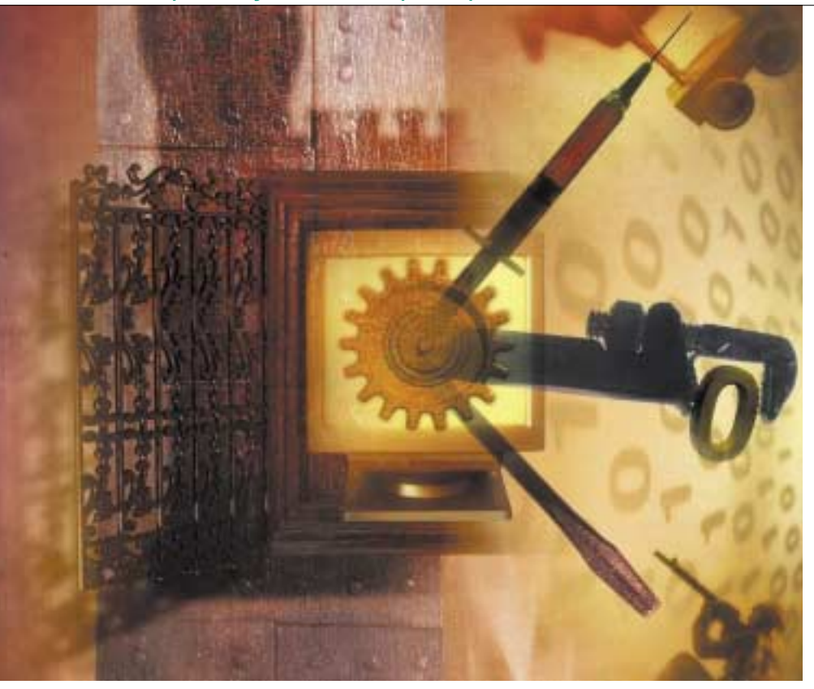
Na internet v zastoupení

Co když stojí v cestě proxy server



Určitě jste na tu situaci už někdy narazili: nainstalovali jste si nějaký nový program pro síťovou komunikaci, chtěli se připojit k internetu a „někde“ to přestalo fungovat. Pokud jste rozluštili chybové hlášení nebo prozkoumali nápovědu, jedna z prvních okolností, na něž jste narazili, byl požadavek na korektní nastavení proxy serveru. Co to ale má vlastně znamenat? Tento článek vám objasní, k čemu proxy server je a především jak se s ním úspěšně spolupracuje.

PATRIK MALINA

Použití technologie, jež bývá běžně označována jako proxy server, dnes patří k naprosté samozřejmosti. Na její bariéru narazí častěji uživatelé větších, typicky firemních sítí, ale stejně tak mohou stát tváří v tvář stejnému problému i „administrátoři“ domácích, menších síťových řešení. Protože jde o záležitost veskrze užitečnou a do budoucna jistě stále běžnější, naleznete v následujících odstavcích podrobnosti nejen o podstatě služby stejného jména, ale především o praktických důsledcích a konfiguraci klientských aplikací. Pokusíme se objasnit, jak vlastně proxy funguje, z čehož posléze jednoduše vyplyne i problematika dodatečné konfigurace, nad níž jste si třeba dodnes lámali hlavu. A třeba úplně zbytečně, neboť nejde o nic výjimečně složitého.

K čemu je proxy?

Mechanismus, označovaný běžně jako proxy či proxy server, je poměrně důležitou síťovou službou. Bývá typicky spouštěna na rozhraní dvou sítí – vnitřního, utajeného segmentu a veřejné, internetové části – ale může být také umístěna někde opodál, jak si uvedeme dále. Služba proxy v obecném pojetí (podrobnosti upřesníme dále) bývá často v souladu s trefným anglickým pojmenováním označována jako zástupný server, ale klidně by se hodil i jiný příléhavý překlad, totiž zplnomocněný zástupce. Koho zastupuje a proč vlastně? Pokud sledujete naše články o bezpečnosti sítí, pak jistě víte, jak nebezpečné je přímé rozhraní mezi veřejným internetem a jakoukoliv vnitřní sítí, třeba firemní nebo domácí. Jistě také znáte něco z problematiky firewallů a třeba používáte ve Windows XP mechanismus tohoto označení pro zabezpečení vašeho počítače před možnými útoky zvenčí. Služba proxy je určena rovněž pro toto rozhraní, avšak typicky je „natočena“ obráceně – do vnitřní sítě. Odtud loví přicházející požadavky, vyhodnocuje je a případně rozhoduje o jejich pokračování dále do internetu. Proč taková funkcionalita? Protože proxy zastupuje typicky klienty vnitřní sítě při putování směrem ven. A důvodů je hned několik.

