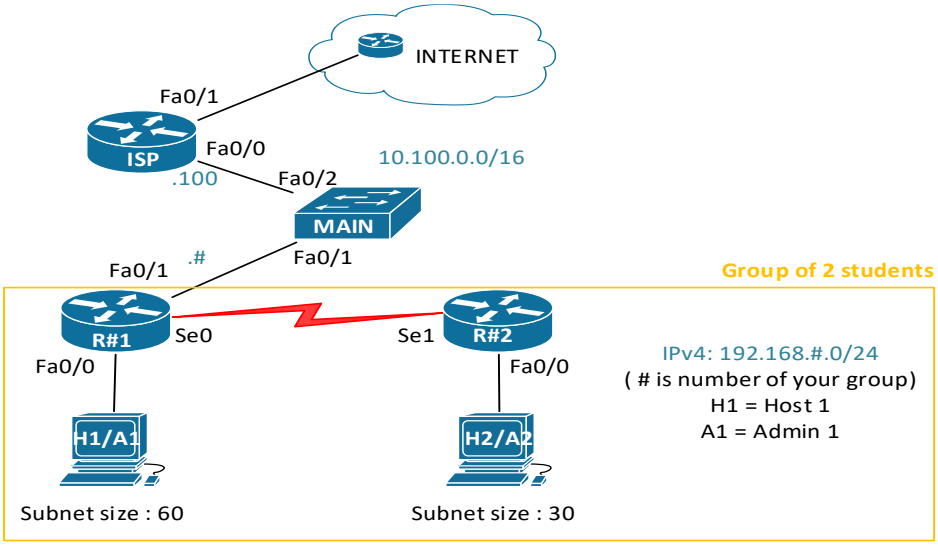
PS1 / Cvičenie 08 / **ACLs**

Topológia



Dôležité upozornenia:

A. Vždy je dôležité rozhodnúť **kde** je najvhodnejšie daný ACL **aplikovať** !
B. **Pred** aplikovaním ACL je treba otestovať či máte požadovanú **konektivitu**! Pri testoch si budete meniť IP adresu na PC, podľa toho, akú prevádzku budete chcieť otestovať.
C. Všetky ACL bude vytvárať **každý** študent a aplikovať ich budú v dvojici vždy **po jednom**, vždy nový ACL nasadíte až potom, ako predošlý odstránite (nie z konfigurácie, len z daného rozhrania).
D. Tiež sa vždy **dohodnite s kolegom** vo dvojici (trojici), kto bude v ktorom čase testovať svoje ACLs, aby ste sa navzájom **nerušili**, nekazili si testy.
E. Využite možnosť logovania správ zachytených na danom ACL tak, aby sa vám zobrazovali na **console**. (pridaj „**log**“ na konci pravidla).
F. Na koniec ACL tam kde sa hodí (kde potrebujete zakázať všetku ostatnú prevádzku), vždy explicitne napíšte **`deny any`**, aby ste videli počet využití daného pravidla (matches v `show ip access`...)
G. Nezabudnite na PCs použiť aj **DNS**, napr. **8.8.8.8**, aby ste mohli testovať aj prístup na web.
H. Do svojho reportu z cvičenia si ukladajte:
   - **runnin-config** - tú časť kde sa "hovorí o ACL" (stačí na záver cvičenia)
   - výsledky **testovania** daného ACL (ping, ...), že zakázal/povolil čo mal
   - na záver posledného ACL výpis: **show ip access list**
I. Učiteľ nakonfiguruje ISP smerovač a budete mať pripojenie do internetu (config máme na Moodle, max. pre 9 skupín).

