Bezpečně? Tunelem!

Co jsou a jak fungují privátní sítě

PATRIK MALINA

Virtuální privátní sítě (VPN) jsou dnes v oblasti síťových technologií již samozřejmým pojmem. Nejde o speciální hračku pro administrátory, jak by se mohlo zdát na první pohled, ale pro mnoho uživatelů je to dávno běžný prostředek pro každodenní práci. Seznámíme vás s tím, jak vlastně pracují a co je jejich podstatou.

Pokud nejste na internetu, na nejrozšířenější počítačové síti, úplnými začátečníky, zřejmě máte alespoň rámcovou představu o tom, jak je momentálně (ne)přátelský a (ne)bezpečný. Vedle toho si také snadno dovedete představit některý z následujících scénářů: firemní obchodní cestující či doma pracující zaměstnanec potřebuje ze svého počítače přístup na dálku k firemní síti; společnost má kromě centrální sítě ještě malé počítačové sítě v mnoha geografických lokalitách a ty spolu potřebují komunikovat; domácí uživatel se chce přes permanentní internetové připojení při pobytu na cestách vzdáleně dostat na svůj domácí počítač či do malé domácí sítě. Všechny popsané situace mají poměrně zřejmý společný požadavek: využít dostupnou síťovou infrastrukturu, často na vzdálenost stovek či tisíců kilometrů, a s její pomocí bezpečně proplout všemi nástrahami až do vzdálené sítě tak, jako bychom seděli přímo v domovské kanceláři u svého pracovního PC.

Proč VPN?

Virtuální privátní sítě jsou řešení, jak toto zajistit co možná nejlevněji, nejbezpečněji a navíc cestou nejmenšího (technologického) odporu. Na důvod nasazování VPN se můžeme podívat i z jiné strany – mnoho nám napoví již samotný název či používaná zkratka. Označení *„Private Networks“*, tedy soukromé (privátní) sítě, naznačuje, že se jedná o síťové propojení pro jakési výhradní použití, především na delší vzdálenost, tedy v prostředí rozlehlých sítí (běžně označovaných jako WAN). Před masivním nástupem technologií VPN se takové privátní spojení skutečně rovnalo fyzickému propojení pomocí stávajících komunikačních linek. Pobočky velkých, tedy často i náročnějších a movitějších společností byly a stále jsou propojovány například digitálními okruhy (linkami) ISDN. Spojením mnohem více kanálů než oněch dvou v „domácí“ variantě EuroISDN může vzniknout pořádný „svazek“ přenosových cest, jejichž výhradní pronájem je možné u telekomunikačních společností dojednat. Fakticky tak získáte pravou privátní síť v podobě vyhrazených telekomunikačních cest, vedoucích z centrály na všechny pobočky. Problémy s tímto řešením jsou nasnadě: takové řešení je nesmírně drahé a často nerentabilní, neboť za výhradní využití platíte stále, přestože po většinu doby nedokážete kapacitu linek vytížit.

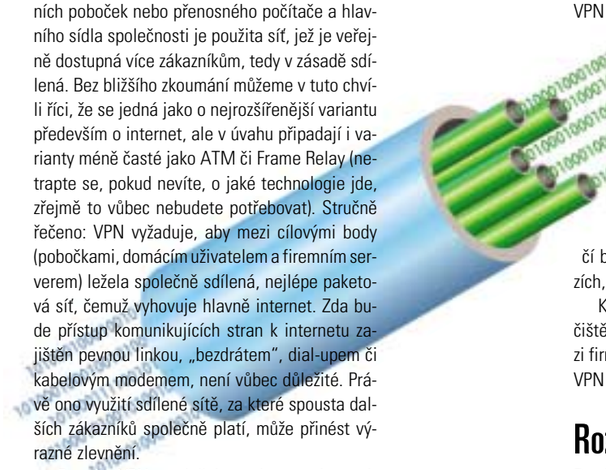
Ve stejné situaci se s tradičním řešením vyhrazené komunikační cesty ocitá i domácí uživatel či vzdáleně pracující zaměstnanec, jenž do centrály přistupuje třeba z přenosného počítače na cestách. V klasickém provedení naváže uživatel pomocí telefonní linky a dial-up modemu přímé spojení s přístupovým serverem ve své firmě (tato služba se často označuje jako RAS) a poté pracuje, jako by byl se svým počítačem přímo připojen k interní firemní síti. I zde je hlavní potíž nasnadě: telefonní poplatky se při delších vzdálenostech razantně zvyšují a navíc je potřeba podobným klientům vyhradit dostatečný počet exkluzivně používaných telefonních linek.

Kromě finančních potíží a problémů s budováním dostatečné infrastruktury fyzických datových okruhů narážíme u tradičních modelů soukromých sítí samozřejmě také na problém se zabezpečením. Ačkoliv si linku můžete pronajmout či momentálně obsadit tím, že zahájíte telefonní hovor, nemáte absolutně žádnou možnost ovlivnit, že vaše data cestou někdo neodposlouchává či nemodifikuje. A právě s tímto nebezpečím je potřeba stále více počítat.

