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 9.12.2012

BranchCache

BranchCache

- Urychluje přístup k souborům a WWW stránkám uložených na vzdálených File a Web serverech
  - Kešování obsahu těchto serverů v rámci lokální sítě
  - Na serverech musí běžet Windows Server 2008 R2
- Novinka v systémech Windows 7 (edice Ultimate nebo Enterprise) a Windows Server 2008 R2
- Může pracovat ve dvou režimech
  - Režim hostované mezipaměti (*Hosted Cache*)
  - Režim distribuované mezipaměti (*Distributed Cache*)

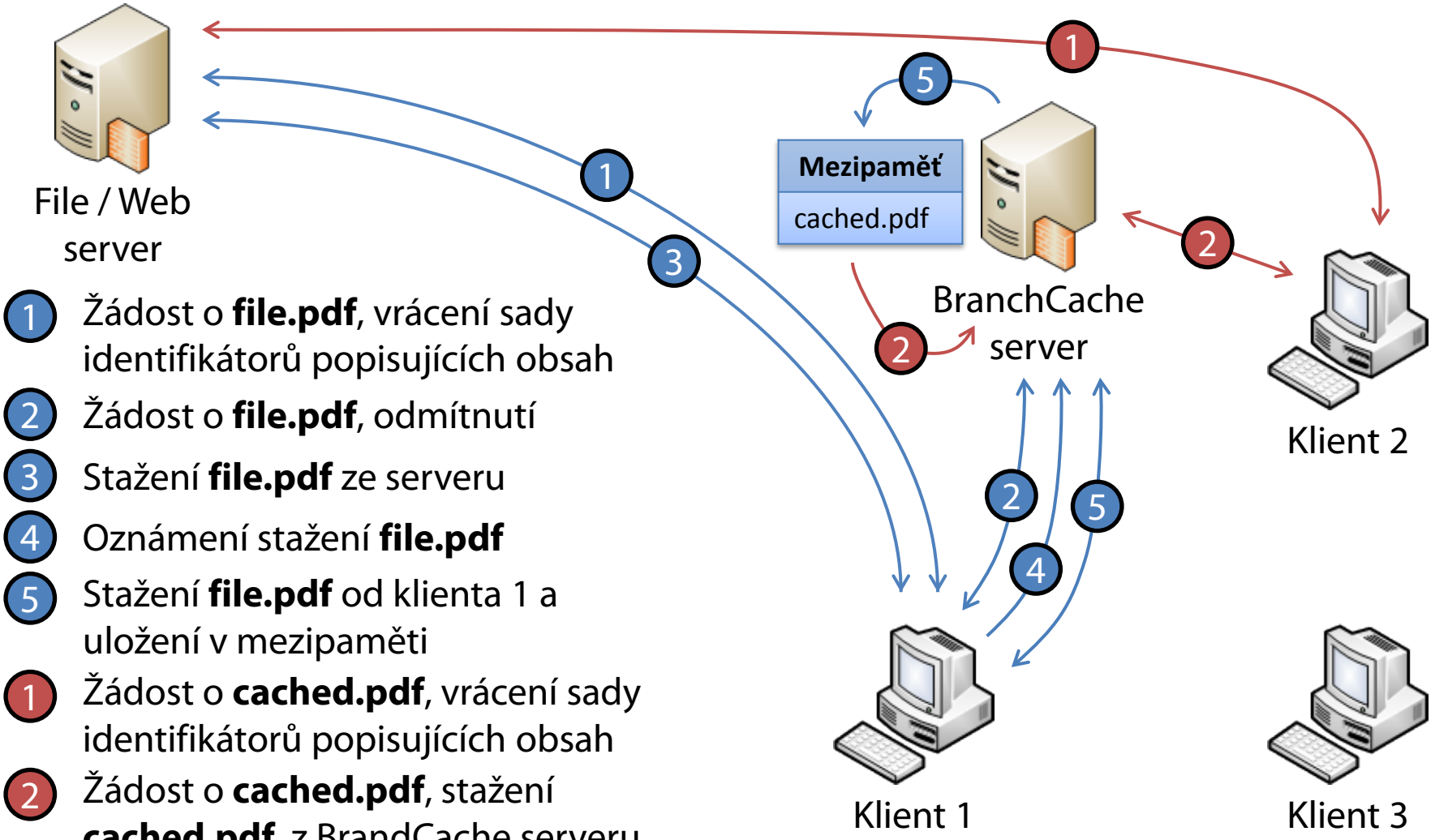
Základní princip činnosti

1) Klient ověří, zda server podporuje BranchCache
2) Klient ověří, zda doba odezvy sítě mezi počítači překračuje nastavenou prahovou hodnotu
   - Ve výchozím nastavení je práh 80 milisekund
3) Klient ověří, zda jsou v mezipaměti v lokální síti přítomna požadovaná data
   - Pokud data v mezipaměti jsou, ověří se, jestli jsou aktuální a zda má klient oprávnění k nim přistoupit
   - Pokud data v mezipaměti nejsou, jsou automaticky stažena ze serveru a uložena v mezipaměti

Režim hostované mezipaměti

- Mezipaměť je umístěna na serveru se systémem Windows Server 2008 R2 nebo novějším
  - Dostupný celý obsah mezipaměti
- Použití vyžaduje
  - Instalaci funkce BranchCache na serveru
  - Spárování SSL certifikátu s BranchCache na serveru
    - **netsh http add sslcert ipport=0.0.0.0:443 certhash=*<otisk>* APPID={d673f5ee-a714-454d-8de2-492e4c1bd8f8}**
  - Nastavení důvěry k tomuto SSL certifikátu na všech klientských počítačích