Základním principem služby proxy je činnost, při níž se hraniční proxy server tváří zároveň jako server a klient některé z aplikačních síťových služeb. Pro zjednodušení si princip můžeme vysvětlit na běžném protokolu HTTP, díky němuž uživatelé získávají obsah webových stránek. Odešle-li uživatel vnitřní sítě, vybavené proxy službou, z prohlížeče požadavek na určitý dokument na internetu, skončí cesta těchto síťových paketů překvapivě brzy. Na hraně sítě je proxy služba zachytí, jako by sama byla oním cílovým serverem, a podrobí průzkumu. Kontroluje, zda je váš požadavek v pořádku, tedy třeba v souladu s nastavenými pravidly, jestli se nepokoušíte získat zakázané či neslušné dokumenty, a pokud je služba dosti přísná, vyžádá si dokonce vaše výslovné ověření jménem a heslem. Pokud projdete kontrolou, proxy server (poté, co původní požadavek zevnitř rozebral) znovu na vnějším rozhraní paket sestaví a odešle dále do internetu. V tuto chvíli se zachová jako držitel své druhé role – stane se dočasně klientem stejné služby, jíž jste použili, a počíhá si na odpověď. Po návratu žádané informace se bezpečnostní procedura opakuje: opět přijde kontrola, zda není vracený obsah závadný, neboť z internetu dnes můžete „chytit“ ledacos, a v případě propuštění se data opět rekonstruují na vnitřním rozhraní a vrací původnímu klientu. Tedy proxy se ocitá opět v roli serveru – z hlediska počítačů uvnitř sítě v roli serveru zástupného, jenž je v internetu plnomocně zastupuje.

Zjednodušeně řečeno, proxy služba plní funkce při komunikaci odchozí (mezi ně patří kontrola oprávněnosti požadavku a identity žadatele) a také při návratu, kdy je odhalován škodlivý obsah či potenciální útok. Navrácené dokumenty pak mohou být typicky ještě skladovány po nějakou dobu v úložišti (tzv. cache), aby příští požadavek na tentýž internetový materiál mohl být vyřízen okamžitě, z nahromaděných zásob. Cíl je tedy zřejmý: výrazné zvýšení bezpečnosti, řízení přístupu k internetu a případné zvýšení výkonu a odlehčení linky díky uložení do cache („keše“, mezipaměti). Velmi důležitý je fakt, že jednotlivé pakety nikdy neprojdou přímo, ale jsou vždy pečlivě rozebrány a znovu sestaveny, což umožňuje jejich totální kontrolu a případné odhalení záměrných konstrukčních závad, jež mohou signalizovat nekalé pokusy o útok. I proto je proxy služba označována jako ochrana na aplikační úrovni: vidí aplikačním protokolům, jako je HTTP, až „do kuchyně“.

Kudy vede cesta?

Když ona proxy služba tak krásně funguje, proč bych se s ní jako uživatel měl vůbec zdržovat? Já odešlu, ona zachytí a zase vrátí… nebo je snad někde háček? Pojďme se podívat blíže, kde mohou vniknout potíže.

