7.1.A

Modul 7 – LAB A: Konfigurácia TCPIP

Príprava
K úspešnému dokončeniu labu je treba mať pripravené nasledujúce:
2 virtuálne počítače s Windows 7, ktoré sú zapojené do rovnakej siete
Poznámka: V tomto labe preskúmame spôsob konfigurácie parametrov TCP/IP.

Obsah LABu:
Statická konfigurácia TCP/IP
Preskúmanie APIPA adries
Definovanie alternatívnej konfigurácie a skúmanie efektu v sieti bez DHCP

Cvičenie 1 Statická konfigurácia TCP/IP

Prihlásenie sa k PC1 pod administrátorským účtom ADMIN a nastavenie statickej adresy 10.0.0.1/24

- Prihlásime sa k PC1 pod administrátorským účtom s heslom Pa$$w0rd
- V pravej oznamovacej oblasti klikneme na ikonu siete a vyberieme voľbu „**Open Network and Sharing Center**".
- Prezrite si zobrazené okno – v hornej časti zobrazujúcej pripojenie Vášho počítača sa zobrazuje **mapovanie siete** – počítač je pripojený do siete s určitým názvom alebo prípadne do domény, pokiaľ je členom domény a má konektivitu na radič domény. Ak je počítač pripojený do Internetu, uvidíte farebnú ikonu glóbusu. Kliknutím na ľubovoľnú ikonu v hornej časti začnete prehľadávať buď lokálny počítač, sieť alebo sa otvorí Internet Explorer.
- V časti „**View your active networks**" si všimnite ikonu a pomenovanie siete a vpravo vedľa vidíte súpis sieťových kariet. Kliknite na sieťovú kartu s popisom **Local area connection** – otvorí sa okno s vlastnosťami danej karty.
- V okne vlastností sieťovej karty kliknite na tlačítko **Details**. Prezrite si nastavenie **IP adries**, či má karta nastavenú statickú konfiguráciu alebo či využíva **DHCP** a tiež, ak získala DHCP adresu, všimnite si parametre **Lease Obtained** a **Lease Expires**, ktoré udávajú životnosť zapožičanej adresy. Kliknite tu na tlačítko **Close**.
- V okne vlastností sieťovej karty kliknite na tlačítko **Properties** – môžete zr
  adaptéru. Prezrite si, ktoré sieťové protokoly sú na danej sieťovej karte ak
- Kliknite na položku „**Internet Protocol Version 4 (TCP/IP)**" a potom na tla
- Pokiaľ má karta **DHCP** konfiguráciu, uvidíte záložku **Alternate configurati**
  nedostupnosti DHCP serveru. Kliknite na voľbu **Use the following IP Addr**
  druhá záložka nazvaná Alternate Configuration.
- Nastavte **IP adresu** na **10.0.0.1** a **masku siete** na **255.255.255.0** a **bránu** na **10.0.0.254**. V spodnej časti nastavte **primárny DNS** server na **10.0.0.253**.
- Potvrďte nastavenia tlačítkom **OK** a zatvorte okno vlastností sieťového pripojenia tlačítkom **Close**.

- Uzavrite okno s detailami daného pripojenia tlačítkom **Close**. Rovnako ukončite okno štatútu.
- Spustíme príkazový riadok v menu Start – All Programs – Accessories (príslušenstvo) vyberieme command prompt
- V command prompte si napíšeme príkaz **ipconfig**

Pozn: Tímto príkazom zobrazíme konfiguráciu protokolu TCP/IP a skontrolujeme, že všetky parametre zodpovedajú nami zadanej konfigurácii. Pretože výpis ipconfig vypisuje len základnú časť, napíšeme príkaz ipconfig /all

Nastavenie statickej adresy 10.0.0.2/24, brány 10.0.0.254 a DNS 10.0.0.253 na PC2 z príkazového riadku