VPN: hlavní koncepce

Překlenutí výše uvedených překážek nabízí koncepce virtuálních privátních sítí, k jejichž plošnému nasazení již doba dozrála. Hlavním posunem od klasických soukromých sítí je samozřejmě ono přetvoření do „virtuální“ podoby – nejde o zásadně nový koncept, ale především o skutečnost, že vývoj na trhu internetové konektivity a také pokrok výrobců aplikací a operačních systémů již dovoluje běžný, rutinní provoz.

VPN se vyznačuje především tím, že při svém provozu nepotřebuje vyhrazený spojovací okruh, tedy třeba ISDN či telefonní linku. Hlavní myšlenka spočívá v tom, že k propojení dvou firemních poboček nebo přenosného počítače a hlavního sídla společnosti je použita síť, jež je veřejně dostupná více zákazníkům, tedy v zásadě sdílená. Bez bližšího zkoumání můžeme v tuto chvíli říci, že se jedná jako o nejrozšířenější variantu především o internet, ale v úvahu připadají i varianty méně časté jako ATM či Frame Relay (netrapte se, pokud nevíte, o jaké technologie jde, zřejmě to vůbec nebudete potřebovat). Stručně řečeno: VPN vyžaduje, aby mezi cílovými body (pobočkami, domácím uživatelem a firemním serverem) ležela společně sdílená, nejlépe paketová síť, čemuž vyhovuje hlavně internet. Zda bude přístup komunikujících stran k internetu zajištěn pevnou linkou, „bezdrátem“, dial-upem či kabelovým modemem, není vůbec důležité. Právě ono využití sdílené sítě, za které spousta dalších zákazníků společně platí, může přinést výrazné zlevnění.

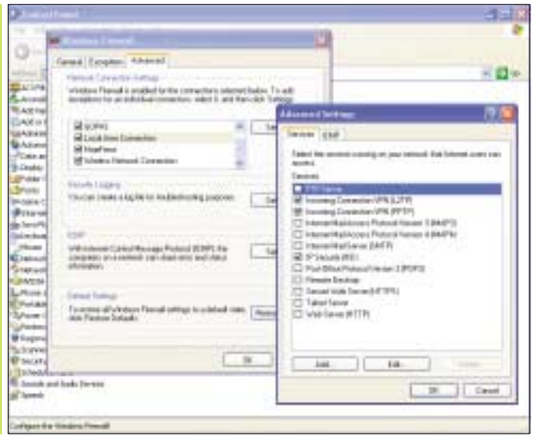


Protože VPN protlačuje soukromou komunikaci přes naprosto nedůvěryhodné prostředí (třeba internet takový prostě je), nastává zvýšená potřeba zajistit ono soukromí. Na tomto místě vstupují do hry další prvky, jako je ochrana přenášených dat šifrováním či digitálním podepisováním a ověření připojovaného uživatele – autentizace. Obě protistrany se totiž musí před zahájením přenosů ujistit, že na druhém konci virtuální sítě není nežádoucí útočník, a posléze zajistit ukrytí citlivých informací před čmuchaly a podvodnými živly, kteří by se mohli pokusit o modifikaci dat na trase.

Protože označení VPN a klasické, výše popsané pojetí privátních sítí může být stále zavádějící, pokusíme se použití VPN v paketové síti (typicky internetu) přiblížit ještě jiným způsobem. Představte si internetovou konektivitu – sdílené médium – jako proudící řečiště, do nějž mohou všichni uživatelé vkládat svá data. Potřebuji-li někoho poslat, prostě to zabalím, vhodím do proudu a příjemce si zboží na konci cesty vyloví. Celá komunikace bude složena z tisíců balíčků, jež budu postupně proplouvat řečištěm, spolu s tisíci balíčky jiných uživatelů sdílené sítě. Koncept VPN zajišťuje následující: mé jednotlivé balíčky budou chráněny šifrou proti falešnému rybáři, jenž by je vylovil a chtěl rozbalit; mnou odeslané balíčky budou správným příjemcem rozpoznány jako originální a nepoškozené; díky využití sdíleného řečiště nebudu muset platit za pronájem celého, protože mi stačí balíček občas pohodit mezi tisíce jiných, cizích, jež unáší stejný proud.

Když ještě připomeneme, že internetové řečiště dnes již poměrně spolehlivě proudí jak mezi firmami, tak do domácností, je zřejmé, proč se VPN utěšeně prosazují.

▶ Při zprovoznění chráněné komunikace se musíte zaměřit na průchod nových protokolů skrze firewally. Windows Firewall, jenž je součástí Windows XP, s touto eventualitou počítá, a pokud z něj vytvoříte VPN server pro příchozí spojení, automaticky potřebné síťové porty otevře a začne naslouchat.