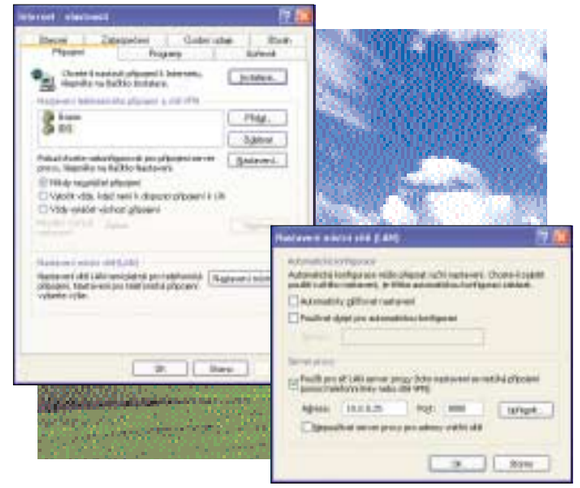
V první řadě nezapomínejme, že služba proxy je velmi speciálně navržena pro „svůj“ vlastní protokol: HTTP si žádá svou službu, FTP jinou a třeba aplikace pro internetovou telefonii s protokoly H.323 nebo SIP (Skype, NetMeeting) rovněž chtějí své.

Pokud jednotlivé služby pro dané protokoly leží na různých fyzických serverech, musíme aplikacím sdělit, kde je mají hledat. Často sice může platit, že více proxy služeb je spuštěno na stejném proxy serveru, ale ten ani v takové situaci nemusí být pro klientský počítač totéž, co tzv. výchozí brána pro ostatní síťovou komunikaci. Jak vše tedy typicky funguje a kam vlastně odesílané požadavky putují?

Začněme nejdříve se situací, kdy proxy server jakoby neexistuje. Vaše síťová karta, pracující třeba na nejběžnější technologii Ethernet, zahrnuje v konfiguraci protokolu TCP/IP základní údaje: IP adresa identifikuje váš počítač, síťová maska příslušnost ke společenstvu vám podobných (podsíť) a výchozí brána (default gateway) pak směr, kudy vede cesta ven, mimo vaši vlastní síť. Dostane-li aplikace příkaz ke komunikaci do internetu, podle cílové adresy rozpozná, že cíl je mimo mateřský segment (při výpočtu ji pomůže právě síťová maska) a v první řadě paket s požadavkem pošle právě směrem na výchozí bránu – jinou možnost ani pro cestu „ven“ nezná. A pozor: pokud je zde, na bráně, navíc nainstalována proxy služba pro všechny potřebné aplikační protokoly, je vše prosté a na klientském počítači není potřeba nic dále nastavovat: cíl je vždy jasný a adresa brány zajistí správný směr.

Zde se však objevuje první zjevný háček – server-brána by musel zajišťovat funkce a služby proxy pro všechny potřebné protokoly a navíc ještě pracovat jako opravdová brána pro ostatní protokoly, jež nejsou pomocí proxy zpracovávány. Pokud tomu tak opravdu je, říkáme celému řešení transparentní proxy. Pro klienta je vše naprosto průhledné a nemusí nic dalšího konfigurovat.

Často tomu tak však není. Běžně vypadá situace jinak: proxy služby leží na jiném stroji než výchozí brána, neboť tato třeba vůbec nemusí směřovat do internetu! Nebo je proxy služeb více a jsou na různých strojích, pro každý typ komunikace někde jinde, a pak jediná adresa výchozí brány ne-



může ukázat, kam příslušná data potečou. A také (především ve větších a složitějších firemních sítích) se může stát, že proxy server leží v úplně jiné vnitrofiremní síti, než k jaké příslušíme, a proto se k ní musím propracovat přes samotnou výchozí bránu! Ze všech těchto situací vyplývá nutnost říci aplikacím a operačnímu systému, kde se vlastně proxy služba nachází a jakému protokolu poslouží, aby vše neputovalo na výchozí bránu, jež nemusí být schopná najít řešení.

V případě operačního systému Windows lze tato základní nastavení provést prostřednictvím ovládacího panelu Možnosti internetu (Internet Options), který můžete otevřít rovněž z prostředí Internet Exploreru v menu Nástroje (Tools). Zde vyhledejte záložku Připojení (Connections) a pomocí tlačítka Nastavení místní sítě (LAN Settings) přejděte do dalšího dialogu.