Postup:

1. **Subsieťujte pridelený IPv4 rozsah pre svoju topológiu s 2 smerovačmi a 2 PCs:**
   a. Subsieťujte pridelený IPv4 rozsah: 192.168.#.0/24.
   b. Počítačom prideľujte IP adresu od najnižšej, smerovačom od najvyššej IP.
2. **Základná konfigurácia**
   a. Najprv si nechajte smerovače nabootovať, až potom zapájajte kabeláž!
      i. Pozn.: Hostname smerovača „DHCP-...“ znamená že ste robili najprv káblovanie, až potom bootovanie.
   b. Nastavte hostname R#1, R#2
   c. Pre efektívnosť práce nastavte:
      i. Zabráňte na prepínačoch výpis hlášok do písaného textu na konzole (zmiešavanie vstupu a výstupu CMD) `(line console 0, logging synchronous)`
      ii. Vypnite prekladanie doménových mien na IP adresy `(no ip domain-lookup)`
   d. Nastavte RIPv2, aby ste mali konektivitu medzi PCs, smerom do Internetu nastavte defaultnú statickú cestu a oznamujte ju v RIP doméne.
   e. Otestujte konektivitu medzi sebou aj do Internetu, až potom rieš nasledovné ACL.
3. **Štandardný číslovaný ACL – zákaz vstupu celej LAN**
   a. Pozn.: Tento aj všetky ďalšie ACL riešte každý za seba na svojom smerovači, ale nasadzujte ich v kooperácií s kolegom v dvojici – t.j. najprv. jeden študent, nasadí, otestuje, odoberie z rozhrania, potom druhý študent, nasadí, otestuje, a odoberie z rozhrania.
   b. Vytvorte ACL, v ktorom zakážte celej susednej LAN (tvoj kolega v dvojici) prístup do svojej LAN, všetko ostatné povoľte. Použite číslovaný štandardný ACL číslo 3.
   c. Nasaďte (aplikujte na vhodné rozhranie vo vhodnom smere in/out) a otestujte vytvorené ACL, že funguje:
      i. Host zo susednej LAN sa nevie pingnúť do vašej LAN.
      ii. Host zo susednej LAN môže ísť do Internetu
      iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
      iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)
   d. Na záver odoberte dané ACL z rohrania, ale nemažte dané ACL z konfigurácie (toto spravíte aj po každom ďalšom ACL).
4. **Štandardný pomenovaný ACL – zákaz vstupu celej LAN, okrem admina**
   a. Zakážte celej susedovej LAN (v dvojici) prístup do svojej LAN, iba adminovi zo susednej LAN prístup povoľ. Všetko ostatné nech je povolené. Použi pomenovaný štandardný ACL s menom: U4_BLOKUJ_LANx_OKREM_ADMINA
   b. Nasaďte a otestuj vytvorený ACL, že funguje:
      i. Admin sa vie pingnúť do danej LAN, aj mu ide konekt do Inetu.
      ii. Host sa nevie pingnúť do danej LAN (využi Wireshark a pozri sa čo príde ako odpoveď cez ICMP - hľadaj... Communication Administratively Filtered...) , ale ide mu konektivita do Internetu
      iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
      iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)
   c. Uprav daný ACL tak, aby povolenie platilo aj pre druhého admina (o 1 vyššia IP adresa). Nemaž celý ACL, iba doplň pravidlo na správne miesto do súčasného ACL.
   d. Otestuj vytvorený ACL, že funguje
      i. Obaja adminovia sa vedia pingnúť do vašej LAN, aj do Inetu
         - Toto nasimuluj tým, že si zmeníš IP adresu na PC.

ii. Host sa nevie pingnúť do vašej LAN, ale ide mu konektivita do Inetu
iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)

