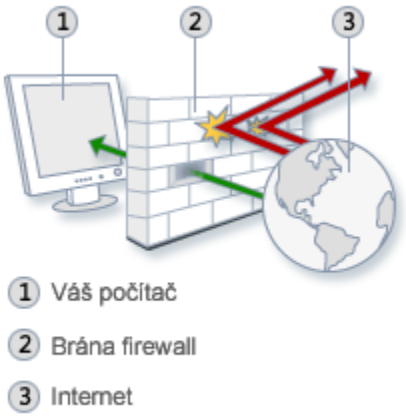
Windows Firewall

[Povinné]

Brána firewall může být software nebo hardwarové zařízení, které kontroluje informace přicházející z Internetu nebo ze sítě, a v závislosti na svém nastavení je buď zablokuje, nebo jim umožní projít do počítače.

Brána firewall se tedy snaží předcházet počítačovým podvodníkům nebo škodlivému softwaru (například červům) získání přístupu k počítači prostřednictvím sítě nebo Internetu. Brána firewall může rovněž zabránit tomu, aby počítač odesílal škodlivý software do jiných počítačů.

Obrázek vpravo znázorňuje, princip funkcionality brány firewall.



Základy Windows Firewall

[Povinné]

Firewall omezuje síťovou komunikaci podle několika základních konfigurovatelných pravidel. Windows Firewall v základním nastavení kontroluje všechny síťové adaptéry. Firewall funguje následujícím způsobem: jakmile komunikace dosáhne rozhraní v počítači, dojde k vyhodnocení paketů a ty jsou buď propuštěny dál, nebo zahozeny, v závislosti na základních pravidlech. Firewall ve Windows obsahuje jak základní *Bránu firewall systému Windows* tak také podrobnější *Bránu firewall systému Windows s pokročilým zabezpečením*[1]. Základní rozdíl je v komplexnosti pravidel a jejich nastaveni v závislosti na různých rozhraních.

Ve Windows XP se nacházel také firewall, avšak na rozdíl od firewallu ve Windows Vista a novějších, nedokázal obstarávat obousměrnou komunikaci a umožňoval jen nastavení pravidel pro příchozí provoz.

Jak již bylo řečeno, Windows Firewall od Windows Vista dokáže nastavovat pravidla pro příchozí i odchozí komunikaci. Filosofie firewallu by se dala shrnout jako: Co není povoleno, je zakázáno, což znamená především použití příkazu Povolit, nežli Zakázat.

Windows Firewall obsahuje také skrytou funkcionalitu, jež není možné vypnout, a tou je znemožnění útočníkovi zjistil na jakou verzi OS a na jaký firewall zaútočit.

Další vlastností je znemožnění útoku na OS během procesu spouštění systému. Jelikož firewall, ať již Windows Firewall nebo produkt třetí strany, se spouští až po startu systému, vzniká zde prostor pro možný útok. A právě proti tomuto útoku je postaven prostředek *Boot time filtering*, který chrání počítač při spouštění systému.

Pro lepší pochopení nastavení jednotlivých parametrů pravidel se potřebujeme seznámit se základními pojmy z oblastí sítí[2]:

- **Protokol**. Pro potřeby konfigurace firewallu jsou pro nás důležité 2 protokoly – *Transmission Control Protocol* (TCP) a *User Datagram Protocol* (UDP). TCP je dnes používaný jako hlavní protokol Internetu, kdežto UDP se používá především pro *broadcast* a *multicast*[3], a často se s ním setkáme také ve spojení s hrami.
- **Port**. Port je důležité číslo které lokalizuje hlavičku TCP nebo UDP datagramu. Port se používá pro mapování sítového provozu k příslušným službám a programů. Např. port 80 je rezervován pro WWW komunikaci a port 25 pro přenos e-mailu přes Internet.
- **IPSec (*Internet Protocol Security*)**. Metoda zabezpečení Internetového provozu používající šifrování a digitální podpisy. Jestliže je IPSec datagram zachycen, jeho obsah nemůže být

[1] Ve Windows 10 verze 1810 přejmenovány na *Firewall v programu Windows Defender* a *Firewall v programu Windows Defender s pokročilým zabezpečením*

[2] Podrobnosti k TCP/IP protokolu, Portům a nastavení sítě naleznete dále.