Ilustrace hostované mezipaměti

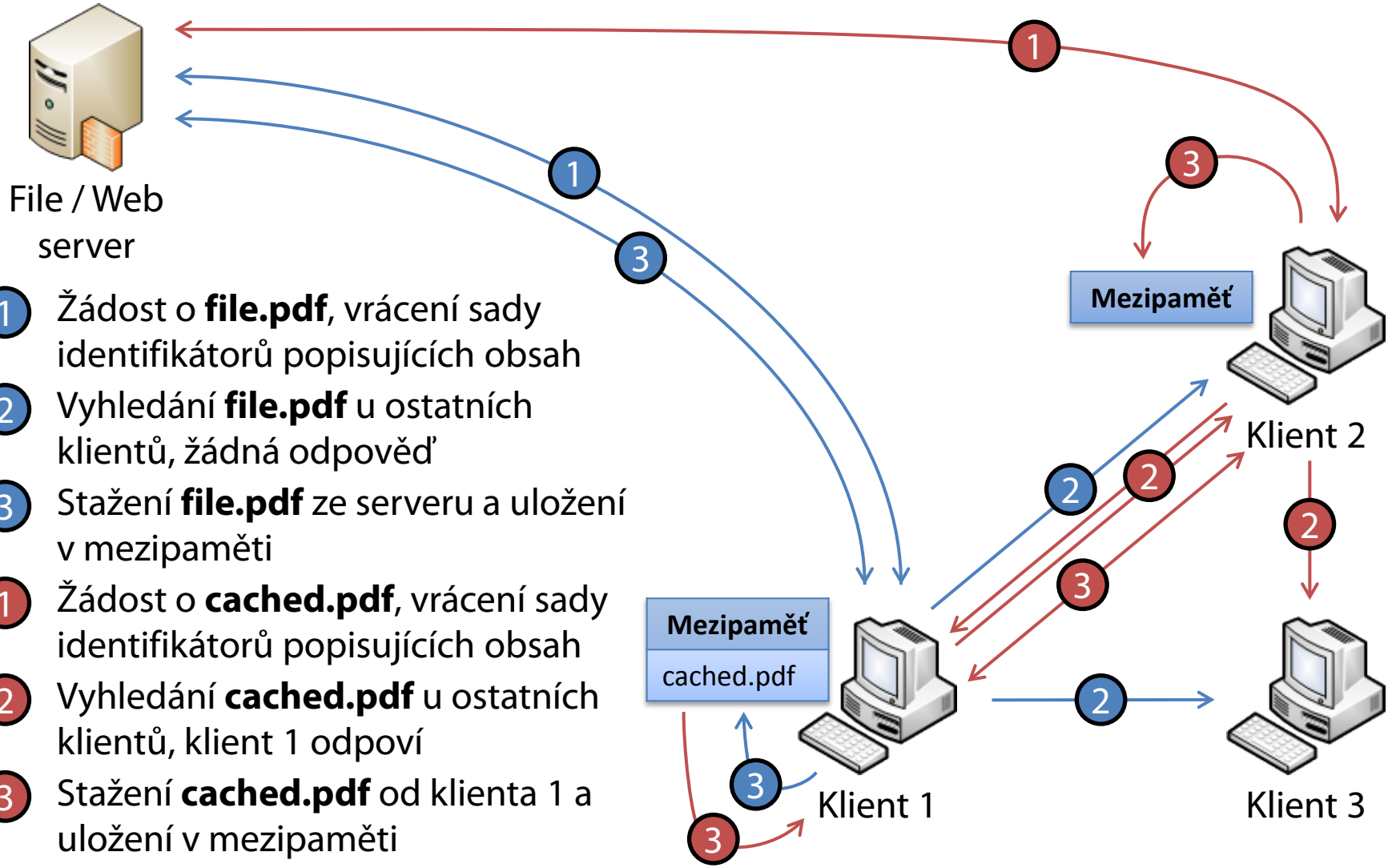


1. Žádost o **file.pdf**, vrácení sady identifikátorů popisujících obsah
2. Žádost o **file.pdf**, odmítnutí
3. Stažení **file.pdf** ze serveru
4. Oznámení stažení **file.pdf**
5. Stažení **file.pdf** od klienta 1 a uložení v mezipaměti
1. Žádost o **cached.pdf**, vrácení sady identifikátorů popisujících obsah
2. Žádost o **cached.pdf**, stažení **cached.pdf** z BrandCache serveru

Režim distribuované mezipaměti

- Mezipaměť je rozprostřena mezi více klientských počítačů (se systémem Windows 7 / 8)
  - Každý klientský počítač obsahuje jen část mezipaměti
  - Nemusí být dostupný celý obsah mezipaměti
- Části mezipaměti se mohou překrývat
  - Jeden soubor může být kešován na více klientských počítačích zároveň
  - Kopírování kešovaných dat mezi klienty, pokud jiný klient již má požadovaná data kešována

