Desktop systémy Microsoft Windows

IW1/XMW1 2013/2014

Jan Fiedor, přednášející **Peter Solár**

ifiedor@fit.vutbr.cz, solar@pocitacoveskoleni.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 14. 12. 2013

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

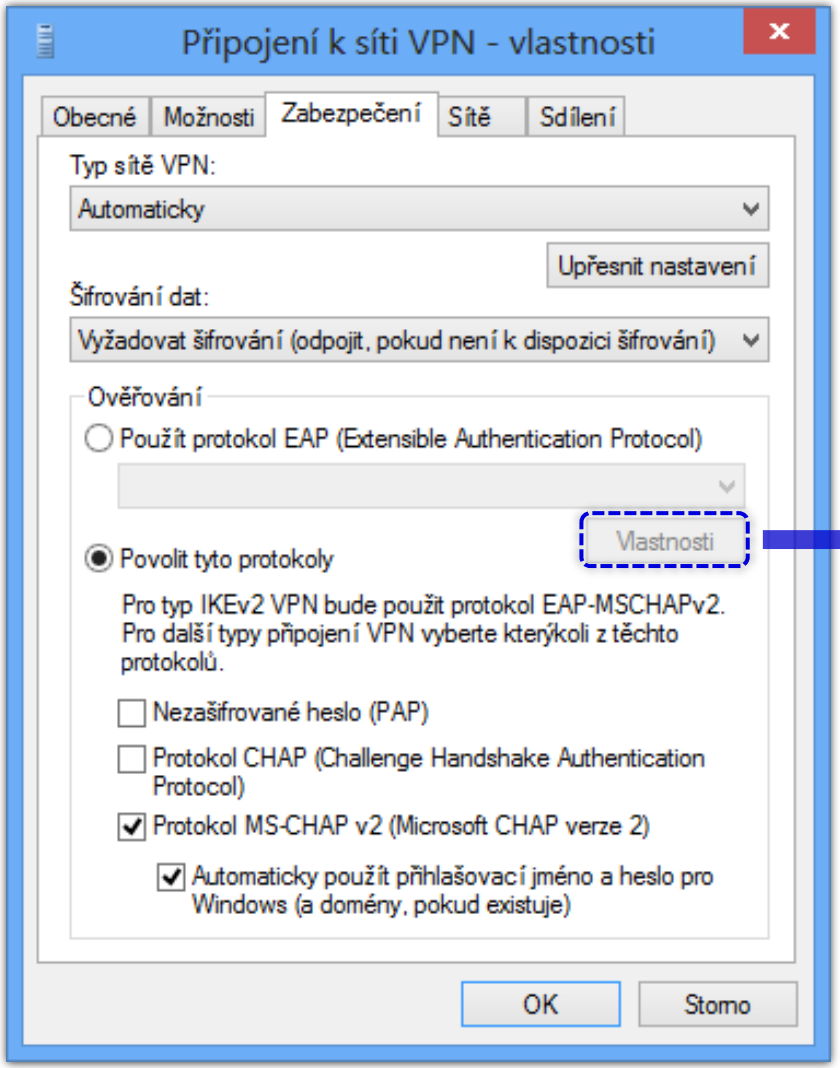
VPN protokoly pro autentizaci (1)

