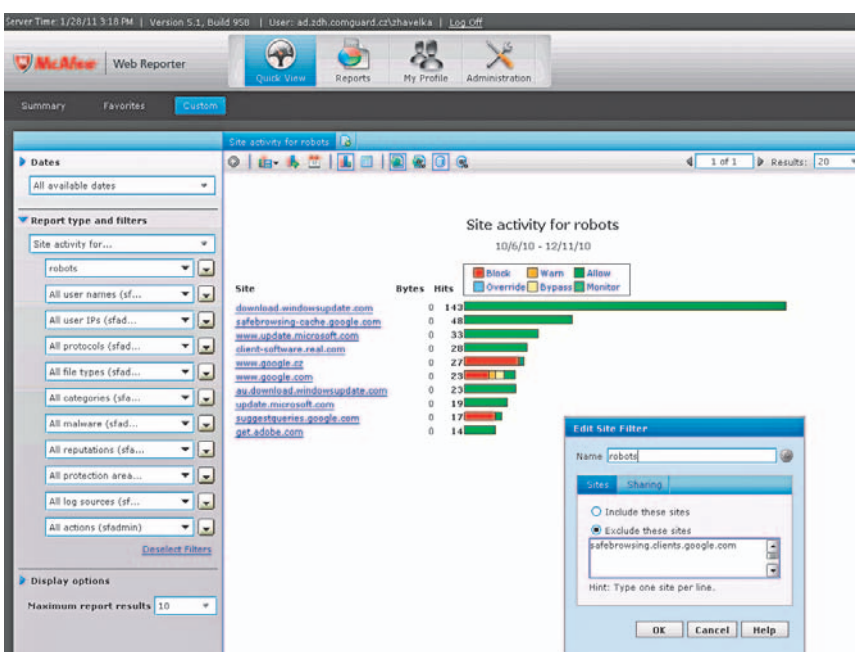


Webová gateway

s flexibilními možnostmi konfigurace

Petr Herman

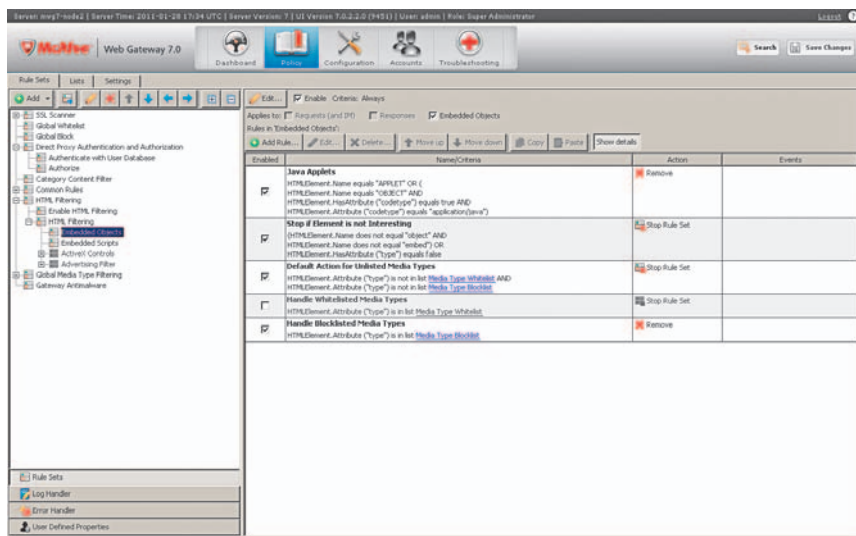
Současný internet přináší uživatelům nové možnosti v podobě dynamicky tvořených stránek a interaktivních aplikací, jejichž složitost umožňuje tvorbu nevídaného množství hrozeb. Pro jejich analýzu již není možné použít standardní bezpečnostní mechanismy, které byly dostačující v minulých letech. Je nutné uplatnit především analýzu na základě chování a globální cloudy pro detekci malwaru.



V loňském roce uvedla společnost McAfee na trh produktovou novinku v portfoliu bezpečnostních proxy bran pro filtraci webového provozu, McAfee Web Gateway 7 (MWG7), která výše uvedené funkce nabízí. Zařízení navazuje na úspěšnou řadu bezpečnostních proxy známých pod dřívějším názvem Webwasher. Verze 7 však byla kompletně přepracována především s ohledem na maximální flexibilitu konfigurace a korporátní použitelnost, případně použitelnost v sítích poskytovatelů internetových služeb.