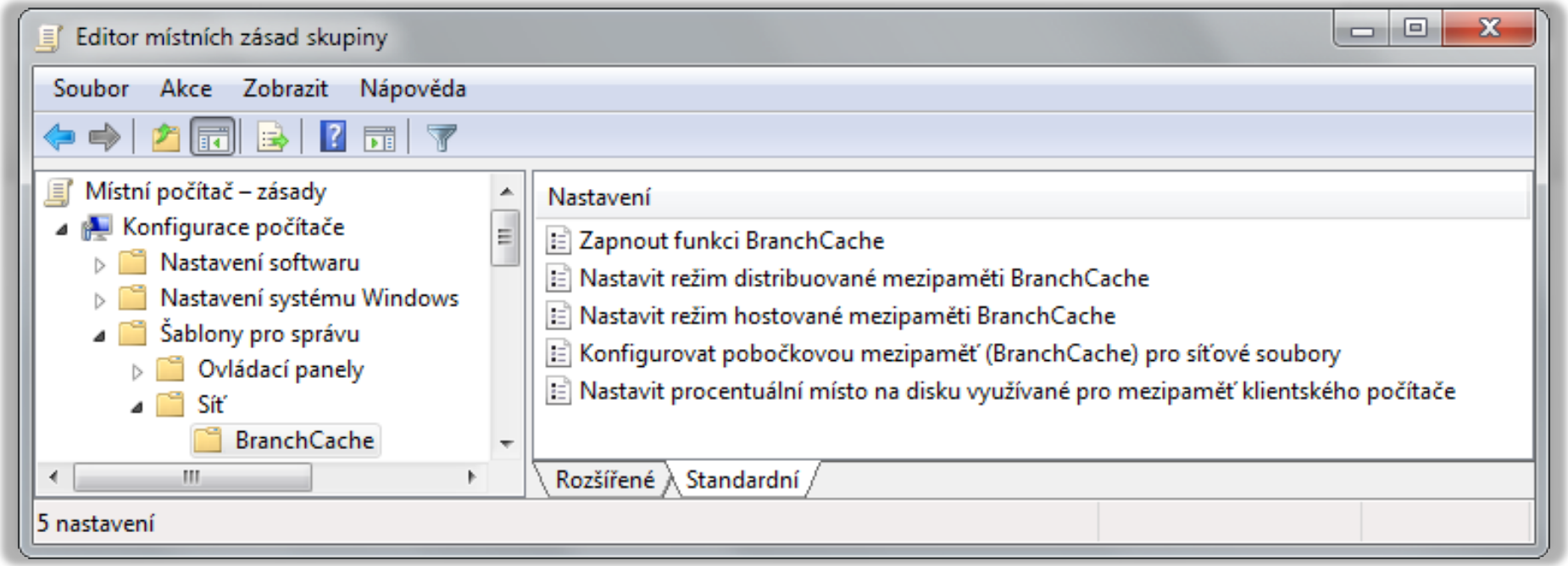
Ilustrace distribuované mezipaměti



1. Žádost o **file.pdf**, vrácení sady identifikátorů popisujících obsah
2. Vyhledání **file.pdf** u ostatních klientů, žádná odpověď
3. Stažení **file.pdf** ze serveru a uložení v mezipaměti
1. Žádost o **cached.pdf**, vrácení sady identifikátorů popisujících obsah
2. Vyhledání **cached.pdf** u ostatních klientů, klient 1 odpoví
3. Stažení **cached.pdf** od klienta 1 a uložení v mezipaměti

Nastavení BranchCache klientů

- Přes zásady skupiny
  - Nevytváří potřebná pravidla brány Firewall



- Pomocí nástroje **netsh**

Potřebná pravidla brány Firewall

- Režim hostované mezipaměti
  - BranchCache - načtení obsahu
    - Příchozí a odchozí pravidlo, protokol TCP, port 80 (HTTP)
  - BranchCache - server hostované mezipaměti
    - Odchozí pravidlo, protokol TCP, port 443 (HTTPS)
- Režim distribuované mezipaměti
  - BranchCache - načtení obsahu
    - Příchozí a odchozí pravidlo, protokol TCP, port 80 (HTTP)
  - BranchCache - zjišťování rovnocenných zařízení
    - Příchozí a odchozí pravidlo, protokol UDP, port 3702 (WSD)

Nastavení pomocí příkazové řádky

- Automaticky vytváří pravidla pro bránu Firewall
- Vyžaduje oprávnění správce
- Povolení a nastavení BranchCache
  - **netsh BranchCache set service mode={distributed | hostedclient | local } [location=<*server*>]**
  - Režim **local** povolí BranchCache s lokální mezipamětí (režim distribuované mezipaměti bez jejího sdílení)
- Nastavení adresáře pro uložení mezipaměti
  - **netsh BranchCache set localcache <*adresář*>**

DirectAccess a VPN spojení

Virtuální privátní sítě (VPNs)

- Zabezpečené tunely zpřístupňující obsah firemní sítě (intranetu) autorizovaným uživatelům
  - Umožňují přístup k prostředkům firemní sítě (sdílené složky, tiskárny, firemní servery, …) přes síť internet
- Vytváření přes Nastavit nové připojení nebo síť v Centru síťových připojení a sdílení
  - Podpora 4 VPN protokolů, lze vybrat manuálně nebo nechat systém zvolit protokol automaticky
  - Při automatickém výběru se volí protokoly postupně podle úrovně zabezpečení, jenž poskytují

VPN protokoly (1)

- PPTP (*Point-to-Point Tunneling Protocol*)
  - Pouze zabezpečuje (šifruje) data
  - Nepoužívá certifikáty
  - Nejméně bezpečný protokol
- L2TP/IPSec (*Layer 2 Tunneling Protocol*)
  - Umožňuje autentizaci odesilatele a příjemce
  - Zabezpečuje (šifruje) data a zajišťuje jejich integritu
  - Chrání proti přehrávacím (*replay*) útokům
  - Autentizace pomocí certifikátů nebo sdíleného hesla

VPN protokoly (2)

- SSTP (*Secure Socket Tunneling Protocol*)
  - Umožňuje autentizaci odesilatele a příjemce
  - Zabezpečuje (šifruje) data a zajišťuje jejich integritu
  - Chrání proti přehrávacím (*replay*) útokům
  - Tuneluje data přes SSL kanál HTTPS protokolu
    - Vyžaduje použití certifikátů
    - Umožňuje jednoduše procházet skrz většinu brán Firewall

VPN protokoly (3)

- IKEv2 (*Internet Key Exchange*)
  - Umožňuje autentizaci odesilatele a příjemce
  - Zabezpečuje (šifruje) data a zajišťuje jejich integritu
  - Chrání proti přehrávacím (*replay*) útokům
  - Podporován jen u VPN klientů od Windows 7 a VPN serverů od Windows Server 2008 R2
  - Podporuje IPv6 a funkci VPN Reconnect
  - Autentizace pomocí EAP nebo certifikátů počítačů
  - Pro komunikaci využívá protokol UDP a port 500

