

Mobilita a roaming v sítích národního výzkumu



Jan.Furman@CESNET.CZ

Program:

- Důvody k mobilitě a roamingu
- Nutnost jednotné AAI
- Popis autentifikačních mechanismů
- Hierarchická struktura RADIUS serverů (AAI)
- Roamingová politika
- Aktuální stav
- Jak se zapojit ???
- Výhledy, plány

Důvody k mobilitě a roamingu

- Volný pohyb uživatelů s možností konektivity (domácí síť, republika, Evropa)
- Transparentní přístup k síti – jednotný ověřovací mechanismus
- Uživatelé s jednotnou „identitou“
- Nejen bezdrátové sítě

TERENA Mobility Task Force



www.TERENA.nl

1.1.2003 – 31.6.2004

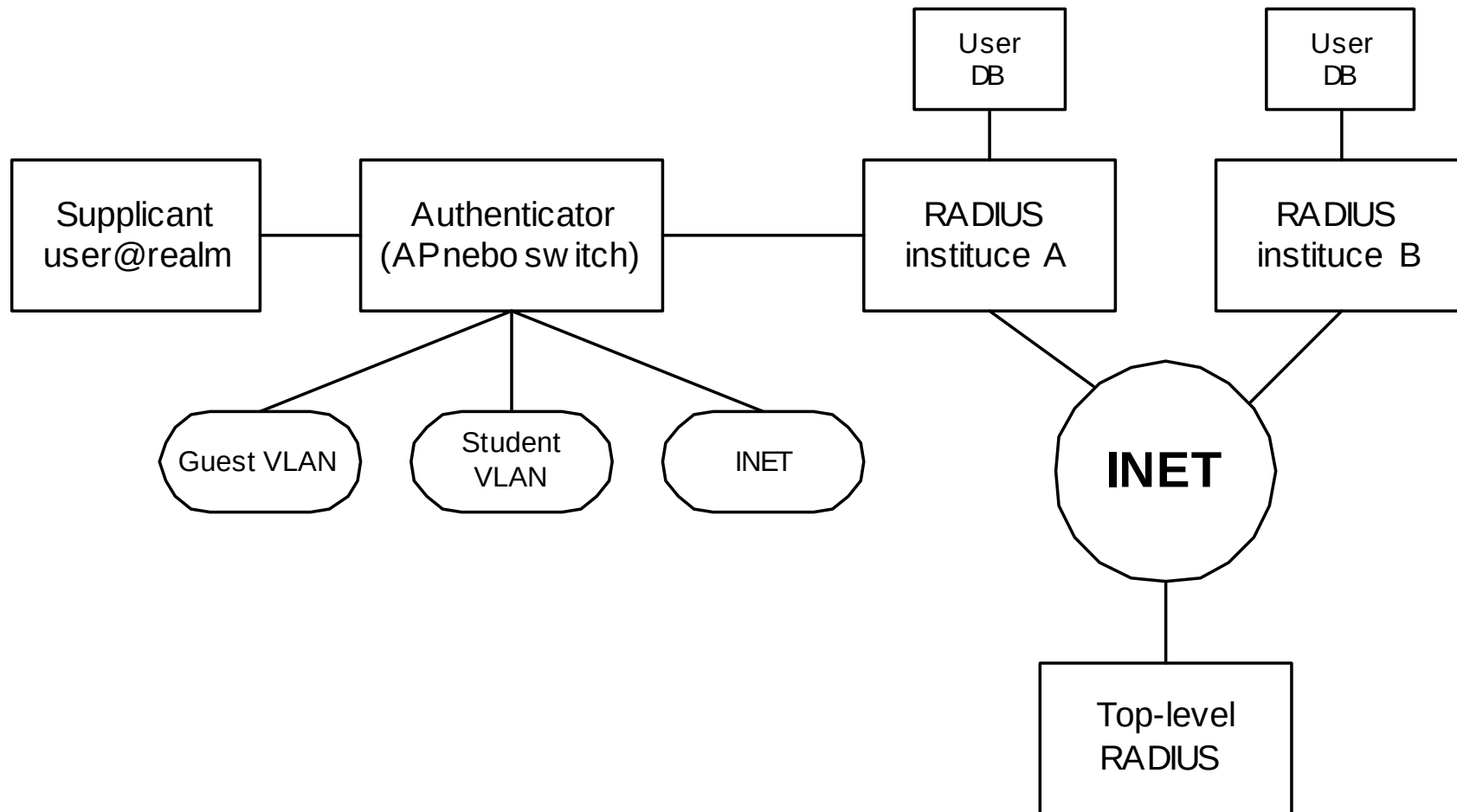
- Snaha sjednotit autentifikaci
- Inter-NREN-Roaming
- Doporučení pro budování WLAN sítí
- Výstupy: dokumenty popisující konkrétní řešení

Autentifikační mechanismy

- 802.1x (deliverable D)
- VPN based (deliverable E)
- Web based (deliverable F)

Všechny dokumenty jsou k dispozici na webových stránkách Tereny (www.terena.nl - pracovní skupina mobility).

