Firewally – dokončení, proxy systémy

Pozor, útok! (10. díl)

Dnešním, desátým dílem, zaměřeným na popis proxy systémů, uzavřeme seriál věnovaný zabezpečení privátních dat, intranetu a bezpečnosti na internetu.

Úvod

Dříve než se pustíme do popisu proxy systému, vrátíme se na úplný počátek věci a položíme si otázku: Co se za tím vším vlastně skrývá, jaká byla možná východiska, co se tím sleduje? Odpověď je velice jednoduchá, díky ní si totiž uvědomíme dvě extrémní bezpečnostní varianty přístupu uživatelů z vnitřních počítačových sítí k internetu. V první variantě mohou k internetu přistupovat všichni hostitelé našeho systému – tato varianta z podstaty věci nenabízí téměř žádné, nebo jen velice komplikované zabezpečení. Naproti tomu druhá varianta, ve které žádný uživatel nemá přístup k internetu, poskytuje požadovanou bezpečnost. Ale co s takovou bezpečností, když jsme zcela odříznuti od okolí? Výsledkem, nebo chcete-li rozumným kompromisem, se jeví varianta umožňující přistupovat k vnějšímu světu všem oprávněným uživatelům pomocí jednoho, maximálně několika málo obousměrných hostitelů či bastion hostitele (s proxy službou) vnitřního systému – to je podstatný základ myšlenky fungování proxy služeb.

A kdo stál v pozadí základů proxy standardu? Byli to pánové Kevin Altis, Ari Luotonen a Lou Montulli, kteří vycházeli z proxy metodologie založené na gateway kódu, který již dříve napsal pan Tim Bernes-Lee.

Jaká je tedy celá filozofie fungování proxy systémů? Namísto toho, aby uživatelé jednali přímo s nějakým vzdáleným serverem na internetu, proxy služba zajistí komunikaci procházející skrz proxy server, přičemž vše probíhá skrytě, a tak si uživatel myslí, že komunikuje přímo se skutečným vzdáleným serverem, místo toho však samozřejmě komunikuje pouze s proxy systémem. Stejně tak i na druhé straně si vzdálený systém myslí, že komunikuje s proxy serverem. Pozn.: Proto se tedy používá termín “proxy” = zástupce.

Podle tohoto principu klientský program uživatele komunikuje pouze s proxy serverem, který vyhodnocuje příchozí požadavky klientů a rozhoduje, které z nich předá dále, a které bude ignorovat. V případě schválení proxy server přenáší požadavky od klienta ke skutečnému vzdálenému serveru a zpětně přijímá i odpovědi na tyto požadavky pro klienta (viz obr. 1.)

Výhody a nevýhody proxy

Existuje spousta výhod, z nichž patrně nejvýznamnější jsou popsány v následujícím textu:

Proxy služby umožňují efektivně zaznamenávat průchozí komunikaci, neboť “rozumí” přenášenému protokolu, a tak jsou výsledné tzv. log-soubory mnohem kratší a přehlednější.

Proxy služby zjednodušují a zrychlují přístup uživatele ke službám internetu – oproti přístupu přes obousměrného hostitele.

Na druhou stranu nic nemá pouze klady, a tak i používání proxy služeb zahrnuje i jisté nevýhody:

Proxy služby nemusí vždy umět zpracovat některé služby. Jako příklad si uveďme službu typu talk, systém umožňující textovou komunikaci dvou lidí.

Reakce proxy SW na vývoj nových nebo méně rozšířených služeb může probíhat s určitou časovou prodlevou. A tak se může stát, že kvůli absenci proxy SW podporujícího novou službu je nutné tuto službu v této etapě umístit za firewall, což může přinést potenciální mezery v bezpečnosti.

Je možné, že bude potřeba pro odlišné protokoly postavit jiné proxy servery, protože ty budou muset danému protokolu porozumět.

Proxy služba nás také neochrání proti všem bezpečnostním slabinám jednotlivých protokolů.

Proč proxy server?

Nyní si blíže popíšeme některé další výhody, které nám přinese používání proxy serverů.

