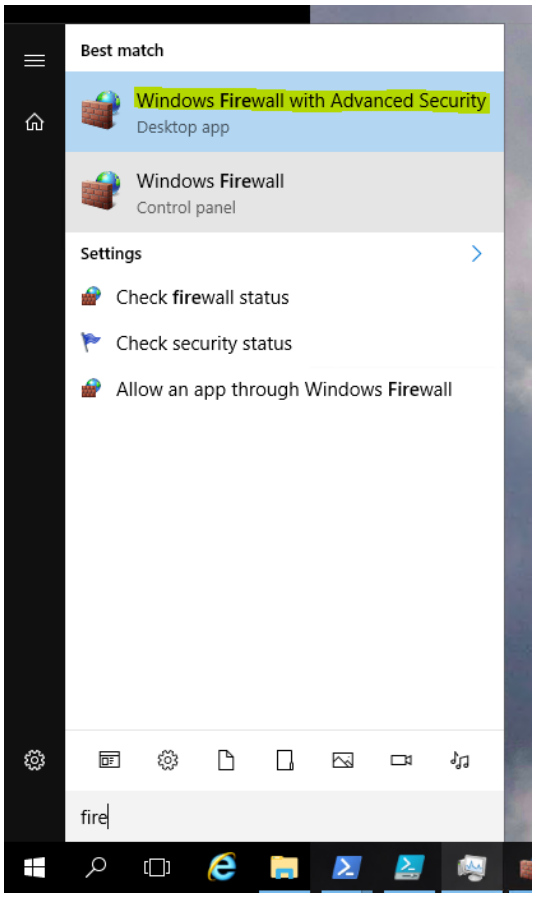
Konfigurácia Windows Firewall – standalone vs. AD domain

V rámci prostredia Microsoft Active Directory môžeme spravovať Windows Firewall (FW) 2 spôsobmi. V prvom prípade sa k zariadeniam v rámci domény môžeme postaviť ako k samostaným celkom a FW spravovať pomocou lokálnych pravidiel. V nasledujúcom popise si uvedieme postup pridania lokálnych FW pravidiel.

Konfigurácia FW pomocou lokálnych pravidiel

1. Spustíme consolu ***Windows Firewall with advanced security***



2. Na úvodnej obrazovke môžeme vidieť prehľad nastavení FW. V rámci FW pracujeme s 3 profilmi:
    a. Domain Profile – používa sa v prípade členstva PC v doméne
    b. Private Profile – zohľadňuje nastavenie sieťového adaptera (verejná/privátna sieť)
    c. Public Profile - zohľadňuje nastavenie sieťového adaptera (verejná/privátna sieť)

