

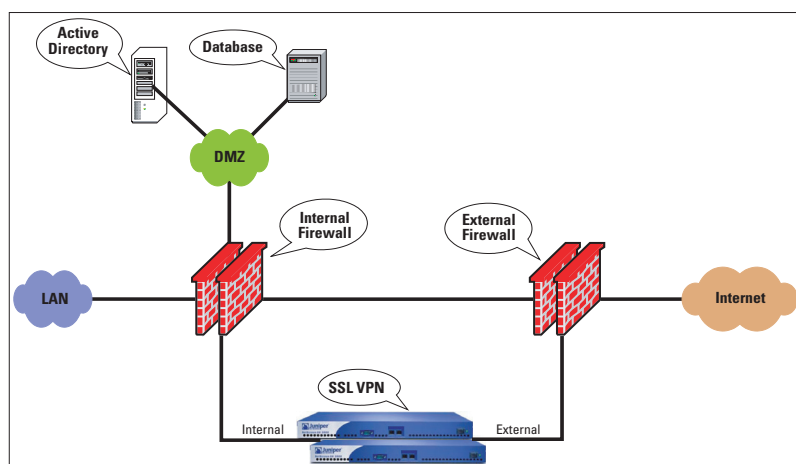
Zaklínadlo jménem SSL VPN

KAREL HENDRYCH, MIREK HOLÝ

Když se před několika málo lety začalo hovořit o SSL VPN, často se vychvalovala možnost přístupu k vnitřním informačním zdrojům organizace z počítačů vybavených pouze webovým prohlížečem s podporou SSL a internetovým připojením.

Tedy v podstatě z jakéhokoliv počítače. Na otázku, zda tomu tak skutečně je, není možné jednoznačně odpovědět. V určitých nasazeních ano. Na druhé straně se mohou vyskytnout očekávání, která ale bez instalace příslušného VPN klienta nelze naplnit. Pak technologie SSL VPN mírně ztrácí své kouzlo.

Cílem SSL VPN je vytvoření co nejtransparentnějšího šifrovaného tunelu, založeného na protokolu SSL. Vzhledem k přítomnosti SSL v běžných webových prohlížečích není nutné pro dosažení většiny nabízené funkčnosti instalovat na klientské počítače žádný speciální klientský software. K rozšíření možností SSL VPN řešení jsou dále používány malé aplikace v podobě Java ap-



Umístění SSL VPN clusteru v demilitarizovaných zónách vnitřního a vnějšího firewallu.

pletů nebo ActiveX prvků. Právě bohatost nadstandardní výbavy významně ovlivňuje užitnou hodnotu implementací SSL VPN od různých výrobců.

Základní funkcionalita SSL VPN spočívá v zabezpečení přístupu k vnitřním informačním zdrojům organizace. Je vytvořen SSL tunel mezi SSL VPN bránou a webovým prohlížečem na klientském počítači. SSL VPN brána se chová obdobně jako reverzní proxy. Požadavek od klienta je bránou přijat, ta jej přepoše na příslušný server, který bráně vrátí odpověď, a ta ji odešle zpět dotazujícímu se klientovi. Komunikace mezi webovým prohlížečem klienta a bránou je zabezpečena silným šifrováním pomocí SSL knihovny.

Úroveň zabezpečení komunikace mezi bránou a interním serverem zůstává nezměněna. V této podobě tedy může SSL VPN velmi dobře posloužit jako implementačně jednoduchý způsob, jak v rámci internetu zabezpečit zpřístupnit webové portály informačních systémů organizace. Další běžnou vlastností SSL VPN řešení je možnost s pomocí brány nabízeného webového rozhraní pracovat se soubory sdílenými v rámci vnitřní sítě pomocí CIFS, tedy sdílení souborů novějších systémů Windows, nebo unixového NFS.

Pomocí Java appletu nebo ActiveX prvku je možné přes SSL VPN „protunelovat“ konkrétní port, podobně jako je to v možnostech unixového Secure Shellu (SSH). Takto lze s SSL VPN provozovat bezpečně klient/server aplikace založené na TCP komunikaci, například lze úspěšně zprovoznit klientskou část informačních systémů organizace. V případě, že existuje také klientský software ve formě Java appletu, je pak možné k příslušnému informačnímu systému organizace skutečně přistupovat z jakéhokoliv počítače s webovým prohlížečem vybaveným SSL a Javou.