5. **Štandardný pomenovaný ACL – zákaz vstupu pre jedného hosta**
   a. Zistili ste, že jedna zo staníc v susednej podsieti (Host), ktorá je pod správou iného administrátora (váš spolužiak z dvojice) je zdrojom mnohých problémov, ktoré ste museli v poslednej dobe vo vašej lokálnej podsieti odstraňovať. Zakážte tomuto hostovi akýkoľvek vstup do vašej siete (zakážte všetky porty). Všetko ostatné má byť povolené. Použi štandardný ACL s menom: U5_BLOKUJ_1HOSTA
   b. Otestuj vytvorený ACL
      i. susedov host sa nevie pingnúť do vašej siete.
      ii. susedov admin má plný prístup... otestuj ping
      iii. susedov smerovač má plný prístup do vašej siete, otestuj ping.
6. **Štandardný pomenovaný ACL – zakáž telnet aj SSH na svoj smerovač pre prvú polovicu LAN**
   a. Vytvorte ACL, ktorý zakáže **iba klientským** staniciam TELNET prístup na router, ktorý je ich bránou do internetu, t.j. adminom prístup povolí.
      i. Uvažujte, že admini majú IP adresy z prvej polovice a klienti z druhej polovice LAN.
      ii. Použite štandardný ACL aplikovaný na rozhranie vty s menom: U6_ZAKAZ_TELNETaSSH_NA_BRANU
   b. Otestujte funkčnosť ACL
      i. Klient (=host) sa nevie pripojiť na svoj smerovač cez telnet ani ssh.
         - Pre testovanie vaše PC musí mať IP adresu z druhej polovice LAN.
      ii. Admin sa pripojí cez telnet aj ssh.
         - Pre testovanie si zmeňte IP adresu PC tak, aby bola z prvej polovice.
      iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
      iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)
7. **Rozšírený číslovaný ACL – zakáž prístup na WWW a TFTP servery v LAN**
   a. Ešte pred tvorbou ACL, overte ukladanie konfigurácie na TFTP server - použite TFTPd utilitu na ploche vášho PC (vyskúšajte obaja zrkadlovo):
      i. Na strane TFTPd servera:
         - Spustite TFTPd utilitu ako admin
         - Nastavte priečinok pre ukladanie súborov na ... \Student
         - Vyber si IP adresu na ktorej beží TFTPd server na IP adresu svojho PC (Cisco NIC)
      ii. Klientom bude kolegov smerovač
         - Uložte konfiguráciu zo smerovača na daný TFTP server príkazom:
            - copy running-config tftp
            - potom zadáte IP adresu TFTP servera (vaše PC)
            - zadáte názov súboru (alebo potvrdíte enter, čo vám smerovač ponúkne ako názov)
            - ak všetko prejde OK, výstup bude: !!
   b. Zistili ste, že niektorí klienti vo vašej LAN sieti si nainštalovali WWW a TFTP server. Z hľadiska bezpečnosti vašej sieti je to neprípustné. Aby ste predišli riziku, zakážete prístup **zvonku** (odkiaľkoľvek) do vašej siete (t.j. na akýkoľvek IP) na tieto služby.
      i. Použite rozšírený číslovaný ACL s č. 107
   c. Otestujte funkčnosť ACL:
      i. ping z PC v susednej LAN na niektorý PC vo vašej LAN – prejde OK

ii. PC v susednej LAN sa nevie pripojiť na TFTP server na počítači vo vašej LAN (použite TFTPd utilitu na ploche vášho PC)
iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)

d. Uprav daný ACL tak, že prístup na WWW a TFTP bude povolený iba na jednu vyhradenú IP adresu vo vašej LAN. Následne otestuj funkčnosť.
i. Znova ti bude fungovať uloženie configu na TFTP server, over.
ii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
iii. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)

8. Rozšírený pomenovaný ACL – zakáž 1 hostovi z LAN prístup do Inetu.. povoľ mu len http

a. Nové použitie jednej zo staníc (**Host**) vo vašej sieti, vás prinútilo nastaviť prísnejšie obmedzenia. Vytvorte také pravidlo, ktoré bude povoľovať danej stanici prístup na Internet len cez HTTP a HTTPs a všetky ostatné porty mu zakáže. Všetko ostatné má ostať povolené.
i. Použite názov ACL: U8_POVOL_IBA_WEB_1HOSTOVI

b. Otestujte funkčnosť ACL:
i. Admin z vašej podsiete môže pristupovať do Internetu cez FTP (nájdite si akýkoľvek otvorený FTP server na Internete, pre testovanie)
ii. Jeden daný host z vašej podsiete:
- nemôže pristupovať cez FTP do Internetu
- môže browsovať po Internete

iii. Pozrite počet „matches“ vo výpise ACL (sh access-lists ...)
iv. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)

