

Desktop systémy Microsoft Windows

IW1/XMW1 2012/2013

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 16.10.2012

Windows Firewall

Brána Firewall

- Omezuje síťový provoz na základě definovaných pravidel (výjimek)
- Systém Windows 7 obsahuje dvě brány Firewall
 - 1) **Windows Firewall**
 - 2) **Windows Firewall with Advanced Security (WFAS)**
 - Sdílejí databázi pravidel
 - Liší se komplexností definovaných pravidel

Windows Firewall

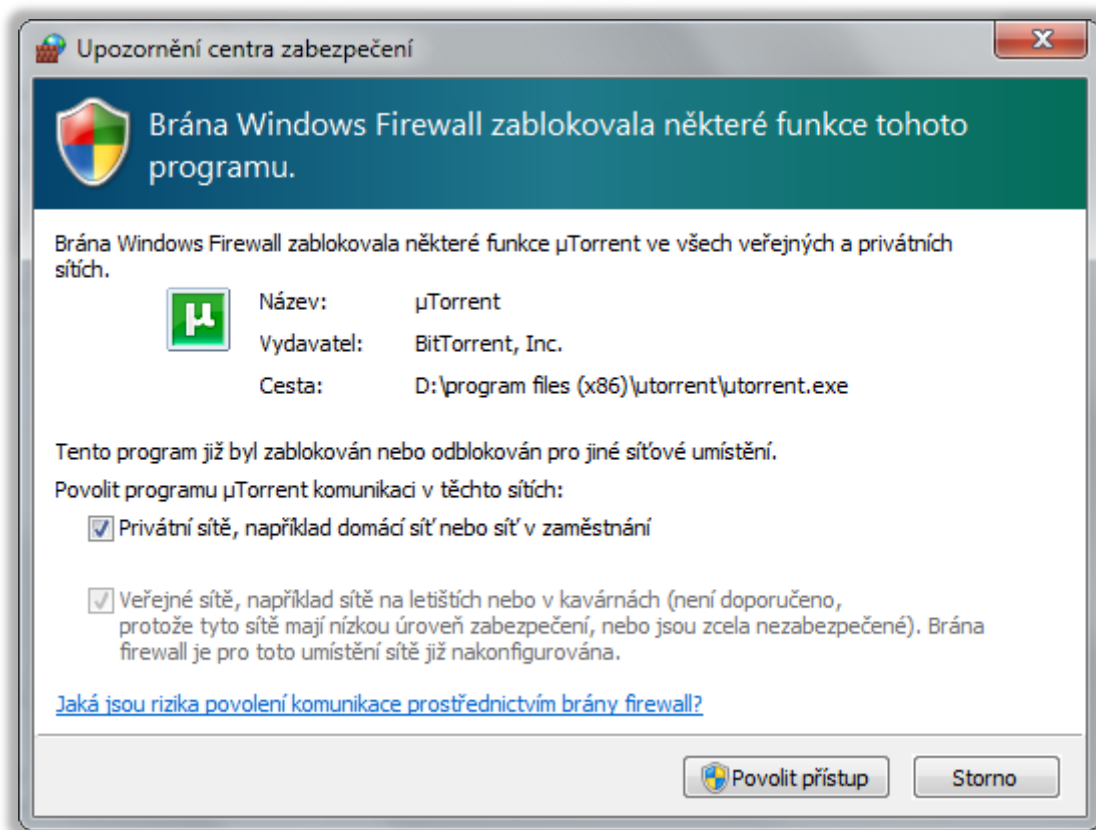
- Umožňuje definovat pouze jednoduchá pravidla
 - Definice programů a funkcí systému Windows, jenž mohou komunikovat na síti
- Uzavřený (*closed*) Firewall
 - Co není explicitně povoleno, je zakázáno
- Ve výchozím nastavení blokuje většinu programů
- Umožňuje blokovat veškerou komunikaci
 - Blokování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

Další funkcionality

- Podpora tzv. zneviditelnění (funkce *Full Stealth*)
 - Zabraňuje zjišťování operačního systému (*Operating System fingerprinting*)
 - 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)