- Prepneme sa na PC2 a zvolíme **Start – All programs – Accessories – Command prompt**, tu klikneme pravým tlačítkom a vyberieme voľbu **Run as administrator**.
- Potvrdíme dialóg riadenia užívateľských účtov tlačítkom Yes a skontrolujeme, že nový príkazový riadok má v záhlaví administrator: .
- V príkazovom riadku napíšeme príkaz netsh, ktorým nastavíme vlastnosti sieťového protokolu rovnako, ako sme to urobili v grafickom rozhraní
- Zadáme príkaz:

  netsh interface ipv4 set address „local area connection" static 10.0.0.2 255.225.255.0 10.0.0.254
  a potvrdíme stlačením enter

Pozn: Týmto príkazom sme nastavili vlastnosti pripojenia s názvom local area connection, na kterom sme nastavili ip adresu 10.0.0.2 s maskou siete 24 bitov a bránou 10.0.0.254. Pretože názov sieťového rozhrania obsahoval medzeru, je nutné reťazec uzavrieť do úvodzoviek!!!

- Nasledujúcim príkazom nastavíme parametre serveru dns z príkazového riadku:
  netsh interface ipv4 set dns „local area connection" static 10.0.0.253
  a potvrdíme voľbou enter.

Ak vidíte varovné hlásenie, že daný DNS server je nesprávny alebo neexistuje, je to v poriadku – Windows 7 sa len snaží overiť, či zadávaný server je možné naozaj v sieti nájsť.

- Opäť si zobrazíme detailne nami zadané parametre pomocou príkazu ipconfig. Pre podrobnejšie informácie si vypíšeme kompletné nastavenia protokolu TCP/IP príkazom ipconfig /all.
- Všimnite si vo výpise, že pole dhcp enabled je nastavené na no čo značí, že náš server má staticky pridelenú adresu. Skontrolujeme tiež v poli IP verzie 4, že máme nami nastavenú IP adresu a skontrolujeme tiež IP adresu dns serveru.
- Kliknite na ikonu siete v oznamovacej oblasti a vyberte „Open network and sharing center"
- Všimnite si, že v časti View your active networks je daná sieť identifikovaná ako **Public network** a objavuje sa pri nej ikona lavičky s popisom **Unidentified netw...**
- Skúste na túto ikonu kliknúť. Objaví sa obrazovka pre zmenu názvu – všimnite si, že nie ste schopní zmeniť názov siete ani typ siete z public na iný. Je to preto, že na danej sieti Windows 7 nemôžu objaviť

7.1.A

- Zadáme príkaz:

  netsh interface ipv4 set address „local area connection" static 10.0.0.2 255.225.255.0 10.0.0.1
  a potvrdíme stlačením enter.

Tento príkaz nastaví IP adresu brány na 10.0.0.1, čo je prvý počítač a teda sme schopní dohľadať jeho MAC adresu (i keď je na ňom aktívny firewall).

- Všimnite si, že Windows 7 automaticky vyhľadajú MAC adresu brány (MAC adresa prvého počítača) a ak ju nájdu, objaví sa dialógové okno „**Set Network Location**" s voľbou umiestnenia danej siete.

- Prejdite do dialógového okna „**Set Network Location**" a kliknite na **Public** network. Potvrďte voľbu siete na finálnej obrazovke tlačítkom **Close**.

- Kliknite opäť na ikonu siete v oznamovacej oblasti a vyberte „**Open network and sharing center**".

- Všimnite si, že v časti **View your active networks** je daná sieť identifikovaná ako **Public network** a objavuje sa pri nej automaticky vygenerovaný názov.

- Kliknite na modrý odkaz „**Public network**". Všimnite si, že pretože sme prihlásení pod administrátorským účtom a daná sieť má identifikovateľnú MAC adresu brány, môžeme zmeniť typ siete – vyberte **Home network** a na finálnej obrazovke kliknite na tlačítko **Close**.