[3] TCP ověřuje, zda pakety opravdu došly, kdežto UDP tuto kontrolu neprovádí. ICMP protokol využívá příkaz ping pro diagnostiku dostupnosti síťové lokace.

přečten, ale IPSec poskytne ověření odesílatele, které dává příjemci záruku s pravostí datagramu.

- **Síťová adresa**. Každý počítač v síti má síťovou adresu. Brána firewall umožňuje odlišné vyhodnocování provozu pro různé síťové adresy nebo jejich rozsahy.
- **Příchozí provoz**. Jedná se o část síťového provozu směřujícího z externího počítače do našeho počítače.
- **Odchozí provoz**. Tímto termínem je označen provoz směřující z našeho počítače do Internetu nebo jiných míst v síti.
- **Síťové rozhraní**. To může být Lokální síť (LAN), bezdrátová síť (Wi-Fi), modemové připojení, VPN nebo FireWire připojení.

Nastavení Windows Firewall [Povinné]

Windows Firewall se dělí do dvou částí – Brána Windows Firewall a Brána Windows Firewall s pokročilým zabezpečením:

- **Brána Windows Firewall**. Základní konfigurace firewallu spustitelná přes Ovládací panely, zapněte klasické zobrazení, Windows Firewall, umožňuje jednoduché zapnutí a základní konfiguraci firewallu.
- **Brána Windows Firewall s pokročilým nastavením**. Windows Firewall od Windows Vista obsahuje Windows Firewall s pokročilým zabezpečením, ve kterém je možno blíže specifikovat jak odchozí tak příchozí pravidla, ale také například přesně definovat pro kterou síť nebo který adaptér se mají aplikovat.

Profily a Network Location Awareness (NLA) [Povinné]

Network Location Awareness (NLA), neboli povědomí o tom v jaké síti se nacházíme, je proces, kterým Windows (Vista a novější) přiřazují síťový profil na základě aktuálního síťového prostředí. Jsou možné 3 síťové profily Soukromý (*Private*), Veřejný (*Public*), Doména (*Domain*). Jednotlivé profily se aktivují pro jednotlivá síťová rozhraní podle následujících pravidel:

- **Soukromý profil**. Soukromý profil se aktivuje, pokud **dané** aktivní (připojené) síťové rozhraní (LAN, Wi-Fi, VPN, Modem, Firewire) je v Soukromé kategorii podle NLA rozdělení. **Princip kategorizování:** Když se počítač připojí do nové sítě, Windows se zeptá, zda daná síť se nachází ve *Veřejné síti*, *Domácí síti* nebo v *Síti v zaměstnání*. Pokud uživatel odpoví, že v *Domácí síti* nebo v *Síti v zaměstnání*, bude síť kategorizována jako *Soukromá*. Je třeba si však uvědomit, že pokud je síť špatně navržena, bude to mít vliv na funkčnost NLA.
- **Veřejný profil**. Windows aktivuje tento profil, v každé situaci pokud nebude aktivní Soukromý ani Doménový profil. Ve výchozím nastavení, pokud je Veřejný profil aktivní, budou pravidla firewallu nejpřísnější.
- **Doménový profil**. Doménový profil se stane aktivním, pokud na daném aktivním sítovém zařízení bude počítač ověřen doménovým řadičem[4].

Remote Assistance [Povinné]

Funkce Vzdálená pomoc je technologie v systémech MS Windows, která uživatelům systému umožňuje vzájemně si pomáhat přes Internet. Pomocí tohoto nástroje jeden uživatel, označený jako Poradce, vidí pracovní plochu jiného uživatele, označeného jako Začínající uživatel. Poradce může na základě oprávnění Začínajícího uživatele také ovládat počítač Začínajícího uživatele, aby mu vzdáleně pomohl řešit potíže.

