. Poslední prohlášení je povinné a vyžaduje se k povolení veškerého dalšího provozu.

Příklad 12: Extended ACL

Jaký je účinek použití následujícího seznamu ACL?

access-list 100 permit ip 172.16.1.0 0.0.0.255 host 192.168.3.1
access-list 100 deny ip 172.16.2.0 0.0.0.255 any
access-list 100 permit ip any any

- První příkaz ACL umožňuje pouze hostitelům přiřazeným k podsíti 172.16.1.0/24 přístup ke všem aplikacím na serveru (192.168.3.1).
- Druhý příkaz odepírá hostitelům přiřazeným k podsíti 172.16.2.0/24 přístup k jakémukoli serveru. To by zahrnovalo všechny další hostitele přidané do této podsítě a všechny nové servery přidané.
- Poslední příkaz ACL je vyžadován, aby umožnil veškerý další provoz neodpovídající předchozím příkazům filtrování.
- ACL se aplikuje na rozhraní s příkazem **ip access-group**. Většina směrovačů má často více rozhraní (podsítí) s přiřazenými hostiteli. ACL použité jako odchozí (outbound) na rozhraní sdílené více podsítěmi bude filtrovat provoz ze všech hostitelů v každé podsíti.

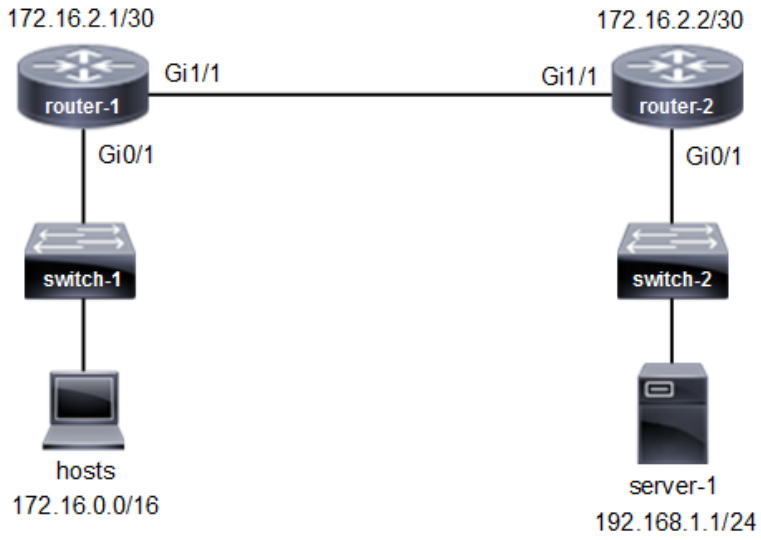
Tabulka 1 Čísla nejznámějších portů aplikací a klíčová slova ACL

Application	Port	ACL
FTP	TCP 21	**ftp**
SSH	TCP 22	**ssh**
Telnet	TCP 23	**telnet**
DNS	TCP | UDP 53	**domain**
TFTP	UDP 69	**tftp**
HTTP	TCP 80	**www**
NTP	UDP 123	**ntp**
SNMP	UDP 161	**snmp**
HTTPS	TCP 443	**https**

Podívejte se na schéma sítě. Následující seznam ACL byl nakonfigurován jako příchozí (inbound) na rozhraní routeru-1 Gi0/1. Jaký bude účinek?

access-list 100 deny tcp any host 192.168.1.1 eq 21
access-list 100 permit ip any any

Příklad 13 Extended ACL



Odpověď

Následující rozšířený seznam ACL zakáže veškerý přenos FTP z jakékoli podsítě určené pro server-1.

access-list 100 deny tcp any host 192.168.1.1 eq 21
access-list 100 permit ip any any

- Rozšířené číslování ACL 100-199 a 2000-2699
- FTP = TCP aplikační port 21
- Klíčové slovo ACL ftp (alternativní)
- ACL popírá veškerý další provoz explicitně s posledním příkazem

Příklad 14: Rozšířený seznam ACL

Viz následující konfigurace routeru. ACL 100 není správně nakonfigurován a odepírá veškerý provoz ze všech podsítí. Jaký příkaz na úrovni rozhraní IOS okamžitě odstraní účinek ACL 100?

access-list 100 deny tcp 172.16.0.0 0.0.255.255 any eq 80
access-list 100 deny ip any any

router# **show ip interface gigabitethernet 1/1**

GigabitEthernet1/1 is up, line protocol is up
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is **100**
Inbound access list is not set
Proxy ARP is enabled

Odpověď

Pro kontrolu a filtrování veškerého provozu musí být na rozhraní použito ACL. ACL se aplikuje s příkazem IOS rozhraní **ip access-group 100 out**. Odebrání filtrování vyžaduje odstranění příkazu **ip access-group** z rozhraní. Existuje podpora pro zadání čísla nebo jména ACL. Příkaz **access-class in | out** filtruje pouze VTY line.

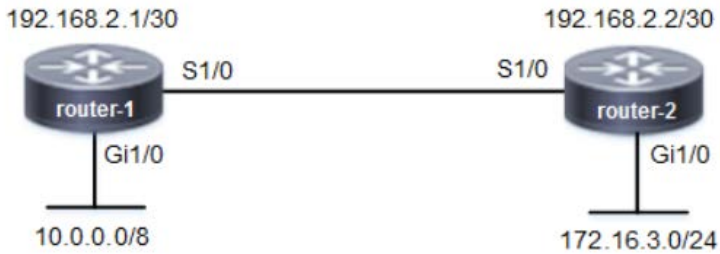
V | klíčové slovo **in | out** určuje směr rozhraní k filtrování paketů. Výstup z příkazu **show ip interface** uvádí seznam ACL a směr nakonfigurovaný pro rozhraní. Na rozhraní Gi1 / 1 je použit odchozí ACL 100.

router(config)# **interface gigabitethernet1/1**
router(config-if)# **no ip access-group 100 out**

Příklad 15: Extended ACL

Podívejte se na schéma topologie sítě. Jaké jsou správné příkazy pro konfiguraci následujícího rozšířeného seznamu ACL?

- Odepřít provoz Telnetu z 10.0.0.0/8 podsítí na router-2.
- Odepřít provoz HTTP z 10.0.0.0/8 podsítí do všech podsítí.
- Povolit veškerý další provoz, který se neshoduje.



Řešení

access-list 100 deny tcp 10.0.0.0 0.255.255.255 host 192.168.2.2 eq 23
access-list 100 deny tcp 10.0.0.0 0.255.255.255 any eq 80
access-list 100 permit ip any any

Další na

https://community.cisco.com/t5/networking-documents/access-control-lists-acl-explained/ta-p/4182349