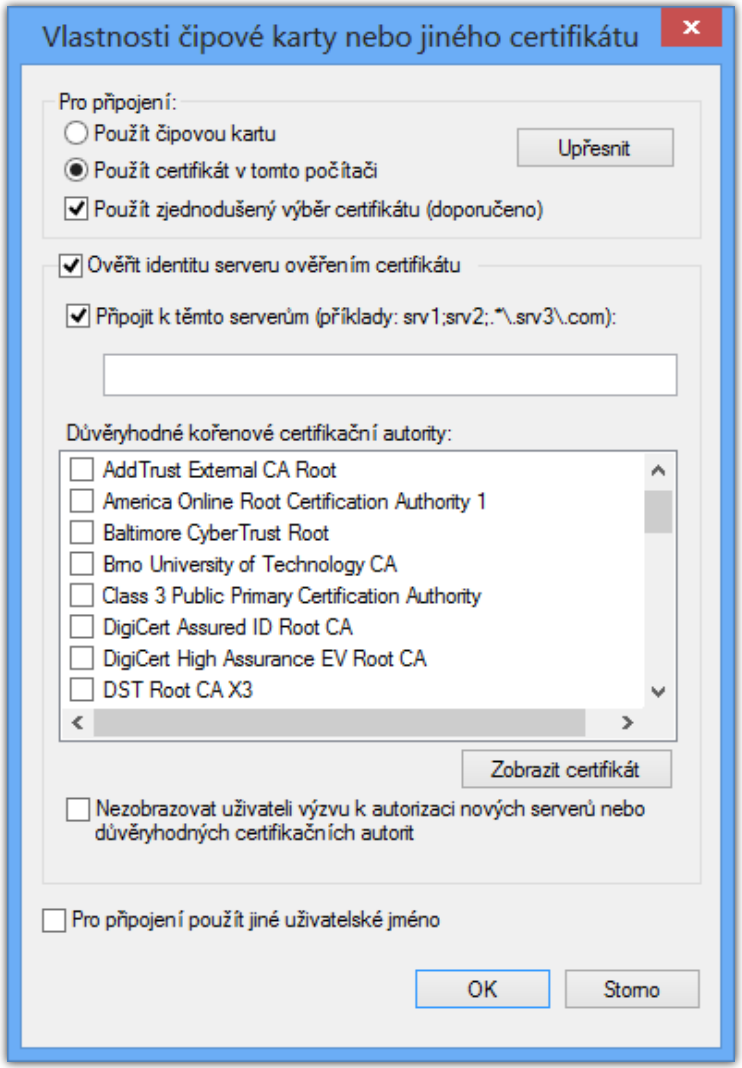
- Založené na heslech (*password-based*)
  - PAP (*Password Authentication Protocol*)
    - Zasílaná hesla nejsou šifrována
    - Nepodporován u VPN serverů od Windows Server 2008
  - CHAP (*Challenge Authentication Protocol*)
    - Je zasílán pouze hash hesla s náhodným textem (*challenge*)
    - Nepodporován 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
- Vyžaduje alespoň Windows 7 a Windows Server 2008 R2 (podpora ve všech dostupných edicích)