Přidání nového pravidla

- Při notifikaci nebo v nastavení **Windows Firewall**
 - Pro přidání pravidla jsou potřeba oprávnění správce



Umístění v síti

- **Network Location Awareness (NLA)**
- Přiřazování síťových profilů jednotlivým síťovým rozhraním podle typu sítě, do níž jsou připojeny
- Typy síťových profilů (výběr při připojení do sítě)
 - Domácí síť
 - Pracovní síť (Síť v zaměstnání)
 - Veřejná síť
 - Doména (nastaven automaticky při přihlášení klienta do domény **Active Directory**)

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
- Windows Firewall nerozlišuje domácí a pracovní síťové profily (brány jako jeden profil)

Rozhraní Windows Firewall

Všechny položky Ovládacích ... Brána Windows Firewall Prohledat Ovládací panely

Hlavní ovládací panel

- Povolit program nebo funkci průchod branou 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 počítačové podvodníci nebo škodlivý software.

[Jak brána firewall pomáhá chránit počítač?](#)
[Co jsou umístění v síti?](#)

Domácí nebo pracovní (privátní) síť	Připojeno
Síť doma nebo na pracovišti, kde znáte uživatele a zařízení v síti a důvěřujete jim.	
Stav brány Windows Firewall:	Zapnuto
Příchozí připojení:	Blokovat všechna připojení k programům, které nejsou v seznamu povolených programů
Aktivní domácí nebo pracovní (privátní) síť:	HomeWiFi
Stav oznámení:	Upozorňovat na zablokování nového programu branou Windows Firewall
Veřejné síť	Nepřipojeno

