

# Desktop systémy Microsoft Windows

IW1/XMW1 2014/2015

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 4. 11. 2014

# Brána Firewall

# Brána Firewall

- Omezuje síťový provoz na základě definovaných pravidel
- Dva nástroje pro správu (pravidel) brány Firewall
  - 1) Brána Windows Firewall
  - 2) Brána Windows Firewall s pokročilým zabezpečením
    - Sdílejí databázi pravidel
    - Liší se komplexností definovaných pravidel

# Rozšíření brány Firewall ve Windows

- Podpora tzv. zneviditelnění (funkce *full stealth*)
  - Zabraňuje zjišťování operačního systému (*operating system fingerprinting*)
    - Ochrana proti útokům na konkrétní verzi Windows
  - Vždy povolena (nelze zakázat)
- Ochrana při bootování (*boot time filtering*)
  - V době, kdy dochází k aktivaci jednotlivých síťových rozhraní (lze komunikovat na síti), již brána Firewall běží (u Windows XP nabíhala až později)

# Brána Windows Firewall

- Umožňuje definovat pouze jednoduchá pravidla
  - Definice programů a funkcí systému Windows, jenž mohou komunikovat na síti
- Uzavřený (*closed*) Firewall
  - Co není explicitně povoleno, je zakázáno
- Ve výchozím nastavení blokuje většinu programů
- Umožňuje blokovat veškerou komunikaci
  - Blokování i explicitně povolených programů

# Nástroj Brána Windows Firewall

Brána Windows Firewall

Ovládací panely > Systém a zabezpečení > Brána Windows Firewall

Soubor Upravit Zobrazit Nástroje Nápověda

Hlavní ovládací panel

Povolit aplikaci nebo funkci průchod bránou Windows Firewall

- Změnit nastavení oznámení
- Zapnout nebo vypnout bránu Windows Firewall
- Obnovit výchozí
- Upřesnit nastavení
- Odstranit potíže se sítí

Viz také

Centrum akcí

Centrum síťových připojení a sdílení

## Chraňte svůj počítač pomocí brány Windows Firewall

Brána Windows Firewall může pomoci chránit počítač před tím, aby k němu prostřednictvím Internetu nebo sítě získali přístup hackeři nebo škodlivý software.

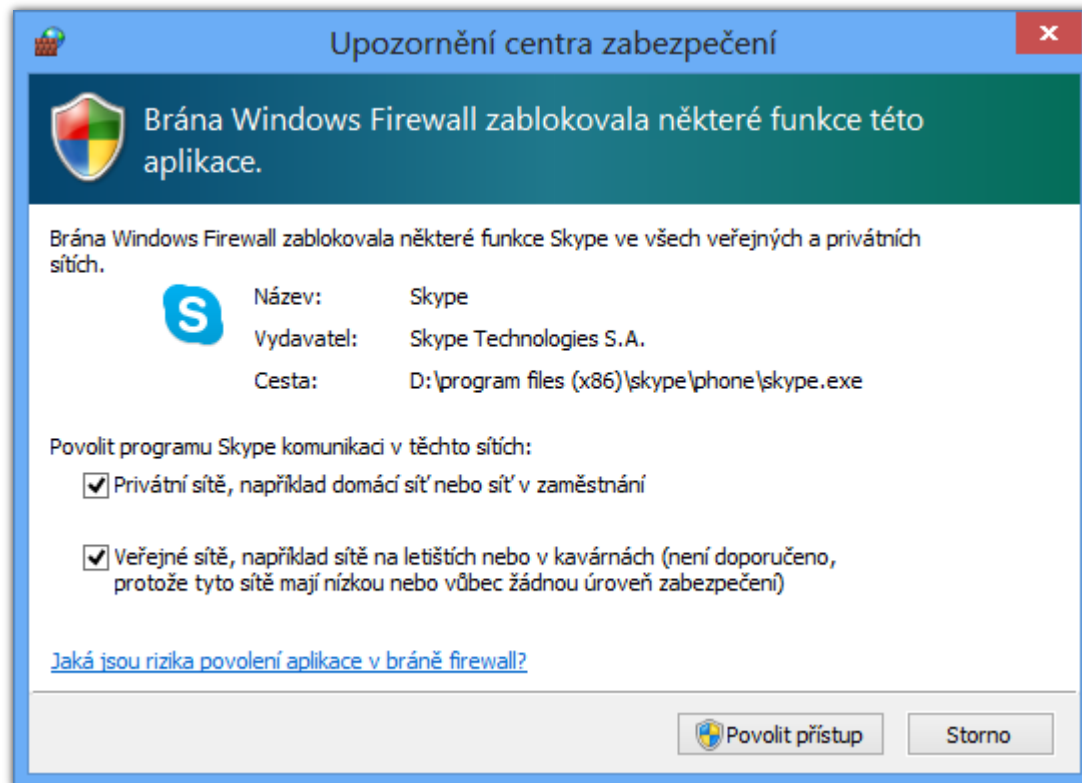
- Privátní síť** Nepřipojeno
- Host nebo veřejné síť** Připojeno