Rozdělení VPN

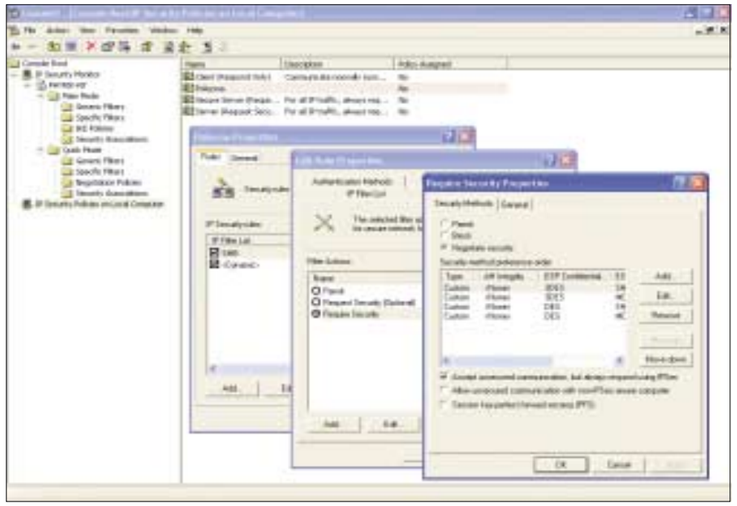
Roztřídit virtuální privátní sítě, což se nám pro jejich podrobnější popis bude hodit, je možné několika způsobů. Jedním z často využívaných hledisek je typ komunikujících protistran, a toho se rovněž budeme držet. Pokud se vrátíme k modelové situaci propojení dvou poboček jedné firmy, dostáváme se k modelu označovanému často jako site-to-site či gateway-to-gateway, tedy propojení dvou vzdálených síťových bran. Pro tuto situaci je typické, že onou bránou je zařízení, do nějž z jedné strany proudí síťová spojení ode všech lokálních počítačů, ukrytých ve vnitřní síti, a z druhé strany vychází pouze ona chráněná podoba VPN. Jakmile tato virtuální linka dorazí k protější bráně, „svazek“ je opět převeden do podoby původních síťových spojení. Ta pokračují k lokálním strojům ve vzdálené síti. Výhody tohoto řešení, jemuž se často říká tunelování, spočívají především v tom, že pro počítače v lokálních síťových segmentech na obou stranách je systém v podstatě neviditelný. Ochranu – tedy hlavně šifrování – a ostatní režijní služby zajišťuje hraniční zařízení, tedy brána, a ta vše schová. Klientské počítače v lokálních sítích mají dojem, že jejich protějšky „za tunelem“ jsou vlastně ve stejném místním segmentu. V praxi se to projevuje hlavně tím, že na ně nemáme žádné dodatečné nároky.

Odlišnou filozofii využívá připojení jednotlivého vzdáleného uživatele, třeba pomocí přenosného počítače. Zde narážíme na první zásadní rozdíl na straně onoho vzdáleného počítače, neboť ten musí sám zajišťovat jeden konec tunelu, tedy přihlásit se vzdálené bráně, šifrovat, digitálně podepisovat atd. Naopak pro počítače ve vzdálené firemní síti se tento stroj jeví, jako by byl „někde poblíž“, tedy ve stejném soukromém segmentu. Tento typ spoje bývá též označován jako client-to-gateway a vyžaduje klíčovou softwarovou komponentu, tzv. VPN klienta. Takovou aplikaci je možné získat od různých dodavatelů (Cisco, Checkpoint…), ale najdete ji také jako nedělitelnou součást operačního systému Windows.

Třetím modelem, o němž jste možná vůbec nepřemýšleli, je nasazení VPN v síti, kde potřebuje chránit komunikaci doslova každý s každým. Tento postup se uplatňuje třeba ve vysoce citlivých vnitrofiremních sítích, kde je nepřípustné, aby si klientské počítače navzájem „povídaly“ s rizikem odposlechu. V takovém případě se lo-

kální firemní síť může hemžit stovkami virtuálních sítí, které mezi sebou sestavují jednotlivé počítače, což se samozřejmě negativně projevuje na jejich výkonnosti: stručně řečeno, každý musí šifrovat. Bezpečnost zkrátka něco stojí.

Předchozí případy zahrnovaly prakticky jen situace, kdy k tvorbě VPN používáme nějakou metodu zabezpečení. Ne vždy je to však zapotřebí – možná se budete divit, ale existují VPN, jež nemusíme tak důkladně chránit. Většinou nám pak jde spíše o to, aby vzniklý tunel pomohl datovým tokům, které by se jinak ve sdíleném médiu mohly poztrácet nebo by jejich roztříštěný přenos způsobil časové ztráty. O těchto variantách nicméně tentokráte hovořit nebudeme, takže jen naznačme, že reprezentantem těchto řešení je například velmi propracovaný protokol MPLS, jenž „balíčky v řečišti" opatřuje speciálními nálepkami s údaji o cestě a přednostním odbavení. Jeho primárním úkolem však není jejich utajení a ochrana.



▲ Přestože operační systém Windows (v tomto případě verze Windows XP) nabízí k administraci technologie IPSec grafické rozhraní, není konfigurace snadnou záležitostí a bez důkladného porozumění této technologii můžete snadno uvíznout.

Protokol: IPSec

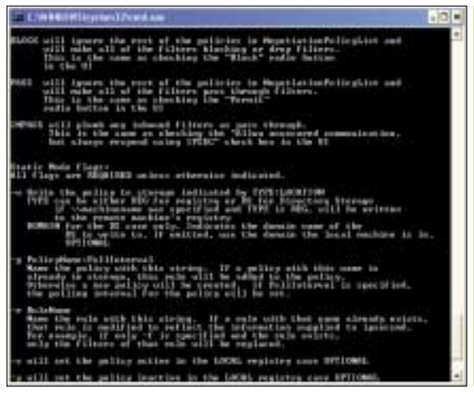
Standard označovaný jako IPSec(urity) v současné době patří mezi nejpopulárnější způsoby realizace VPN, takže se s ním seznámíme blíže. Jde o řešení, popsané veřejnými internetovými dokumenty z dílny IETF, a to především normami RFC 2401-2409. Zajímavá je historie jeho vzniku: původně byl vyvinut jako závazná součást nově chystaného internetového síťového protokolu IPv6, ale protože „šestka" se nakonec dosti opozdila, byl IPSec přednostně adoptován do stávajících internetových i lokálních síťových prostředí, neboť jeho potenciál byl velmi slibný. Realita tyto odhady plně potvrdila.