    https://technet.microsoft.com/en-us/library/cc731634(v=ws.11).aspx

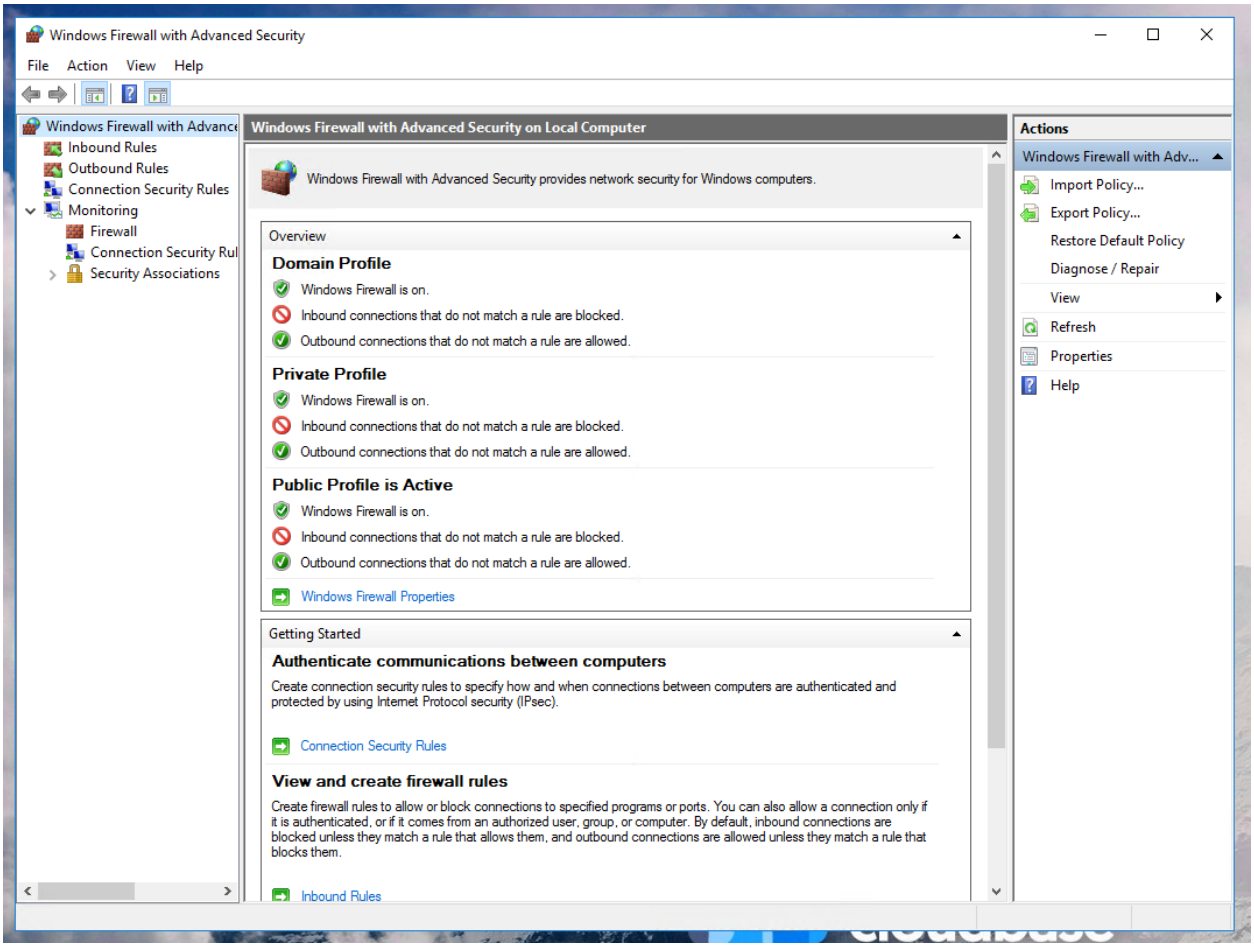
    Aktívny profil je označený, napr. P*ublic profile is Active*. Okrem profilov nas zaujímajú ešte nastavenia pravidiel. Pravidlá su rozdelené do 2 skupín:

a. Inbound rules – Komunikácia smerujúca na server
b. Outbound rules – Komunikácia smerujúca zo serveru

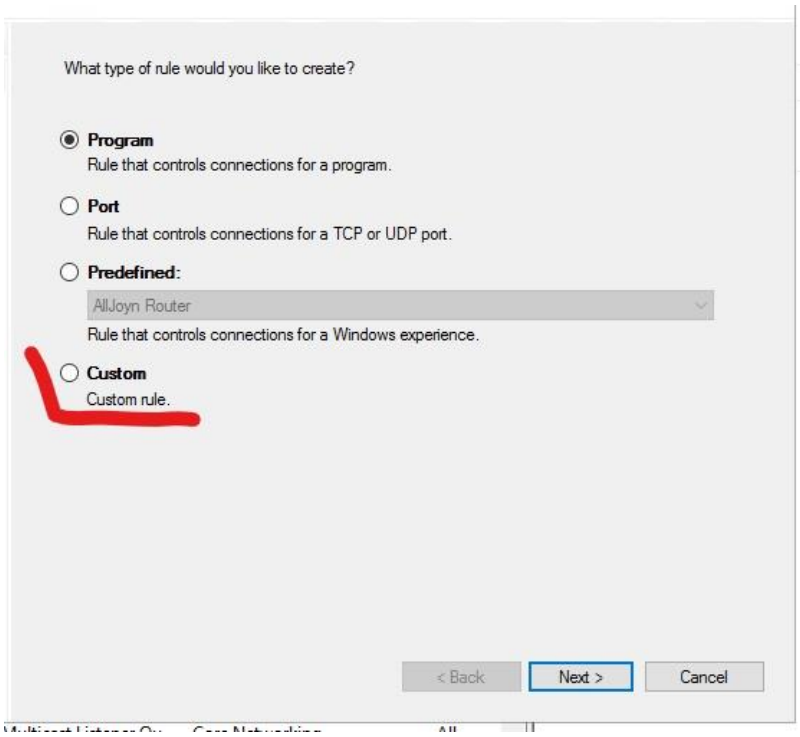
Vyššie popísane časti umožňujú špecifikovať lokálne pravidla. V rámci doménoveho prostredia môžu byť pravidlá kombinované:

a. Aplikujú sa len lokálne pravidla
b. Aplikujú sa lokálne + Doménou (GPO) nastavené pravidla
c. Aplikujú sa len doménove pravidla

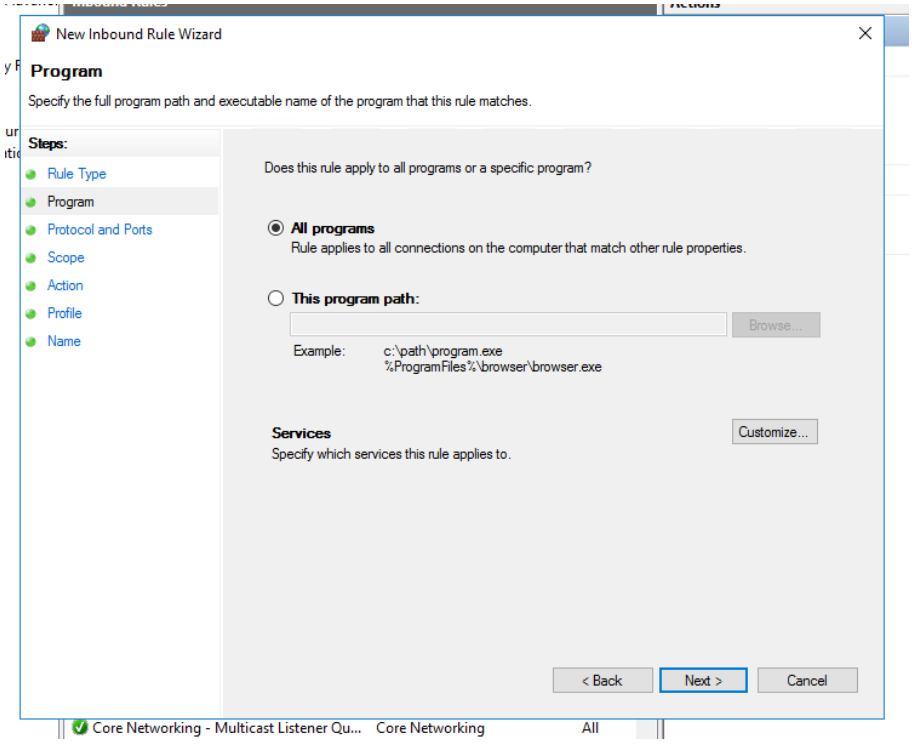
Záložky ***Inbound*** a ***Outbound*** rules zobrazujú všetky dostupné pravidla za každých okolnosti. V prípade, že chceme zistiť, ktoré pravidla sa reálne aplikujú podľa nastavení PC (Doménové vs. lokálne) môžeme použiť záložku ***Monitoring/Firewall***, ktorá zobrazuje len aplikované pravidla.