Sítě na veřejných místech, například na letištích nebo v kavárnách

Stav brány Windows Firewall:	Zapnuto
Příchozí připojení:	Blokovat všechna připojení k aplikacím, které nejsou v seznamu povolených aplikací
Aktivní veřejné síť:	<ul style="list-style-type: none"> <li>VUT v Brně</li> <li>eduroam</li> </ul>
Stav oznámení:	Upozorňovat na zablokování nové aplikace bránou Windows Firewall

# Přidání nového pravidla

- Při notifikaci nebo přes nástroj Windows Firewall
  - Pro přidání pravidla jsou potřeba oprávnění správce



# Brána WF s pokročilým zabezpečením

- **WFAS** (*Windows Firewall with Advanced Security*)
- Umožňuje definovat komplexní pravidla
- Filtrování síťového provozu na základě
  - Směru připojení (příchozí / odchozí)
  - Typu protokolu (TCP, UDP, ICMP, ...) a čísla portu
  - Komunikujícího programu, funkce nebo služby
  - IP adres komunikujících počítačů
  - Zabezpečení komunikace
  - Komunikujících počítačů nebo uživatelů



# Výchozí chování

- Uzavřený (*closed*) Firewall pro příchozí připojení
  - Co není explicitně povoleno, je zakázáno
  - Zde náleží pravidla definovaná ve Windows Firewall
- Otevřený (*open*) Firewall pro odchozí připojení
  - Co není explicitně zakázáno, je povoleno
- Chování lze změnit v nastavení WFAS pro každý síťový profil zvlášť

