Využití protokolu SSL pro vytváření VPN

Využití protokolu SSL pro vytváření VPN (1)

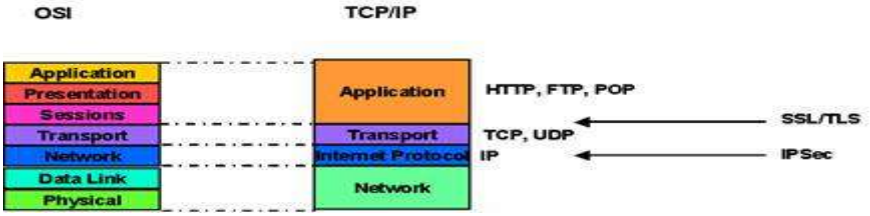
Spojení SSL VPN, tj. využití SSL pro VPN, je pro mnoho lidí stále velice překvapivé a nezvyklé. A skutečně se jedná o relativně novou technologii. První produkty se začaly objevovat v roce 2000 a v nejbližších letech se čeká obrovský boom. Oč se jedná?

Slovo bezpečnost je v IT skloňováno ve všech pádech a bezpečný přístup „k čemukoliv" představuje samostatnou a dynamicky se rozvíjející oblast bezpečnosti. Platby přes internet, e-commerce aplikace (B2B, B2C...), vzdálený přístup do firmy pro obchodní cestující nebo zaměstnanci pracující doma (teleworkers), to vše dnes může reálně existovat jen díky bezpečnému přístupu k prostředkům IT. Riziko odposlechu komunikace, respektive zcizení dat během přenosu, není jen fikce. V současné době se prosadily dva způsoby řešení.

- Prvním je SSL (Secure Socket Layer) - typicky se používá pro přístup k webovým aplikacím, tj. například pro aplikace typu e-banking, apod.
- Druhým je IPSec pro VPN (Virtual Private Network – virtuální privátní sítě), používaný pro bezpečný přístup například do sítě vaší společnosti.

Spojení SSL VPN, tj. využití SSL pro VPN, je pro mnoho lidí stále velice překvapivé a nezvyklé. A skutečně se jedná o relativně novou technologii. První produkty se začaly objevovat v roce 2000 a v nejbližších letech se čeká obrovský boom. Oč se jedná? Nejdříve pár slov o SSL. Secure Socket Layer (SSL) byl vyvinut firmou NetScape. Základní úkoly SSL jsou bezpečně zašifrovat přenášená data a ověřit totožnost uživatele (autentikace). Existuje řada informací a článků o SSL, takže jen ve stručnosti a poněkud zjednodušeně: bezpečné šifrování je zajištěno asymetrickou šifrou, která používá známý veřejný a utajený privátní klíč. Zprávu zašifrovanou příslušným veřejným klíčem, který může znát prakticky kdokoliv, lze dešifrovat jen konkrétním privátním klíčem a naopak. Jedná se o relativně nový způsob šifrování, nalezený kryptografy během posledních desetiletí. Tento způsob eliminuje problém s dohadováním a výměnou klíče před přenosem, což představuje jedno z hlavních rizik symetrického šifrování. Klíče jsou vytvořeny (vygenerovány) certifikační autoritou a vazbu na konkrétní jméno a uživatele zajistí certifikát. Pokud uživatel X zašle svůj veřejný klíč a certifikát uživateli Y, ten si pak může u certifikační autority ověřit díky certifikátu, že tento klíč skutečně patří uživateli X.

SSL představuje mezivrstvu vloženou mezi TCP/IP a aplikační vrstvu, viz. obrázek.



SSL a IPSec z pohledu OSI modelu

Zásadní výhodou SSL je, že je dnes součástí všech webových prohlížečů. Je docela možné, že jste již výhod SSL někdy využili aniž jste si to uvědomili, například při komunikaci s bankou nebo potvrzování platby platební kartou v internetovém obchodě. To, že je provoz šifrovaný, poznáte podle zámku, který se „uzamkne" a zobrazí v dolní liště prohlížeče.

Využití protokolu SSL pro vytváření VPN (2)

U IPSec VPN jde vždy o spojení bod-bod, tudíž se složitostí topologie sítě roste i složitost implementace a následně údržba, obzvláště v případech, kdy uživatel používá softwarových VPN klientů na přenosných počítačích. Jaké výhody přináší SSL VPN a v kterých případech ji použít?