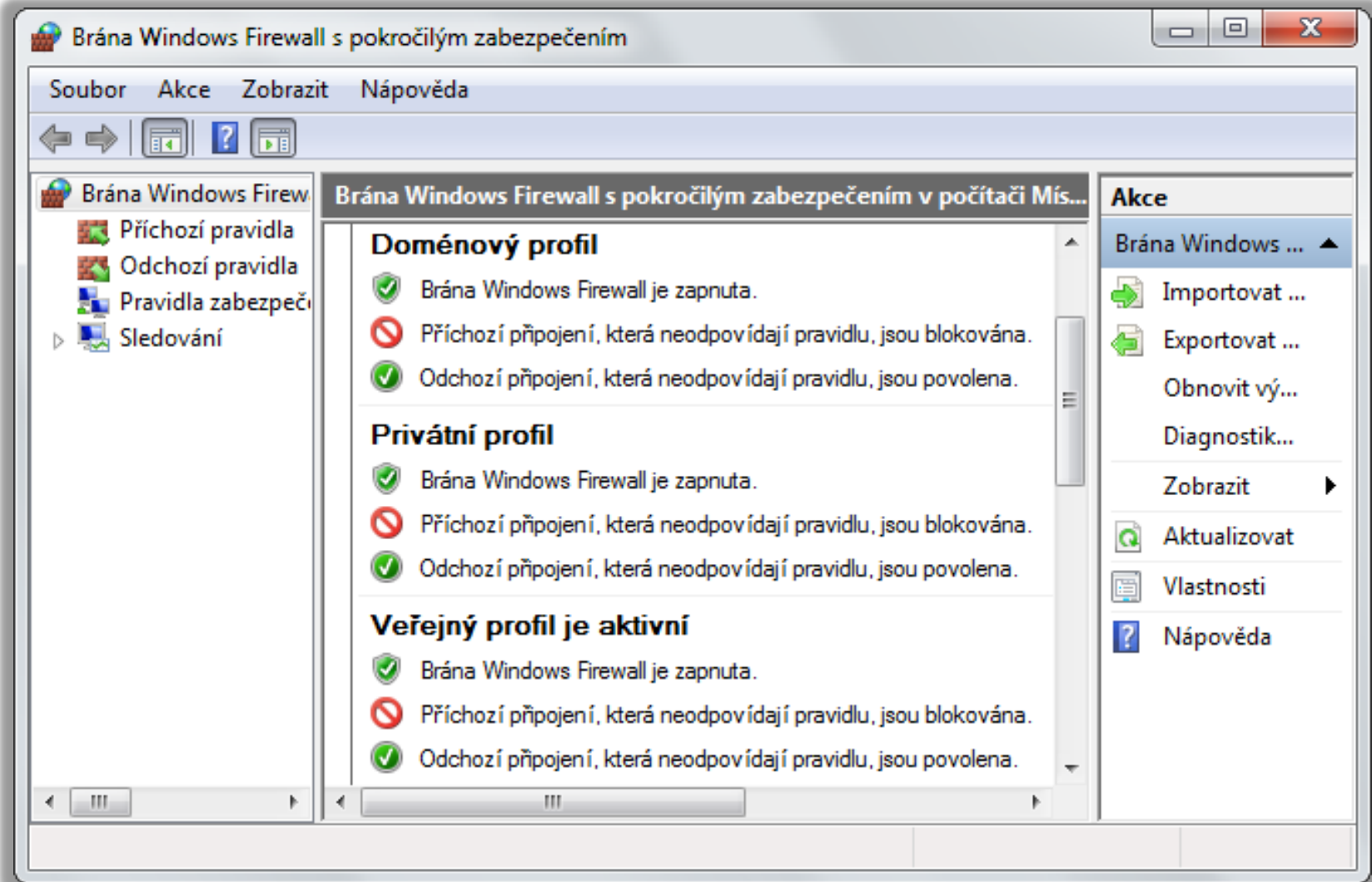
WFAS

- **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 WFAS

- Uzavřený (*closed*) Firewall pro příchozí připojení
 - Co není explicitně povoleno, je zakázáno
 - Uložení pravidel definovaných ve **Windows Firewall**