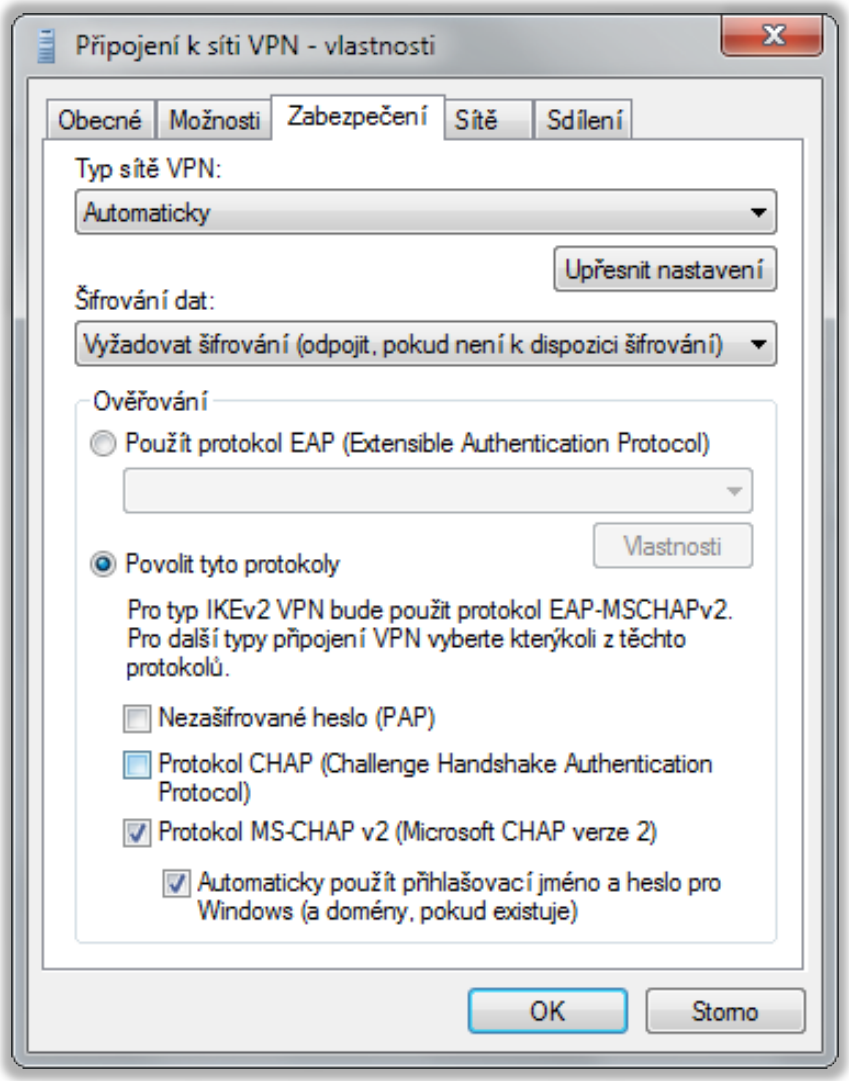
VPN protokoly pro autentizaci (1)

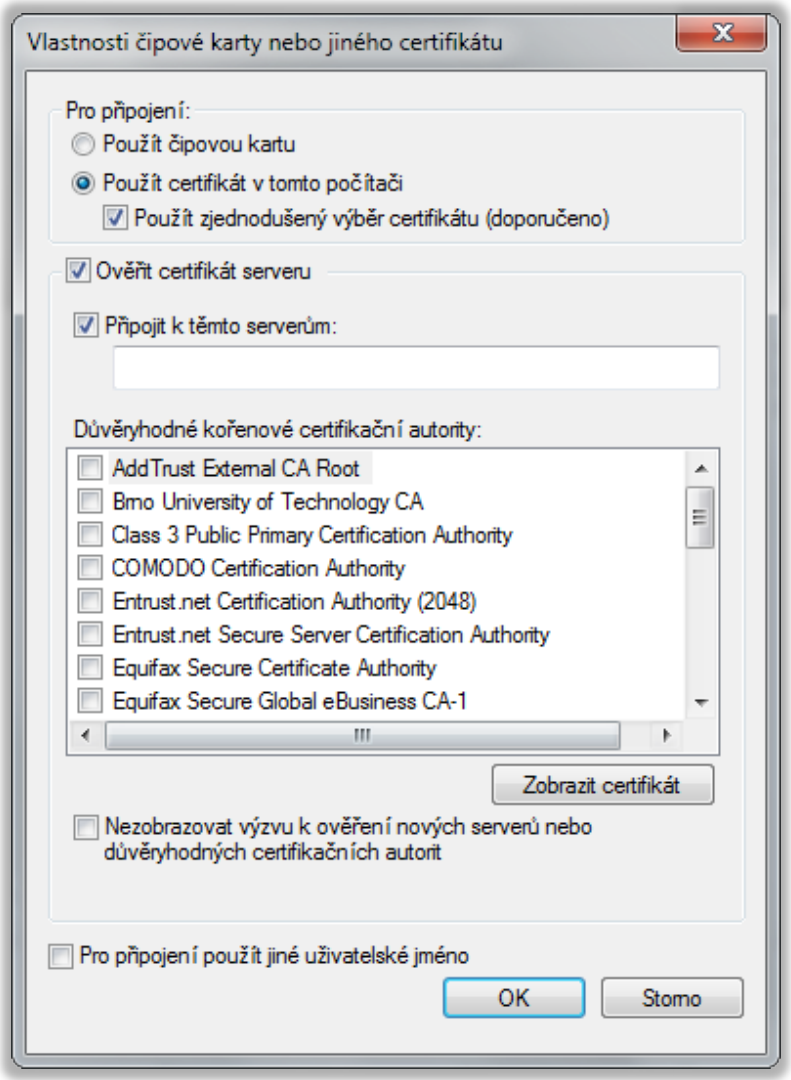
- Založené na heslech (*password-based*)
  - PAP (*Password Authentication Protocol*)
    - Zasílaná hesla nejsou šifrována
    - Nepodporován u VPN serverů od Windows Server 2008
  - CHAP (*Challenge Authentication Protocol*)
    - Je zasílán pouze hash hesla s náhodným textem (*challenge*)
    - Nepodporován u VPN serverů od Windows Server 2008
  - MS-CHAPv2 (*Microsoft Challenge Handshake Authentication Protocol version 2*)
    - Umožňuje použít pověření aktuálně přihlášeného uživatele

VPN protokoly pro autentizaci (2)

- Založené na certifikátech (*certificate-based*)
  - PEAP/PEAP-TLS (*Protected Extensible Authentication Protocol with Transport Layer Security*)
    - Uživatelé se autentizují certifikáty uživatelů
    - Vyžaduje instalaci certifikátu počítače na VPN server
  - EAP-MS-CHAPv2/PEAP-MS-CHAPv2
    - Uživatelé se autentizují heslem
    - Vyžaduje instalaci certifikátu počítače na VPN server
  - Čipová karta nebo jiný certifikát
    - Uživatelé i server se autentizují vybranými certifikáty