- Kliknite na ikonu domčeku – otvorí sa okno „**Type a network name and choose an icon**" – všimnite si, že môžete napísať ľubovoľný názov siete a tiež zmeniť ikonu siete tlačítkom Change. Zmeňte názov na **DomaciSit**, kliknite na tlačítko **Change** a vyberte ľubovoľnú ikonu podľa vlastného vkusu a potvrďte tlačítkom OK. Uzavrite okno typu a názvu siete tlačítkom OK.

Upozornenie: Obe možnosti (zmenu typu siete i zmenu ikony a názvu) sme mali dostupné, pretože Windows 7 detekovali MAC adresu siete a tiež pretože sme prihlásení pod administrátorským účtom.

Vypnutie Firewallu na PC1 a PC2

- Prepneme sa na počítač 1 a pre zjednodušenie našich nastavení vypneme firewall:

- Spustíme Start – Control panel – System and security – Windows Firewall

- V ľavej časti kliknite na odkaz „**Turn Windows Firewall on or off**"

- V oboch častiach (Home or work i v časti Public) vyberte voľbu **Turn off Windows Firewall (not recommended)** a potvrďte tlačítkom OK.

- Všimnite si zmenu zafarbenia okna a tiež bubliny Action center v oznamovacej oblasti, ktorá hlási nezabezpečený stav.

Rovnakým spôsobom vypnite firewall i na počítači PC2.

Testovanie spojenia PC1 a PC2 pomocou príkazu ICMP Echo request

- Prepneme sa na počítač 1, tu v príkazovom riadku zadáme ping 10.0.0.2

Pozn: Pokiaľ sa objavilo hlásenie o request timed out presvedčte sa, že ste na druhom počítači naozaj vypli firewall!

- Prepneme sa na PC2 a príkazom ping otestujeme konektivitu na PC1:
- Zadáme ping 10.0.0.1 a potvrdíme enterom
- V príkazovom riadku si všimnite, či sa vám vrátili späť odpovede v príslušnom čase. Ak sa opäť objavilo hlásenie request timed out, skontrolujte si, či ste skutočne vypli firewall na opačnom počítači

Pozn.: príkazom ping testujeme konektivitu medzi dvoma sieťovými uzlami prostredníctvom protokolu ICMP

Týmto sme úspešne otestovali statickú konfiguráciu protokolu TCP/IP. V prípade problémov spustite príkaz ipconfig /all a skontrolujte parametre vašich pripojení. Presvedčte sa, že je vypnutý firewall.

Cvičenie 2 Testovanie automatického prideľovania IP adries pomocou APIPA

Testovanie automatického prideľovania IP adries pomocou mechanizmu APIPA

- Prepneme se na PC1. Tentokrát vyskúšame iný spôsob prístupu k nastaveniu siete:
- Kliknite na Start a do poľa „**Search programs and files**“ napíšte **ncpa.cpl**.
- V okne network connections klikneme pravým na „**Local Area Connection**“ a vyberieme **Properties**.
- Zvolíme protokol „**Internet protocol version 4**“ a zvolíme **Properties**.
- Vo vlastnostiach protokolu IP verzie 4 zvoľte voľbu „**obtain an ip address automatically**“ (získať adresu zo siete automaticky) v spodnej časti vyberte voľbu „**obtain dns server address automatically**“ (získať adresu dns serveru zo siete)
- Na záložke Alternate Configuration sa presvedčte, že je tu ponechaná východisková voľba Automatic Private IP Address

Pozn: Táto voľba znamená, že nemáme zadanú alternatívnu konfiguráciu

Pretože v našom prípade znamená, že nemáme server DHCP, znamená to, že náš server si po určitej dobe vygeneruje automaticky adresu z rozsahu APIPA 169.254.X.X s maskou siete 255.255.0.0

- Uzavrite vlastnosti protokolu internet protocol version 4 tlačítkom **OK**.
- Zavrite vlastnosti sieťového pripojenia „**Local Area Connection**“ tlačítkom **Close**.
- Prepneme sa do príkazového riadku a tu zadáme príkaz ipconfig