- Otevřený (*open*) Firewall pro odchozí připojení
 - Co není explicitně zakázáno, je povoleno
- Chování lze změnit v nastavení **WFAS**

Výchozí nastavení 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

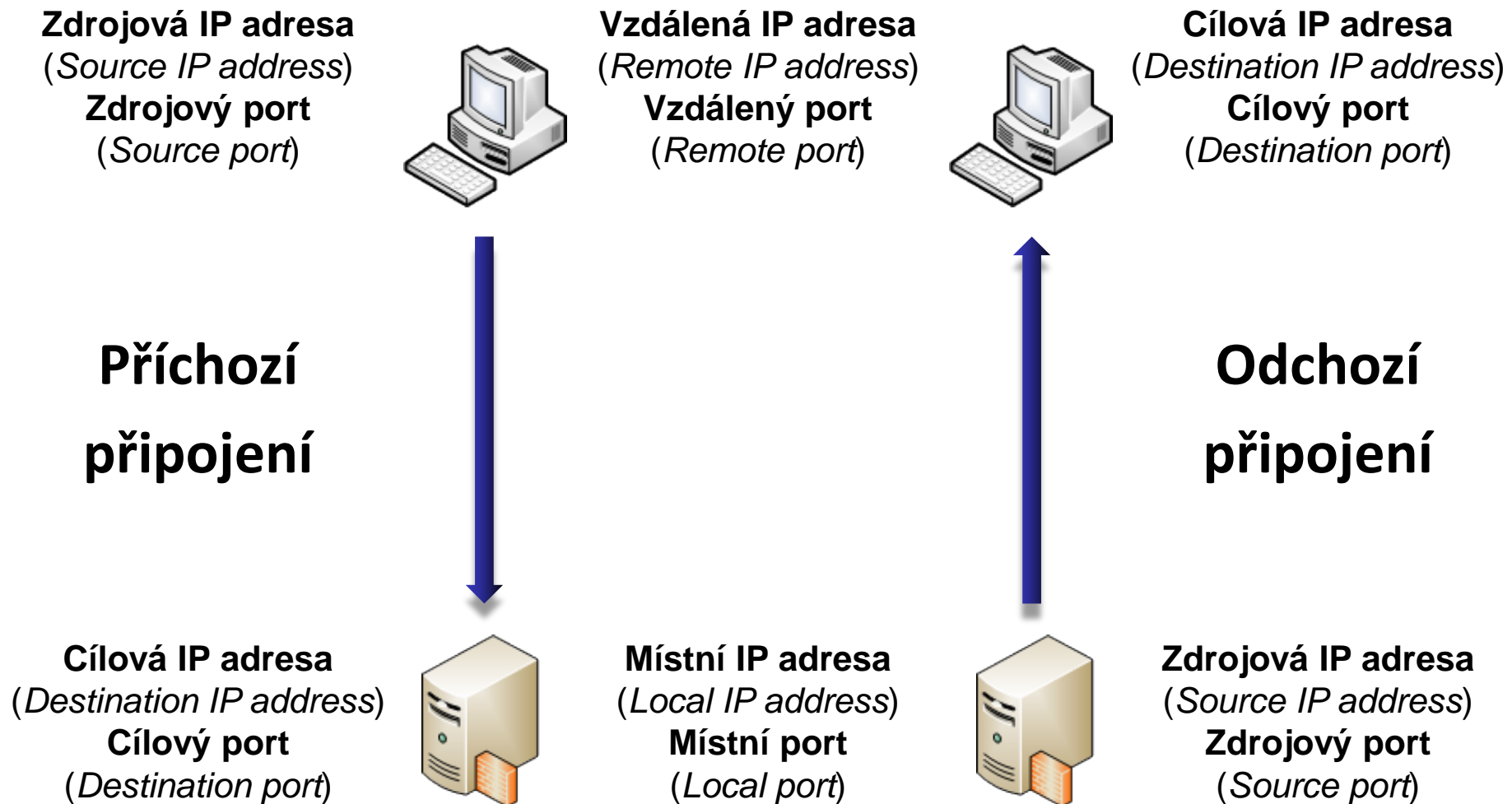
Odchozí pravidla Filtrovat podle: Povolené