Nastavení VPN protokolů a ověřování





VPN Reconnect

- Automatické opětovné připojení k přerušenému VPN sezení
  - Vyžaduje použití VPN protokolu IKEv2
  - Přerušení VPN spojení může trvat až 8 hodin
  - Nenarušuje běh operací probíhajících přes VPN (tisk, kopírování souborů, stahování pošty, …)
  - Umožňuje změny IP adres VPN klientů bez toho, aby bylo nutné se opětovně autentizovat u VPN serveru
- Novinka ve Windows 7 (podpora u všech edicí) a Windows Server 2008 R2

NAP (Network Access Protection)

- Omezení přístupu k (firemní) síti na základě
  - Přítomnosti aktualizovaného antiviru a antispywaru
  - Stavu Windows Firewall a Windows Update
  - Nainstalovaných bezpečnostní aktualizací
- Rozdělení klientů na vyhovující a nevyhovující
  - Vyhovující klienti získají plný přístup do (firemní) sítě
  - Nevyhovující klienti nemají žádny nebo jen omezený přístup do (firemní) sítě
- Lze použít i např. u DirectAccess klientů

NAP Remediation

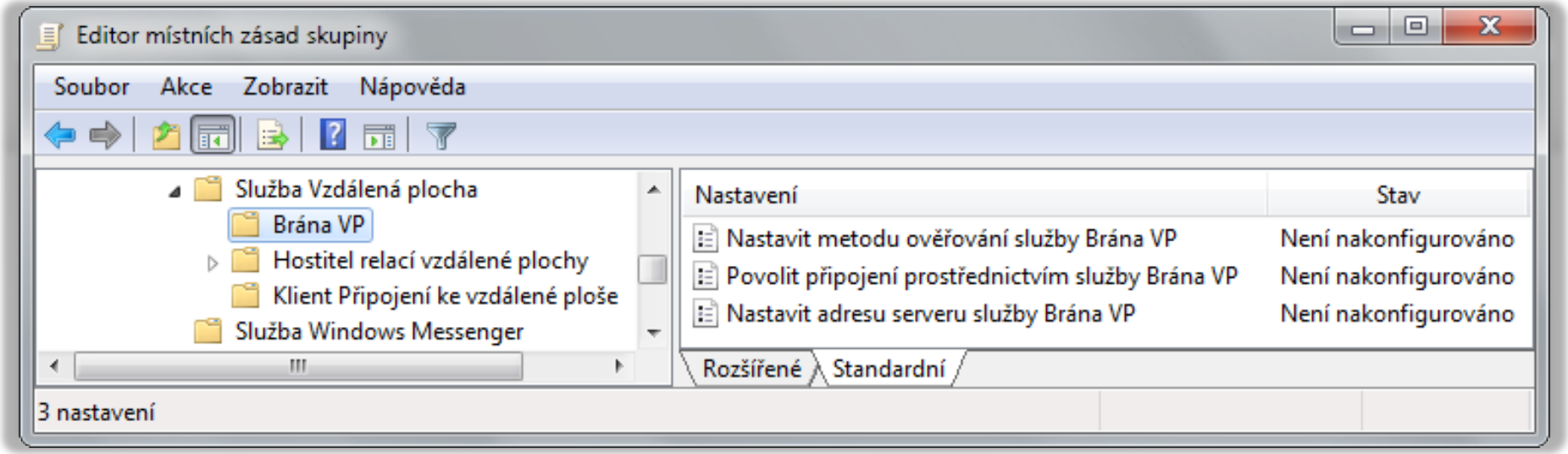
- Proces nápravy nevyhovujících klientů
  - Nápravu lze provést manuálně nebo automaticky
- Automatická náprava nevyhovujících klientů
  - Klienti jsou přesměrováni do speciální části sítě, tzv. nápravné sítě (*remediation network*)
  - Klienti mohou komunikovat jen s počítači z této sítě
  - Počítače z této sítě poskytují různé služby potřebné pro nápravu počítače (např. server Windows Server Update Services (WSUS) pro aktualizace apod.)

Brána vzdálené plochy (RD Gateway)

- Umožňuje připojení k serverům vzdálené plochy umístěným ve firemní síti (intranetu) z internetu
  - Přístup pouze ke konkrétním serverům na síti
  - Připojení k aplikacím RemoteApp z internetu
- Aplikace RemoteApp
  - Aplikace tunelované skrz protokol vzdálené plochy
  - Zobrazení aplikace na straně klienta vzdálené plochy
  - Integrace do systému (jeví se jako lokální aplikace)
  - Nutno nejprve publikovat na straně serveru