Standard IPSec je určen pro tvorbu zabezpečených VPN tunelů jak v modelu gateway-to-gateway pro kompletní ochranu komunikace mezi pobočkami, kde je velmi populární, tak v situacích client-to-gateway, v nichž se již také zdárně prosazuje. Dříve byla zásadní brzdou při jeho nasazování poměrně obtížná implementace, neboť se jedná o dosti komplikované řešení, avšak plné zabudování tohoto standardu do všech operačních systémů firmy Microsoft od Windows 2000 výše jeho prosazení dosti napomohlo.

IPSec je jedna z nejbezpečnějších metod pro sestavení VPN, jaké vůbec máme k dispozici. Všechny fáze komunikace jsou velmi dobře propracovány: vzájemné ověření protistran při navázání spojení, šifrování dat či jejich digitální podepisování. Jak již bylo řečeno a jak též vyplývá z názvu, k ochraně dochází tím, že původní datová jednotka mezisíťového protokolu IP (běžně nazývaná jako paket) je digitálně podepsána či zašifrována a poté vhozena do internetového „řečiště". Změna tedy probíhá na úrovni modifikace původního IP záhlaví. Použití protokolu IP je v tomto případě nutností, což však není problém: jedná se o základní internetový protokol a většina lokálních sítí jej rovněž využívá.

Technologie IPSec dokáže pracovat ve dvou základních režimech, jež dokáží postihnout odlišné nároky. V režimu tunelovacím pracuje tak, že umí „pravým" tunelem propojit hraniční zařízení různých sítí (gateway-to-gateway) a přesně tak se také hojně využívá. Pro lokální sítě je pak především určen režim transportní, jenž sestavuje bezpečné spojení mezi jednotlivými koncovými počítači a žádný další provoz netuneluje. Využívá se pro ochranu citlivých lokálních sítí. Nejrozšířenější klientský OS Windows zvládá obě varianty od verze 2000 výše, především tunelovací režim pak podporuje nespočet hardwarových zařízení typů firewall, zabezpečený router apod. Některé z těchto produktů byly zmíněny např. v přehledu v minulém čísle PC WORLDu. Faktický rozdíl mezi oběma režimy je jasně dán tím, co IPSec provede s původním IP paketem. V případě transportního módu je hlavička IP jen mírně modifikována tak, aby původní informace o cestě paketu v lokální síti zůstala zachována. Naopak tunelovací mód to bere z gruntu: na hraničním zařízení je původní IP paket zcela zabalen, opatřen novým IP záhlavím pro cestu ve „venkovní" nepřátelské síti, po dosažení cílové brány je posléze opět vybalen do původní podoby. Když se obzvláště nad tunelovacím režimem zamyslíte a uvědomíte si, že každý IP paket projde poměrně složitým přípravným procesem, je zřejmé, že spuštění této funkce na hraniční bráně značně sníží strojový výkon.

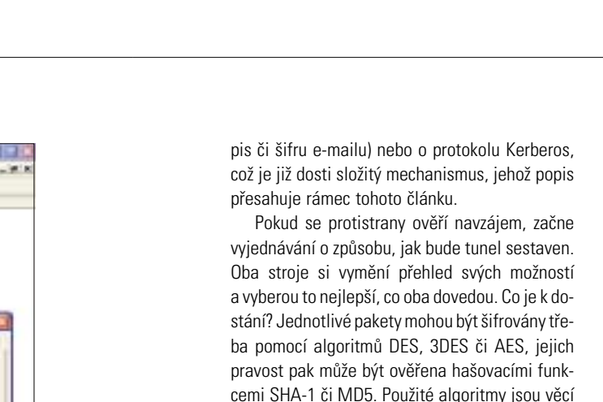
Při první fázi sestavování IPSec spojení dochází k velmi důležité operaci, a to vzájemnému ověření komunikujících stran. Oba zúčastnění musí předložit potvrzení své totožnosti, jinak VPN nevznikne. Provádí se to několika možnými způsoby: nejprimitivnější, ovšem častou metodou je použití tzv. pre-shared key, neboli sdíleného tajemství. Stručně řečeno: oba účastníci si vymění stejnou textovou frázi, kterou administrátoři předem ručně nastavili na obou koncích. Nastane-li shoda, je vše v pořádku. Ze silnějších metod se zmiňme o ověření pomocí digitálních certifikátů (velmi podobných těm pro digitální podpis či šifru e-mailu) nebo o protokolu Kerberos, což je již dosti složitý mechanismus, jehož popis přesahuje rámec tohoto článku.



◀ Pro dobře obeznámené uživatele či zkušenější administrátory je určena možnost konfigurace IPSecu ve Windows pomocí nástrojů v konzole. Mimo jiné dovolují provádět administraci automatizovaně, dávkovým spouštěním. Toto je Ipseccmd.exe ve Windows XP.