Presvedčte sa, že vaše rozhranie Local Area Connection má IP adresu v rozsahu 169.254.x.x s maskou siete 255.255.0.0 (kde x sú náhodné čísla).
Týmto náš počítač automaticky vygeneroval záložnú adresu APIPA, prostredníctvom ktorej komunikuje s ostatnými uzlami na lokálnej sieti bez DHCP servera. Všimnite si, že APIPA logicky nemôže vygenerovať adresu brány ani DNS servera a preto se počítač môže spojiť len s APIPA uzlami na rovnakej fyzickej sieti.

netsh interface ip set address „local area connection“ dhcp a potvrďte stlačením enter

- Zadajte príkaz: ipconfig
- Presvedčte sa, že sa opäť vygenerovala automatická IP adresa

Testovanie konektivity medzi našimi počítačmi prostredníctvom príkazu ping

- Prepneme sa na PC1 a tu zadáme príkaz ping IP adresa druhého počítača a potvrdíme stlačením enter (túto adresu sme na druhom počítači získali výstupom príkazu ipconfig)
- Presvedčte sa, že sa vám vrátili časy odpovedí a že spojenie nevypršalo hlásením request timed out
- Spustite príkaz ipconfig a poznamenajte si IP adresu PC1
- Prepneme sa na druhý počítač
- Zadáme príkaz ping IP adresa opačného počítača a presvedčíme sa, že sa nám tiež vracajú odpovede v čase určenom hodnotou TTL.

V nasledujúcom príkaze si overíme, že naše počítače sú schopné sa dohľadať prostredníctvom sieťových broadcastov a že môžeme kontaktovať druhý počítač priamo pomocou jeho názvu

- Na oboch počítačoch na príkazovom riadku zadajte príkaz hostname – hostname vracia názov aktuálneho počítača
- Na PC1 zadajte na príkazovom riadku:

  ping -4 PC2

  a presvedčte sa, že odpovede chodia včas

- Prepnite sa na PC2 a opäť zadajte príkaz

  ping -4 PC1

- V oboch prípadoch by testy pingu mali byť dostupné a úspešné.

Poznámka: Parameter 4 len vynucuje použitie IPv4 protokolu. Windows Vista a Windows 7 možu využívať aj IPv6.

Cvičenie 3 Nastavenie alternatívnej konfigurácie

V nasledujúcom cvičení vyskúšame efekt alternatívnej konfigurácie, ktorý môžete využiť pri prechode zamestnancov medzi podnikovou sieťou so serverom DHCP a domácou sieťou, v ktorej majú na ostatných počítačoch statickú IP konfiguráciu a DHCP klient by tu normálne vygeneroval APIPA adresu.

- Na **PC1** si zobrazíme okno network connections príkazom ncpa.cpl
- Zvolíme vlastnosti sieťového pripojenia „**Local Area Connection**“ a zobrazíme si vlastnosti protokolu „Internet protocol version 4“

- Overte, že na záložke internet protocol version 4, Properties, na záložke General je ponechaná východisková voľba „**Obtain an IP address automatically**“ a v spodnej časti je zvolené „**Obtain DNS server address automatically**“

- Kliknite na záložku „**Alternate configuration**“, zvoľte voľbu user configured a tu zadajte parametre: IP adresa 172.16.0.1 s maskou siete 255.255.255.0 a východiskovou bránou 172.16.0.254 a preferovaným dns serverom 172.16.0.253

- Ostatné polia ponecháme prázdne. V spodnej časti zrušte zaškrtnutie pre validáciu.

- Potvrdíme vlastnosti protokolu IP verzie 4 tlačítkom OK.

