

Řízení bezpečností sítě pomocí identit uživatelů

Hlavním rizikem bezpečnosti každé organizace jsou uživatelé. To je známý problém. Potřebujeme-li ale nastavit politiky, získat zpětné údaje o činnosti a nejsme zrovna velká banka s množstvím různých sofistikovaných systémů, máme problém. Jen málo profesionálních bezpečnostních řešení dnes nabízí možnost nastavení politik dle uživatelů či skupin uživatelů, například spoluprací s Active Directory nebo LDAP, nebo prostým zadáním do zařízení.



Potřebu identifikace konkrétního uživatele můžeme ale rozšířit ještě dále, na obsahovou filtraci, schopnost řídit přístupy uživatelů ke zdrojům internetu, přidělování šířky pásma uživatelům či skupinám uživatelů včetně zohlednění jednotlivých aplikací. Doplníme i navazujícím monitoringem a reportingem, vždy máme jasnou představu o konkrétním uživateli a skupině, do které patří. Než začneme využívat všech těchto funkcionalit, máme možnost definice pravidel na síťových prvcích tak, aby vycházela z potřeb konkrétních uživatelů nebo jejich skupin. Je až s podivem, jak málo doposud tradiční firewally toto umožňovaly...

Přitom zejména v menších organizacích (obvykle bez jasně daných bezpečnostních

pravidel) by striktní uplatnění politiky, jen dle identity uživatele a možnost doplnění žurnálů taktéž o identitu uživatelů, ušetřilo administrátorovi spoustu času! Ruku na srdce, ve firmách do 100 uživatelů je situace často taková, že administrátor nemá na pravidelné režijní činnosti ani 20 minut denně!

Nabízí se ale řešení UTM firewall Cyberoam, které společnost Gartner vyzdvihla právě pro jeho spojení s Identitami uživatelů. Stručně si tedy řekneme, jak vlastně v praxi funguje ona identifikace uživatelů. Firewall Cyberoam umí ověřovat identitu uživatelů proti Microsoft Active Directory serveru (i starší NT4), pomocí LDAP protokolu, pomocí Radius protokolu, nebo definovat účty uživatelů a skupiny přímo na firewallu (nebo lze účty z MS AD vyexportovat a naimportovat na Cyberoam). Ověření příslušnosti do skupiny se provádí LDAP protokolem.

Z pohledu nasazení má správce možnost nejprve definovat tzv. clientless uživatele, tj. účty pro zařízení, která se identifikovat nemohou, ale pro která by také rád využil možnost definice pravidel per identita (Internet Access policy, Bandwith Policy). Typicky jsou to servery, síťové tiskárny atp. Lze definovat jejich pevnou IP adresu, nebo rozsahem adres. Pro stolní počítače je nevhodnější použít v prostředí Active Directory spojení SSO mechanismu s využitím logon scriptu. Pro mobilní počítače využívající jak vestavěnou SSL VPN, tak klasickou IPSec VPN je nevhodnější agent (k dispozici i pro Linux) běžící na Windows v systémové liště. Zprostředkovává přihlášení uživatele k Cyberoam, který pak provede ověření proti autentizačnímu serveru (AD, Radius, LDAP) či lokální databázi.

Zařízení samotné je založeno na linuxovém jádře a stavovém firewallu doplněném o transparentní proxy bránu, které se používají pro obsahovou filtraci (kategorizovaná URL filtrace), antispam a antivirovou kontrolu.

Kromě samotných proxy bran je na zařízení rovněž IPS s periodicky aktualizovanými signaturami, dodávanými výrobcem (IDP modul). Pro každé ACL pravidlo lze připravit konkrétní nastavení chování IPS, aby se detekovaly jen vzorky provozu, který opravdu může daným pravidlem procházet, a snížila se jak zátěž zařízení, tak i případné false-positive události. Pomocí IDP modulu lze detekovat i IM a P2P aplikace (ICQ, Skype...), rovněž s aktualizacemi od výrobce.

Pro každé ACL pravidlo nebo každou skupinu uživatelů i jednotlivce lze předem připravit tzv. „Internet Access Policy“, která sdružuje do jednoho profilu nastavení URL filtrace, omezení dle typu souborů, omezení dle detekovaného typu aplikace, atp. Obdobně lze pro skupinu uživatelů i jednotlivce definovat politiku pro využití šířky pásma (tzv. Bandwith Policy) a politiku vymežující maximální objemy stahovaných a odesílaných dat (tzv. Data Transfer Policy).

Na závěr nezbyvá než konstatovat, že společnost Cyberoam, která je na trzích v ČR, SR a Ukrajině zastoupená společností COMGUARD, myslí na každého zákazníka. K dispozici jsou modely CR15i začínající s cenou na úrovni 15 000 korun až po vysoce výkonné modely 2U modely CR1500i s propustností 6 Gbps.