Pokud se protistrany ověří navzájem, začne vyjednávání o způsobu, jak bude tunel sestaven. Oba stroje si vymění přehled svých možností a vyberou to nejlepší, co oba dovedou. Co je k dostání? Jednotlivé pakety mohou být šifrovány třeba pomocí algoritmů DES, 3DES či AES, jejich pravost pak může být ověřena hašovacími funkcemi SHA-1 či MD5. Použité algoritmy jsou věcí dohody, a protože parametry vyjednávání je potřeba uchovat, spravuje každý počítač svou databázi, v níž se ukládají tzv. bezpečnostní vazby (SA). Jde vlastně o záznam o tom, s kým a na čem jsem se dohodl a jak po určitou dobu budeme svou VPN realizovat. Mimochodem, asi vám neušlo, že pokud se protistrany nikdy předtím „neviděly", budou si muset pro šifrovací postupy vyměnit nějaké tajné klíče tak, aby tajemství při přenosu nebylo vyzrazeno. Využívá se k tomu geniální postup Diffie-Hellman, jenž doslova pronese tajemství špionům „pod nosem" tak, že se nic kloudného nedá zachytit. Jedná se o velmi bezpečný mechanismus z oblasti tzv. asymetrické kryptografie.

Tato úvodní fáze vzájemného vyjednávání je označována jako IKE neboli Internet Key Exchange a může být nahrazena též statickým sestavením záznamu SA.



Pak ovšem musí administrátor všechny technické specifikace definovat na obou stranách VPN ručně. Pro praktickou realizaci dynamické fáze IKE se využívá protokol ISAKMP. Pokud jste správci síťového zabezpečení, pak nezapomeňte, že právě pro tuto fázi vyjednávání je potřeba na zařízeních typu firewall otevřít komunikační port 500/udp.

Už jsme se zmínili o přípravě na ochranu paketů a o tom, jak se protistrany ověřují, takže nastala chvíle říci, co přesně IPSec vlastně s původními IP pakety provádí. Můžeme jej totiž nasadit ve dvou různých úrovních, které zajišťují odlišné nároky na zabezpečení. Varianta skromnější, ale také rychlejší se označuje jako AH (authenticated headers), tedy „ověřená záhlaví". Název dobře vystihuje, že cílem je opatřit celý paket speciální digitální pečetí, aby si příjemce mohl ověřit, že data nebyla cestou pozměněna nebo že nepocházejí z falešného, podvrženého zdroje. Takže jde (přibližně řečeno) vlastně o jakousi variantu digitálního podpisu. Varianta druhá pak provádí ochranu paketů se vším všudy: obsah je chráněn jak proti změně a podvrhu, tak proti odposlechu, a to samozřejmě kompletním šifrováním obsahu. Postup je označován jako ESP (encapsulated security payload) a pochopitelně vyžaduje větší část procesorového času, neboť jde o velké množství výpočtů. Zde je třeba upozornit, že volba jedné z úrovní ochrany (AH či ESP) nijak nepředurčuje, v jakém režimu IPSec nasadíte – transportní mód pro lokální sítě tedy může jak šifrovat, tak pouze chránit proti změně. Fakt, že se v případě tunelování ve valné většině případů nasazuje ESP, je věcí praktické nezbytnosti, nikoliv technologické nutnosti.

▲ Princip zabezpeční pomocí IPSecu souvisí se začleněním speciálních záhlaví do původních struktury paketu: obrázek naznačuje, jak se originální IP paket proměňuje do chráněné podoby s ověřeným záhlavím (AH) jak v transportním, tak v tunelovacím režimu.

Protože většina z nás pracuje s operačním systémem Windows, zmíníme se zde i o implementaci na této platformě. Windows podporují standard IPSec od své verze 2000, a to prakticky se všemi základními možnostmi. Je možné jej nasadit jak v transportním, tak tunelovacím režimu, takže počítač se může chovat jako zabezpečený klient v nebezpečné lokální síti, ale také jako koncový bod pro sestavení internetového tunelu. Konfiguraci parametrů IPSecu lze definovat jak z grafického rozhraní přes konzolu MMC pomocí snap-inu Politika IPSecurity, tak z příkazové konzoly pomocí nástroje Ipsecpol.exe (Windows 2000), Netsh ipsec (Windows 2003) a Ipseccmd.exe (Windows XP). V novějších verzích XP a 2003 navíc přibyl výrazně vylepšený grafický nástroj IP Security Monitor, s jehož pomocí lze velmi dobře monitorovat, jak se nasazené politiky skutečně projevují a případně tak hledat chyby. Z ověřovacích metod podporují Windows tři: protokol Kerberos je vhodný pro větší lokální sítě se službou Active Directory, výměnu certifikátů pak lze s úspěchem využít především při komunikaci se zařízením na jiné platformě, preshared key je vhodný pro řadu situací, včetně testování.