- Potvrdíme nastavenie „**Local Area Connection Properties**“, stlačíme tlačítko OK

- Rovnakým spôsobom nastavte na PC2 nasledujúcu alternatívnu konfiguráciu:

ip adresa 172.16.0.2, maska siete 255.255.255.0, východisková brána default gateway 172.16.0.254 a preferovaný dns server 172.16.0.253. Zrušte zaškrtávaciu voľbu „**Validate settings...**“

- Ostatné voľby ponecháme prázdne a potvrdíme vlastnosti IP verzie 4 tlačítkom **OK**.
- Zavrieme vlastnosti sieťového rozhrania tlačítkom OK.

- Spustíme príkazový riadok.

Pozn.: Všimnite si, že na krátku dobu sa môže zmeniť ikona siete v oznamovacej oblasti na nedostupnú a je možné, že keď zadáme príkaz ipconfig, potom sa po určitú dobu bude používať predchádzajúca adresa APIPA (táto adresa sa používa v dobe, keď sa náš počítač snaží kontaktovať server DHCP). Po určitej dobe, keď vypršia požiadavky na DHCP adresu, začne náš počítač používať alternatívnu konfiguráciu.

- Na príkazovom riadku si zvoľte príkaz ipconfig

- Overte si, že náš počítač má teraz adresu, ktorú sme zvolili ako alternatívnu konfiguráciu

- Na príkazovom riadku zadáme príkaz: ipconfig /all

- Vo výpise sa presvedčte, že je zvolená voľba dhcp enabled na YES a že zároveň máte zvolenú voľbu internet ip verzie 4 adresu s našou alternatívnou konfiguráciou

Pozn: To znamená, že náš server neskontaktoval DHCP server a na miesto toho použil alternatívnu konfiguráciu

Rovnakým spôsobom skontrolujte nastavenie na druhom počítači.

<u>Test spojenia oboch počítačov s alternatívnou konfiguráciou prostredníctvom príkazu ping</u>

- Na PC1 na príkazovom riadku zadáme príkaz:

- ping 172.16.0.2

- Presvedčte sa, že sa odpovede vrátili včas (neobjavil sa timeout)

- Na PC2 zadáme príkaz ping 172.16.0.1 a skontrolujeme si, že sa požiadavky vrátili včas (nevypršali pomocou timeout)

7.1.4

- Na PC1 zadajte príkaz ping -4 PC2 a stlačte enter.
- Počítače si na pozadí dohľadajú IP adresy susedov pomocou rozlišovania názvov a opäť by sa vám mali zobraziť odpovede, ktoré prišli včas.
- Rovnaký postup vykonajte i s počítačom 2, kde zadáte príkaz ping -4 PC1.
- Opäť sa presvedčte, že odpovede prišli včas

LAB B: Preskúmanie základného firewallu a firewallu s pokročilým zabezpečením

Príprava

K úspešnému ukončeniu labu je potrebné mať pripravené nasledujúce:
Dva počítače s Windows 7 pripojené do rovnakej siete
V tomto labe sa naučíte ovládať základný firewall aj firewall s pokročilým zabezpečením.

Cvičenie 1 Prieskum základného firewallu

- Prihlásime sa na PC1 pod administrátorským účtom s heslom Pa$$w0rd

- Na počítači PC1 nastavte nasledujúce parametre TCPIP:

Statické pridelenie IP adresy:
IP adresa 10.0.0.1
maska 255.255.255.0
brána 10.0.0.2

- Prihlásime sa na PC2 pod administrátorským účtom s heslom Pa$$w0rd

- Na počítači PC2 nastavte nasledujúce parametre TCPIP:

Statické pridelenie IP adresy:
IP adresa 10.0.0.2
maska 255.255.255.0
brána 10.0.0.1

Na oboch počítačoch by sa mal objaviť dialóg pre zadanie umiestnenia siete – vyberte Home network. Pokiaľ sa na PC1 tento dialóg neobjavil, potom spustite ncpa.cpl, kliknite pravým tlačidlom na Local area connection a vyberte Disable. Potom opäť kliknite pravým na Local area connection a vyberte Enable.