Na tomto místě můžete provést prvotní konfiguraci pro přesměrování požadavků na službu proxy, ať se nachází kdekoliv. Všimněte si, že v první řadě zadáváte adresu protokolu IP, na níž služba „číhá“, a posléze případně ještě port, neboť protokoly jsou na serveru proxy běžně přijímány na jiném portu, než je u aplikačních protokolů běžné. Oba údaje vám samozřejmě sdělí buď v případě firemních či školních sítí administrátor, nebo si je musíte zjistit sami, pokud instalujete třeba doma malé řešení pro přístup do internetu s integrovanou službou proxy. Nezapomeňte, že adresa IP služby proxy může být klidně umístěna mimo vaši mateřskou síť a aby posléze vše korektně fungovalo, je nezbytně nutné mít zároveň definovánu dříve zmíněnou výchozí bránu. Poslední drobností je zaškrtávací pole, zakazující použití proxy pro adresy ve vnitřní síti – použijte je pouze v případě, že chcete přistupo-

vat prohlížečem či jinými aplikacemi na servery nikoliv v internetu, ale také ve vašem bezprostředním lokálním síťovém okolí.

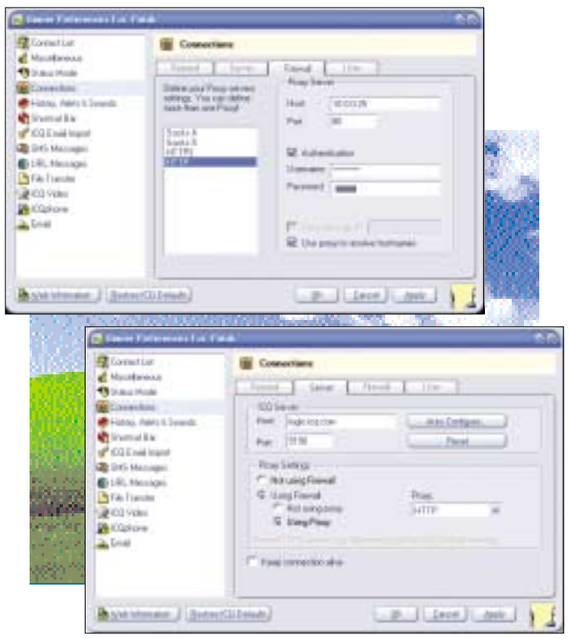
V tuto chvíli zatím není zcela jasné, pro jaké aplikační služby jsme vlastně službu proxy nastavili, takže použijeme tlačítko Upřesnit.

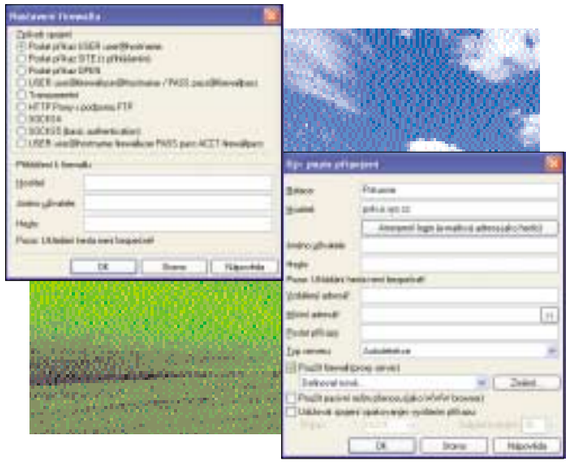
Nově otevřený dialog nejen vše prozradí, ale také případně dovolí definovat pro jednotlivé síťové služby různé cílové servery proxy: v seznamu vidíme běžný protokol HTTP pro webové stránky, pod ním jeho zabezpečenou variantu, dále službu FTP a mírně zapomenutý Gopher a specifické rozhraní Socks (bude podrobněji zmíněno dále). Všimněte si, že v dolním okně je možné výslovně říci, pro které adresy ve vašem bezprostředním sousedství nemá být služba proxy použita. Jde o dosti důležité nastavení, protože proxy server obvykle vaše sousedy nezná, netuší, že provozují třeba webový server, snaží se je najít v internetu a po neúspěchu požadavek zahodí jako neproveditelný – jinými slovy: proxy služba se nedívá zpět do vlastních řad a vy s tím musíte počítat.