9. Riešte nasledovný firewall pomocou dvoch ACLs pre dva smery komunikácie (DO/VON z LAN):

a. Smer VON z vašej lokálnej siete:
i. Povoľte prístup na službu Remote Desktop Protocol (TCP/3389) v rámci celej topológie
ii. Povoľte odpovede na službu Remote Desktop Protocol odchádzajúce z LAN siete
iii. Prístup na službu http (TCP/80) povoľte len na susedný smerovač
iv. Službu PING (ICMP echo) do celej topológie povoľte len stanici s poslednou použiteľnou IP adresou v LAN sieti
v. Voľte politiku – čo nie je povolené, je zakázané

b. Smer DO lokálnej siete:
i. Povoľte vstup odpovedí na TCP spojenia vychádzajúce zvnútra LAN siete (nápoveda: ... established)
ii. Povoľte prístup na službu Remote Desktop Protocol na počítače v LAN sieti
iii. Povoľte zodpovedajúce prichádzajúce ICMP odpovede
iv. Voľte politiku – čo nie je povolené, je zakázané

c. Premyslite ako tento ACL otestujete, aby ste overili funkčnosť, a pozrite počet „matches“ vo výpise.
d. Spravte si záznam týchto výsledkov do reportu do wordu (print screen, alebo copy)

10. Zvýšte bezpečnosť RIP protokolu blokovaním RIP updatov na rozhraní zo svojej LAN

a. Ak ešte nemáte, nastavte vhodné rozhrania na smerovači ako pasívne. To vás ale neochráni proti útokom, pri ktorých by útočník z LAN generoval falošné smerovacie informácie. Preto vytvorte ACL, ktorý bude blokovať RIP updates prichádzajúce na ethernetové rozhranie z vašej LAN (UDP/520).
i. Keby ste pripojili na prepínač vo vašej LAN nejaký PC, z ktorého by ste vygenerovali útok – podvrhnutie smerovacej informácie vášmu smerovaču, videli by ste, či vás

dané ACL pred týmto útokom ochráni (použiť na ukážku môžete aj prídavný smerovač, ktorý bude mať spustené RIP a nejakú LAN sieť na loopback rozhraní).

11. ACL pre filtrovanie paketov v príkaze debug (možno ponechať na budúce cvičenie, kedy sa bude robiť DHCP)

a. Predpokladajte, že vo vašej lokálnej sieti nemáte IP adresy pre hostov pridelené staticky, ale žiadate ich od DHCP servera, ktorým je smerovač, ktorý je zároveň ich bránou do internetu. Chcete si nechať zobrazovať správy o všetkých paketoch, ktoré si vymieňajú DHCP server s ľubovoľným klientom (hostom).

Vytvorte preto ACL pre filtrovanie IP paketov pre príkaz:
debug ip packet <cislo_vaseho_ACL>

Príkaz **debug ip packet** vám zobrazí všetky pakety prichádzajúce alebo odchádzajúce z vašeho smerovača. Vašou úlohou je ale nechať si vypisovať informácie iba o IP paketoch, ktoré sa prenášajú medzi DHCP serverom a ľubovoľným DHCP klientom (správy DHCP Discovery, Offer, Request, Acknowledgment - viac bude na prednáške o DHCP a na budúcom cvičení). DHCP komunikácia medzi serverom a klientmi sú nespojovo orientované, t.j. používajú UDP ako transportný protokol, pričom pre posielanie dát od klienta na server sa používa **UDP port 67**, a pre posielanie dát zo servera ku klientovi sa používa **UDP port 68**. (pozn.: DHCP používa rovnaké dve čísla portov, ktoré sú pridelené organizáciou IANA pre protokol bootp)