- Na počítači PC1 vykonajte nasledujúce:

- Vyberieme voľbu Start – Control panel – System and Security – Windows Firewall

- Všimnite si, že v časti **Home or work** (private network) sa objaví stav **Connected**. Oproti tomu v časti **Public networks** je stav **Not connected**. Windows 7 si pamätajú typ umiestnenia pre každé sieťové rozhranie zvlášť.

- V ľavej časti zvolíme voľbu „**Allow a program or feature through windows firewall**"

Prezrite si výpis a porovnajte východiskový rozdiel medzi profilmi Private a Public.

- Kliknite v hornej časti na tlačítko **Change settings**.

- Dvakrát kliknite na ktorúkoľvek položku v zozname programov a funkcionalít.

- Všimnite si, že oproti predošlému firewallu vo Windows XP nemáte možnosť nastavení rozsahu IP adries, z ktorých je možné sa pripojiť na porty danej aplikácie a nevidíme ani žiadne porty.

7.2.B

- Vyberte **Windows Media Center** a kliknite na tlačítko **Add**.

Pozn.: Pridanie programu medzi výnimky vo firewalle je vhodné v prípade, že si náš program automaticky vyberá porty, na ktorých bude ponúkať svoje služby. Kliknite na tlačítko OK pre zatvorenie okna výnimiek.

- Voľba Turn Windows Firewall on or off vypína/zapína firewall. Restore defaults obnovuje nastavenie firewallu do východiskového stavu, pokiaľ omylom poškodíme nastavenie firewallu.

- Kliknite na voľbu „**Change notification settings**" a prezrite si východiskové nastavenia.

Všimnite si, že v základnom okne firewallu nemôžeme nastaviť výnimky TCPIP ani podrobnosti logovania!!! Pre podrobnejšie podmienky použijeme pokročilú konzolu **firewall with advanced settings** (Firewall s pokročilým nastavením).

Cvičenie 2 Windows firewall with advanced security

- Pre pokročilejšie nastavenia v ľavej časti v oblasti zvolíme voľbu „Advanced settings"

Firewall s pokročilým zabezpečením

- V konzole Windows firewall with advanced security on local computer si v strednej časti všimnite, že je firewall aktívny pre všetky tri profily (doménový, privátny aj verejný).

- V ľavej časti si vyberte položku Windows firewall with advanced security a zvoľte vlastnosti

- Všimnite si, že je možné nastaviť oddelene každý z profilov – môžete si nastaviť stav firewallu na zapnutý alebo vypnutý, a rovnako môžete zmeniť východiskový režim blokovaním odchádzajúcich, či prichádzajúcich spojení. Východiskové nastavenia firewallu sú: zakazuje prichádzajúce nevyžiadané spojenia a povoľuje odchádzajúce pripojenia bez obmedzení. Hodnota default znamená, že Povoľovanie/Zakazovanie môže mať nadefinované výnimky.

- V časti Protected network connections kliknite na **Customize** – tu môžete z daného profilu vyňať určitú sieťovú kartu – kliknite na **Cancel**.

- V sekcii **Settings** kliknite na **Customize** – môžete si zvoliť vlastnosti firewallu, prípadné upozornenia pri detekcii nových programov, ktoré sa snažia otvoriť porty k načúvaniu. Je tiež možné dopĺňať východiskové pravidlá firewallu z Group Policy o vlastné lokálne pravidlá.

- Uzavrieme vlastnosti customize setting stlačením **CANCEL**.

- V časti **Logging** stlačte **Customize** – tu môžete určiť umiestnenie a maximálnu veľkosť logu, do ktorého firewall zapisuje svoje aktivity.

- Nastavte veľkosť logu na **32 MB**

- Zvoľte voľby tak, aby firewall logoval **zahodené pakety**. Potvrďte nastavenia tlačítkom **OK** a zavrite vlastnosti firewallu.

- V ľavej časti konzoli firewallu zvolíme **Inbound rules** a v pravej časti si všimnite možnosti filtrovania.