Možnost tzv. cashing dokumentů – zpravidla klienti na vnitřní síti požadují přístup ke stejným serverům. Některé proxy servery reagují na tuto skutečnost tím, že umožňují dočasně ukládat kopie dokumentů v lokální síti, takže proxy server nepotřebuje znova a znova požadovat pro jednotlivé klienty tyto dokumenty. Je logické, že ukládáním dokumentů na jedno centralizované místo (oproti ukládání na každý klientský systém) mnohdy uspoří již tak nedostatečné místo na discích uživatelů. Touto procedurou je také umožněno "surfovat" po internetu dokonce i tehdy, pokud není daný web server či externí síť v daném okamžiku k dispozici.

Možnost selektivní kontroly přístupu na internet a naopak do vnitřní sítě. Pokud užíváme proxy server, je umožněno filtrovat klientské transakce na úrovni protokolu. Proxy může kontrolovat přístup k službám dle individuálních metod, hostitelů a domén. Některé proxy servery navíc umožňují přidělit vyšší prioritu danému požadavku od specifického uživatele a mohou dále určovat, které klientské protokoly mohou být užívány na základě jejich IP adres.

Poskytují přístup k internetu pro společnosti užívající soukromé sítě. Organizace, které užívají jedno nebo více soukromých síťových adresových míst, jako je např. třída sítě A 10.*.*.*, mohou stále užívat internet právě pomocí proxy serveru.

Tomuto postupu se říká konfigurace pomocí tzv. špatných adres, což jsou speciální adresy, které nelze směrovat na internet a běžně se používají k testovacím účelům konfigurace sítě, např. adresa 10.0.0.0.

Vlastní konfigurace vyžaduje proxy server se dvěma kartami rozhraní pro připojení k sítím. Adresa jedné z karet má skutečnou adresu například 147.228.42.1, naproti tomu druhá karta využívá tzv. špatnou adresu 10.0.0.1. V dalším kroku kartu se skutečnou směrovatelnou adresou 147.228.42.1 připojíme ke směrovači na internet a druhou kartu k vnitřní chráněné síti. Po tomto úkonu konfigurujeme pomocí brány 10.0.0.1 příslušné adresy každé pracovní stanice sítě 10.0.0.0. Všechny aplikace, které server využívá, se nakonfigurují pomocí adresy 10.0.0.1. Tímto jsme zařídili vše podstatné, nyní pokud klient požaduje přístup k internetu, zašle svůj požadavek na kartu rozhraní serveru 10.0.0.1. Proxy server pak připojí k požadavku svoji směrovatelnou adresu 147.228.42.1 a takto upravený požadavek pošle na vzdálený server. Po získání odpovědi od vzdáleného serveru ji dále předá klientu.

Typy proxy serverů

Proxy systémy nevyžadují žádný speciální hardware, ale pro většinu služeb nabízených těmito systémy je nutný speciální software. U proxy systémů rozlišujeme čtyři základní typy:

1) proxy na úrovni aplikace (Application-Level proxy) – tento systém zná konkrétní aplikaci, pro kterou poskytuje své služby, jako příklad aplikace Sendmail obsahující protokol (store and forward);

2) proxy na úrovni spojení (Circuit-Level proxy) – tento systém vytváří spojení mezi uživatelem a vzdáleným serverem bez znalosti aplikačního protokolu, například moderní hybridní brány, navenek vypadající jako proxy, ale uvnitř vypadající jako filtrující směrovač.

Kromě těchto typů se dále můžeme setkat s obdobným dělením těchto systémů na všeobecné proxy servery, které umožňují obsluhovat více protokolů, a vyhrazené proxy servery, které dokáží obsloužit pouze jediný protokol.

Pozn.: Pokud máte zájem o využívání proxy služeb, můžete se podívat např. na poslední odkaz v infotipech a vyzkoušet si práci s některým z nabízených produktů.

Závěr

Tímto posledním dílem jsme zakončili naši cestu informativního poznávání vybraných forem zabezpečení privátních dat vyskytujících se v prostředí počítačových sítí. Je ovšem důležité si uvědomit, že k jisté úrovni bezpečí počítačových sítí může vést teprve řádně navržená, bezchybně implementovaná bezpečnostní politika zahrnující ochranu pokud možno proti všem možným druhům útoků na tato data spolu s neustálou reakcí na vývoj v této oblasti, školením personálu atd.

[Milan Pinte I pinte@atlas.cz]