

MCAFFEE ENTERPRISE FIREWALL

McAfee představilo zcela nový firewall

Heslem nové generace hardwarového firewallu od společnosti McAfee je řízení bezpečnosti organizace podle „business“ potřeb pod heslem: **Identity, aplikace, řízení a vizualizace**. Nová verze přináší velké množství novinek zaměřených na schopnost identifikace aplikací a provázání pravidel s identitou uživatelů včetně zjednodušení a zrychlení správy celého řešení.

Pod pojmem „Discover“ přináší technologii AppPrism identifikující použitý aplikační protokol podle předdefinované aplikační signatury pro více než 1 000 denně aktualizovaných aplikací. Detekce aplikačního protokolu nám přináší další, dříve nemyslitelné možnosti. Jako příklad můžeme zmínit často používaný a pro svou komplexnost a rozšířenost často i zneužívaný program Skype. Díky znalosti aplikačního protokolu je firewall schopen nejen Skype zakázat, i když je webový provoz v organizaci povolen, ale umí Skype i povolit a v rámci tohoto protokolu zakázat potenciálně zneužitelné funkce, jako je sdílení souborů a P2P provoz (čímž se vaše PC nestane tzv. supernodem). Umožňuje také případně kompletně zablokovat VoIP provoz. Navíc, pokud takto definujeme jediné pravidlo, povolení Skype znamená, že z webového provozu bude fungovat jen Skype a nic jiného. To je poměrně dokonalá ochrana. Detailní znalost aplikačního protokolu je v době hrozeb spojených např. s komplexním WEB 2.0 protokolem jednoduše nutností. Pro definici firewallového pravidla již nemusíte znát cílový port, IP adresu nebo použitý L4 protokol, postačuje pouze jméno aplikace.

Novinkou, přicházející s další generací McAfee Enterprise Firewallu (Sidewinder v8), je možnost svázání pravidel s identitou uživatele získanou po úspěšné autentizaci oproti MS Active Directory serveru, umožňující nadefinovat pravidla dle konkrétních „business“ požadavků a jednoduše napařovat, které služby je uživatel oprávněný využívat.

K tomuto účelu byl vyvinut Logon Collector zajišťující automatizované přebírání dat z MS Active Directory a umožňující uživatelům přístup k externím službám bez dodatečné autentizace.

Šifrovaný provoz není problém

Stálou hrozbou z hlediska šíření malware je pro mnoho firewallů šifrovaný provoz. Převážná většina aktuálních hrozeb je založena na využití šifrovaného kanálu, a to především z důvodu neschopnosti mnoha bezpečnostních zařízení si s tímto provozem poradit.

McAfee přichází s široce nastavitelnou obousměrnou SSL/TLS dešifrací, po které již není problém provést obsahovou kontrolu. Firewall funguje na principu man-in-the-middle, kdy je šifrované spojení terminováno na firewallu, provedena kontrola certifikátů a po analýze provozu následuje vytvoření nového SSL/TLS spojení (tj. opětovně zašifrováno). Nově můžeme pro různá spojení využívat různé SSL certifikáty, a to jak mezi klientem a firewallem, tak i mezi firewallem a serverem s možností detailní konfigurace nastavení jednotlivých SSL/TLS relací. Je podporován nejenom protokol HTTPS, ale též i další protokoly využívající SSL/TLS, jako jsou např. SFTP, SSH nebo SCP. Nyní není pro nás hrozbou SSH provoz na klíčové systémy od správců z externích organizací. Můžeme kontrolovat, zda se netuneluje žádný jiný než povolený provoz (včetně příkazů), navázat IPS kontroly i AV pravidla.

Každý správce firewallu se jistě již dostal do situace, kdy potřebuje rychle a jednoduše zjistit příčinu problému v síti, zda a proč konkrétnímu uživateli nefunguje specifická služba. Zjištění příčiny je často práce s ne-

jistým výsledkem trvající i hodiny! McAfee si je této skutečnosti vědom a současně s novou generací Enterprise Firewallu vyvinul aplikaci s názvem Firewall Profiler poskytující v reálném čase unikátní náhled na změny chování v síti, a to včetně zachování historie.

Propojením aplikační discovery s uživatelskými identitami, aktuálním nastavením firewallu a veškerým provozem procházejícím firewallem umožňuje jednoduše zjistit pomocí bublinových grafů (detaily jsou k dispozici také), jaké změny v rámci porovnávaných období v provozu nastaly. Lehce zjistíme, že po updatu serveru v DMZ již neexistuje žádný provoz na tento server od oddělení HR, i když před týdnem byl... Zjistíme také, že po změně pravidla na externím interface 4 firewallu je zvýšený provoz, který zde v minulosti nebyl apod.

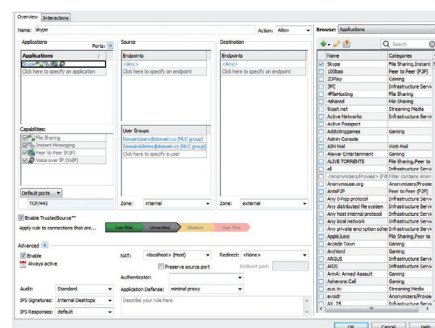
Reputační systém

Standardní součástí řešení je již dlouhou řadu let využití globálního reputačního systému TrustedSource, kdy reputace lze provázat na definici každého jednotlivého pravidla, a to včetně Geo-location (kam nebo odkud provoz směřuje a zda je to žádoucí).

Pro detailní filtraci URL na základě kategorií je možné využít integrovanou databázi Smartfilter. Denně aktualizovaná databáze obsahuje více než 35 mil. stránek rozdělených do více než 90 kategorií! Využitím Smartfilteru lze jednoduše odfiltrovat stránky s nevhodným, případně škodlivým obsahem, ale též i zvýšit efektivitu práce zaměstnanců a výrazně snížit využívané přenosové pásmo. URL filtraci je možné nakonfigurovat s využitím technologie SafeSearch Enforcer pro filtraci výsledků vyhledávání z hlediska nevhodného obsahu.

Samozřejmostí každého firewallu je integrovaný IPS, v případě McAfee firewallu s možností hardwarového urychlení specializovanou ASIC kartou a Antivirus zajišťující ochranu, umožňující kontrolu jak webového, mailového, tak i ftp provozu.

Koupi zařízení získá zákazník nejenom komplexní ochranu sítě zajišťující dlouhodobou investici do firemní bezpečnosti, ale též i možnost bezplatného využití centralizovaných řešení pro sběr, vyhodnocování a reporting auditovacích záznamů Firewall Reporter, případně Web Reporter pro analýzu a reporting využití webových služeb. □



Konfigurace pravidel pro využití programu Skype v síti.