Jak tedy bude v našem konkrétním případě paket cestovat? Zadejme do prohlížeče třeba požadavek na stránky *www.pcworld.cz*. Windows rozpoznají, že jde o aplikační protokol HTTP, přečtou si adresu proxy a zjistí, že leží mimo naší síť – nezapomeňte, že (viz dřívější obrázky) jsme s adresou 192.168.1.3 úplně jinde než služba proxy s adresou 10.0.0.25. Paket je tedy odeslán na výchozí bránu – 192.168.1.1 – a dále putuje jinými síťovými segmenty k proxy (udržuje si její adresu), dále v zastoupení do internetu a zpět přes proxy a bránu k nám. Zdá se vám to složité? Ani ne, vždyť stačily tři údaje: výchozí brána, adresa serveru proxy a jeho odpovídající číslo portu.

Proxy a typické aplikace

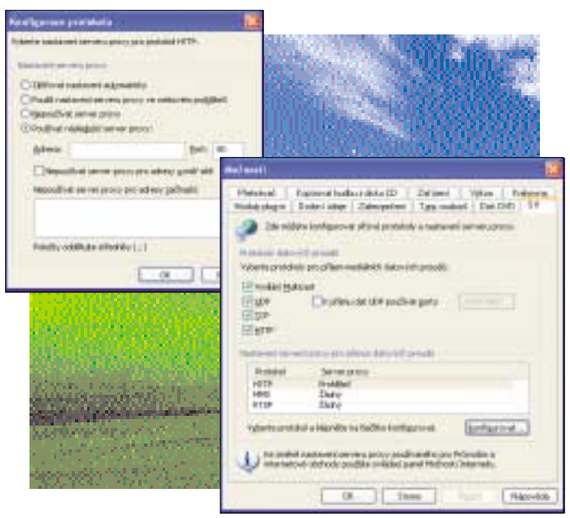
Náš dosavadní postup nás dovedl do částečně uspokojivé situace, kdy řada aplikací díky nastavení Windows získala informaci, kde naleznou proxy službu a jak se díky tomu dostanou k odpovědím na své internetové požadavky. Bezvýhradně jsme náš problém ovšem zdaleka nevyřešili, neboť popsaná nastavení si dokáže přečíst Internet Explorer a případně několik dalších aplikací, ovšem zdaleka ne všechny. V první řadě jste si jistě všimli, že seznam aplikačních protokolů byl až příliš krátký, navíc možná již z vlastní zkušenosti tušíte, že jiné programy si žádají svá specifická nastavení. V následujících řádcích si tedy popíšeme ukázkové případy nastavení některých dalších aplikací, na něž můžete běžně narazit.





Jednou z běžných služeb je instant messaging, takže nahlédněme do rozhraní programu ICQ. V hlavním menu najdeme část Preferences s různými konfiguračními volbami – položka Connections zahrnuje parametry, o něž nám jde. Na kartě Server v dolní části v první řadě rozhodneme, zda bude služba proxy vůbec použita. Pakliže ano, můžeme vybrat z několika variant (typicky HTTP) a posléze na kartě Firewall upřesníme nám již známé údaje v podobě adresy a portu cílového proxy serveru. Pamatujete, jak jsme v úvodu hovořili o tom, že služba proxy umí také donutit klienta k ověření totožnosti? Pak přesně tohle můžete vyřešit vyplněním polí u funkce Authentication, neboť ICQ následně předá potřebné údaje za vás.

Dalším pěkným případem volby příslušného proxy serveru je konfigurace nástroje Total Commander, přesněji jeho komponenty FTP klient. Z názvu je jasné, že cílem je správně přesměrovat požadavky aplikačního protokolu FTP, jež budou sestavovány právě a jenom tímto programem. Pomocí příslušného tlačítka FTP se přesuňte do dialogu se seznamem příslušných připojení, u jednoho z nich použijte volbu Editovat a v následujícím okně v dolní části pak zatrhněte pole Použít firewall (proxy server). Díky tomu se zpřístupní tlačítko Změnit a vstoupíte do těch nejtajemnějších zákoutí: povšimněte si v cílovém dialogu řady možností, jak lze pomocí různých FTP příkazů inteligentně se službou proxy navazovat FTP relaci. Total Commander je v tomto ohledu vybaven opravdu velmi slušně. I zde, jak vidíte, je možné napevno zadat uživatelské jméno a heslo pro ověření vůči nekompromisní službě proxy. Nezapomeňte rovněž na důležitou skutečnost: zde předvedené nastavení se týká aplikace, v níž se nyní pohybujeme, a pokud FTP požadavek odešle třeba Internet Explorer, bude se pro změnu řídit svými parametry, tedy třeba úplně jinou adresou proxy serveru! Možná trošku podivné, ale hlavně účinné a jasně konfigurovatelné.