Pozn.: Aktívne znamená, že v stĺpci enabled máme hodnotu YES. Aktívne pravidlo je vynucované. To, či pravidlo povoľuje alebo zakazuje, je definované v stĺpci Action.

Filtrovanie výpisu pravidiel

- Prezrite si rozsiahly výpis v prostrednom okne, ktoré teraz obmedzíme prostredníctvom **filtrovania.**
- V pravej časti si klikneme na **Filter by profile,**
- Klikneme na **Filter by domain profile,**
- Opakujeme opäť stlačením **Filter by profile** a naviac zvolíme hodnotu **Filter by private profile**
- Týmito voľbami môžeme ľubovoľne meniť zobrazenie firewallu pre konkrétne profily. Naviac môžete v konkrétnom profile vyhľadať aktívne pravidlá:
- Stlačíme voľbu **Filter by state** a vyberieme **Filter by enabled**
- Všimnite si, že v prostrednom okne teraz máme zobrazené iba aktívne pravidlá, ktorá sú aktívne v privátnom a doménovom profile – tzn. v bezpečnom prostredí.
- V pravej časti si zvoľte **Filter by group**
- Všimnite si, že zo zobrazených pravidiel si môžete vyberať konkrétne skupiny
- V pravej časti v poli **Filter by profile** nastavte len hodnotu **private** a v poli **Filter by state** si zvolíme **show all.**
- V poli **Filter by group** si zobrazíme voľbu **Filter by file and printer sharing**
- Pokiaľ nie je aktívne pravidlo **File and printer sharing (echo request – icmpv4-in),** kliknite pravým tlačítkom na toto pravidlo a vyberte hodnotu **enabled rule**

Pozn.: týmto sme povolili príchodzie požiadavky na echo request – ping

Testovanie ICMP paketov

- Prepneme sa na PC2 a presvedčíme sa, že sme schopní poslať ping cez otvorený firewall
- Zadáme ping 10.0.0.1
- odpovede na naše žiadosti by mali prísť včas a nemalo by dôjsť k timeoutu

Týmto sme úspešne nastavili firewall pre príchodzie požiadavky ping na PC1.

Povolenie výnimiek vo firewalli stanice PC2

- Na **PC2** kliknite na start, napíšte wf.msc a stlačte Enter pre spustenie **Advanced firewallu**
- Presvedčíme sa, že v prostrednom okne máme zapnutý firewall na **všetkých troch profiloch**

7.2.B

Potvrdíme APPLY a OK. Znovu sa presvedčíme, že firewall v prostrednom okne overview je zapnutý na všetkých profiloch.

- Opäť klikneme na voľbu **inbound rules**.
- V pravej časti actions klikneme na voľbu **Filter by group**
- Zvolíme **Filter by file and printer sharing**
- V pravej časti vyberieme **Filter by profile** a vyberieme filtrovanie v **privátnom profile**
- V prostrednom okne sa presvedčíme, že máme zapnutú voľbu **File and printer sharing (echo request - icmpv4-in)**, máme aktívne pre privátny profil
- V pravej časti v poli actions klikneme na **Filter by profile**, zvolíme **Public profile** a presvedčíme sa, že dané pravidlo na verejnom rozhraní nie je aktívne (ak by bolo, zvolíme pravé kliknutie a zaškrtneme voľbu disabled rule)
- Presvedčíme sa, že môžeme poslať ping z prvého počítača: Na prvom počítači spustíme príkazový riadok pomocou **cmd** a pošleme ping na IP adresu druhého počítača ~~172.16.0.2~~ 10.0.0.2 príkazom:

ping -w 100 -t 10.0.0.2

- Tento príkaz bude trvale posielať požiadavky na odozvu. Ponechajte toto okno spustené ako monitorovanie prevádzky až do konca labu.

Ak požiadavky na odozvu vypršia prostredníctvom timeout, potom sa na druhom počítači presvedčte, že dané sieťové rozhranie na PC2 je skutočne v privátnom profile.