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

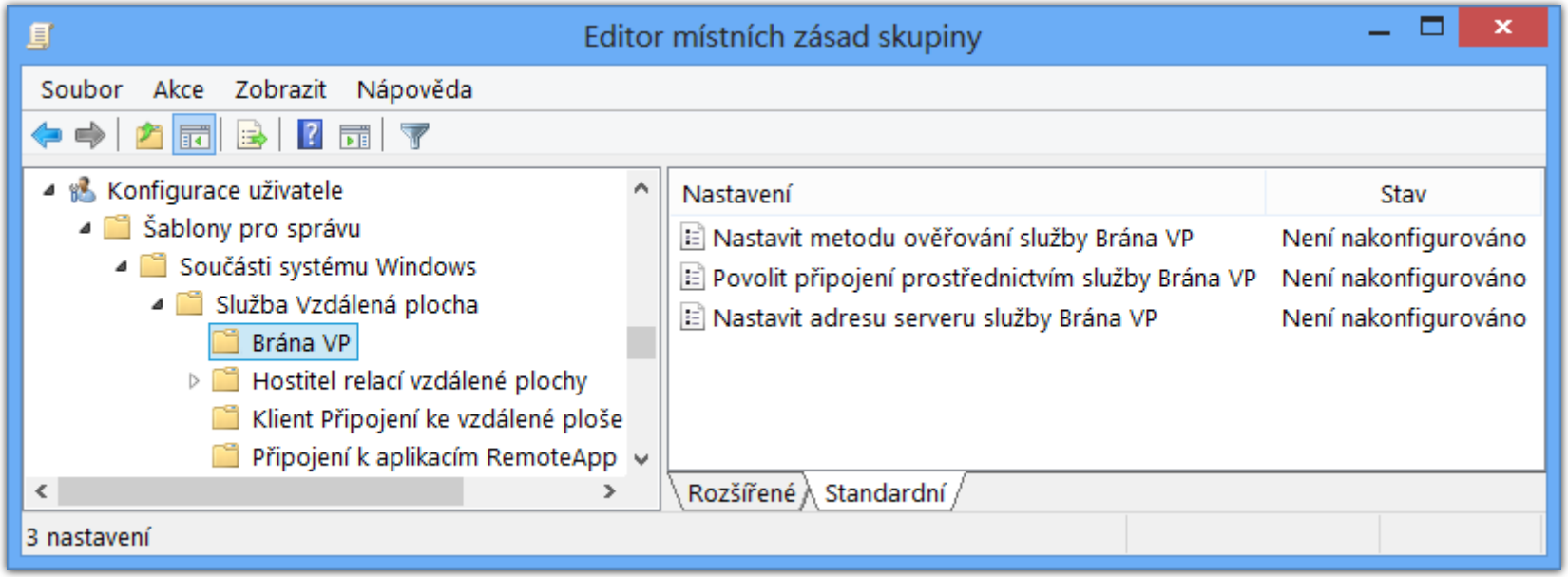
- Proces nápravy nevyhovujících klientů
  - Nápravu lze provést manuálně nebo automaticky
- Automatická náprava nevyhovujících klientů
  - Klienti jsou přesměrováni do speciální části sítě, tzv. nápravné sítě (*remediation network*)
  - Klienti mohou komunikovat jen s počítači z této sítě
  - Počítače 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

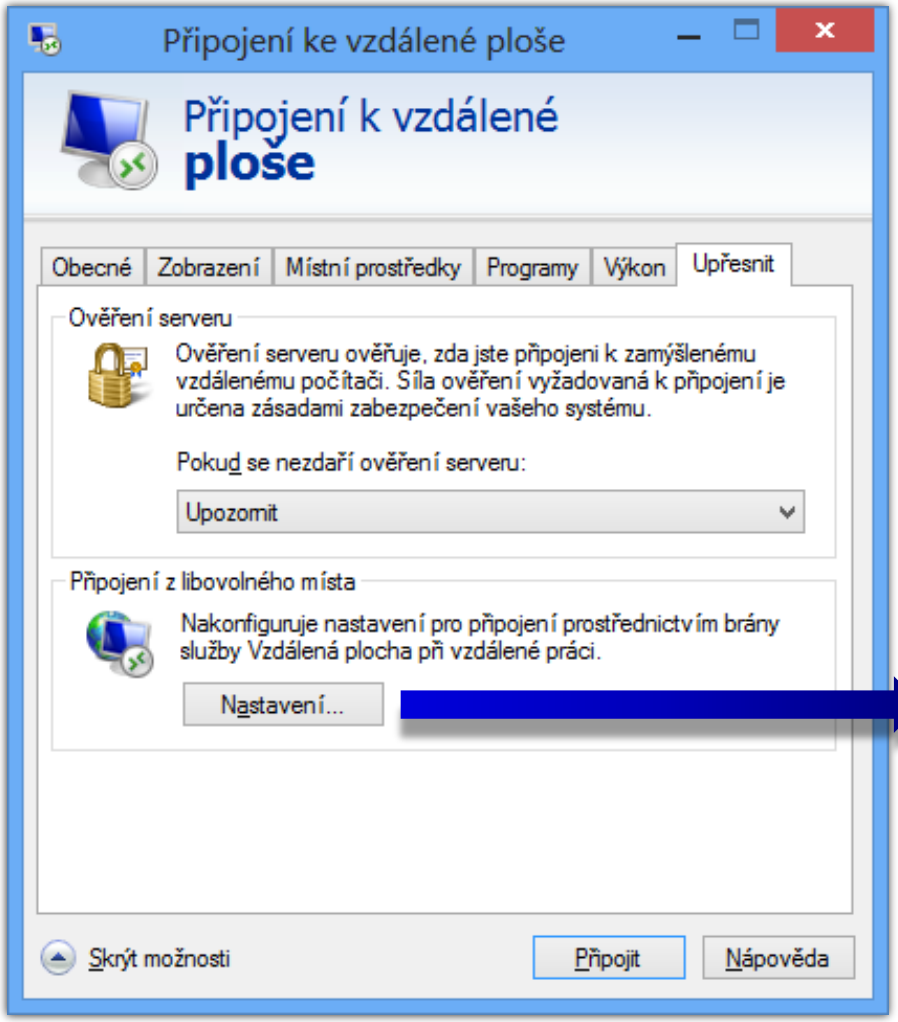
- Manuálně v nástroji Připojení ke vzdálené ploše
- Pomocí zásad skupiny
  - Lze aplikovat na jednotlivé uživatele (uzel konfigurace uživatele)