Nastavení brány vzdálené plochy

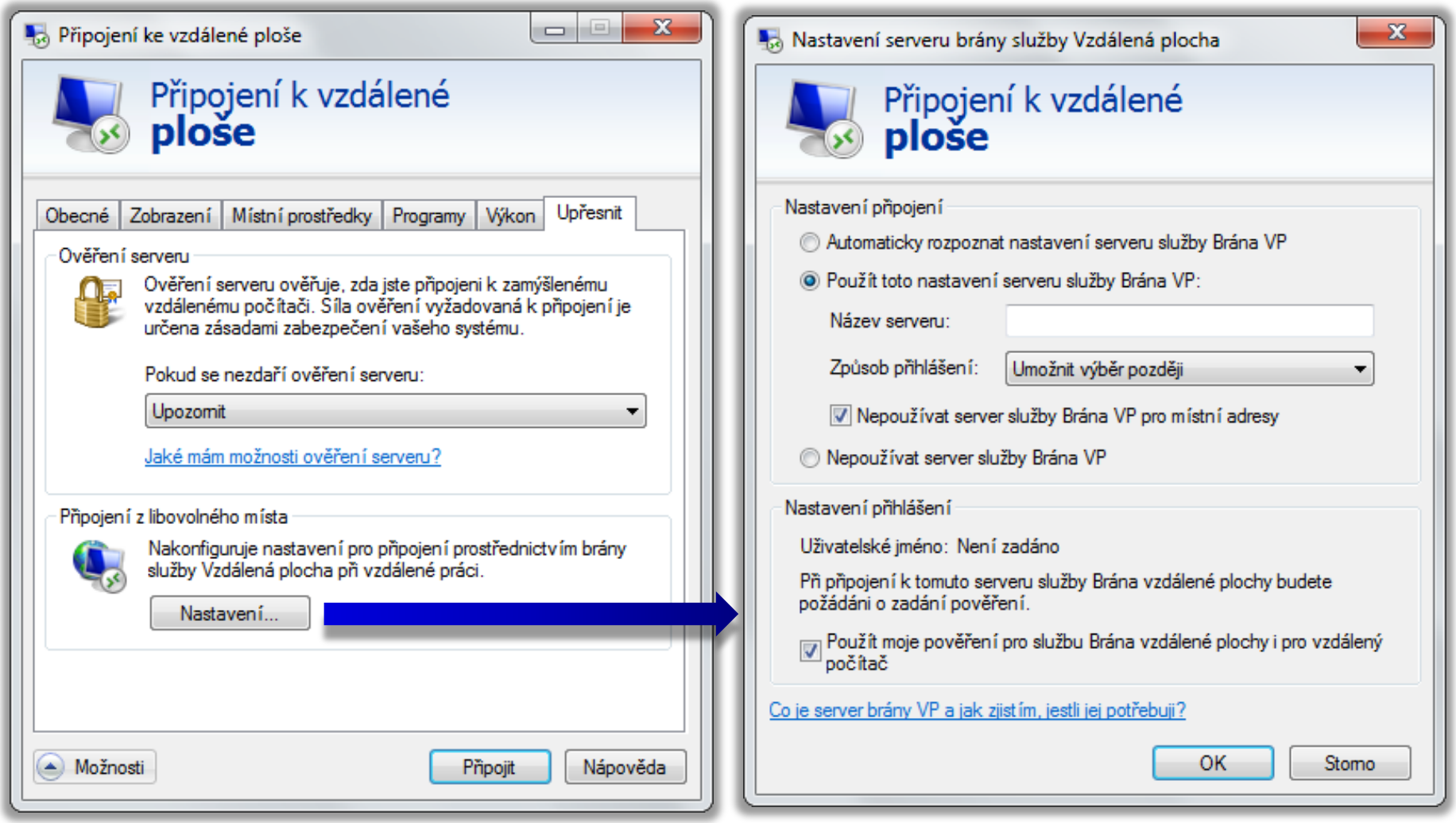
- Manuálně v nástroji Připojení ke vzdálené ploše
- Pomocí zásad skupiny
  - Lze aplikovat na jednotlivé uživatele (uzel konfigurace uživatele)



Možnosti nastavení brány VP

- Možné metody ověřování
  - Zadáním pověření uživatelem
    - Ověřování pomocí protokolů NTLM nebo Basic (nevhodné)
  - Použitím pověření přihlášeného uživatele
  - Pomocí čipové karty (*smart card*)
- Pro připojení k bráně vzdálené plochy se používá protokol HTTPS zapouzdřující protokol RDP
  - Adresa serveru brány vzdálené plochy musí odpovídat názvu uvedeném v použitém SSL certifikátu

