

Nový firewall od McAfee

PETR HERMAN

Společnost McAfee před nedávnem představila novou generaci enterprise firewallů vycházející ze známého a díky své nepromítnutelnosti světově uznávaného firewallu Sidewinder. Firewall dostal označení McAfee Enterprise Firewall v8 a na trhu by se měl objevit koncem tohoto roku. Již nyní si však můžeme představit novinky, se kterými bude přicházet.

Nová generace McAfee firewallu si vzala za cíl především zjednodušení a zrychlení správy celého řešení s ohledem na obchodní zájmy firem. Nabízí možnost svázat konkrétní identitu uživatele s využívanou aplikací nebo aplikačním protokolem, případně pro definici pravidel využít již předdefinované skupiny aplikací s nastaveným rizikem spojeným s jejich použitím.

Technologie „AppPrism“ pro identifikaci použitého aplikačního protokolu využívá pro detekci integrovanou databázi aplikačních signatur. Pro definici firewallového pravidla již tedy nemusíme znát cílový port, IP adresy nebo použitý transportní protokol, ale postačuje znát pouze jméno aplikace.

Využitím aplikačních signatur došlo k výraznému posunu v možnostech nastavení a využití firewallu, kdy signatury neslouží pouze k detekci použitého aplikačního protokolu, ale detailně znají jeho funkční použití a umí tyto specifické funkce filtrovat.

Databáze aplikačních signatur nyní obsahuje více než 1 000 denně aktualizovaných aplikačních signatur a podle vyjádření výrobce jich můžeme při zahájení prodeje očekávat okolo 1 500.

Novinkou z pohledu autentizačních možností firewallu je vývoj Logon Collectoru pro automatizované přebírání dat MS Active Directory serveru, umožňující přihlášeným uživatelům přístup k externím službám bez dodatečné autentizace.

Odhalený šifrovaný provoz

Pro mnohé firewally je šifrovaný provoz neustálou hrozbou z pohledu šíření malwaru. Převážná většina aktuálních hrozeb je totiž založena na využití šifrovaného kanálu, a to především z důvodu neschopnosti mnoha bezpečnostních zařízení si s tímto provozem poradit. Společnost McAfee však našla cestu v široce nastavitelné obousměrné SSL/TLS dešifraci, 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. 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. SSH provoz na klíčové systémy od externích pracovníků už není pro společnost žádnou hrozbou. Společnost může kontrolovat, zda se netuneluje žádný jiný než povolený provoz, provádět kontrolu použitých příkazů, navázat na IPS kontroly i AV pravidla.



Rodina firewallů McAfee

Pokročilá správa

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 nejistým výsledkem, trvající i hodiny! McAfee tento problém vyřešil vyvinutím aplikace s názvem Firewall Profiler, která je součástí právě nové generace enterprise firewallů. Tato aplikace umožňuje vidět 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, jaké změny v rámci porovnávaných období v provozu nastaly.

Lehce zjistíme, že po aplikování bezpečnostních záplat na náš web server již neexistuje žádný provoz spojený s tímto serverem od HR oddělení, i když před týdnem zde byl, zjistíme, že po změně pravidla je na externím portu zvýšený provoz, který zde v minulosti nebyl apod.

Další funkce

Standardní součástí řešení je již dlouhou řadu let využití globálního reputačního systému TrustedSource, monitorujícího chování jednotlivých IP adres v rámci internetu a automaticky generujícího míru rizika spojenou s jejich využitím. V kombinaci se systémem Geo-location a navázáním na konkrétní firewallové pravidlo mohou organizace omezit veškerá spojení na spojení s dobrou reputací, pocházející z požadované oblasti, a tím výrazně zvýšit ochranu proti možným hrozbám.

Výrazného snížení potřebného přenosového pásma internetové konektivity a zvýšení efektivity práce zaměstnanců lze dosáhnout pomocí detailní URL filtrace na základě kategorií, kdy se využívá integrovaná databáze SmartFilter. Denně aktualizovaná databáze, obsahující více než 35 mil. stránek rozdělených do více než 90 kategorií, zaručí jednoduché odfiltrování stránek s nevhodným, případně i se škodlivým obsahem. 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, případně kartou pro urychlení SSL provozu. Antivirus zajišťuje antivirovou ochranu a umožňuje jak kontrolu webového, mailového, tak i ftp provozu.

Nákupem zařízení získá společnost nejenom komplexní ochranu sítí zajišťující dlouhodobou investici do firemní bezpečnosti, ale také pokročilý reportovací nástroj, jako možnost bezplatného využití centralizovaných řešení pro sběr, vyhodnocování a reporting auditovacích záznamů Firewall Reporter, případně Web Reporter pro analýzu a reporting využívání webových služeb.

Autor pracuje jako IT Security Consultant ve společnosti Comguard. Technologickým partnerem tohoto příspěvku je společnost Comguard.