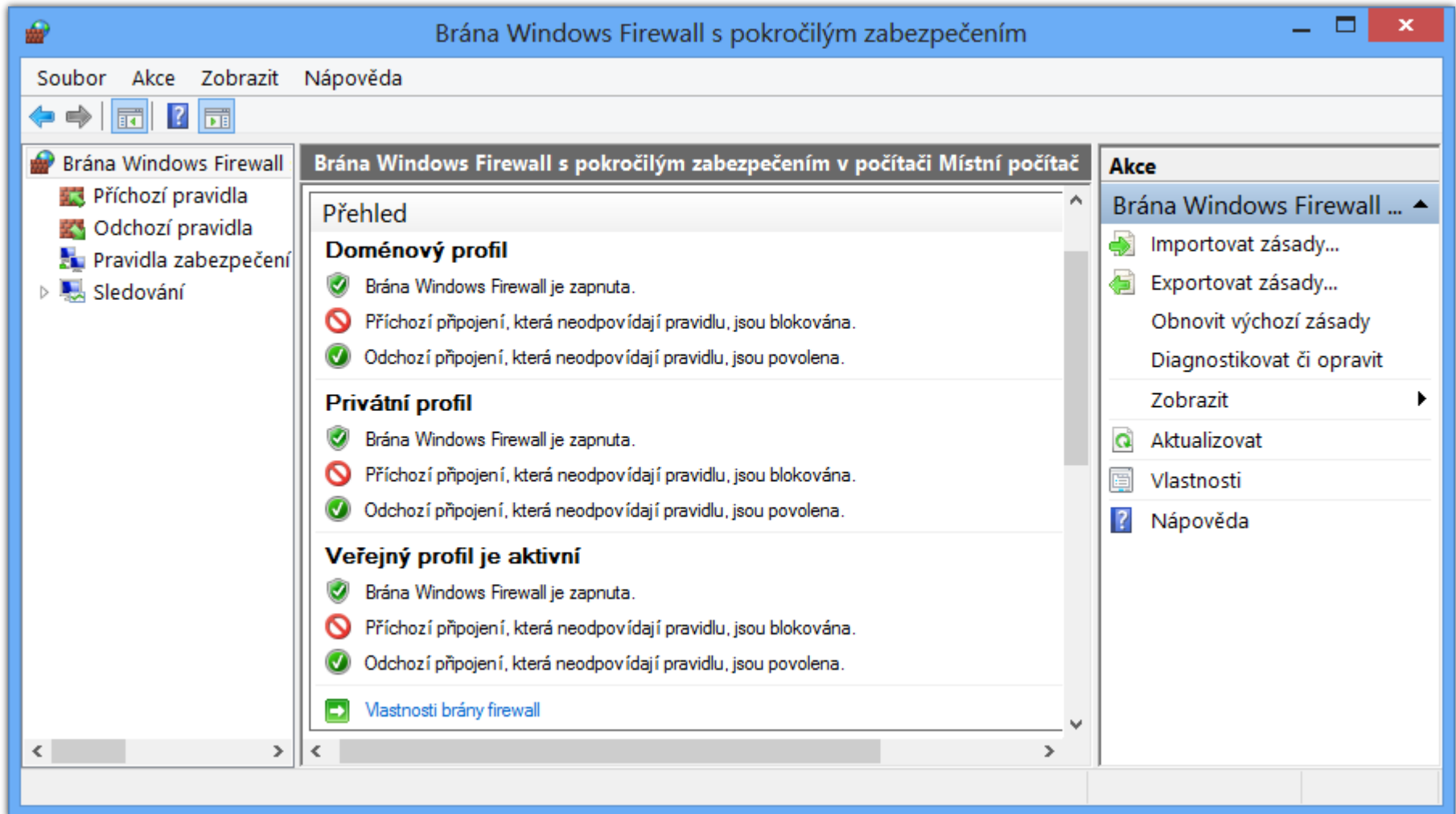
# Síťové profily

- Určují, která pravidla brány Firewall jsou aktivní
  - Jedno pravidlo může být aktivní ve více profilech
- Ovlivňují síťový provoz na konkrétních síťových rozhraních (na rozdíl od Windows Vista)
  - Na každé rozhraní je aplikován právě jeden profil
  - Jeden profil může být aplikován na více rozhraní

# Umístění v síti

- **NLA** (*Network Location Awareness*)
- Přiřazování síťových profilů jednotlivým síťovým rozhraním podle typu sítě, do níž jsou připojeny
- Typy síťových profilů (výběr při připojení do sítě)
  - Privátní síť
  - Veřejná síť
  - Doména
    - Nastaven automaticky při přihlášení klienta do domény

# Výchozí nastavení síťových profilů



# Pravidla brány Firewall

- Povolují (zakazují) síťovou komunikaci (připojení) na základě definovaných podmínek
- Podle směru připojení se dělí na
  - Pravidla pro příchozí připojení (příchozí pravidla)
  - Pravidla pro odchozí připojení (odchozí pravidla)
- Podpora *edge traversal*
  - Možnost povolit či zakázat přijímání nevyžádaných příchozích paketů (např. od zařízení podporujícího překlad adres NAT)