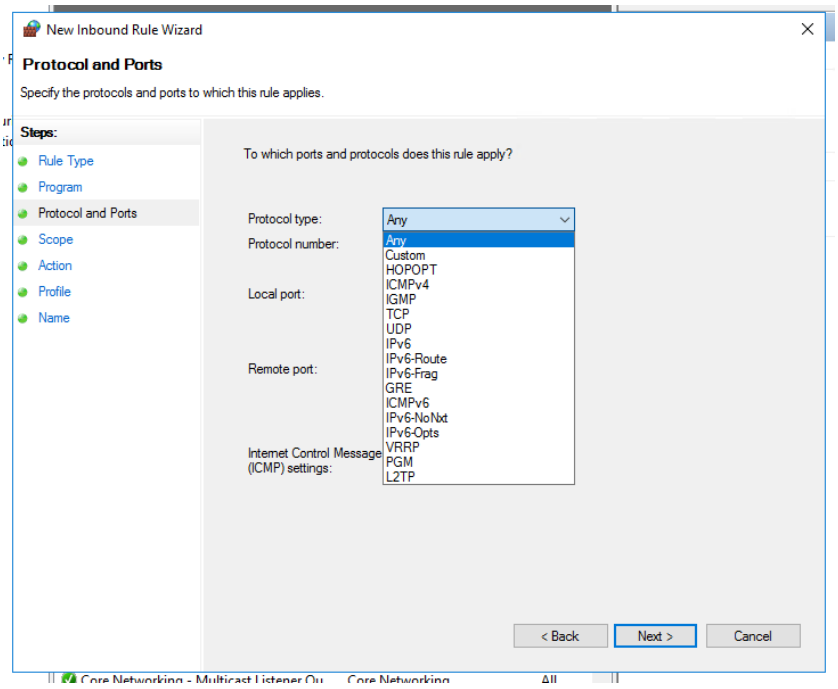
3. Pravidlo upravujúce chovanie FW môžeme pridať nasledujúcim spôsobom:
    a. Pravým kliknutím na ***Inbound*** alebo ***Outbound rules*** a následne možnosť ***New rule***
    b. V ďalšom kroku zvolíme, či chceme použiť preddefinované pravidlo, pridať výnimku pre program, alebo port, prípadne vytvoriť vlastné pravidlo. V nasledujúcej časti využijeme možnosť pridať vlastné pravidlo.



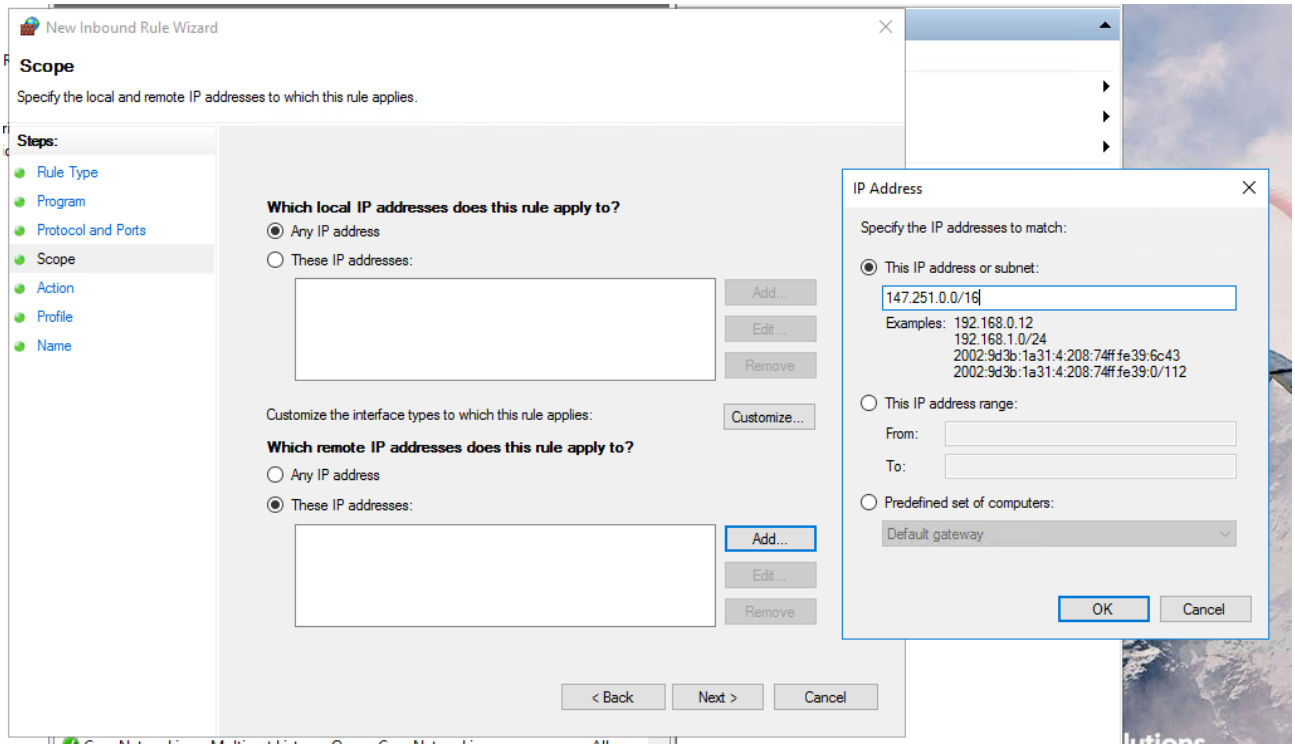
c. Vyberieme typ výnimky, pre ktorú aplikujeme pravidlo: všetky programy/špecifický program/služba