Protokol: PPTP

Dávno předtím, než se výrazněji prosadil standard IPSec, se v oblasti VPN poměrně rozšířil protokol, navazující na svého slavného předchůdce. Dodnes velmi populární protokol PPP stále patří mezi důležité mechanismy propojení počítačů především po sériových linkách, jejichž všem důvěrně známým zástupcem je především klasický modem na vytáčené lince (dial-up). Když před časem společnost Microsoft hledala cestu, jak osvědčený mechanismus využít a na jeho základě vybudovat technologii pro VPN, sáhla právě k prověřenému PPP. Výsledkem bylo řešení s názvem Point-to-Point Tunneling Protocol, jež k běžné výbavě svého předchůdce přidávalo klíčovou možnost: šifrování obsahu. Přestože se jedná o původní řešení z Redmondu, tvůrci časem o tomto protokolu zveřejnili informace v dokumentu RFC 2637 a řada firem jej rovněž začala implementovat do svých zařízení, takže se dnes jedná o poměrně populární a rozšířenou variantu.

Základem ochrany dat je u protokolu PPTP jejich speciální balení do rámců typu PPP. Možná si právě teď, po bližším „ohledání" situace, říkáte, že tady něco nehraje: PPP je přece protokol pro sériovou linku a pracuje na úplně jiné „vrstvě" než síťové pakety IP! Tak jak to tedy je s VPN v internetovém řečišti, když dial-up modem vždy obsadí celou linku (okruh), aby po ní PPP mohl běžet? To je samozřejmě pravda a celá věc je provedena poněkud rafinovaněji. Původní síťová data jsou nejdříve zabalena jako vždy, tedy jsou běžně opatřena záhlavím protokolu IP. Zvolíme-li pro VPN řešení PPTP, nastane na rozdíl od technologie IPSec poněkud odlišná situace: původní IP paket je zabalen do bezpečného záhlaví PPTP, jako bychom jej chtěli poslat po telefonní lince, avšak nic takového se samozřejmě nestane. Naopak: příslušné ovladače jej znovu (ještě jednou!) opatří záhlavím IP (tedy vnějším) a takto zakuklenou formu pošlou běžnou internetovou – IP sítí. Pokud bychom tedy hlavičky kontrolovali znovu od vnějšího „obalu", narazíme na běžné veřejné IP záhlaví, pod ním bude PPTP (resp. PPP), pak znovu IP (tentokráte to vnitřní, chráněné) a nakonec běžné TCP/UDP a až pak užitečná data. Zdá se to možná podivné, ale má to své důvody, jež vysvětlíme.

V první řadě původní protokol PPP, z něhož se vycházelo, dokáže krásně zapouzdřit z vaší lokální sítě nejen provoz IP, ale i jiné varianty (třeba starší NetBEUI), což se rozhodně hodí. Další výhodou je to, že protokol PPP a upravený PPTP nabízejí mechanismus pro úvodní ověření klienta, jenž přistupuje do vzdálené sítě a chce VPN tunel sestavit. V této fázi dojde nejen k samotné autentizaci (tedy k prověření, s kým máme tu čest), ale také k výměně šifrovacích klíčů, jež budou následně potřeba. Další nezanedbatelnou výhodu představuje u mateřského PPP schopnost jisté komprese přenášených dat, čímž také ušetříme na provozních nárocích.

Jedinou zásadně chybějící součástí bylo v případě původního protokolu PPP šifrování. Zde Microsoft přistoupil k implementaci svého mechanismu s názvem MPPE, který zdaleka není tak variabilní jako IPSec, neboť nabízí pouze jeden šifrovací algoritmus a při konfiguraci lze v pod-

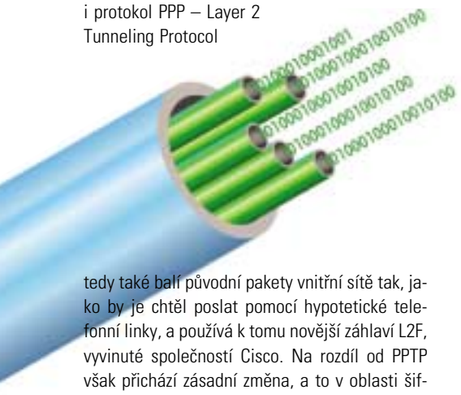
statě volit jen z několika možností délky šifrovacího klíče.

Protože technologie PPTP pochází z dílen Microsoftu, asi nikoho nepřekvapí, že jsou jí vybaveny především systémy Windows, a to včetně verzí 9x či NT 4.0. I klientské stanice jsou schopny jako základní PPTP server přijmout příchozí VPN volání a samozřejmě není problém sestavit spojení opačně, tedy v roli volajícího klienta. Protokol PPTP se stále hojně používá, a to především tam, kde není možné z nějakých důvodů nasadit IPSec. Pro správce firewallů opět jedno důležité upozornění: protokol PPTP přenáší své pakety v síti TCP/IP na portu 1723.

Protokol: L2TP over IPSec

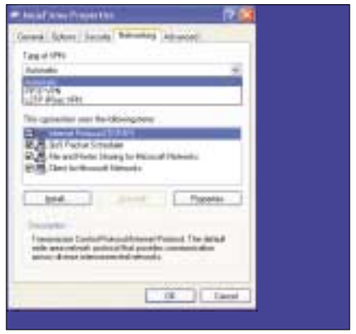
Pokud standard IPSec představuje zavedenou cestu především v oblasti tunelování mezi pobočkami či jinými sítěmi a protokol PPTP je hojně rozšířenou, byť mírně zastarávající variantou při komunikaci mezi serverem a klientem (client-to-gateway), nyní vám představíme řešení, jež spojuje výhody obou.