# Pravidla pro základní síťové služby

Brána Windows Firewall s pokročilým zabezpečením

Soubor Akce Zobrazit Nápověda

Brána Windows Firewall

- Příchozí pravidla
- Odchozí pravidla**
- Pravidla zabezpečení
- Sledování

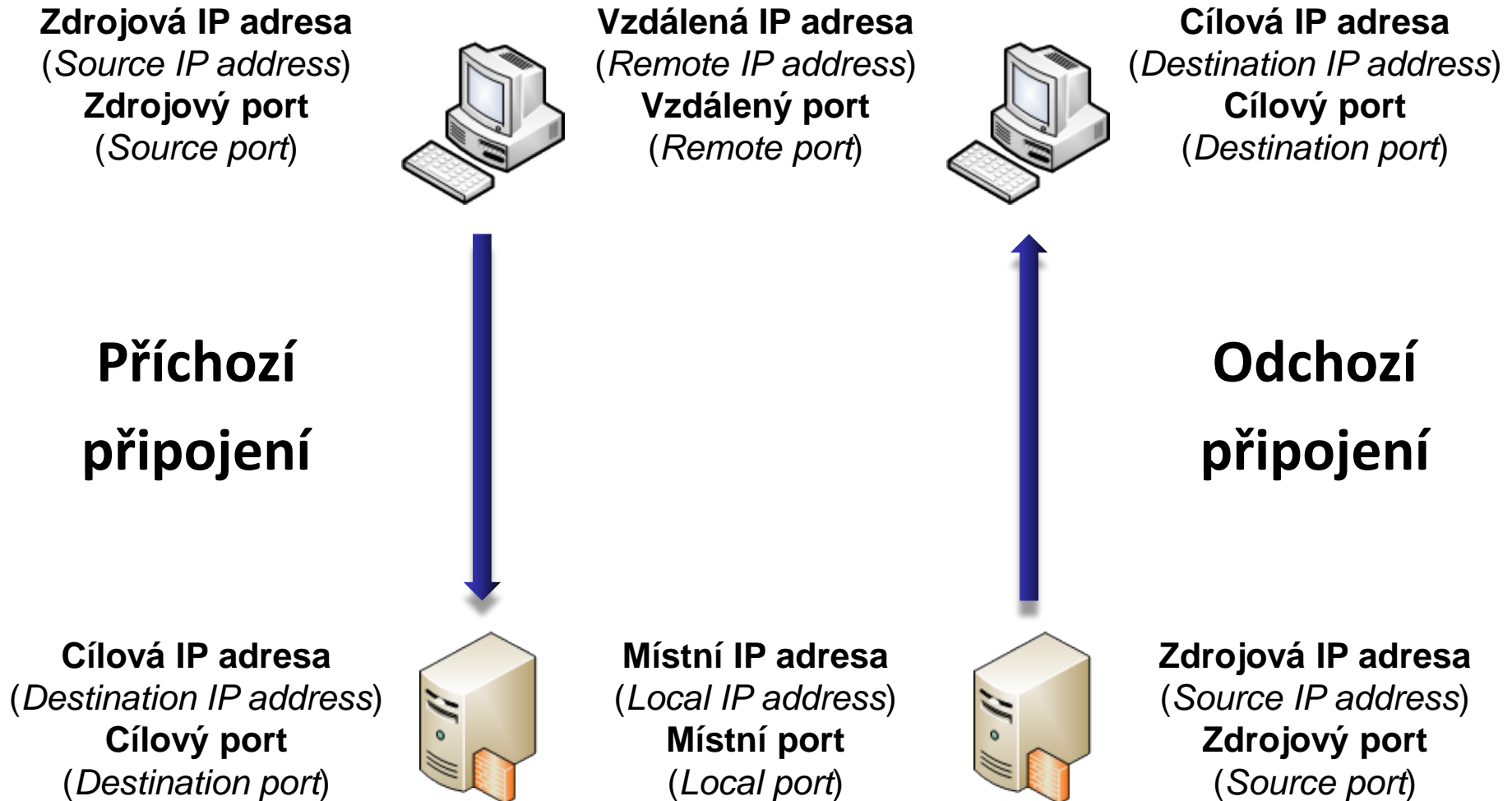
**Odchozí pravidla**

Název	Profil	Akce
✓ Základní síťové služby – byl překročen časový limit (ICMPv6-Out)	Vše	Povolit
✓ Základní síťové služby – dotaz na modul pro naslouchání víces...	Vše	Povolit
✓ Základní síťové služby – inzerování protokolu Neighbor Discov...	Vše	Povolit
✓ Základní síťové služby – inzerování směrovače (ICMPv6-Out)	Vše	Povolit
✓ Základní síťové služby – IPHTTPS (TCP-Out)	Vše	Povolit
✓ Základní síťové služby – modul pro naslouchání vícesměrového...	Vše	Povolit
✓ Základní síťové služby – oslovení protokolu Neighbor Discover...	Vše	Povolit
✓ Základní síťové služby – oslovení směrovače (ICMPv6-Out)	Vše	Povolit
✓ Základní síťové služby – problém parametru (ICMPv6-Out)	Vše	Povolit
✓ Základní síťové služby – protokol DHCP (Dynamic Host Configu...	Vše	Povolit
✓ Základní síťové služby – protokol DHCP (Dynamic Host Configu...	Vše	Povolit
✓ Základní síťové služby – protokol IGMP (Internet Group Manag...	Vše	Povolit
✓ Základní síťové služby – protokol IPv6 (IPv6-Out)	Vše	Povolit
✓ Základní síťové služby – příliš velký paket (ICMPv6-Out)	Vše	Povolit
✓ Základní síťové služby – sestava modulu pro naslouchání víces...	Vše	Povolit
✓ Základní síťové služby – sestava modulu pro naslouchání víces...	Vše	Povolit

**Akce**

- Odchozí pravidla
  - Nové pravidlo...
  - Filtrovat podle profilu ▶
  - Filtrovat podle stavu ▶
  - Filtrovat podle skupiny ▶
  - Zobrazit ▶
  - Aktualizovat
  - Exportovat seznam...
  - Nápověda
- Vybrané položky
  - Povolit pravidlo
  - Vyjmout
  - Kopírovat
  - Odstranit
  - Nápověda