[4] Jelikož kurz IW1 a ani zkouška 70-697 nebo 70-698 se nezabývají doménovým prostředím, bližší informace se dozvíte v některém s následujících kurzů IW zabývajících se problematikou práce v doméně.

Zabudovaná ochrana

[Povinné]

- Vzdálená pomoc používá protokol RDP (*Remote Desktop Protocol*) pro koncové spojení.
- Osoba žádající o pomoc musí povolit počáteční připojení Poradce předtím, než může Poradce vidět plochu Začínajícího uživatele.
- Osoba žádající pomoc musí zaslat pozvánku, která je chráněná 12místným heslem, které musí Poradce zadat během připojování.
- Osoba žádající pomoc může omezit životnost pozvánky.
- Osoba žádající pomoc má plnou kontrolu nad relací po celou dobu, může ji kdykoli ukončit nebo odebrat kontrolu Poradci nad touto relací.

Postup

[Povinné]

Uživatel žádající pomoc (*host*) vystaví *pozvánku* a zašle ji osobě, od níž žádá pomoc (*poradce*). Ten se pak může připojit k počítači hosta. Uživatel, jenž vytvořil pozvánku, má plnou kontrolu nad relací. Tudíž ji může kdykoliv ukončit. V doménovém prostředí lze pomocí zásad skupiny (*group policy*) určit účty, jež budou moci asistenci nabízet členům domény. Tudíž odpadá nutnost vystavovat a zasílat pozvánku. Stále platí, že nad relací má plnou kontrolu host.

Pozvánka ve formátu XML musí být předána Poradci a to je možno několika způsoby:

- **E-mail**. Windows spustí defaultní emailový program, vytvoří email, jenž bude v příloze obsahovat pozvánku a uživatel pouze doplní emailovou adresu poradce.
- **Uložení pozvánky do souboru**. Pozvánku po uložení musí host sám „bezpečně“ dopravit k poradci.
- **Easy Connect**. Ve skutečnosti nepotřebuje pozvánku, umožňuje vytvoření spojení pouze se zadáním hesla.

Po vytvoření relace se objeví poradci okno vzdálené pomoci, kde vidí plochu hosta. Nemůže ji ovládat. Může však zažádat o převzetí kontroly. Uživatel, který žádal o pomoc, musí tuto akci nejprve schválit. Má dokonce možnost povolit poradci spouštění programů, které vyžadují zvýšení oprávnění. Pokud mu to neumožní, v případě potřeby administrátorských oprávnění poradci obrazovka ztmavne do té doby, než uživatel potvrdí zvýšení oprávnění. Uživatel má stále kontrolu nad relací a může kdykoli odebrat poradci kontrolu.

Remote Desktop

[Povinné]

Na rozdíl od RA se RD relace nesdílí. K počítači se lze připojit, i když nikdo jiný na něm není přihlášen. U klientských Windows je k dispozici jedno RD spojení. Ve výchozím nastavení je RD zakázaná.

Remote Settings: Allow connections only from computer running Remote Desktop with Network Level Authentication. Toto nastavení umožňuje vyšší bezpečnost díky silnějšímu šifrování, avšak počítač, jenž bude na počítač, na němž povoluji RD, musí mít operační systém Windows XP SP2 nebo novější.

Pokud se bude připojovat počítač s jiným OS (Linux, Mac, Windows Server 2003), musí být zatrženo nastavení **Allow connections from computers running any version of Remote Desktop**.

Aby se uživatel mohl připojit k RD, musí mít příslušná práva. Členové skupiny **Administrators** mají právo k RD automaticky. Ostatní účty, které mají mít právo přístupu přes RD, musí být přidáni přes tlačítko **Select Users** nebo lépe tak, že bude jejich účet zařazen do skupiny **Remote Desktop Users**.

