13 Konfigurácia Zone-Based Policy Firewall-u na Cisco smerovači

Cieľom tejto kapitoly je na jednoduchom príklade ukázať konfiguráciu ZPF (angl. Zone Based Policy Firewall-ov).

13.1 Základná teória k ZPF

ZPF umožňujú vytvárať komplexné konfiguračné pravidlá. Významovo sú podobné ako prístupové zoznamy, avšak ich aplikácia sa vykonáva vzhľadom k zónam a nie rozhraniam, čo značne zvyšuje flexibilitu konfigurácie a tiež jej udržateľnosť. Konfigurácia je rozdelená do 4 logických častí a to:

- **Class-map**: Umožňuje identifikovať prevádzku.
- **Policy-map**: Umožňuje definovať pravidlá komunikácie.
- **Zone-pair**: Umožňuje definovať komunikačný kanál medzi zónami.
- **Zone**: Umožňuje priradenie rozhraní do logických častí - zón.

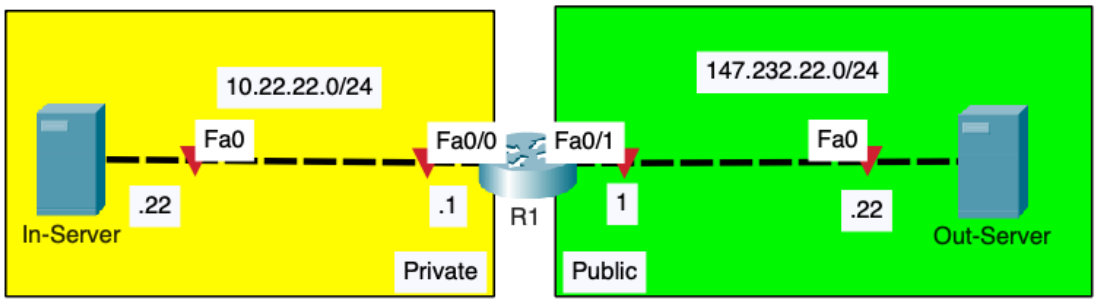
13.2 Topológia a úlohy

Konfigurácia bude demonštrovaná na jednoduchej topológii obsahujúcej jeden smerovač a dvojicu serverov, kde jeden server sa nachádza vo vnútornej zóne a druhý vo vonkajšej. Z pohľadu bezpečnosti je požiadavka zabezpečiť nasledujúce pravidlá pre komunikáciu:

1. Umožniť ICMP komunikáciu z vnútornej siete na akúkoľvek sieť v internete.
2. Umožňiť webovú komunikáciu z vnítra siete len na server Out-Server.

Z pohľadu pravidiel žiadna ďalšia komunikácia povolená nebude, čo nijak implementovať netreba, keďže čo nie je povolené, je zakázané. Štandardne pri implementácii ZPF je potrebné povoľovať komunikáciu v oboch smeroch zvlášť (pri pravidle **pass** a **deny**). Pri použití pravidla **inspect** je automaticky povolená odpoveď na povolenú komunikáciu, čo pre jednoduchosť bude využité pri riešení uvedených úloh.

Obr. 13.1 znázorňuje demonštračnú topológiu.



Obr. 13.1: Logická topológia

Všetka konfigurácia sa bude vykonávať na smerovači R1. Pred konfiguráciou ZPF je ale najskôr potrebné nakonfigurovať sieťové nastavenia na koncové zariadenia a samotný smerovač podľa údajov uvedených v topológii. Nasledujúci výpis 13.1 znázorňuje konfiguráciu smerovača a zariadení In-Server a Out-Server.

```
In-Server
  Adresa: 10.22.22.22
  Maska: 255.255.255.0
  Brana: 10.22.22.1

Out-Server
  Adresa: 147.232.22.22
  Maska: 255.255.255.0
  Brana: 147.232.22.1

R1:
  hostname R1
  interface fa0/0
    ip add 10.22.22.1 255.255.255.0
    no shutdown
  interface fa0/1
    ip add 147.232.22.1 255.255.255.0
    no shutdown
```

Zdrojový kód 13.1: Základná konfigurácia

13.3 Konfigurácia ZPF

Konfigurácia ZPF bude pozostávať z konfigurácie 4 hlavných logických častí, ktoré sú bližšie opísané v nasledujúcich sekciách.