VPN

VPN se stalo magickým slovem a dnes se za virtuální privátní síť označuje „ledacos". V úzkém slova smyslu se jedná o protokol IPSec a opravdu šifrovaný provoz. Nejedná se o nic nového a dnes se tato technologie běžně používá. Praxe ukázala i na problémy, které nasazení IPSec přináší. Jde vždy o spojení bod-bod, tudíž se složitostí topologie sítě roste i složitost implementace a následně údržba, obzvláště v případech, kdy uživatel používá softwarových VPN klientů na přenosných počítačích.

V této souvislosti je potřeba zmínit i fakt týkající se propojitelnosti. IPSec má totiž charakter doporučení a implementace VPN od výrobce A nemusí vždy spolupracovat s řešením výrobce B. Z toho také vyplývá, že VPN lze poměrně dobře použít pro přístup do firmy poskytnutý zaměstnancům, ale stejná služba nabídnutá partnerů (třetím stranám), kteří potřebují přistupovat k podnikovým zdrojům, už to může být netriviální problém. Ti totiž mohou používat VPN klienty jiného výrobce a je potřeba buď zprovoznit vzájemnou komunikaci, nebo nainstalovat dva VPN klienty na jedno PC. Obojí se může ukázat jako neřešitelný problém.

Problém může být i s tím, odkud uživatel přistupuje. Jednak může být tento provoz blokován na firewallu, a jednak IPSec špatně snáší překlad adres (NAT). Pokud se obchodní cestující pokouší připojit do firmy například ze sítě zákazníka, je velká pravděpodobnost, že bude mít problémy.

Nicméně je zde i řada věcí jednoznačně pozitivních. VPN jsou dnes téměř samozřejmou součástí firewallů, což přináší možnost nejenom zabezpečit přenos, ale i definovat pravidla, kam a jakým protokolem se přistupující může dostat. IPSec totiž zpřístupňuje celou síť a pokud hovoříme o bezpečném propojení sítí, potom dnes nemá lepší alternativu.

SSL VPN

Pokud se zaměříme na vzdálený přístup jednotlivých uživatelů a shrneme předchozí poznatky, můžeme si položit otázku: jak by tedy mělo vypadat ideální řešení?

Mělo by být jednoduché na instalaci a údržbu. A co může být jednoduššího než žádná instalace softwaru nebo VPN klienta na koncovém zařízení? Jak už bylo řečeno, SSL je součástí všech prohlížečů. Stačí jenom zajistit, aby se uživatel ověřil/autentikoval, nejlépe stejným způsobem jako když je v síti – například proti adresářovým službám jako je LDAP (Active Directory), RADIUS apod.

Do firemní sítě z internetové kavárny

Řešení by mělo zohlednit nejen to, kdo přistupuje do sítě, ale i odkud, přesněji řečeno – z jakého zařízení. Prohlížeč je na každém počítači, tak proč by vlastně nemohl obchodní cestující přistupovat ke svým datům například z internetové kavárny? Řada správců sítí si teď klepe na čelo – taková lehkovážnost! Na cizím počítači může být skryt program, který odchytí heslo uživatele, může být nakažen virem atd. Nicméně, možná by i v tomto případě bylo dobré, aby se dostal alespoň k omezené množině dat. Jinými slovy, jde právě o zohlednění faktu z jakého zařízení přistupuje. A dále - pokud někdo používá notebook mimo síť, může se s ním ledacos stát. Takže by se hodilo vědět, co vlastně na jeho počítači běží. Je spuštěn personal firewall, je instalována poslední verze antiviru?