Společnou aktivitou firem Microsoft a Cisco vstoupil před časem do oblasti VPN nový protokol, jenž by mohl časem nahradit právě PPTP. Název L2TP naznačuje, že je jedná o koncepčně podobné řešení jako výše zmíněné PPTP, neboť jde opět o tunelování na „druhé" vrstvě, kde běží i protokol PPP – Layer 2 Tunneling Protocol

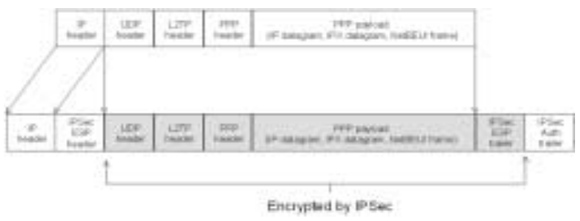


tedy také balí původní pakety vnitřní sítě tak, jako by je chtěl poslat pomocí hypotetické telefonní linky, a používá k tomu novější záhlaví L2F, vyvinuté společností Cisco. Na rozdíl od PPTP však přichází zásadní změna, a to v oblasti šifrování: L2TP sám o sobě žádný šifrovací mechanismus nemá, což vypadá jako značný problém. Ve skutečnosti však tento protokol pro svou práci využívá možností standardu IPSec, což jej činí velmi silným a odolným, a dává mu dobrou naději do budoucna. Pokud se nad uvedeným protokolem technologií zamyslíme, zjistíme, že jeho síla nespočívá jen ve využití IPSecu, ale také ve dvojím mechanismu autentizace. Jak je to možné? Stejně jako protokol PPP a PPTP i L2F totiž provádí ověření vzdáleného klienta na úrovni uživatele, jenž je nucen zadat jméno a heslo či předložit svou identitu nějakou jinou formou (třeba na chytré čipové kartě nebo „kalkulačce typu eBanka"). Jenže pokud si vzpomínáte, jak pracuje IPSec, tak tímto vše zdaleka nekončí, neboť je rovněž potřeba ověřit identitu vzájemně se spojujících počítačů, což právě IPSec striktně vyžaduje. Jinak řečeno, pokud se chcete třeba z notebooku přihlásit do vzdálené sítě, bude nejen prověřeno, zda jste to vy, ale také zda se připojujete z určeného, ověřeného počítače.

Právě ony zmíněné bezpečnostní důvody bezesporu vedly společnost Microsoft k tomu, že od verze Windows 2000 je VPN typu L2TP over IPSec implementována jak v podobě klientů, tak serveru, což umožňuje její plné nasazení.



▲ **Klientská aplikace pro sestavení VPN řešení podle scénáře client-to-gateway je přímou součástí Windows. Po jejím prvotním nastavení pomocí průvodce Nové síťové připojení lze kdykoliv změnit právě třeba protokol, pomocí nějž bude tunel od klienta k serveru (bráně) sestavován.**



▲ **Protokol L2TP over IPSec se může na první pohled zdát opravdu komplikovaný. O způsobu ochrany paketů nám hodně napoví tento obrázek – původní IP paket je zabalen do PPP (jakoby patřil na telefonní linku), pak ale následují další ochranná a režijní záhlaví, která jej vrátí do internetového IP řečiště.**

Protokol: SSL/TLS

Výše popsané technologie pro sestavování VPN spojení jsou dnes v podstatě zvládnuty, a proto se zdá, že jsme nalezli řešení problému cesty veřejnou, nebezpečnou sítí. Vývoj však neustává a přináší další zajímavé možnosti, jež odstraňují některé existující překážky.

Jednou z nejnovějších cest při budování VPN je využití protokolu SSL, případně jeho velmi podobné varianty TLS. Ne že by se jednalo o nějakou převratnou novinku: podpora SSL je dnes v každém pořádném internetovém prohlížeči samozřejmá a obdobným způsobem lze chránit třeba přenos pošty nebo souborů pomocí serverů FTP. Dalšího využití se protokoly SSL/TLS dočkaly právě díky tomu, že začaly být používány i pro účely tunelování. Tvůrce podobných řešení k tomu mimo jiné vedla jedna důležitá skutečnost: popularita a rozšíření SSL či TLS jsou takové, že projdou prakticky všemi síťovými cestami, neboť většina správců sítě je považuje za užitečné a jako takové je propouští. Dalším důležitým „plusem" je to, že obzvláště protokol SSL je prověřen dlouhodobým služebním nasazením a prokázala se vysoká kvalita jeho původního návrhu i způsobu ochrany dat. Další nezanedbatelnou okolností je silná autentizace komunikujících stran, pro niž je v případě SSL/TLS využívána výměna certifikátů.

Nasazení uvedených protokolů pro tvorbu VPN se stále více prosazuje a jeho masivnější prosazení je zřejmě jen otázkou času. Z různých implementací můžeme zmínit třeba produkt Kerio WinRoute Firewall, jenž dokáže tunel na bázi protokolu SSL využít k propojení vnitřních sítí jednotlivých poboček přes nechráněnou internetovou síť.