Zmena sieťového profilu na PC2

- Na PC2 kliknite pravým na ikonu siete v oznamovacej oblasti a vyberte **Open network and sharing center**.
- Kliknite na link **Home network** a zmeňte profil pripojenia na **Public network**.
- Prepnite sa na **PC1** a prezrite si stav odosielaných pingov – pretože má PC2 v public profile zakázané ICMPv4, všetky požiadavky teraz **vypršia**.
- Na **PC2** zmeňte profil sieťového pripojenie späť na **Home network**.
- Skontrolujte na **PC1**, že požiadavky na odozvu opäť **fungujú**. Stále ponechajte okno s požiadavkami otvorené.

Prezeranie výstupných pravidiel a blokovanie ICMP výstupných paketov

- Na **PC1** sa prepneme do ľavého okna windows firewall with advanced security a klikneme na voľbu **Outbound rules**. Windows 7 a Vista umožňujú blokovanie aj odchádzajúcej komunikácie a programov.
- V strednej časti vyberte pravidlo **File and printer sharing (echo request – icmpv4-out)**, ktoré má v stĺpci profile uvedenú hodnotu Private (v ňom sa naše PC1 nachádza).

- V okne **Advanced firewallu – Outbound rules** – dvakrát kliknite na pravidlo, ktoré sme práve zapli a v jeho vlastnostiach vyberte na záložke **General** voľbu **Block the connection** a potvrďte OK

Touto voľbou sme zakázali odchádzajúce spojenia prostredníctvom protokolu icmpv4 echo request.

- Prepnite se na príkazový riadok a všimnite si, že ICMP požiadavky nemôžu dokonca ani opustit PC1 a preto sa zobrazuje hlásenie **General failure**.

Týmto krokom sme sa presvedčili, že sme schopní blokovať ľubovoľné odchádzajúce spojenie.

- Prepnite sa opäť do okna windows firewall with advanced security,
- Vyberte opäť časť **Outbound rules** a v pravej časti si zvoľte voľbu **Filter by group**
- Vyberte položku **Filter by file and printer sharing**.
- V prostrednom okne nájdeme zakázané pravidlo (ikona v zákaze) pre **File and printer sharing (echo request – icmpv4-out)**.
- Kliknite pravým tlačítkom, zvoľte **vlastnosti** a na záložke **general** v spodnej časti vyberte voľbu „**Allow the connections**"
- Potvrdíme stlačením **APPLY**.

Pozn.: Prostredná voľba allow the secure connections by si vyžiadala pripojenie cez zabezpečné ipsec spojenie.

- Na záložke **general** si všimnite, že toto pravidlo je aktívne vďaka voľbe **enabled**.
- Na záložke **Program and services** si všimnite, že môžete blokovať odchádzajúce spojenia ľubovoľného programu či služby
- Na záložke **Computers** si všimnite, že môžete obmeziť spojenia len na niektoré autorizované počítače (overenie ipsec protokolom)
- Na záložke **Protocols and ports** si všimnite, že by ste mohli obmedziť spojenie z ľubovoľného portu na ľubovoľný vzdialený port
- Na záložke **Scope** by sme mohli obmedziť spojenia na určité IP adresy, prípadne z určitých IP adries nášho počítača
- Na záložke **Advanced** si všimnite, že si môžete zvoliť, v ktorom profile bude toto pravidlo aktívne.
- Voľbou **Interface types** by sme mohli zvoliť aktívne pravidlo len na určitých rozhraniach
- Potvrdíme naše voľby, ktoré sme vykonali na záložke general stlačením tlačítka OK
- Všimnite si, že sa zmenila ikona pri našom pravidle **File and printer sharing (echo request – icmpv4-out)** na povoľujúce.
- Prepneme sa na príkazový riadok a všimnite si, že požiadavky na odozvu opäť bez problémov odchádzajú. Ping by mal opäť prejsť v poriadku, pretože sme povolili odchádzajúce spojenia icmp