# Příchozí a odchozí pravidla



# Typy a priorita zpracování pravidel

- 1) Pravidla povolující připojení přepisující pravidla blokující připojení (*authenticated bypass*)
  - Vždy povolují pouze zabezpečená připojení
  - Vyžaduje specifikaci autorizovaných počítačů
- 2) Pravidla blokující připojení (*block connection*)
- 3) Pravidla povolující připojení (*allow connection*)
  - Mohou povolovat i nezabezpečená připojení
- 4) Výchozí chování brány Firewall
  - Pravidlo povolující nebo blokující jakékoliv připojení



# Zabezpečená připojení

- K zajištění zabezpečení připojení se využívá IPSec
- Vždy musí být ověřená, liší se zabezpečením dat
  - Ověřená připojení s chráněnou integritou
    - Vyžadována pouze integrita dat (pouze systémy Windows Vista a novější)
  - Šifrovaná připojení
    - Kromě integrity dat je navíc vyžadováno i jejich utajení
  - Připojení s nulovým zapouzdřením
    - Žádné nároky na zabezpečení dat, je vyžadováno pouze ověření připojení (pouze systémy Windows 7 a novější)

# Pravidla zabezpečení připojení

- Definují kdy a jakou metodou musí být ověřeno připojení, aby bylo považováno za zabezpečené
  - Ověření lze vyžadovat nebo jen preferovat
- Nepovolují připojení
- Způsoby ověřování (uživatelů a počítačů)
  - Kerberos v5
  - NTLMv2 (*NT LAN Manager*)
  - Certifikáty
  - Předsdílený klíč (*pre-shared key*) (jen u počítačů)

# Typy pravidel zabezpečení připojení

- Izolace (*isolation*)
  - Omezení komunikace na počítače, jenž jsou schopny se autentizovat pomocí konkrétního pověření
- Výjimka z ověření (*authentication exemption*)
  - Vyloučení specifických počítačů z izolace
- Server-to-server
  - Ověřování připojení mezi konkrétními počítači
- Tunel (*tunnel*)
  - Ověřování připojení v tunelovém režimu IPSec