Název	Skupina	Profil	Povoleno
✓ Základní síťové služby – byl překročen č...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – dotaz na modul...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – inzerování prot...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – inzerování smě...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – IPHTTPS (TCP-...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – modul pro nasl...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – oslovení protok...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – oslovení směro...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – problém param...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – protokol DHCP ...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – protokol DHCP ...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – protokol IGMP (...)	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – protokol IPv6 (I...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – příliš velký pake...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – sestava modulu...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – sestava modulu...	Základní síťové služby	Vše	Ano
✓ Základní síťové služby – služba Teredo (...)	Základní síťové služby	Vše	Ano

Akce

- Odchozí pravidla
- Nové pravi...
- Filtrovat po...
- Filtrovat po...
- Filtrovat po...
- Vymazat vš...
- Zobrazit
- Aktualizovat
- Exportovat ...
- 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

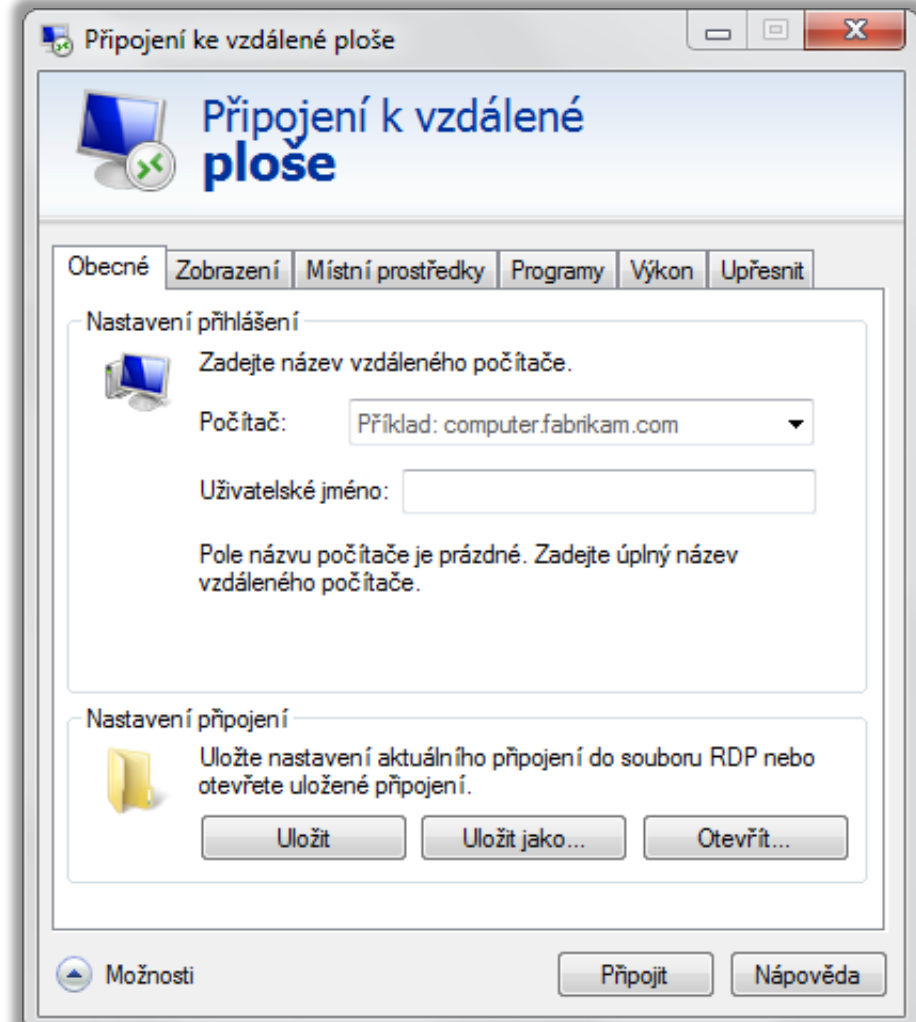
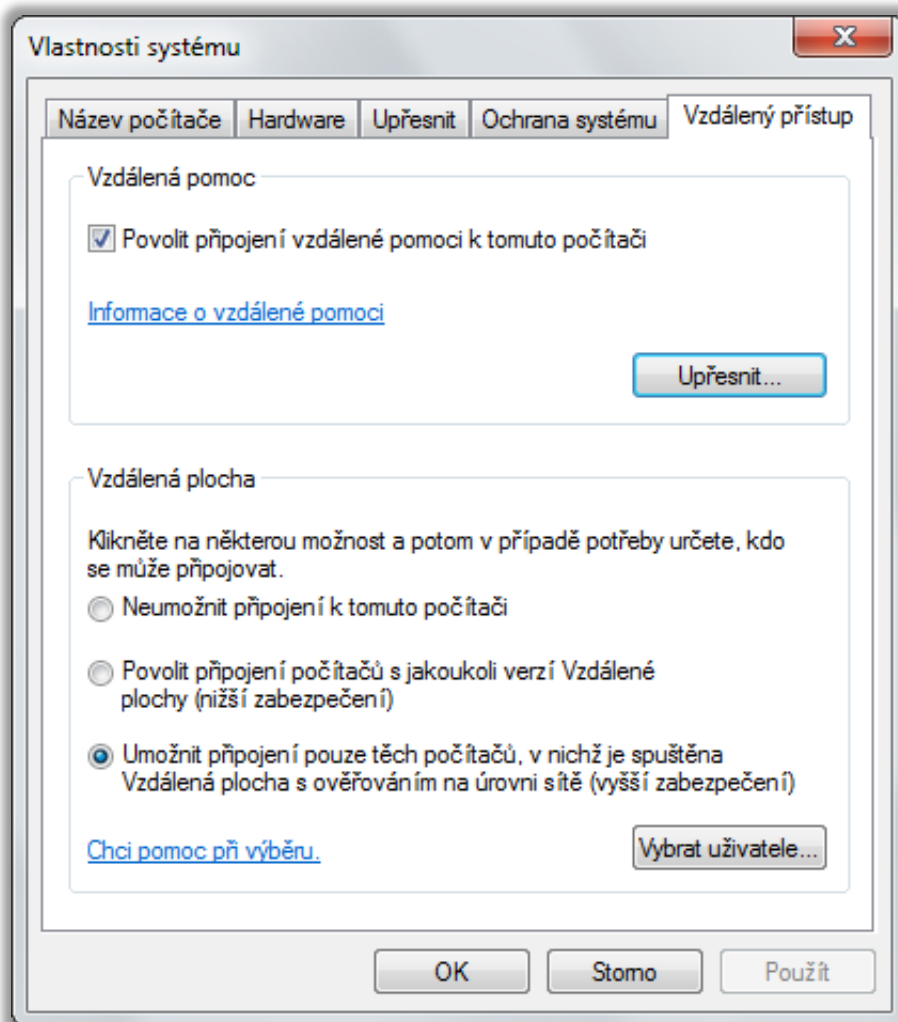
- Pomocí **netsh advfirewall**
 - Vyžaduje oprávnění správce
- Přidání nového pravidla
 - **netsh advfirewall firewall add rule name="<název>" dir={in | out} action={allow | block | bypass} ...**
 - Název pravidla (<název>) nesmí být **all**
 - Zastupuje všechna pravidla brány Firewall
 - Při nastavení 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 (*Network Level Authentication*)
 - Vyžaduje systém Windows XP SP3 nebo novější
- 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