Při připojování k RD může dojít k několika situacím:

- Lokálně je nalogován uživatel a přes RD se hlásí stejný uživatel. Pak bude uživatel, jenž se hlásí přes RD, připojen k právě probíhající relaci. (Platí i na opak probíhá relace přes RD a lokálně se přihlásí stejný uživatel, tak se přihlásí k již běžící RD relaci.)

- Lokálně je přihlášen uživatel a přes RD se hlásí jiný uživatel. Pak lokálně přihlášený uživatel je upozorněn na žádost o přístup přes RD. Pokud lokálně přihlášený uživatel do 30 sekund nezamítne přístup přes RD, bude jeho relace odhlášena a bude vytvořena nová relace pro uživatele, jenž se hlásí přes RD. (Platí i na opak – probíhá relace přes RD a jiný uživatel se hlásí lokálně. Uživatel využívající RD má 30 sekund na zamítnutí lokální relace, pokud tak neučiní, bude jeho relace odhlášena.)

Vylepšení RD ve Windows 7:

- Podpora Aera
- Podpora aplikací využívajících Direct 2D a Direct 3D 10.1
- Podpora více monitorů
- Vylepšení výkonu RDP
- Podpora Media Foundation
- Podpora DirectShow
- Low Latency audio playback
- Bi-directional audio
- Podpora RemoteFX (přenos HW akcelerované grafiky, přesměrování USB) v SP1

Některá vylepšení RD ve Windows 8:

- Adaptivní grafika
- Podpora přenosu dotyků a gest (multitouch)
- Intelligent Transports
- Optimalizace streamování multimédií
- Single sign-on
- Modern UI Remote desktop klient

Některá vylepšení RD ve Windows 10:

- Vylepšení RemoteFX včetně podpory OpenGL 4.4, 4K rozlišení
- Podpora kodeku H.264/AVC 444
- Vylepšená podpora dotyku a gest
- Podpora pera

Při nefunkčním RD připojení:

- Mám RD povolenu?
- Mám právo přístupu přes RD? Jsem členem **Administrators** nebo **Remote Desktop Users**?
- Mám výjimku pro RD na firewall?

Studentské úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server file: **nepal\hstudent** heslo: **aaa**

Lab S01 – Firewall

[Povinné]

Cíl cvičení

Vyzkoušet si základní práci s konzolí **Windows Firewall with Advanced Security** a následné uplatnění vytvořených pravidel s profily **Network Location Awareness**.

Potřebné virtuální stroje

w10-base (w10-base)

1. Přihlaste se na **w10-base** pod účtem **student** (heslo **aaa**).
2. Zapněte **Firewall** (pokud je vypnutý).
3. Spusťte **Windows Firewall with Advanced Security**.
4. Spusťte **Microsoft Edge** a vyzkoušejte přístup na internet.
5. V **Outbound Rules** vytvořte pravidlo pro blokaci odchozí komunikace – **New Rule…**
6. Zvolte **Custom** Next > **All programs** Next > Protocol type: **TCP** a nastavte **Remote port** na **Specific Ports** a napište **80, 443** Next >
7. Zvolte **Any IP address** pro **local IP** i **remote IP** Next >
8. Nastavte **Block the Connection** Next >
9. Vyberte pouze **Public** Next > a zadejte jméno **A - Blokace Public Internetu** a kliknete na Finish.
10. Podívejte se na nastavení v **Network and Sharing Center** a následně nastavte profil u adaptéru LAN1 na **Private**.
    - Varianta 1
        i. Přejděte do **Settings \ Network & Internet \ Ethernet**
        ii. Klikněte na síťové rozhraní s připojenou sítí (místo názvu adaptéru LAN1 bude zobrazeno jméno sítě)
        iii. Přepněte přepínač u **Make this PC discoverable** na **On**
    - Varianta 2
        i. Spusťte powershell jako administrátor
        ii. **Set-NetConnectionProfile -interfacealias LAN1 -NetworkCategory Private**
        nebo
        Set-NetConnectionProfile -name "jménosítě" -NetworkCategory Private
        iii. Ověřte změnu v **Network and Sharing Center**
11. Zkuste spustit **Microsoft Edge** a zadat např. http://www.seznam.cz
12. Nastavte profil u adaptéru LAN1 na **Public**.
    - Varianta 1
        i. Přejděte do **Settings \ Network & Internet \ Ethernet**
        ii. Klikněte na síťové rozhraní s připojenou sítí (místo názvu adaptéru LAN1 bude zobrazen název sítě)
        iii. Přepněte přepínač u **Make this PC discoverable** na **Off**
    - Varianta 2
        i. Spusťte powershell jako administrátor
        ii. **Set-NetConnectionProfile -interfacealias** LAN1 **-NetworkCategory Public**

