VPN server Masarykovy univerzity

Jakub Morávek a Radim Peša, ÚVT MU

V rámci univerzity neustále roste počet aplikací vyžadujících zabezpečený přenos údajů po veřejné nezabezpečené počítačové síti nebo dočasné připojení vzdáleného počítače jako součást univerzitní sítě. Jako typický příklad takovýchto aplikací může posloužit přístup k licencovaným elektronickým informačním zdrojům MU nebo kontrolované připojení „cizích“ počítačů do univerzitní sítě (například autentizaci bezdrátových připojení). Jednou z technologií umožňující poměrně efektivní řešení těchto požadavků je VPN – Virtual Private Network.

Základní informace o VPN

Virtual Private Network umožňuje vytvořit přímé spojení mezi dvěma body, které může být zabezpečené šifrováním veškeré komunikace šifrovacími algoritmy. Dá se říci, že se na veřejné síti vytvoří mezi těmito dvěma body *tunel*. VPN se dá využívat k různým účelům – například k propojení dvou vzdálených sítí (dvě pobočky jedné společnosti v různých městech) nebo k připojení jednoho počítače do vzdálené sítě (zaměstnanec pracující doma se připojí do počítačové sítě společnosti, pro kterou pracuje). V prvním zmíněném případě se dvě propojené sítě po vytvoření VPN chovají jako jeden celek. Ve druhém případě se po vytvoření VPN počítač zaměstnance stane součástí firemní sítě, tj. vypadá to, jako by jeho vlastní počítač byl umístěn uvnitř počítačové sítě společnosti. Právě pro tento účel byl vytvořen *VPN server Masarykovy univerzity* popsaný dále v tomto článku.

Princip fungování virtuálních sítí spočívá v zapouzdření síťového paketu do dalšího paketu (původní data mohou být přitom také komprimována nebo šifrována). Takto upravený paket je poslán přes otevřenou síť adresátovi, u kterého je zase rozbalen. Virtuální privátní sít je možné realizovat různými způsoby – pomocí různých protokolů. Mezi nejznámější a nejpoužívanější z nich patří IP-tunelling, IPSEC a PPTP.

Způsob realizace VPN serveru MU

Pro VPN server Masarykovy univerzity byl jako jeden ze základních požadavků stanovena jednoduchost použití. Očekává se, že klienti přistupující k VPN serveru budou v drtivé většině případů, i když ne výlučně, používat operační systém Windows. Serverové a síťové komponenty jsou založeny na principech otevřeného kódu z důvodu větší bezpečnosti a nižších cenových nákladů.

Server byl postaven na architektuře Intel, procesoru Pentium-III s kmitočtem 800MHz, 256kB l2 cache, 256MB RAM a 100Mbit ethernetovou síťovou kartou. Operačním systému je Debian GNU/Linux (verze 3.0 Woody). Dále byly při implementaci serveru zvoleny následující aplikace: VPN je realizováno prostřednictvím protokolu PPTP; jako pptp-server byl vybráno řešení z PoPToP projektu, který využívá ppp protokol. Pro autentizaci byl zvolen RADIUS, konkrétně FreeRADIUS, který komunikuje s adresářovou službou LDAP, konkrétně OpenLDAP serverem. Na serveru `pptp.ics.muni.cz` jsou také spuštěny HTTP a HTTPS servery Apache , které poskytují uživatelům základní informace o VPN serveru, návody na vytvoření VPN spojení a potřebný software. Dále byly vytvořeny webové aplikace pro samoobslužné založení účtu a administrativní rozhraní.

PPTP protokol

Jak již bylo uvedeno, pro realizaci virtuální privátní sítě Masarykovy univerzity byl zvolen protokol **PPTP**, který je podporován ve většině operačních systému (MS Windows 95/98/NT/2000/XP, Linux, aj.). Operační systémy MS Windows, které jsou mezi našimi uživateli nejrozšířenější, obsahují implicitně podporu tohoto protokolu, takže odpadají problémy se sháněním instalací a složitou konfigurací. Společnost Microsoft se podílí na specifikaci PPTP protokolu. Hlavní silou PPTP je schopnost podporovat i jiné protokoly než IP. Hlavním nedostatkem je pak neexistence jednoho standardu pro šifrování a autentizaci. Proto dva produkty, které dodržují specifikace PPTP, mohou být vzájemně naprosto nekompatibilní, například pokud šifrují data různým způsobem.

Téměř vše z funkcionality protokolu PPTP je obstaráváno výhradně pomocí PPP (Point to Point Protocol), který momentálně podporuje autentizační metody PAP, CHAP, MSCHAP a MSCHAPv2 a několik šifrovacích a kompresních protokolů. Mezi nejpoužívanější šifrovací a komprimovací protokoly patří MPPE (Microsoft Point to Point Encryption) a MPPC (Microsoft Point to Point Compression).