- Je možné pouze u edicí Professional a vyšších
- 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 tento uživatel se připojuje i vzdáleně, je tento uživatel připojen do aktuálního sezení a lokálně odpojen

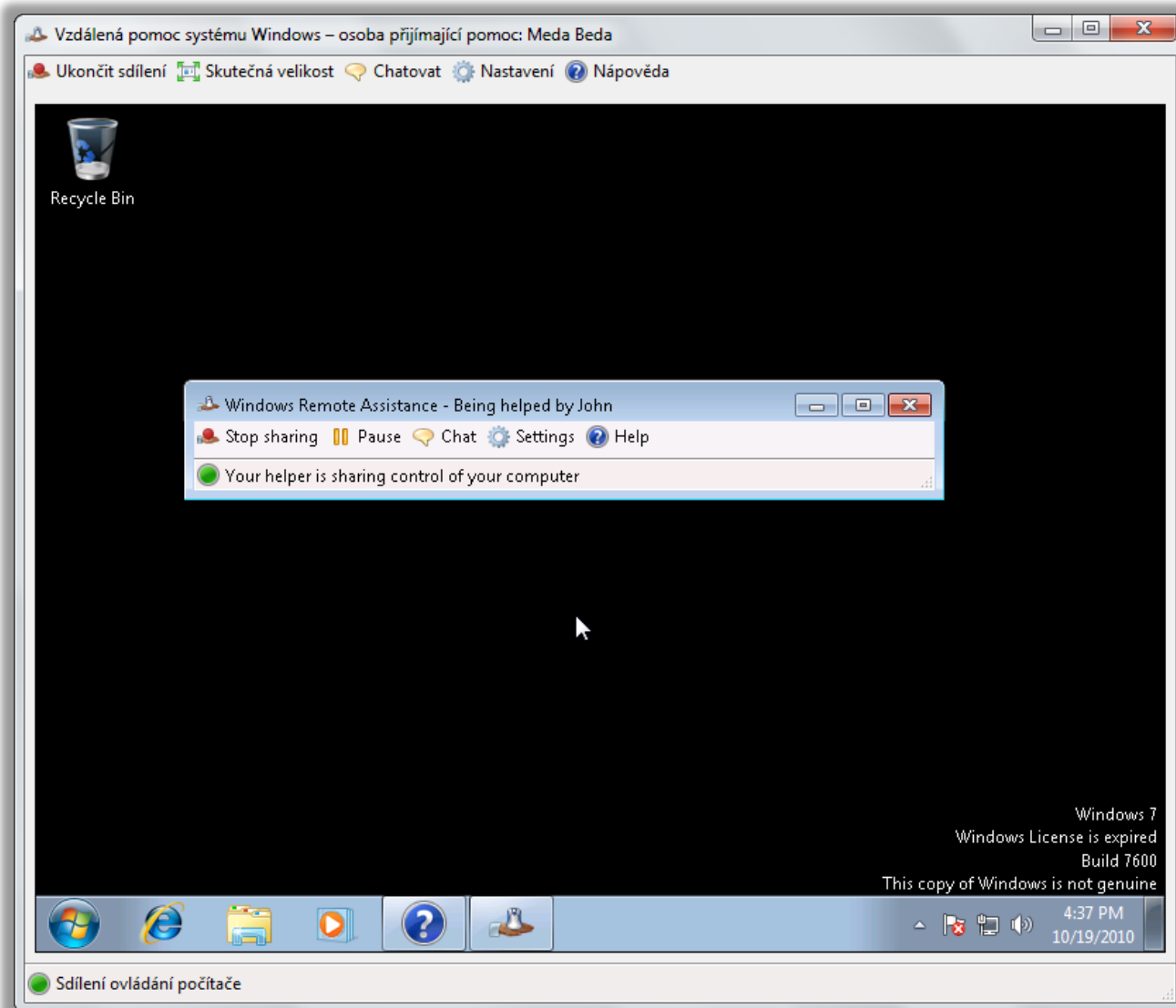
Místní prostředky ve vzdálené relaci

- 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**
 - Vyžaduje systém Windows 7 nebo novější
 - Lokalizace vzdáleného počítače na základě zadaného hesla pomocí protokolu PNRP (*Peer Name Resolution Protocol*)
 - Pracuje i napříč sítí internet