nebo

Set-NetConnectionProfile -name "jménosítě" -NetworkCategory Public

iii. Ověřte změnu v **Network and Sharing Center**

13. Zkuste spustit **Microsoft Edge** a zadat např. http://www.seznam.cz
14. Deaktivujte pravidlo **A - Blokace Public Internetu**.

Lab S02 – Firewall (ICMP, ping)

[Povinné]

Cíl cvičení

Vyzkoušet si možnosti filtrování síťového provozu na základě protokolu nebo IP adresy.

Potřebné virtuální stroje

w10-base (w10-base)
w10-domain (w10-domain)

1. Přihlaste se na **w10-domain** pod účtem **w10-domain\student**.
2. Spusťte příkazový řádek. Zjistěte IP adresu počítače **w10-base** na LAN2 adaptéru.
3. Spusťte příkaz ping na stanici **w10-base**, neměla by být vidět:
   - **ping -t <*w10-base_IP*>**
4. Přesuňte se na **w10-base**.
5. Otevřete **Network and Sharing Center** a nastavte odpovídající adaptér (který má IP adresu, kterou se pokoušíte pingnout) na **Public** (viz Lab S01, pokud nemá adaptér nastavenou výchozí bránu, bude nutné použít powershell). Zkusme tedy vytvořit pravidlo, které nám dokáže povolit komunikaci přes **ICMP** na **Public** síti.
6. Spusťte **Windows Firewall with Advanced Security**.
7. V **Inbound Rules** vytvořte pravidlo pro blokaci příchozí komunikace – **New Rule**…
8. Zvolte **Custom** Next > **All programs** Next > **ICMPv4** (podívejte se na možnosti tlačítka **Customize**) Next >.
9. V části **local IP** zvolte **These IP addresses**, klikněte na **Add** a napište **192.168.0.0/24**.
10. V části **remote IP** nastavte **Any IP** Next >
11. Nastavte **Allow the Connection** Next >
12. Vyberte jen **Public** a zadejte jméno **A - povolení ICMP protokolu pro Public** a klikněte na Finish.
13. Přesuňte se na **w10-domain** a podívejte se, jestli došlo ke změně.
14. Zkuste deaktivovat pravidlo **A - povolení ICMP protokolu pro Public**. Co se změnilo na **w10-domain** ?
15. Ukončete příkaz ping pomocí Ctrl+C.

Lab S03 – Remote Desktop

[Povinné]

Cíl cvičení

Povolení, nastavení a vyzkoušení služby **Remote Desktop**.