# Správa pomocí příkazové řádky

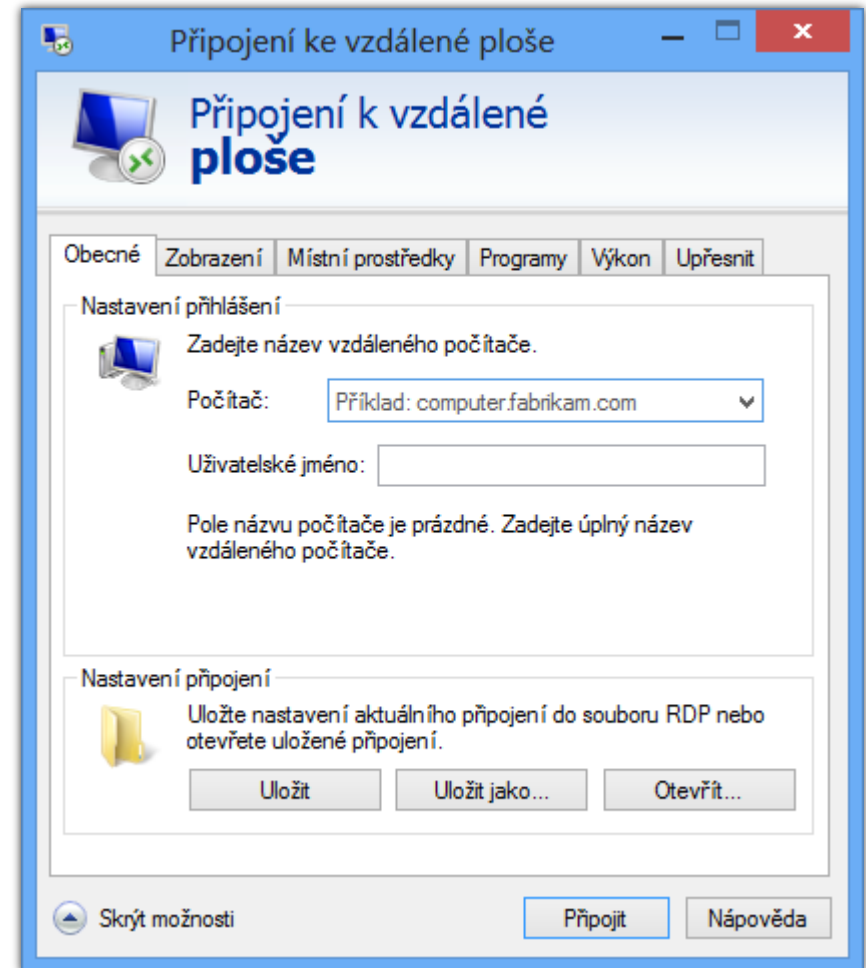
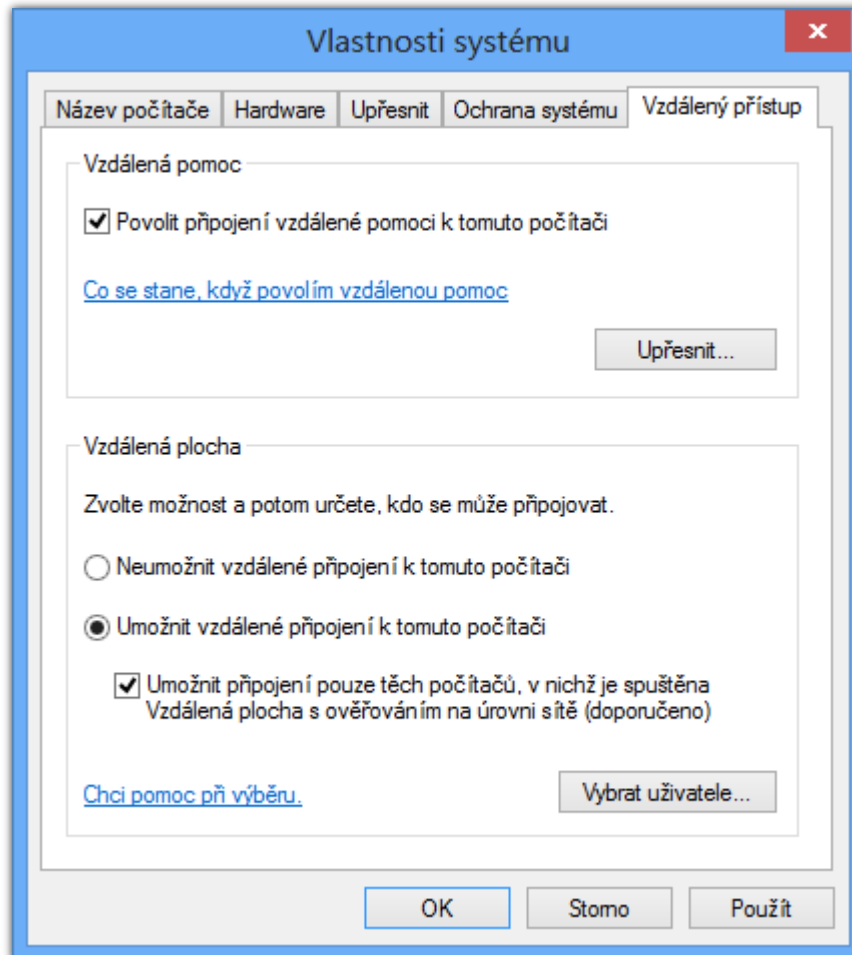
- Pomocí **netsh advfirewall**
  - Vyžaduje oprávnění správce
- Přidání nového pravidla
  - **netsh advfirewall firewall add rule name="<název>" dir={in | out} action={allow | block | bypass} ...**
  - Název pravidla (<název>) nesmí být **all**
    - Zastupuje všechna pravidla brány Firewall
  - Při nastavení akce **bypass** a směru **in** musí být určena skupina vzdálených počítačů a vyžadováno ověření

# Vzdálená správa

# Vzdálená plocha (Remote Desktop)

- Umožňuje se vzdáleně přihlásit k počítači
  - Připojení k odpojenému či nově vytvořenému sezení
- Podpora ověřování na úrovni sítě
  - **NLA** (*network level authentication*)
  - Vyžaduje alespoň Windows XP SP3
- Automatická konfigurace brány Firewall
  - Přidání pravidel brány Firewall povolujících připojení ke vzdálené ploše při povolení vzdálené plochy
- Využívá protokol TCP, naslouchání na portu 3389

# Připojení ke vzdálené ploše



# Vzdálené přihlášení

- Podporováno pouze u edicí Pro a Enterprise
- Mohou se přihlásit
  - Správci počítače (členové skupiny Administrators)
  - Uživatelé vzdálené plochy (členové skupiny Remote Desktop Users)
- Vždy je vyžadováno heslo
  - K účtu, který není chráněn heslem se nelze přihlásit
- V jednom okamžiku může být přihlášen (lokálně nebo vzdáleně) maximálně jeden uživatel