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

- **Windows Remote Management (WinRM)**
- 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

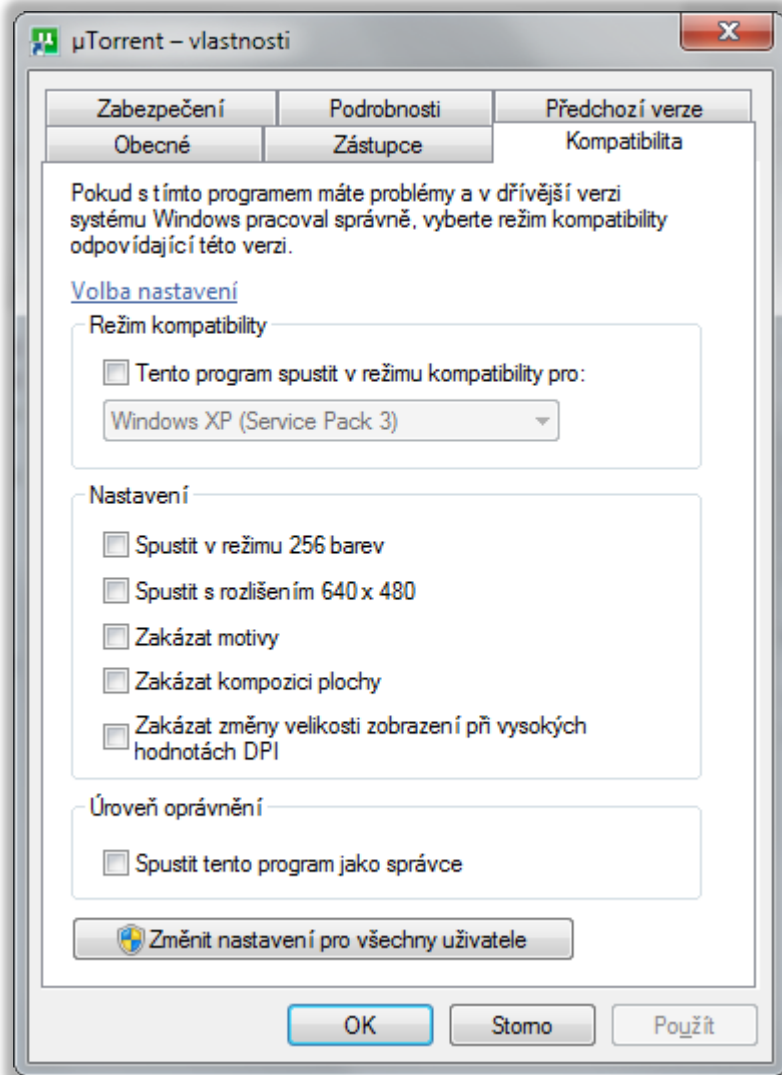
- Základní (*Basic*)
 - Přihlašovací údaje zasílány jako čitelný text
- Algoritmem Digest
 - Zasílán otisk (*hash*) hesla, nevhodný při použití HTTP
- Na základě klientských certifikátů (*Certificate*)
- Protokolem Kerberos
- Metodou Vyjednávat (*Negotiate*)
 - Kerberos pro doménové účty, NTLM pro lokální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