13.3.1 Identifikácia prevádzky

Na identifikáciu prevádzky bude použitý rozšírený prístupový zoznam, napr. s číslom 122. Pozor, v tomto prípade ACL nerozhoduje o tom, či komunikácia bude preposlaná alebo zakázaná, v tomto prípade permit v ACL znamená identifikovanie prevádzky a deny znamená neidentifikovanie prevádzky. Daný prístupový zoznam bude následne použitý v Class-map-e s názvom CM. Výpis 13.2 znázorňuje potrebnú konfiguráciu.

```
1 ! Identifikacia prevadzky vyuzitim ACL
2 access-list 122 permit icmp 10.22.22.0 0.0.0.255 any
3 access-list 122 permit tcp 10.22.22.0 0.0.0.255 host 147.232.22.22
4
5 ! Vytvorenie class-map - identifikacia prevadzky
6 class-map type inspect match-all CM
7   match access-group 122
```

Zdrojový kód 13.2: Identifikácia prevádzky

Ako si je možné všimnúť vo vzorovej konfigurácii, tak Class-map-a umožňuje identifikovať viacero parametrov pre identifikáciu prevádzky, pričom ich je možné logicky vyhodnocovať nasledovne:

- **match-all**: Všetky atribúty v class-map-e musia identifikovať daný paket.
- **match-any**: Aspoň jeden atribút v class-map-e musí identifikovať daný paket.

Paket môže byť identifikovaný parametrami v ACL, ale môže byť tiež použité kľúčové slovo **protocol**, ktorým sa identifikuje typ protokolu.

13.3.2 Definovanie politík

Po identifikácii prevádzky je na ňu možné aplikovať komunikačné pravidlá. Pravidlá, ktoré je možné definovať sú nasledovné:

- **pass**: Automatické povolenie komunikácie v jednom smere.
- **drop**: Automatické zakázanie komunikácie v jednom smere.

- **inspect**: V prípade povolenia komunikácie automatické povolenie odpovedí.

Nasledujúca konfigurácia 13.3 znázorňuje vytvorenie policy-map-y s názvom PM.

```
! Definovanie politik
policy-map type inspect PM
  class type inspect CM
    inspect
```

Zdrojový kód 13.3: Definovanie politík

13.3.3 Vytvorenie zón a zónového páru

Teraz je potrebné vytvoriť dvojicu zón, v našom prípade s názvami Private a Public. Medzi týmito zónami bude následne vytvorený komunikačný kanál v podobe zónového páru s názvom ZP. Nasledujúci výpis 13.4 znázorňuje vzorovú konfiguráciu pre túto úlohu.

```
! Vytvorenie zon:
zone security Private
zone security Public

! Vytvorenie zonoveho paru
zone-pair security ZP source Private destination Public
  service-policy type inspect PM

```

Zdrojový kód 13.4: Vytvorenie zón a zónového páru

13.3.4 Priradenie rozhraní do zón

Posledným krokom je priradenie fyzických rozhraní do zón, pričom do Private zóny bude priradené rozhranie Fa0/0 a do Public zóny rozhranie Fa0/1. Výpis 13.5 znázorňuje vzorovú konfiguráciu pre riešenie tohto kroku.

```
! Priradenie rozhrani do zon
int fa0/0
  zone-member security Private
int fa0/1
  zone-member security Public
```