# Souběžné přihlášení více uživatelů

- Pokud je lokálně přihlášen nějaký uživatel a jiný se přihlašuje vzdáleně, musí lokálně přihlášený uživatel povolit vzdálené připojení (a naopak)
  - Po povolení přihlášení jiného uživatele je aktuálně přihlášený uživatel odpojen (*disconnected*)
  - Povolení je vyžadováno i v případě, že se přihlašuje správce (a je přihlášen standardní uživatel)
- Pokud je lokálně přihlášen nějaký uživatel a daný uživatel se připojuje i vzdáleně, je tento uživatel připojen do aktuálního sezení a lokálně odpojen

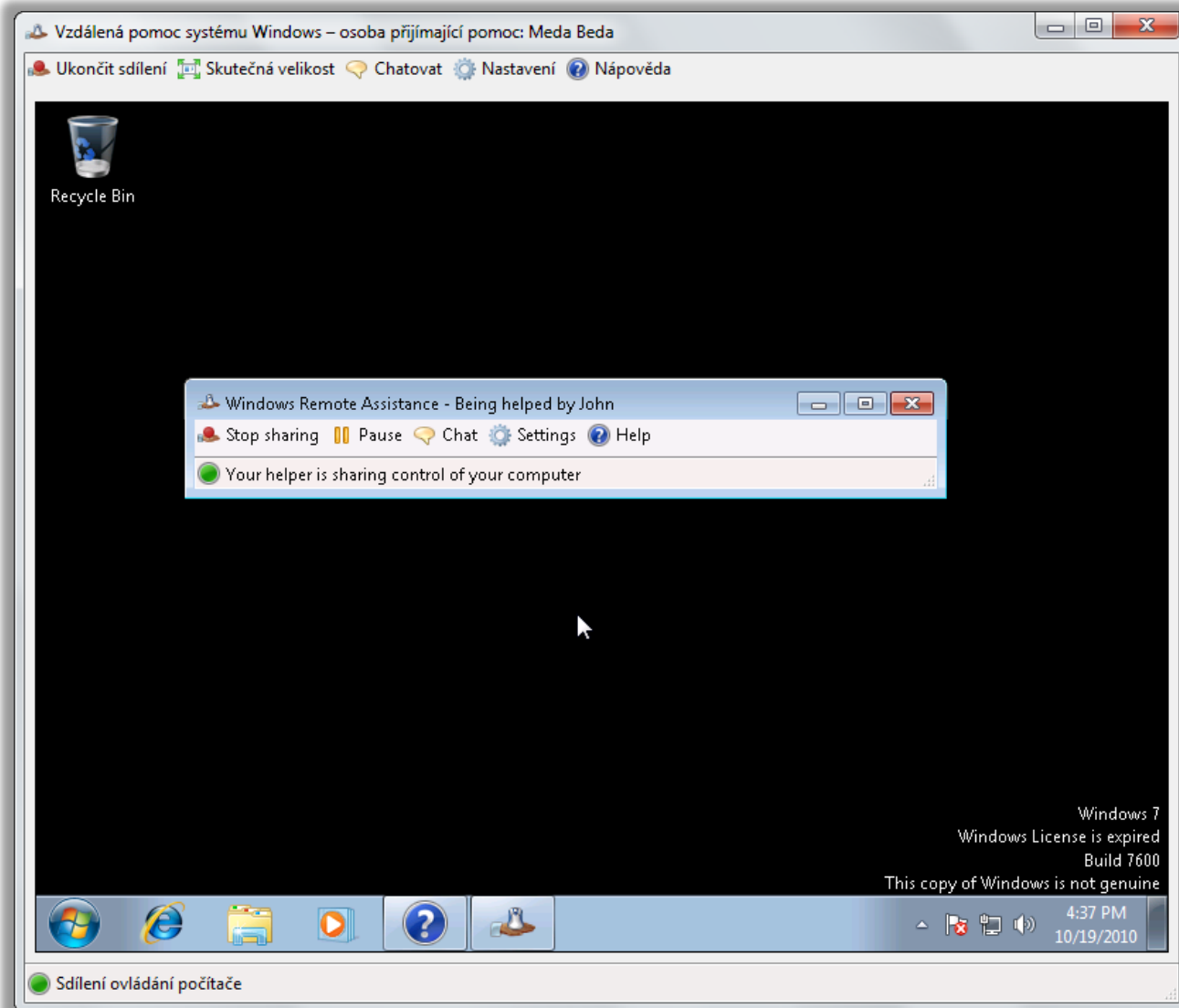
# Místní prostředky ve vzdálené relaci

- Možnost použití místních zařízení a prostředků na vzdáleném počítači (ve vzdálené relaci)
  - Jeví se jako fyzicky přítomné na vzdáleném počítači
- Ve vzdálené relaci lze použít místní
  - Tiskárny
  - Schránku (*clipboard*)
  - Diskové jednotky (oddíly disku)
  - Čipové karty
  - Jiná podporovaná zařízení Plug and Play

# Vzdálená pomoc (Remote Assistance)

- Umožňuje se vzdáleně připojit k počítači
  - Připojení k aktuálně běžícímu sezení
- Automatická konfigurace brány Firewall
- Využívá protokol TCP, naslouchání na portu 3389
- Musí být iniciována na vzdáleném počítači
  - Vzdálený počítač musí odeslat pozvánku (s omezenou dobou platnosti)
  - Uživatel na vzdáleném počítači musí povolit následné připojení (odpověď na pozvánku)

# Vzdálená pomoc systému Windows



# Možnosti vystavení pozvánky

- Uložit pozvánku jako soubor (chráněn heslem)
- Odeslat pozvánku pomocí e-mailu
  - Soubor pozvánky je uložen jako příloha e-mailu
- Použitím nástroje Snadné připojení
  - Automatické ustanovení spojení mezi dvěma počítači
    - Lokalizace vzdáleného počítače na základě zadaného hesla pomocí protokolu PNRP (*Peer Name Resolution Protocol*)
  - Pracuje i napříč sítí internet
  - K dispozici od Windows 7

# Vzdálené připojení

- Připojení lze uskutečnit pouze pokud
  - Nevypršela doba platnosti pozvánky
  - Uživatel na vzdáleném počítači ještě neuzavřel okno Vzdálená pomoc systému Windows