802.1x



Výhody:

- Relativně jednoduché na implementaci
- Bezpečné
- Dobře škálovatelné

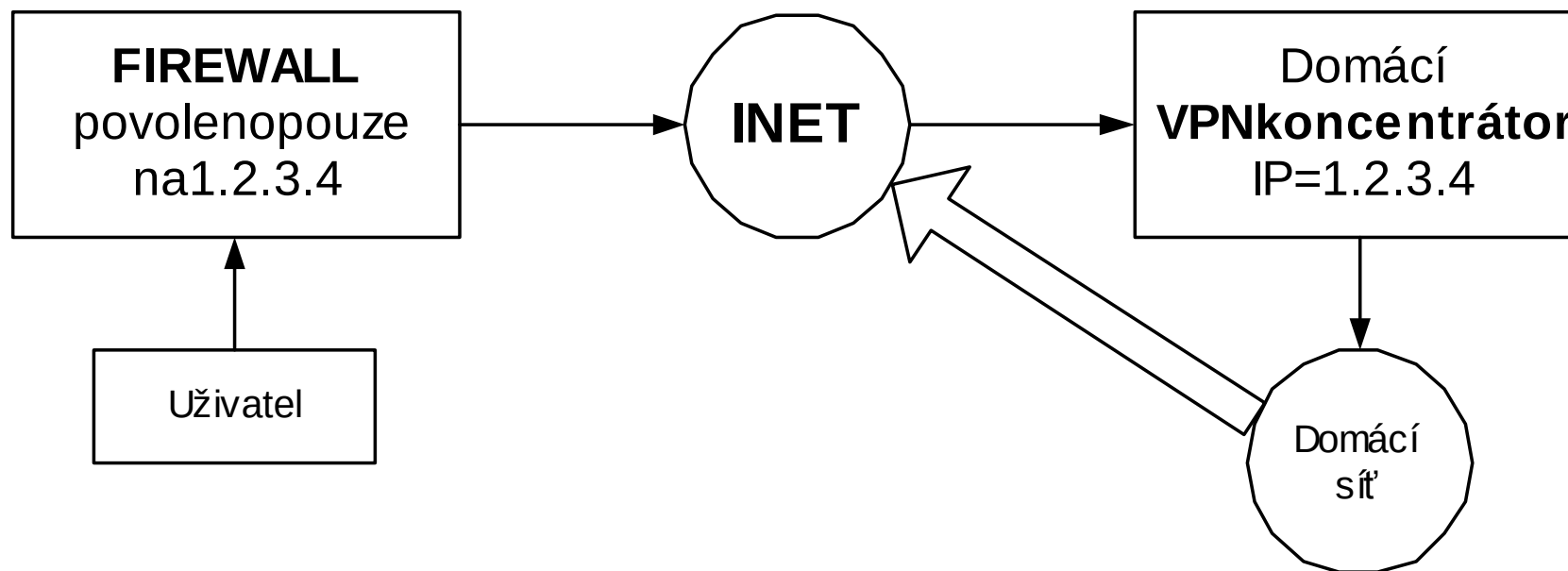
Nevýhody:

- Nutná podpora výrobce (klient i přístupový bod)

Odkazy:

- www.open1x.org ... implementace 802.1x pro Linux
a množství odkazů
- hostap.epitest.fi ... HostAP driver pro Linux
- www.surfnet.nl/innovatie/wlan ...802.1x řešení SURFNetu

VPN based



Výhody:

- VELMI VYSOKÁ míra bezpečnosti

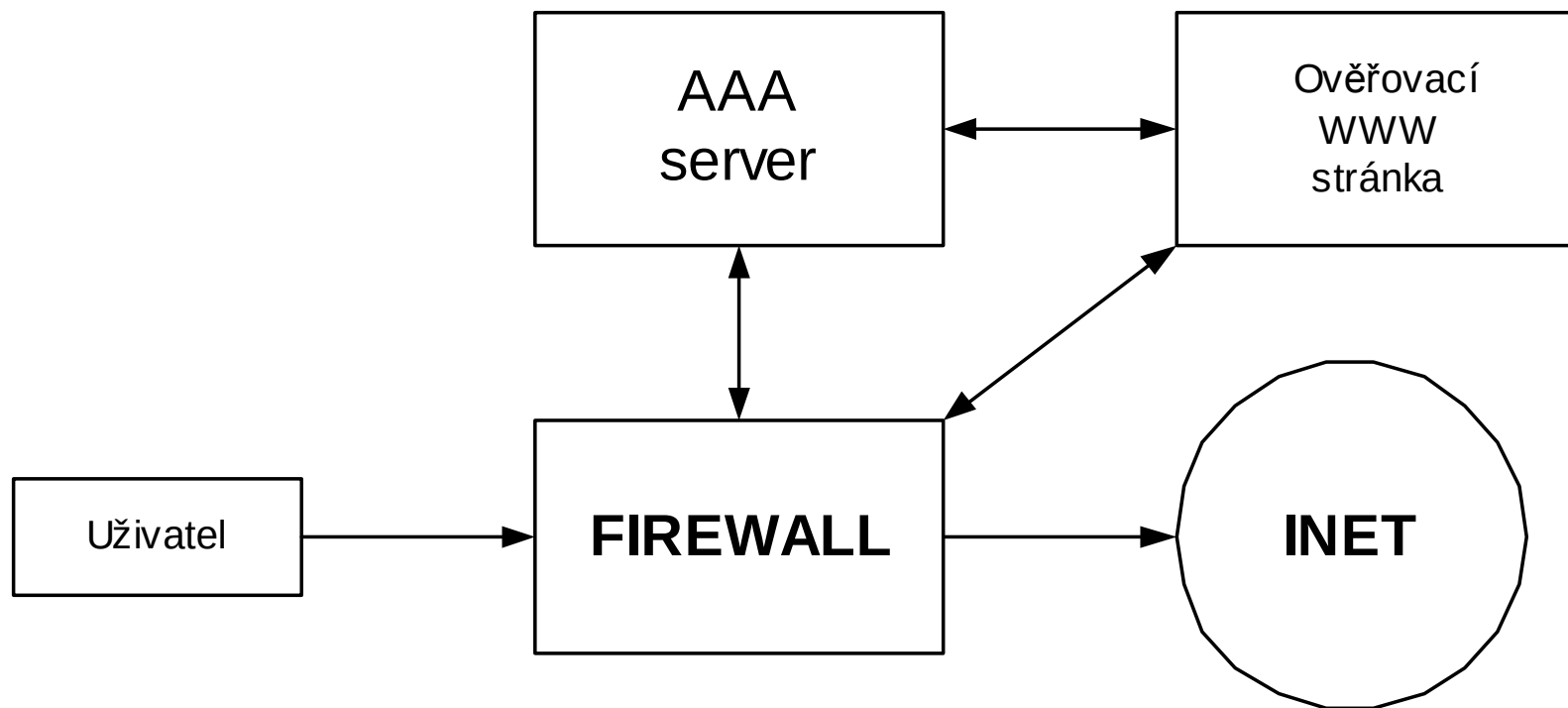
Nevýhody:

- Hůře škálovatelné
- Problém toku dat (provoz jde od klienta do jeho domovské sítě a pak teprve k cíli)

Odkazy:

- www.switch.ch/mobile ... VPN based řešení autorizace
- www.wbone.org ... WLAN roaming – University of Bremen

Web based



Výhody:

- Není potřeba žádný speciální software na straně klienta – jen web browser
- Dobrá škálovatelnost

Nevýhody:

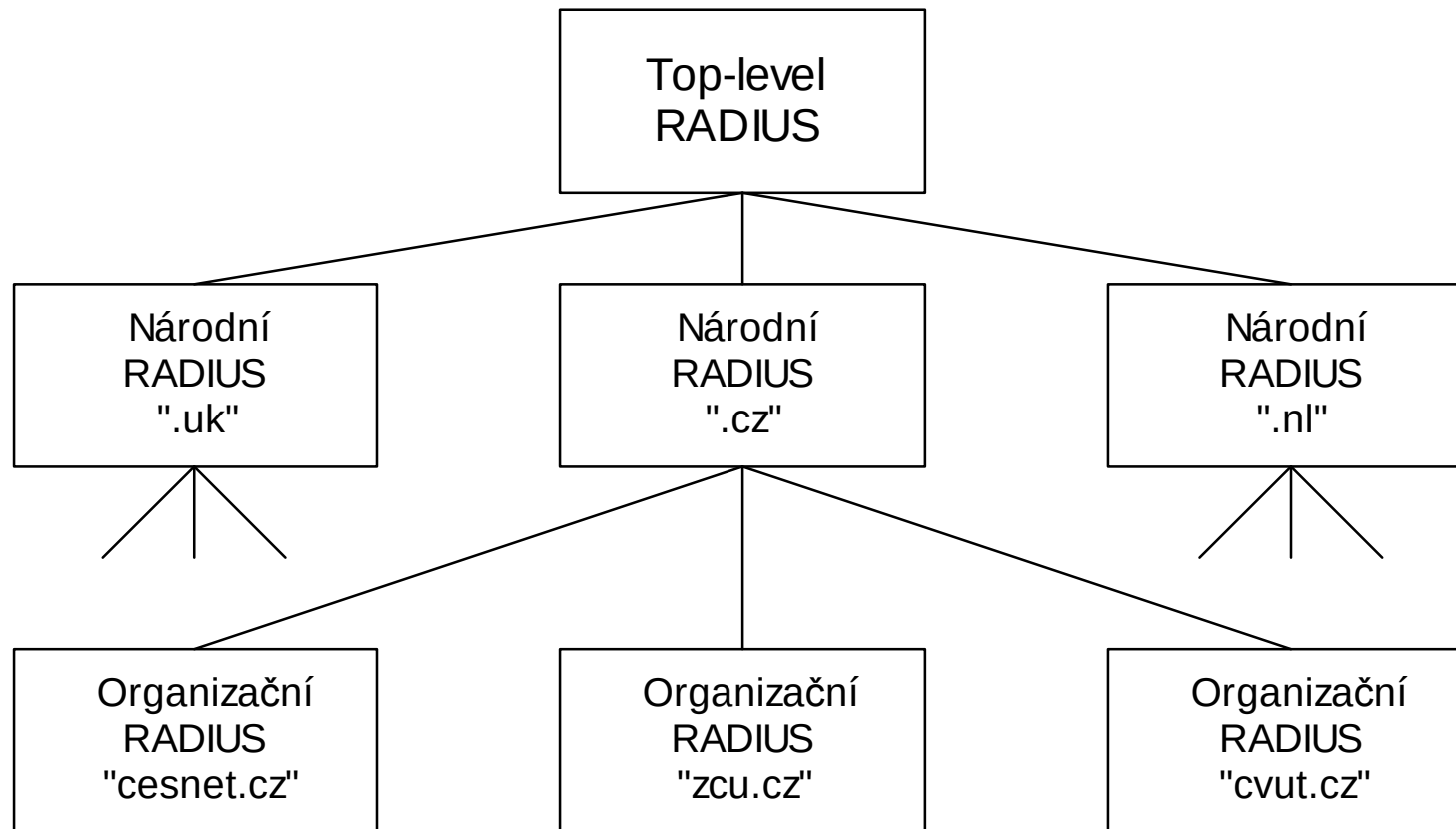
- Poněkud nižší míra bezpečnosti než např. u VPN řešení

Odkazy:

- www.atm.tut.fi/tut-public-access ...web based řešení z Tampere university of technology
- www.atm.tut.fi/public-access-roaming ... stránka se zaměřením na roaming

Inter-NREN-Roaming

- Autorizace přes RADIUS servery (popsáno v Del D)



Hierarchická struktura RADIUS serverů

- Není univerzální AAI, pro mobilitu dostačuje
- Organizační, národní, top-level servery
- RADIUS backend k lokálnímu AAS
- Koncepce realmů
- Připojení k národnímu RADIUS serveru pomocí IPSec protokolu

Roamingová politika

- Pravidla pro
 - Chování uživatelů
 - Domácí síť uživatele
 - Hostující síť
 - Autentifikační proxy systém
- Sankce při nedodržování pravidel
- Postupy řešení bezpečnostních incidentů

Aktuální stav

- Běží národní RADIUS servery (radius1.eduroam.cz a radius2.eduroam.cz)
- Pracujeme na připojení k top-level RADIUSu
- Je vyčleněn IP blok pro VPN koncentrátory (195.113.214.0/25)
- Probíhá diskuse nad návrhem roamingové politiky
- Testují se různé konfigurace
- Pracujeme na informačním portálu www.eduroam.cz

Jak se zapojit ???

- Schválení roamingové politiky
- Vytvoření vlastních zásad přijatelného užití sítě (jak pro domácí uživatele, tak pro návštěvníky)
- Zapojení do RADIUS hierarchie – přes IPSec (.1x, web)
- Vybudování VPN brány, žádost o IP adresu, otevření definovaných bloků na firewallu (VPN)
- Velmi doporučeno je použití jednotného ssid EDUROAM
- Zveřejnění informací o konfiguraci sítě (z pohledu uživatele – ssid, autentifikační mechanismy, pokrytí, ...)

Výhledy, plány, ...

- Pilotní projekt (s největší pravděpodobností: VŠB Ostrava, TUL Liberec, ZČU Plzeň, ČVUT Praha, VŠCHT Praha, Cesnet)
- Informační portál www.eduroam.cz
- Vybudování univerzální AAI (nejen pro účely mobility)
- Napojení do celoevropského roamingu
- Spolupráce na aktivitě GN2-JRA5 (Geant 2)