Potřebné virtuální stroje

w10-base (w10-base)
w10-domain (w10-domain)

1. Přihlaste se na **w10-base**.
2. Ve **Windows Firewall with Advanced Security** povolte příchozí RDP spojení (**Inbound Rules** – pravidla skupiny **Remote Desktop**)
   (*alternativně*: vypněte firewall)

3. V průzkumníku klikněte pravým tlačítkem myši na **This PC** a zvolte **Properties**. Klikněte na **Remote Settings**.
   (*alternativně*: v nabídce start dejte vyhledat „remote“ v settings a zvolte **Allow remote access to your computer**)
4. V části Remote Desktop zvolte možnost **Allow remote connections to this computer**.
5. Zaškrtněte **Allow connections only from computers running Remote Desktop with Network Level Authentication**.
6. Kliknutím na tlačítko **Select Users** byste mohli přidat uživatele, kteří by měli právo využívat vzdálenou plochu. Uživatel student by již měl mít právo se připojit.
7. Na počítači **w10-domain** spusťte klienta vzdálené plochy **mstsc.exe**.
8. Prozkoumejte možná nastavení klienta před samotným připojením kliknutím na **Options**. Například záložky **Local Resources**, **Experience** nebo **Display**.
9. Připojte se k počítači **w10-base** pomocí IP adresy nebo jména počítače. Použijte účet student (w10-base\student) a heslo **aaa**.
10. Prozkoumejte chybu certifikátu a informace o certifikátu (**View certificate**) a potvrďte **Yes**.
11. Všiměte si, že došlo k přerušení sezení na stanici w10-base a systém je nyní ovlánán ze stanice w10-domain.
12. Ukončete připojení klienta vzdálené plochy.

Lab S04 – Remote Assistance

[Povinné]

1. Přihlaste se na **w10-base**.
   Nyní povolte Vzdálenou pomoc:
2. Ve **Windows Firewall with Advanced Security** ověřte povolení příchozích RA spojení (Inbound Rules – pravidla skupiny Remote Assistance)
   (*alternativně*: vypněte firewall)
3. V průzkumníku klikněte pravým tlačítkem myši na **This PC** a zvolte **Properties**. Klikněte na **Remote Settings**.
   (*alternativně*: v nabídce start dejte vyhledat „remote“ v settings a zvolte **Allow Remote Assistance invitations to be sent from this computer**)
4. Zatrhněte **Allow Remote Assistance Connections To This Computer**. Klikněte na **Advanced** a zatrhněte **Allow this computer to be controlled remotely**.
5. V nabídce **Start** dejte vyhledat „remote assistance“ v settings a zvolte **Invite someone to connect to your PC and help you, or offer to help someone**
6. V průvodci volte následující možnosti:
   - **Invite someone you trust to help you**.
   - **Save the invitation as a file** a vyberte uložení pozvánky do sdíleného adresáře **C:\share**.
     - Pozvánka je xml soubor s koncovkou .msrcIncident a můžete si ji prohlédnout pomocí textového editoru, např. poznmkového bloku.
7. Nyní se Vám objeví okno s heslem. Nezavírat, pozvánka by již nebyla platná.
8. Na **w10-domain** otevřete pozvánku ze sdíleného adresáře **\\w10-base\Share** a zadejte heslo z předchozího bodu.
9. Na **w10-base** akceptujte připojení.
10. Na **w10-domain** se přesvědčte, že nemůžete ovládat vzdálený počítač (*read-only* režim). Zažádejte o předání kontroly (tlačítkem **Request control**).

11. Na **w10-base** povolte převzetí kontroly, ale nedovolte odpovídat na UAC.
12. Na **w10-domain** ověřte, že můžete ovládat počítač, ale nemůžete provádět operace vyžadující zvýšení práv. Pokuste se spustit příkazovou řádku jako **Administrator**. Výzva UAC se zobrazí jen na w10-base.
13. Na **w10-base** zamítněte dotaz UAC**.**
14. Na **w10-base** klikněte na **Stop sharing**, čímž odejmete protistraně kontrolu.
15. Na **w10-domain** znovu zažádejte o převzetí kontroly.
16. Na **w10-base** povolte převzetí kontroly a dovolte odpovídat na UAC.
17. Pokuste se z **w10-domain** spustit příkazovou řádku jako **Administrator**. Nyní se výzva zobarzí oběma a i uživatel, který „pomáhá“ na ni může reagovat.