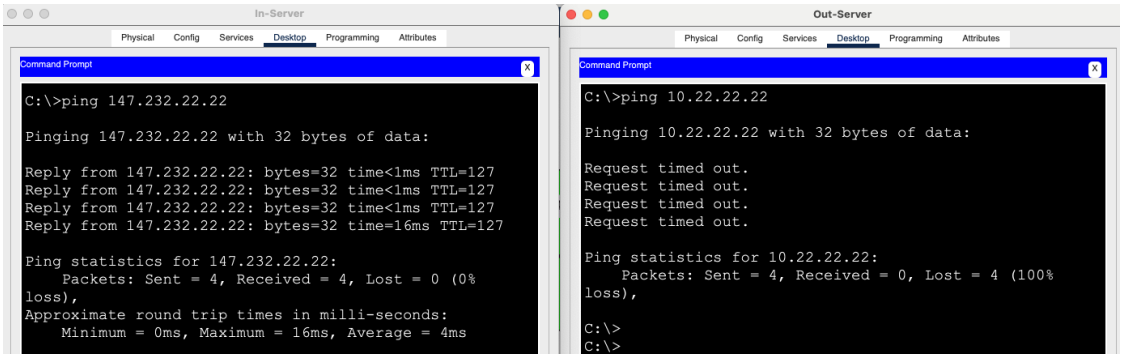
Zdrojový kód 13.5: Priradenie rozhraní do zón

13.4 Overenie úspešnosti splnenia úloh

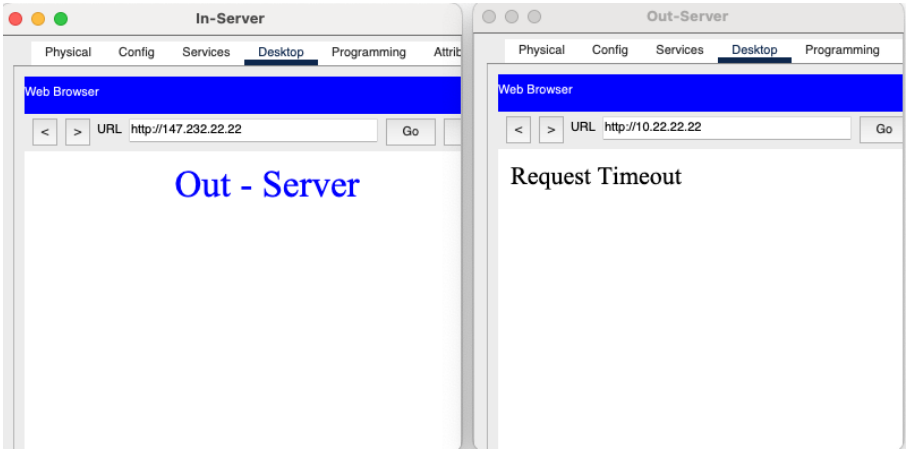
V tejto chvíli je možné overiť úspešnosť konfigurácia vykonaním nasledujúcich testov:

- Ping zo zariadenia In-Server na Out-Server bude úspešný no v opačnom smere ping úspešný nebude.
- Webová komunikácia zo zariadenia In-Server na Out-Server bude úspešná, no v opačnom smere webová komunikácia úspešná nebude.

Úspešnosť prvej úlohy je znázornená na obr. 13.2 a úspešnosť druhej úlohy je znázornená na obr. 13.3.



Obr. 13.2: Overenie úspešnosti prvej úlohy - ICMP



Obr. 13.3: Overenie úspešnosti druhej úlohy - WEB

Odporúčanie do vzdelávacieho procesu je, že najskôr je vhodné implementovať len prvý príkaz v ACL, čím bude identifikovaná len ICMP komunikácia. Následne overiť úspešnosť komunikácie a uistiť sa, že webová komunikácia úspešná nebude v žiadnom smere. Následne je možné pridať aj druhý záznam do ACL a overiť finálny stav úspešnosti splnenia úloh.