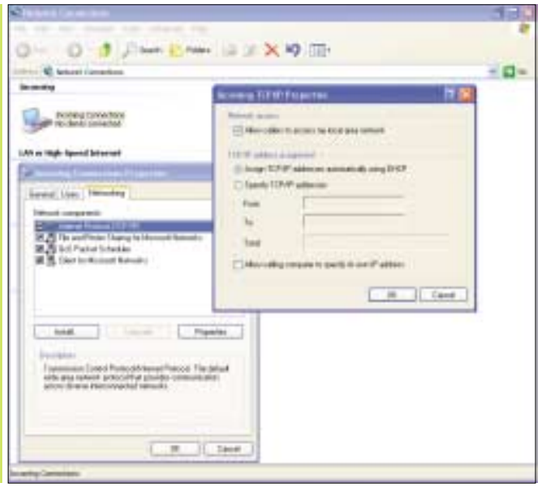
Související služby s VPN

Předchozí odstavce nám poskytly základní přehled, v němž bylo prozatím ukryto několik úskalí. Naznačme si nyní některá z těch, jež jsou řešena souvisejícími službami.

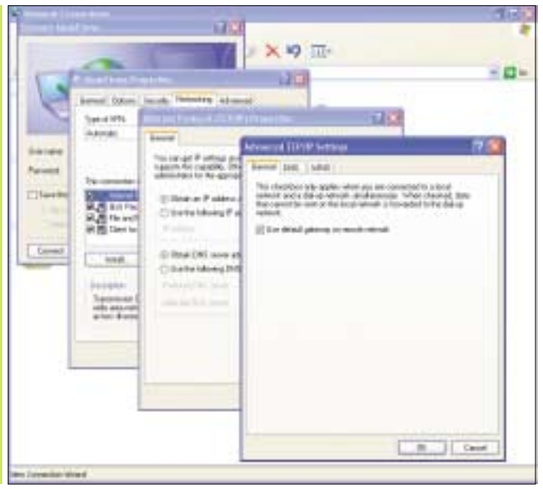
Připomeňme, co se vlastně stane při vzniku VPN: počítače, jež se dosud „neviděly", se stanou součástí jediného virtuálního síťového prostředí. Vůbec při tom nezáleží na faktu, zda jsme přiřadili ve scénáři client-to-gateway jediného uživatele do zbytku sítě, nebo jsme při nasazení gateway-to-gatewy propojili najednou desítky počítačů z různých poboček. Takto vzniklý společný síťový „rybník" je však potřeba řídit. V první řadě je nutné dohlédnout na to, aby všechny počítače měly odpovídající IP adresaci. Problémy mohou být jak rázu konfliktního (ve stejné, náhle sestavené síti se vyskytnou duplicitní adresy), tak charakteru „nedostupnosti", pokud se síťové segmenty nacházejí jakoby v jiných IP adresovacích prostorech a nemáme zajištěno směrování (routing). V případě vzdálených klientů, tedy třeba cestujících uživatelů s notebooky, bývá problém řešen jednoduše: novému „příchozímu" přidělí VPN server při připojování adresu ze své zásoby nebo prostřednictvím DHCP služby dynamicky, takže je vystaráno.

Velmi podobně je třeba dohlédnout na práci služby DNS, která překládá klientským počítačům internetová jména na IP adresy. Připojením pomocí VPN totiž může dojít k přesměrování toku DNS dotazů, což může způsobit porušení funkcionality. Právě proto je často VPN klientům zasílána, spolu s DHCP konfigurací, i nová adresa služby DNS, aby byla zajištěna její dostupnost.

Poslední „drobnost", kterou předložíme zvídavému čtenáři k zamyšlení, je změna nastavení výchozího směru odchozí komunikace po připojení klientského počítače k VPN. Klientský software totiž většinou předpokládá, že tou nejdůležitější sítí je VPN, a proto se snaží veškerý odchozí provoz „natlačit do tunelu". Důsledkem je, že veškerou komunikaci směřující do internetu posílá klient třeba z domova po trase: domácí počítač-VPN tunel-firemní VPN server-firemní brána-výstupní proxy server (firewall)-veřejný internet a zpět. To může být žádoucí stav, ale také nepříjemný druhotný důsledek: často chceme tunelem posílat jen data pro interní služby ve firmě, ale internetové požadavky pak chceme posílat přímo z domova. Problémem může být, že ne všechny klientské VPN aplikace takové rozdvojení dovolují, což je potřeba blíže prozkoumat případ od případu.



▶ **Ani v případě, že jako nejjednodušší VPN server použijete svá Windows XP, nejste zbaveni problému s přidělováním IP adres uvnitř vznikajícího tunelu. Volit lze mezi DHCP službou nebo ručně vybraným zásobníkem IP adres, jež budou klientům přidělovány.**



▶ **Některé užitečné volby jsou ukryty ve Windows opravdu hluboko. Tento přepínač slouží k tomu, aby jakékoliv odchozí síťové požadavky (ne)byly směrovány do sestaveného tunelu VPN. Chcete-li využívat na klientském počítači jinou výchozí bránu, než tu ve firmě na druhém konci tunelu, volbu zrušte.**

Závěrem

Pevně věříme, že náš úvod do technologií virtuálních privátních sítí vám přinesl alespoň základní pohled na principy jejich fungování. Pochopitelně jde o téma tak rozsáhlé, že je nelze zpracovat v jediném článku. Protože dobře víme, že předložený text přinesl zvídavému čtenáři řadu odpovědí a ještě více otázek, k některým dílčím tématům se samozřejmě budeme na stránkách PC WORLDu v budoucnu postupně vracet.

5 0104/FEL ❑