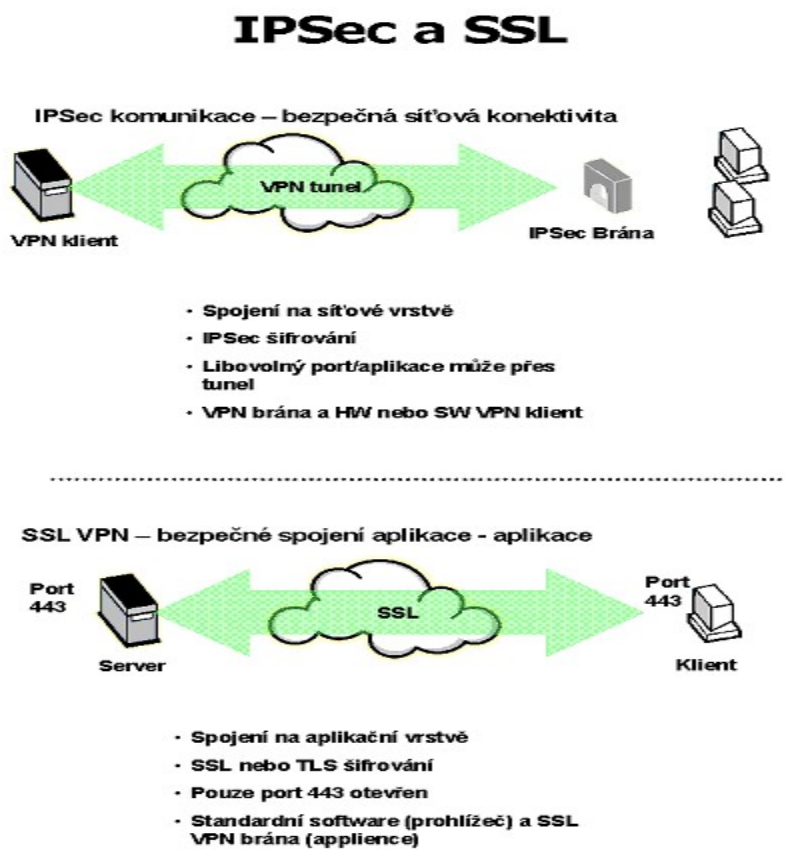
Už víme, kdo a odkud přistupuje. Zbývá ještě možnost ověřit, zda je uživatel v daném okamžiku „důvěryhodný" a potom, na základě vyhodnocení všech podmínek, umožnit přístup k daným aplikacím. Takto můžeme definovat například následující pravidlo: „Uživatel X z vlastního notebooku dostane přístup ke všem aplikacím, ale jen pokud bude mít poslední verzi antiviru. Při přístupu z libovolného jiného zařízení nebo s neaktuálním antivirem se dostane jen k omezené sadě aplikací".

Technické hledisko

Z technického hlediska to rozhodně není jednoduché řešení, z pohledu praktického nasazení však předchozí popis odpovídá realitě. Nyní pár slov o tom, v čem teoreticky může být problém.

Pokud se podíváme na obrázek 1, je zřejmé, že řešení SSL VPN je aplikačně závislé. Toto řešení, na rozdíl od IPSecu, zpřístupňuje aplikace, nikoliv síť. Pozitivum je větší bezpečnost - SSL VPN brána ukončuje spojení a směrem do sítě navazuje nové. Negativem by mohl být fakt, že SSL je v praxi podporováno pro omezenou sadu aplikací typu webový přístup, přenos souborů a mail. Co však SAP, SIEBEL, ORACLE, Citrix a další?

Tyto aplikace musí být podporovány konkrétním SSL VPN řešením, nicméně není potřeba explicitně řešit každou zvlášť. Jedná se o klient–server aplikace a lze je řešit obecně, všechny najednou. Zde je však nutno připustit existenci klientského softwaru na PC. Většinou se nazývá „konektor" a jedná se nejčastěji o javovskou aplikaci, která odchytává komunikaci na síťové vrstvě, „balí" jí do SSL a na druhé straně ji opět transparentně „rozbalí". Ale stále platí, co bylo řečeno – žádná instalace software. Javovská aplikace se dokáže nainstalovat sama na „popud" ze strany SSL VPN brány. Dokáže po sobě dokonce i „uklidit", například včetně vyčištění lokální vyrovnávací paměti cache..



Shrnutí

SSL VPN přináší řadu výhod. Pro správce, kteří již řešili vzdálený přístup do firmy, se řada výše uvedených vlastností může zdát téměř neuvěřitelná.

Na stanice není potřeba instalovat žádný software – jako klient se použije webový prohlížeč. Náklady na údržbu (TCO – Total Cost of Ownership) jsou pak výrazně nižší, nežli je tomu u IPSec VPN.

Jedná se o novou technologii a mezi jednotlivými výrobci je stále velký rozdíl. Zdaleka ne každý dokáže nabídnout všechny výše popsané vlastnosti. Při výběru je potřeba všechny funkce důkladně ověřit, a nejlépe otestovat s ohledem na konkrétní provozované aplikace.

Nejedná se ovšem náhradu IPSec a pro bezpečné propojení sítí, například pobočky s centrálou se SSL VPN nehodí. Pro bezpečný přístup klientů respektive jednotlivých uživatelů však tato technologie v brzké době začne převažovat (viz studie společností Gartner Group, Frost&Sullivan atd.).