  - Uživatel připojující se na vzdálený počítač zadal heslo
- Vzdáleně připojený uživatel může
  - Sledovat nebo ovládat plochu lokálního uživatele
  - Zasílat zprávy a soubory lokálnímu uživateli
  - Být kdykoliv odpojen lokálním uživatelem

# Vzdálená správa systému Windows

- **WinRM** (*Windows Remote Management*)
- Umožňuje vzdáleně spouštět příkazy na počítači
- Pro zadávání příkazů lze použít
  - Windows Remote Shell (WinRS)
  - Windows PowerShell
- Komunikace pomocí protokolů HTTP nebo HTTPS
  - Data jsou šifrována (při použití HTTP lze vypnout)
  - Pokud není možné ověřovat důvěryhodnost počítačů je potřeba je zadat manuálně (nastavit trusted hosts)

# Konfigurace vzdáleného počítače

- Pomocí WinRM (příkaz **winrm quickconfig**)
  - Konfigurace vyžaduje oprávnění správce
- Konfigurace zahrnuje
  - Spuštění služby Vzdálená správa systému Windows
  - Povolení přihlašování s oprávněními správce (nastavení local account token filter policy)
  - Nastavení naslouchání na portu 5985 pomocí HTTP protokolu (příjem zpráv protokolu WS-Management)
  - Přidání pravidel brány Firewall povolujících připojení ke službě Vzdálená správa systému Windows



# Vzdálené spouštění příkazů

- Pomocí WinRS
  - **winrs -r:[<protokol>://]<počítač> -u:<uživatel> [-p:<heslo>] <příkaz>**
  - Konfigurace pomocí WinRM nebo zásad skupiny
- Pomocí Windows PowerShell verze 2 nebo vyšší
  - **icm -ComputerName [<protokol>://]<počítač> -Credential:<uživatel> <příkaz>**
  - **icm** je alias pro **Invoke-Command**
  - Pro zadání hesla lze místo *uživatele* předat přepínači **-Credential** objekt typu **PSCredential**

# Možnosti ověřování

- Základní (*basic*)
  - Přihlašovací údaje zasílány jako čitelný text
- Algoritmem Digest
  - Zasílán otisk (*hash*) hesla, nevhodný při použití HTTP
- Na základě klientských certifikátů (*certificate*)
- Protokolem Kerberos
- Metodou Vyjednávat (*negotiate*)
  - Kerberos pro doménové účty, NTLM pro lokální účty
- CredSSP (*Credential Security Support Provider*)