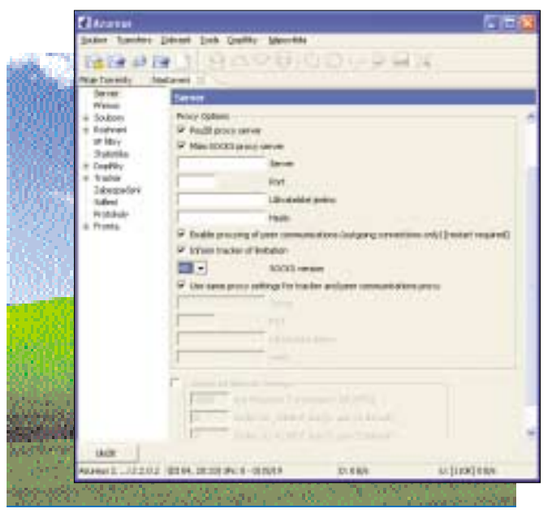


Podobně jako běžný prohlížeč a FTP klient, vyžadují nastavení proxy serveru i další programy, u nichž byste to možná na první pohled nečekali. Vzpomeňte třeba na antivirové programy, jež potřebují provádět obnovu svých databází a automaticky sahají na internet – v případě absence nastavení proxy služby může dojít k zásadnímu ohrožení funkcionality! Velkou výhodou je skutečnost, že řada takových aplikací využívá rovněž protokol HTTP, a proto lze zadat adresu stejného serveru jako u prohlížeče. Na obdobnou situaci narazíte třeba i u programu Windows Media Player, jenž pracuje s různými protokoly a dovoluje definovat proxy servery pro každý z nich nezávisle. Velmi důležité je nastavení této služby rovněž u řady aplikací pro internetovou telefonii či jiné multimediální přenosy.

Absolutní klient služby proxy

Z předchozího povídání vyplynulo, že komunikace mezi klientským počítačem a serverem služby proxy je vlastně dohadováním s menší či větší mírou volnosti na straně klientského operačního systému a aplikací. Možná vás napadla myšlenka, zda by nebylo lepší rovnou poradit aplikacím, aby si s proxy službou nejdříve vše domluvily a pak, bez nutnosti něco lokálně konfigurovat, byly odesílány požadavky přesně tam, kde jsou očekávány. Tento princip je natolik zajímavý, že byl pochopitelně dávno realizován v praxi a používá se třeba jako proxy typu SOCKS (případně ještě doplněno číslem verze). Když se nad tímto principem zamyslíte, jedná se vlastně o jakési absolutní řešení, neboť služba proxy je ze vzdáleného serveru předsunuta až na každý klientský počítač a samotné aplikace ji mají blízko po ruce. Jedinou podmínkou samozřejmě je, aby ji uměly zavolat.

Možnosti služby SOCKS jsou poměrně široké, neboť klient a server si mohou domluvit řadu důležitých parametrů. V první řadě proxy může nezávisle na protokolu, o nějž následně půjde, provést ověření (autentizaci) klienta. V dalším „kole" si mohou speciálním kanálem dohodnout, na který port budou aktuální požadavky zasílány a v případě, že si určitá aplikace žádá více komunikačních portů zároveň, je i toto možno dojednat. Jde tedy o řešení dosti univerzální, jež se především rozšířilo ve světě operačních systémů UNIX, resp. Linux, avšak i četné klientské aplikace na Windows si s ním dokáží poradit. Z výše uvedených příkladů podporují SOCKS třeba Total Commander nebo ICQ a vaším úkolem je pouze zvolit variantu protokolu SOCKS v souladu s instalovanou verzí proxy serveru. Dnes patří mezi nejběžnější varianty V4 a V5, jak je dobře vidět třeba u aplikace Azureus pro komunikaci v sítích BitTorrent.