d. Zvolíme typ komunikácie, pre ktorú bude pravidlo platiť. Napr. ***TCP -> specific remote port -> 3389***



e. Nastavíme rozsahy IP adries, pre ktoré aplikujeme pravidlo. Pozor na zámenu local vs. Remote IP.



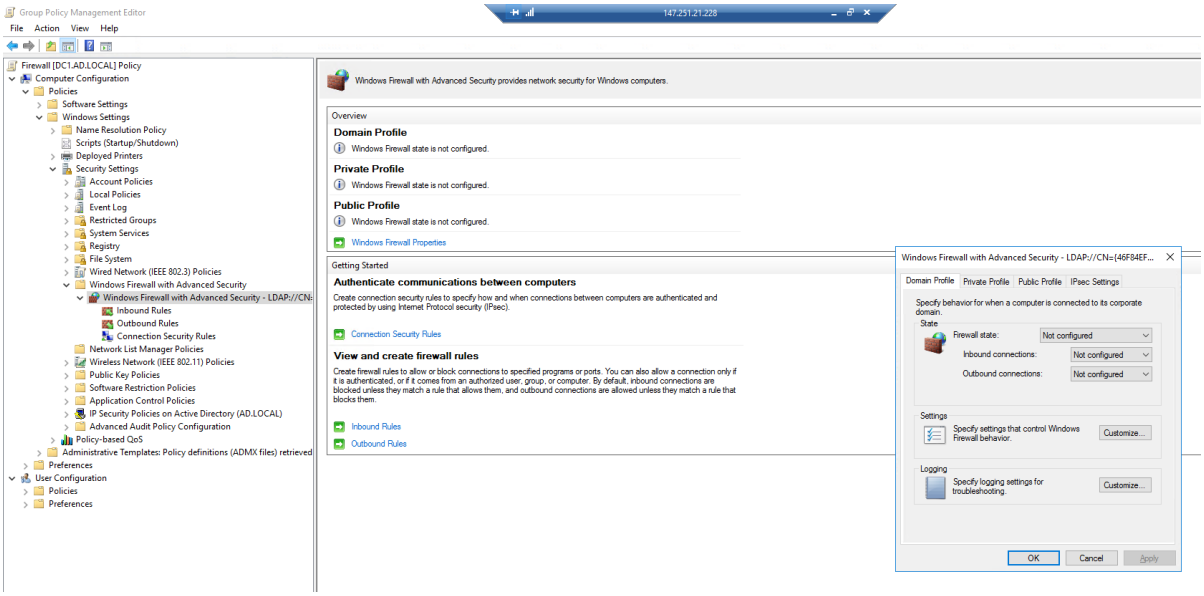
f. Rozumne pomenujeme pravidlo. Rozumný popis pravidla sa v buducnosti môže hodiť, najmä ak potrebujete dohľadať dôvod jeho existencie.

4. Vytvorené pravidlo sa po refreshy consoli objaví v časti ***Inbound*** resp. ***Outbound rules*** a súčasne aj v časti ***Monitoring***.