S elektronickou poštou lze pracovat prostřednictvím protokolů IMAPS, POPs, SMTPS (písmenko S na konci znamená protokol IMAP, POP, SMTP nabízený přes spojení zabezpečené pomocí SSL), SSL VPN pak zpravidla funguje jako bezpečná proxy, na níž je zakončeno šifrované SSL spojení. Dále může být klient elektronické pošty ve formě vlastního Java appletu, což opět znamená přístup prakticky z jakéhokoliv standardně vybaveného počítače.

Poslední možností je opustit čistotu pouhého webového prohlížeče, byť sem tam „poskvrněnou“ nutností instalované Javy, a nainstalovat plnohodnotného SSL VPN klienta. Tento krok tak smaže hlavní výhodu SSL VPN, zato se ale SSL VPN pak plně vyrovná tradičnímu VPN řešení a umožní obecnou směrovanou IP komunikaci s domovskou sítí.

Autentizace

Implementace SSL VPN od různých výrobců obvykle spolupracují s externími uživatelskými databázemi typu LDAP včetně plné podpory pro Active Directory, což je tradiční Windows NT doména, a s RADIUS servery. To umožňuje hladké začlenění do většiny

existujících infrastruktur. Standardem je rovněž podpora vícefaktorové autentizace, jako jsou třeba RSA SecurID tokeny, pracující na principu jednorázových hesel. Samozřejmostí je u lepších SSL VPN řešení pokračování podpora infrastruktur veřejných klíčů (PKI), kdy je možné jednoduše přiřazovat jednotlivým klientům role na základě atributů jejich klientských certifikátů.

Zvláštní forma nasazení SSL VPN je pak bez použití jakékoliv autentizace. Zařízení potom funguje jako místo, kde je zakončen SSL tunel. Výhody tohoto řešení mohou být v odlehčení koncového webového serveru, tedy v akceleraci SSL, případně i ve využití ověřené a velmi bezpečné SSL knihovny.

Topologie

SSL VPN zařízení bývají vybavena dvěma síťovými rozhraními. První je určeno pro připojení do nedůvěryhodné sítě, druhé do sítě vnitřní. Umísťují se zpravidla do dvou vyhrazených demilitarizovaných zón (DMZ), jedné u vnitřního a druhé u vnějšího firewallu. Možné je i využití jedné DMZ, kdy je aktivní pouze jedno rozhraní SSL VPN. Síťový provoz poté prochází pouze jedním firewallem.

Více SSL VPN zařízení lze spojit do jednoho logického celku za účelem dosažení vysoké dostupnosti, případně vyššího výkonu. Možností je buď horká záloha, nebo rozkládání zátěže mezi dvě a více SSL VPN bran s využitím externího balanceru. V případě poruchy nedochází v obou případech k přerušení klientských relací.

Někteří výrobci nabízejí ve svých implementacích SSL VPN zajímavé možnosti spojené s kontrolou přistupujících počítačů. SSL VPN zařízení na nich smí vyžadovat skupiny vlastností, jako je verze operačního systému nebo stav běžícího osobního firewallu, a dokonce i provádět kontrolu na přítomnost zákeřného softwaru. Na základě získaných poznatků o klientském PC změnit práva přistupujícímu uživateli. To vše je možné velmi detailně konfigurovat.

Vzdálené přistupující klienti, ať již jde o vlastní zaměstnance, obchodní partnery nebo zákazníky, mohou pomocí SSL VPN k vybraným informačním zdrojům organizace přistupovat přes nedůvěryhodné prostředí bezpečně a jednoduše – tedy bez nutnosti instalovat na počítač klientský software a následně ho konfigurovat. Ve většině případů lze tak použít i veřejně dostupná PC v internetových kavárnách nebo knihovnách. Administrátoři se ve většině případů také nemusejí starat o instalaci, konfiguraci a správu VPN klientského software na mobilních počítačích.