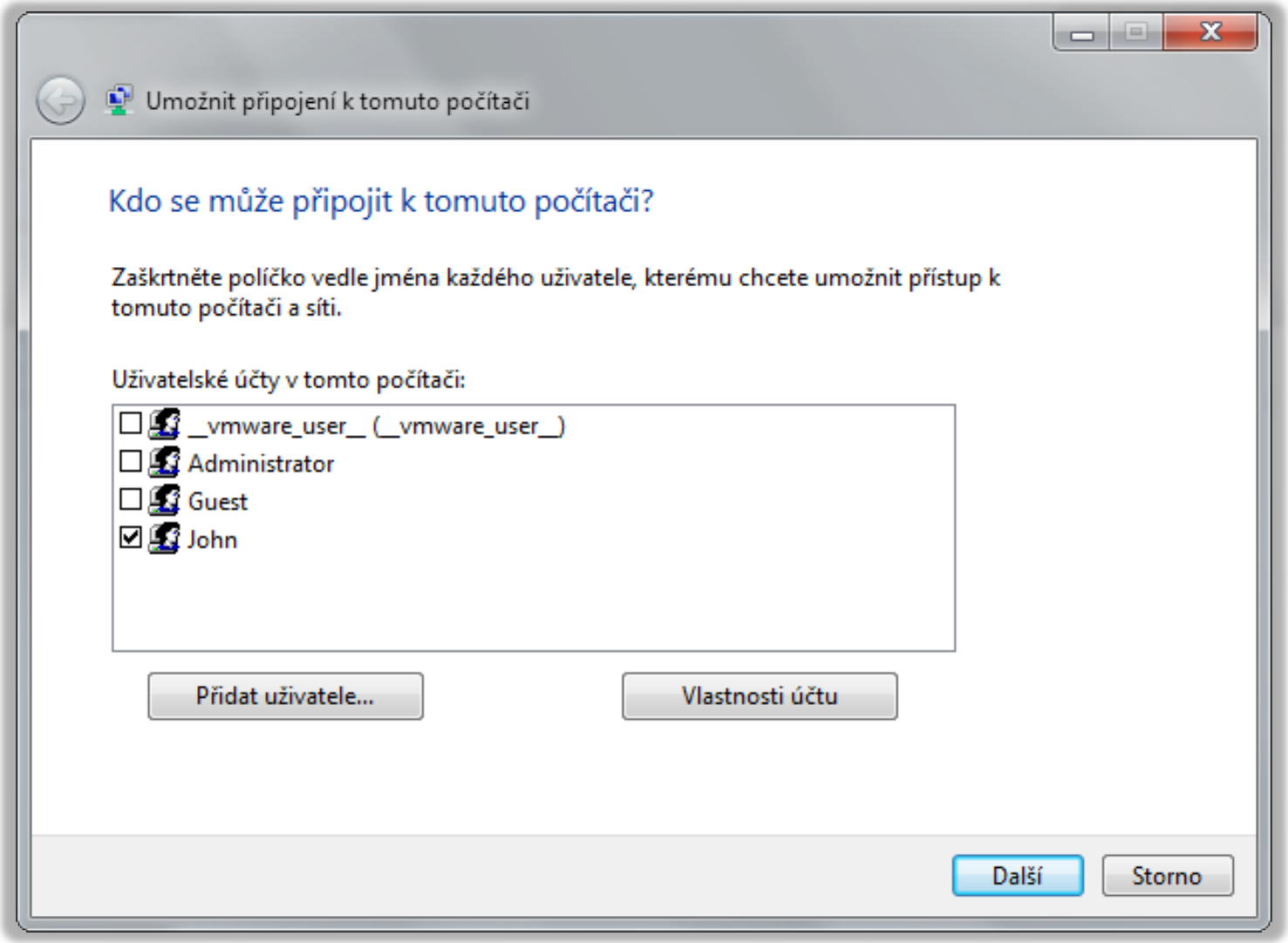
Manuální nastavení brány VP



Příchozí spojení

- Povolují VPN a vytáčená připojení k počítači, jenž není VPN ani dial-up server (např. Windows 7/8)
  - Podpora pouze VPN protokolu PPTP
  - Maximálně jedno příchozí spojení současně
  - Připojovat se mohou pouze vybraní uživatelé
- IP adresa přidělena přes DHCP nebo ze zadaného rozsahu IP adres
  - Připojujícímu se klientovi lze povolit nastavení vlastní IP adresy

Nastavení příchozích spojení



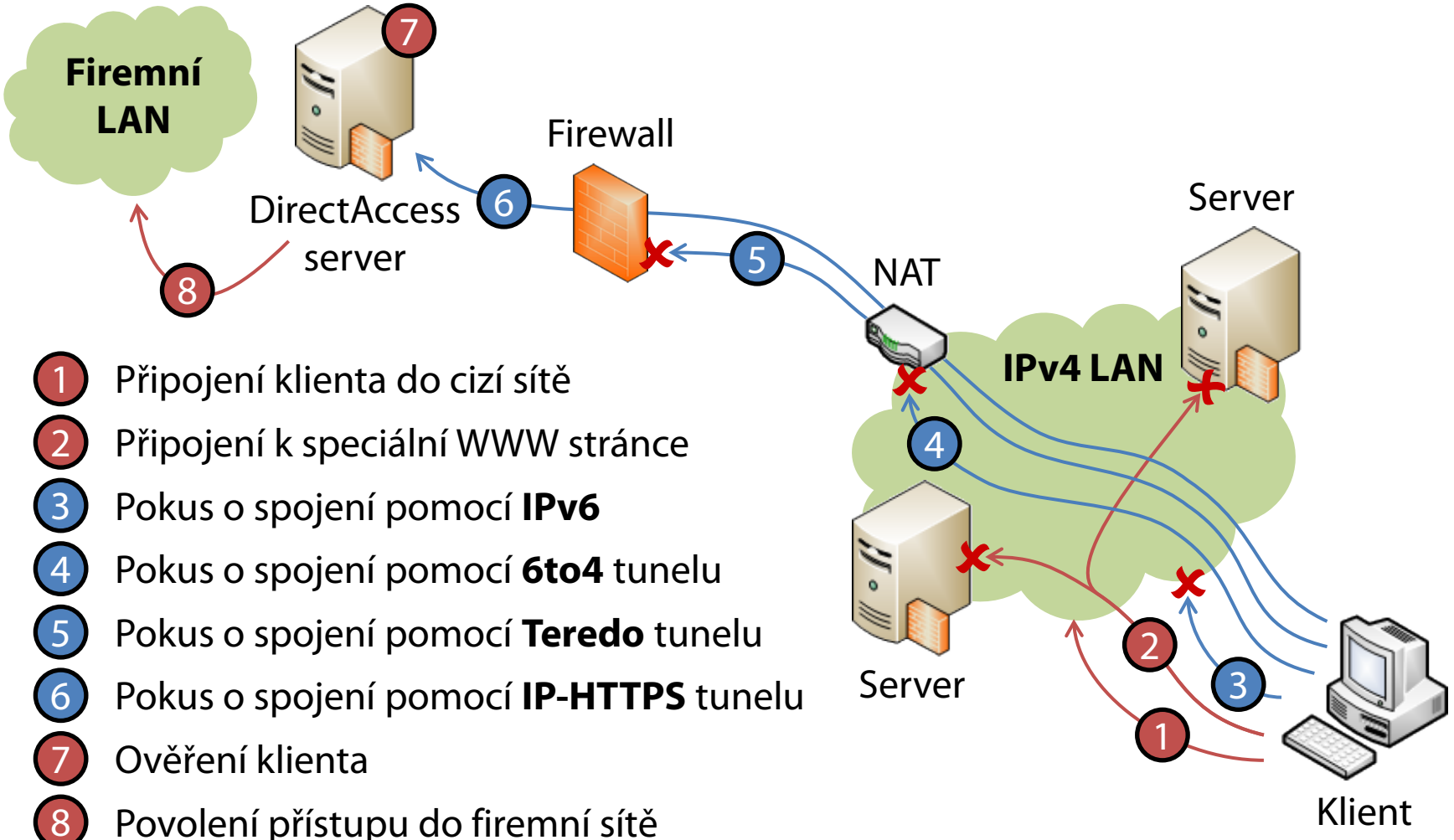
DirectAccess

- Automatické připojení do firemní sítě (intranetu) při připojení k internetu
  - VPN spojení zabezpečené pomocí IPSec, jenž využívá protokol IPv6 (ověřování na základě certifikátů)
- Novinka v systémech Windows 7 (edice Ultimate nebo Enterprise) a Windows Server 2008 R2
  - Musí být připojeny do domény

Výhody oproti VPN spojení

- Plně automatické připojení
- Obousměrné spojení
  - Servery na firemní síti mohou normálně komunikovat s připojenými klienty (připojovat se ke klientům)
- Integrace s NAP
  - Zamezení přístupu klientů do firemní sítě jestliže daní klienti nesplňují požadavky NAP
- Izolace klientů a serverů
  - Omezení přístupu klientů na konkrétní servery