Aby to však nevypadalo, že mechanismus SOCKS se týká jen sítí s Linuxem, je potřeba podrobnějšího vysvětlení, přesněji dvou poznámek. Pokud používáte Windows jako klientský operační systém, možná máte pocit, že se vás to netýká, avšak opak může být pravdou. Pokud na vašem proxy serveru opravdu Linux je, tak se podle toho vaše aplikace mohou či musí chovat a výše popsaná nastavení se vám mohou hodit. A druhá poznámka zase platí v případě, že na vašem síťovém rozhraní je v roli proxy serveru právě software společnosti Microsoft, označovaný v současných verzích jako MS ISA Server. Toto řešení se umí chovat buď jako klasická služba proxy, ale také obdobně jako systém SOCKS. Tvůrci jeho použití vyřešili tím, že do operačního systému je instalována speciální komponenta s názvem MS Firewall Client, jež zařídí přímo na zdrojovém počítači přesměrování na zástupné knihovny WinSock a následnou cestu k SOCKS/Proxy serveru. Toto řešení má své výhody a řadě aplikací dokáže transparentně pomoci, takže nemusíte provádět složité konfigurace, avšak také je zde jedna nevýhoda: klient se nedodává pro jiné OS než Windows. Těm zbývají jen klasické možnosti, jako je nastavení prohlížeče či FTP klientu.

Limity služby proxy

Již v úvodu článku jsme zmínili, že hlavním významem služby proxy je ochrana vnitřní sítě před požadavky, na něž klienti nemají nárok nebo díky nimž by dovnitř mohla být zavlečena nežádoucí „infekce" v podobě červů, trojských koní nebo nebezpečných aktivních komponent ve webových stránkách, třeba v podobě tzv. ActiveX prvků. Služba to dokáže díky tomu, že nahlédne do nejhlubšího nitra aplikačních protokolů a data dokonale proseje, jak by to udělal třeba neúplatný a důsledný celník.

Problém však nastane v situaci, kdy pohled do nitra aplikační vrstvy je proxy serveru odepřen. Kdo si to může dovolit? No přece vaše klientská aplikace, a to přímo na vaše vyžádání, tedy právě třeba internetový prohlížeč! K těmto situacím dochází tehdy, když se pokusíte přistoupit na zabezpečené webové stránky (internetové bankovnictví, nákupní košíky atd.) a do hry vstoupí ochranný prvek v podobě technologie SSL/TLS. Jde samozřejmě o žádoucí mechanismus utajení vašich osobních dat proti útočníkům a slídilům v internetu, ovšem službě proxy tím vzniká nepřekonatelné dilema. Pokud vám chce bezpečné spojení do banky či internetového obchodu dovolit a umožnit, musí rezignovat na svou ochrannou funkci a nepokoušet se tato spojení „rozlousknout", neboť by je tak jako tak nejen nedokázala zkontrolovat a navíc by je zbytečně zničila. Tím se provoz uvnitř SSL/TLS tunelu ocitá mimo kontrolu se všemi možnými následky: pokud uživatel „naletí" podvodníkům a místo banky se připojí na jakékoliv útočnější stránky, jež si vyžádají šifrovaný spoj, bude proxy služba bezmocná a vy si dovnitř zavlečete nežádoucí obsah. Jaké je řešení? Již při odesílání odchozího požadavku na chráněný server musí proxy server zkontrolovat, zda je tento cíl možné považovat za důvěryhodný. Pokud se vyskytnou pochybnosti, celá relace musí být odmítnuta. Jakmile totiž jednou dojde ke schválení a klientovi se vrátí šifrovanou cestou odpověď, proxy služba již pouze přihlíží a poslední instancí v boji se záškodnickým obsahem už je jen personální firewall či antivirový program na klientském počítači, číhající na potenciální „zakuklené" nebezpečí.

Závěrem

Věříme, že pro vás funkce proxy služby již nepředstavuje žádné velké tajemství a při konfiguraci aplikací si dokážete poradit. Nezapomeňte, že ve firemních či jiných rozsáhlých sítích je dobré začít od konzultace s administrátorem, neboť bez znalostí základních údajů o serverech s proxy službou je konfigurace prakticky nemožná. Protože však již víte, jak vše funguje, budou vám k tomu, abyste aplikace přiměli ke hledání správné cesty do internetu, stačit jen základní údaje.

5 0202/FEL ❑