Využití VPN-MU

Typickým cílem nasazení VPN bývá zajištění bezpečného spojení přes veřejnou síť do zabezpečené privátní sítě. V případě VPN serveru MU se jedná o poněkud netypické použití: počítačová síť MU je z velké části řešena jako otevřená, tj. bez jakéhokoli oddělení od zbývajícího Internetu. VPN server proto neslouží jako nástroj pro vzdálený přístup do privátní sítě, nabízí však jiné služby – jako je přístup ke komerčním elektronickým informačním zdrojům vázaným na stroje z počítačové sítě Masarykovy univerzity a autentizace přístupu k síti, kdy je možné kontrolovat přístup jednotlivých strojů k síťovým segmentům. VPN se například používá k autentizaci bezdrátových připojení.

Prostřednictvím VPN serveru se univerzitní počítačová síť dá rozšířit na geograficky vzdálená místa buď propojením několika vzdálených sítí nebo připojením jednotlivých počítačů. Ve výsledku to vypadá, jako by se jednalo o jedinou síť a ne několik nezávislých.

Co se týče aktuálně používaných aplikací: v nedávné době byl ukončen testovací provoz bezdrátové sítě v celouniverzitní počítačové studovně, kde se pro autentizaci využívá právě VPN server. V současnosti většina uživatelů připojující se k VPN serveru přistupuje právě z CPS. Dále se tento server využívá pro autentizaci nově vzniklé bezdrátové sítě na rektorátě MU. Mimoto někteří zaměstnanci MU využívají VPN pro přístup k univerzitním elektronickým informačním zdrojům z domova ze svých vlastních počítačů.

Připojení do univerzitní virtuální sítě

Co vše potřebuje uživatel zařídit, aby se mohl připojit do univerzitní virtuální sítě? Nejprve je třeba mít založen účet v LDAP. Každý, kdo je zaregistrován v informačním systému Masarykovy univerzity (`http://is.muni.cz`), má možnost si účet zřídit samostatně přes www rozhraní na adrese `http://pptp.ics.muni.cz/samoska/`. Ve speciálních případech je možné požádat o zřízení účtu administrátory serveru. Administrátoři mají k dispozici www rozhraní pro správu uživatelských účtů.

Druhým krokem je vytvoření a nastavení síťového připojení. Pro operační systémy Microsoft (Windows 9x, 2000, XP) existují podrobné návody, které jsou přístupné na adrese `http://pptp.ics.muni.cz/navod/` v části *Návod, jak vytvořit a nastavit sítové připojení pro připojení k VPN Masarykovy univerzity*. Na stejné adrese je také návod pro operační systém Linux. Ten je zatím pouze velmi orientační a slouží spíše jako úvod do problematiky VPN v Linuxu. Pro operační systémy Windows 2000 a Windows XP byl vytvořen konfigurační soubor s přednastavenými parametry. Jediné, co potřebujete, je stáhnout si tento soubor z adresy `http://pptp.ics.muni.cz/samoska/VPN-muni.cz.pbk` a uložit ho. Následným poklikáním na soubor se spustí aplikace, která aktivuje VPN síťové připojení. Posledním krokem k připojení do VPN je již jen aktivace síťového spojení.

Plány do budoucna

Největší úkol který je před námi, s vývojem VPN pouze souvisí. Jedná se o zřízení centrálního univerzitního adresáře, který by měl vzniknout synchronizací s různými univerzitními informačními systémy jako jsou `is.muni.cz`, `inet.muni.cz` a jiné.

Dalším nevyhnutelným krokem souvisejícím s očekávaným nárůstem používaní VPN je povýšení hardwarové konfigurace serveru. Operační systém zůstane Debian GNU/Linux 3.0 woody. Na nově nasazeném serveru již nepoběží všechny výše zmíněné služby, bude zde spuštěn pouze pptp-démon. Radius, LDAP, Apache a MySQL zůstanou i nadále na současném serveru, který bude zároveň sloužit jako záložní VPN server. Zjednodušeně lze říci, že nový server bude sloužit „pouze“ k šifrování dat. Do budoucna se

také zvažuje pořízení hardwarového VPN zařízení.

Dalším, spíše permanentním, úkolem je vývoj administrativního www rozhraní, které by mělo sloužit ke správě uživatelů, sledování provozu na serveru, zobrazování statistik, monitorování zátěže a odhalování úzkých míst. Rozhraní by také mělo by také umožnit odhalování „nekalých aktivit“ a pomoci při řešní problémů při připojování uživatelů.

Další služba, kterou momentálně připravujeme, je uživatelské www rozhraní. Toto rozhraní je je zjednodušená verze administrativního rozhraní, a mělo by poskytovat uživateli přehled o jeho aktivitě ve virtuální síti a pomáhat jednodušeji, rychleji a samostatněji řešit problémy s připojením k VPN serveru.

Literatura

[1] `http://www.poptop.org`. PoPToP projekt.

[2] `http://www.freeradius.org`. FreeRADIUS projekt.

[3] `http://www.openldap.org`. OpenLDAP projekt.

[4] `http://www.linuxdocs.org/HOWTOs/mini/VPN.html`. Dokumentce k VPN. □