Ilustrace připojení

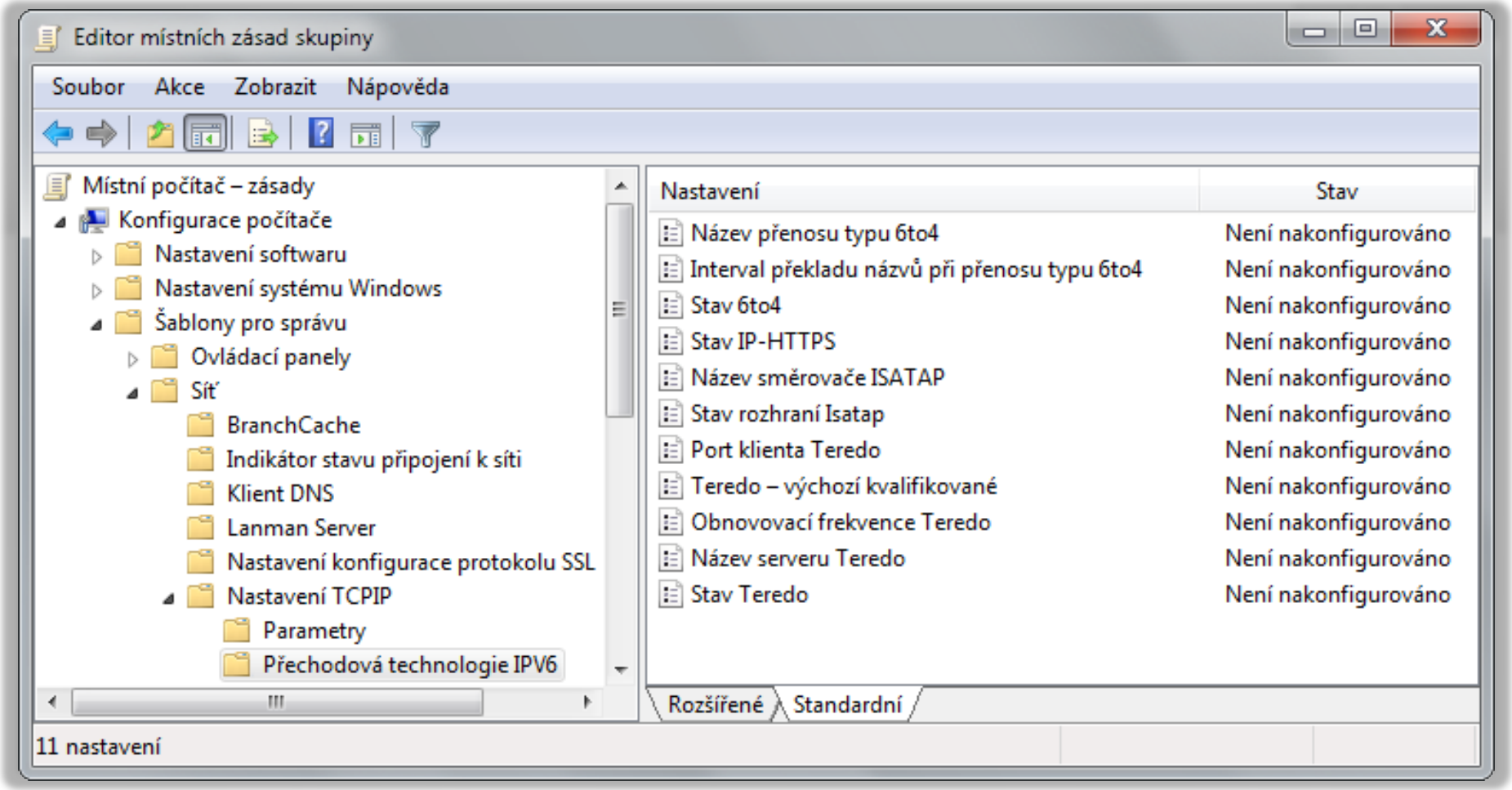


1. Připojení klienta do cizí sítě
2. Připojení k speciální WWW stránce
3. Pokus o spojení pomocí **IPv6**
4. Pokus o spojení pomocí **6to4** tunelu
5. Pokus o spojení pomocí **Teredo** tunelu
6. Pokus o spojení pomocí **IP-HTTPS** tunelu
7. Ověření klienta
8. Povolení přístupu do firemní sítě

Postup připojení

1) Klient se připojí k síti (lokální síti nebo internetu)
2) Klient se pokusí připojit k speciální (intranetové) WWW stránce, pokud se mu to podaří, není DirectAccess potřeba
3) Klient se pokusí spojit s DirectAccess serverem pomocí veřejné IPv6 adresy (pokud ji má přidělenu)
4) Klient se pokusí spojit s DirectAccess serverem nejprve pomocí 6to4 tunelu a pak pomocí Teredo tunelu (IPv6 nad IPv4 tunely)
5) Klient se pokusí spojit s DirectAccess serverem HTTPS tunelem (pomocí protokolu IP-HTTPS, jenž zapouzdřuje protokol IPv6)
6) Klient se autentizuje certifikátem a vytvoří se IPSec sezení
7) Server ověří, že se klient smí připojovat pomocí DirectAccess
8) Klient získá přístup do firemní sítě (intranetu)

Nastavení pomocí zásad skupiny



Nastavení pomocí zásad skupiny

- Zásady jsou aplikovány jen na klienty (počítače) v konkrétních bezpečnostních (*security*) skupinách
  - Výběr skupiny při konfiguraci DirectAccess serveru
- Pro správné fungování je potřeba nastavit zásady překladu IP adres (*Name Resolution Policy*)
  - Zajišťují použití firemních DNS serverů při překladech jmen počítačů z firemní sítě
- Generována při konfiguraci DirectAccess serveru
- Přepisují nastavení provedené nástrojem **netsh**

Nastavení pomocí příkazové řádky

- Vytvoření Teredo IPv6/IPv4 tunelu
  - **netsh interface ipv6 set teredo enterpriseclient *<ipv4-adresa>***
- Vytvoření 6to4 IPv6/IPv4 tunelu
  - **netsh interface 6to4 set relay *<ipv4-adresa>***
- Vytvoření IP-HTTPS IPv6/HTTPS tunelu
  - **netsh interface httpstunnel add interface client https://*<server>*/IPHTTPS**