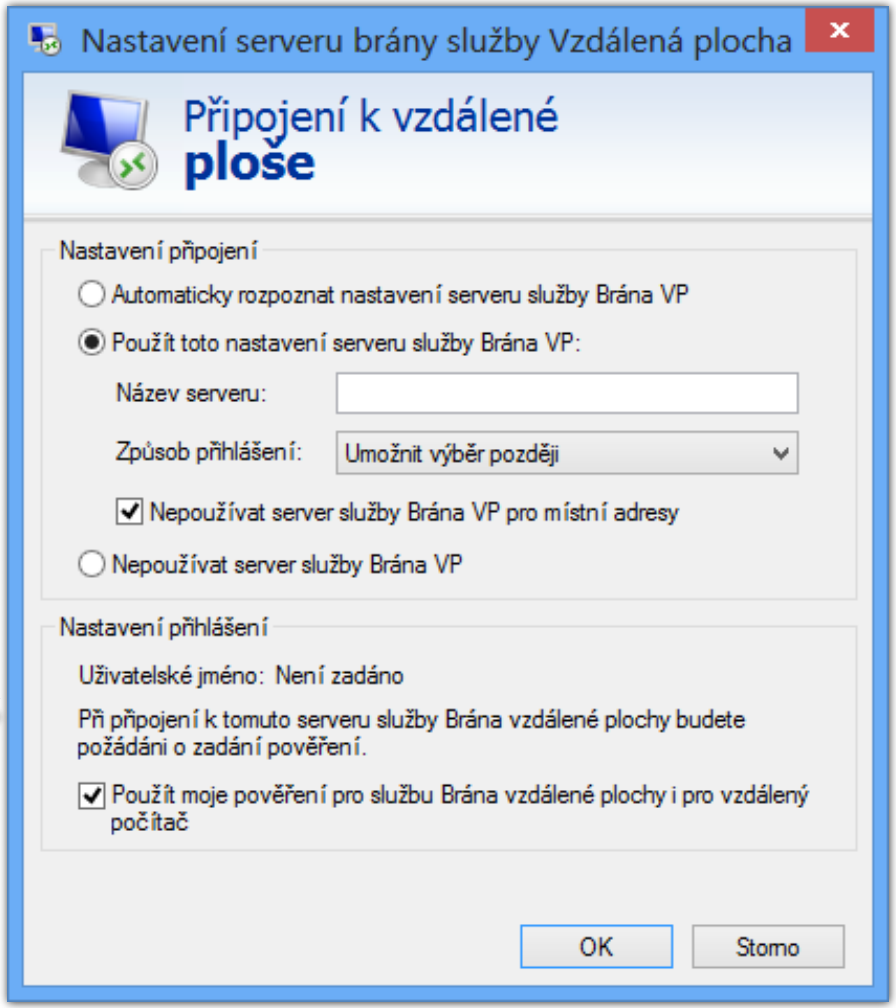


Možnosti nastavení brány VP

- 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 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