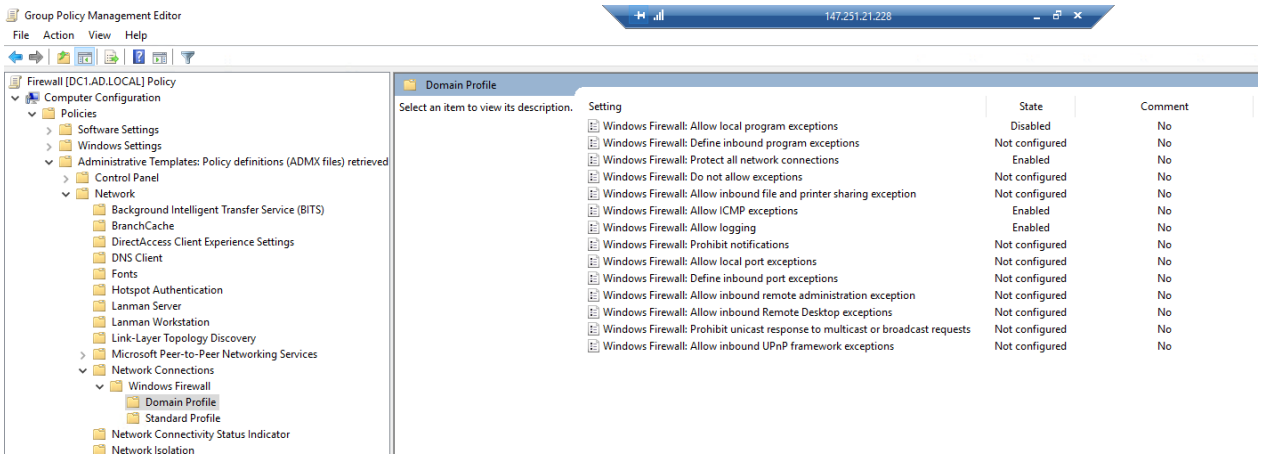
Konfigurácia FW pomocou AD domény – GPO

Konfiguráciu FW nájdete v nasledujúcich 2 častiach GPO:

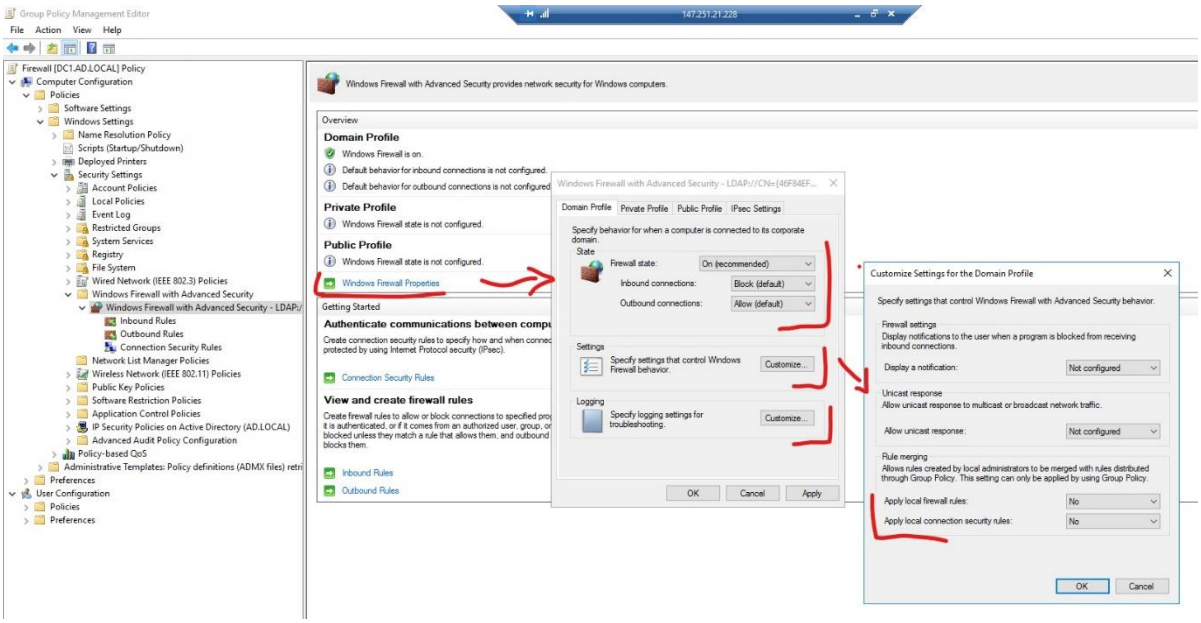
1. *"Computer Configuration/Windows settings/Security settings/Windows Firewall with advanced security"* – zhodné rozdelenie ako v prípade práce s FW priamo na cieľovom PC.