Kompatibilita aplikací

Kompatibilita programů

- Řešení problémů s během starších programů
 - Neřeší problémy s instalací
- Simulace chování starších systémů Windows
 - Windows 95 až Vista / 7, NT 4.0 až Server 2008 (R2)
- Konfigurace kompatibility programů
 - Manuálně ve vlastnostech daného programu
 - Automaticky nástrojem Kompatibilita programů
- Nelze nastavovat u programů systému Windows

Nastavení kompatibility programu



- Zakázat kompozici plochy vypíná některé funkce uživatelského rozhraní Aero, např. průhlednost
- Pokud má být program spouštěn s oprávněními správce, musí uživatelé, jenž ho chtějí spouštět, sami disponovat těmito oprávněními

Application Compatibility Toolkit (ACT)

- Sada nástrojů pro usnadnění řešení problémů s kompatibilitou aplikací
 - Součást Windows ADK
- Obsahuje
 - Application Compatibility Manager (ACM)
 - Compatibility Administrator
 - Internet Explorer Compatibility Test Tool
 - Setup Analysis Tool
 - Standard User Analyzer

Application Compatibility Manager

- Umožňuje sběr a následnou analýzu dat
- Sběr veškerých dat zajišťují tzv. balíky kolekcí dat (DCP, *Data Collection Packages*)
 - Zahrnují jeden či více monitorovacích nástrojů (tzv. Compatibility Evaluators)
 - Nasazovány manuálně nebo pomocí zásad skupiny, logon skriptů či SCCM
 - Uložení dat v Microsoft SQL Server databázi
- Analýzou dat lze dopředu určit možné problémy s kompatibilitou používaných aplikací

Compatibility Evaluators

- Inventory Collector
 - Sbírá informace o systému a obsažených aplikacích
- User Account Control Compatibility Evaluator
 - Identifikuje možné problémy s UAC
- Update Compatibility Evaluator
 - Identifikuje možné dopady instalací aktualizací
- Windows Compatibility Evaluator
 - Identifikuje možné problémy s používáním starých komponent nebo dynamických knihoven systému

Compatibility Administrator

- Spravuje a poskytuje řešení problémů týkajících se kompatibility aplikací
- Compatibility fix (také označován jako Shim)
 - Speciální software odchyťující API volání z aplikací a modifikující tyto volání tak, aby se chovaly tak jako v předchozích verzích systému Windows
 - Řešení pro velkou řadu aplikací lze najít v Microsoft Application Compatibility Database
 - Lze vytvořit manuálně nebo pomocí různých nástrojů obsažených v ACT

Další nástroje

- Internet Explorer Compatibility Test Tool
 - Umožňuje ověřovat kompatibilitu webových stránek a webových aplikací v Internet Explorer 8
- Setup Analysis Tool
 - Monitoruje instalace aplikací (např. změny souborů a registrů chráněných systémem apod.)
- Standard User Analyzer
 - Hledá problémy, jenž může způsobovat UAC

Windows XP Mode

- Virtuální stroj obsahující systém Windows XP
 - Běží v prostředí Microsoft Virtual PC
- Veškeré nainstalované aplikace jsou k dispozici přímo v hostitelském systému (Windows 7)
 - Běží ve svém vlastním okně (jeví se jako standardní součást hostitelského systému)
 - Po instalaci se automaticky přidají do nabídky Start (složka Aplikace prostředí Windows XP Mode)
 - Mají vyšší nároky na zdroje (pro jejich spuštění musí běžet celý virtuální stroj)

Spuštění aplikace



Požadavky a omezení

- K dispozici jen v edicích Professional a vyšších
- Vyžaduje podporu hardwarové virtualizace (buď AMD-V nebo Intel VT)
- Vyžaduje alespoň 2 GB RAM
 - 256 MB využívá virtuální stroj
- Podporuje pouze 32 bitový systém Windows XP
 - Nelze instalovat 64 bitové aplikace
- Potřeba údržby virtuálního stroje
 - Obsažený systém je nutné aktualizovat a spravovat