2. *"Computer Configuration/Network/Network connections/Windows Firewall"* – Pomocou týchto nastavení môžete vynútiť globálne nastavenie FW, prípadne zapnúť/vypnúť samotný FW.



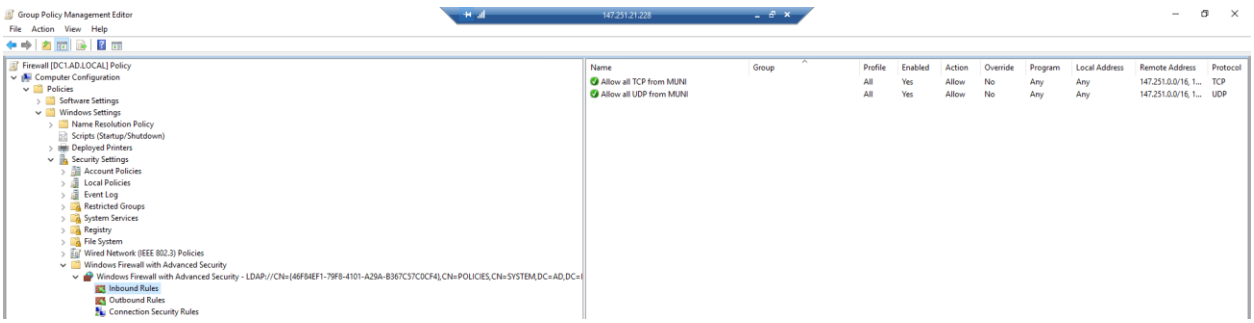
Konfigurácia samotných pravidiel prebieha rovnako, ako pre standalone režim (uvedenné vyššie). V prípade GPO si však musíme uvedomiť, že pravidla môžu byť konfigurované pomocou GPO, ale zároveň aj manuálne administrátorom na cieľovom PC. GPO umožňuje špecifikovať, či sa lokálne pravidla majú, alebo nemajú aplikovať.



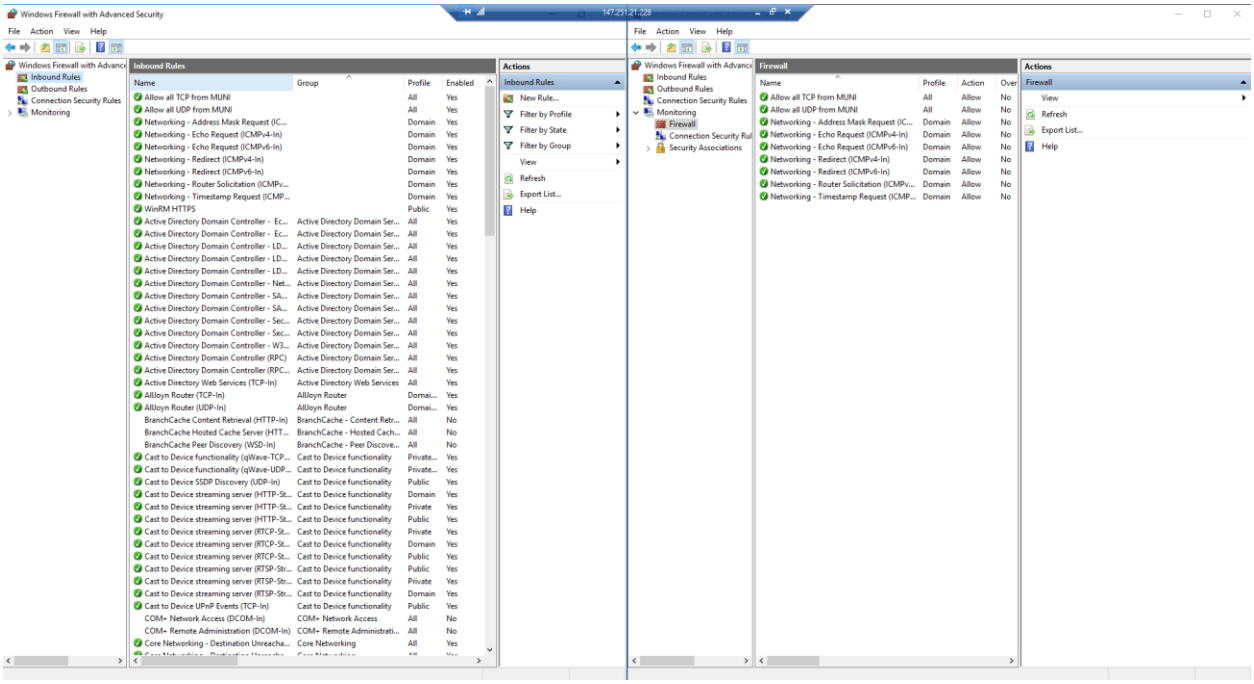
Následny rozdiel v aplikovaných pravidlách môže na základe konfigurácie aplikácie lokálnych pravidiel a profilu FW vyzerať aj takto:

Nastavenie politiky:

- Aplikácia lokálnych pravidiel je zakázana
- Pravidla su nastavené rovnako pre všetky profil
- Pravidla pre ICMP su konfigurované pomocou GPO taktiež

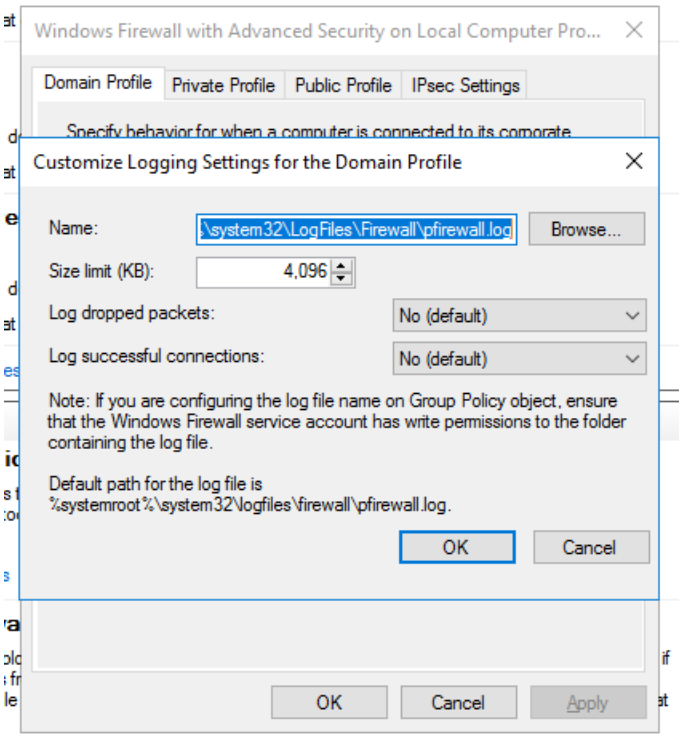


Výsledny rozdiel existujúcich a aplikovaných pravidiel na cieľovom PC:



Logovanie

V rámci FW môžete využiť možnosti logovania informácií o prijatých resp. zahodených paketoch do súboru:



Pozor:

- V prípade konfigurácie FW je potrebné dať si pozor na profily. PC detekuje pre každý sieťový adaptér jeho profil a podľa toho následne aplikuje pravidla. V prípade, že detekcia neprebehne korektne a vaša konfigurácia pravidiel rozlišuje profily, môže nastať stav, kedy sa vaše pravidlá aplikujú inak ako predpokládate.
- Nastavenie FW je dobré vynútiť pomocou GPO a nenechávať na náhodu pomocou lokálneho nastavenia, ktoré môže byť ovplyvnené lokálnym administrátorom
- Dajte si pozor na ktoré profily a sieťové adaptéry aplikujete nastavenie.
- Využite možnosti logovania – úspešne aj zahodené pakety. Pozor na veľkosť logu.
- Zmeny v GPO sa prejavia až po jej aplikovaní – ***gpudpate /force***
- Deny pravidlo je nadradené nad Allow

Ďalšie zdroje informácii:

https://www.youtube.com/watch?v=XD4KVGs_xFQ&t=11s

https://technet.microsoft.com/en-us/library/cc754274(v=ws.11).aspx