Z hlediska bezpečnosti reaguje společnost McAfee především na hrozby spojené s využitím Web 2.0 aplikací, a to na několika úrovních. V době neustále se měnících hrozeb již není možné spoléhat se pouze na virovou detekci založenou na signaturách, ale je nutné využívat komplexnější přístup. Specializovaný antimalware engine pro webové brány přináší nejen stále nezbytnou kontrolu na základě virových signatur jednoznačně

odhalující známé hrozby, ale především kontrolu chování tzv. mobilního kódu.



Mobilním kódem McAfee označuje různé webové aplikace založené například na ActiveX, JavaScriptu, Flash a dalších, u kterých je antimalware engine schopen detekovat nežádoucí chování a určit, zda se jedná o Rootkit, Keylogger, Backdoor, případně jiné nežádoucí hrozby. Dokáže také odhalit podezřele vypadající funkce, například JavaScriptu, a tyto funkce z webového provozu odfiltrovat.

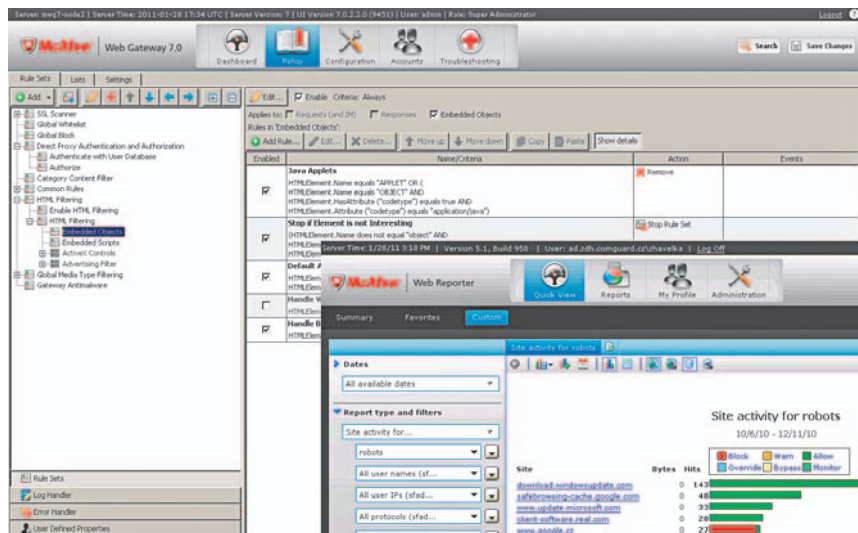
Obecným problémem všech antivirových engineů je časové okno, které vznikne mezi objevením nového viru, vydáním a stáhnutím aktualizované virové databáze. U McAfee je tento problém vyřešen systémem Artemis, který v reálném čase dotazuje internetovou databázi McAfee a zjišťuje, zda kontrolovaný soubor již nebyl uživateli reportován jako podezřelý, a v případě, že ano, je takový soubor blokován. Zkušený čtenář by mohl namítnout, že aplikací této kontroly bude docházet ke generování velkého množství false positives. Ano, byla by to jistě pravda. McAfee však využívá systém globálních whitelistů, díky kterému je toto chování prakticky vyloučeno.

Jednou z nejvíce využívaných funkcí proxy bran je URL filtrace, oblíbená především podniky pro zvýšení efektivity práce zaměstnanců a blokování přístupu k nevhodnému, případně nebezpečnému obsahu. McAfee Web Gateway využívá k tomuto účelu systém TrustedSource aktuálně udržující databázi sto milionů kategorizovaných URL s rozšířením o reputační kontrolu a geolokační systém.

V databázi se jistě nenacházejí všechna internetová URL. Pokud tedy data z lokální databáze nejsou dostatečná, přichází ke slovu dodatečná automatická dokategorizace na základě klíčových slov v URL, vnořených odkazů, případně dotaz v reálném čase do internetové databáze TrustedSource, ve které se mohou nacházet informace, které web gateway nemá aktuálně k dispozici.

Častým zdrojem šíření malware a problémů se ztrátou firemních dat se v posledních letech staly různé „instant messaging“ služby. McAfee se proto rozhodla implementovat do MWG7 IM proxy brány nabízející nad těmito specifickými datovými toky stejné funkce jako nad webovým provozem. Již není problém provádět antivirovou kontrolu nad zasílanými přílohami, kontrolovat, kdo s kým komunikuje, případně provádět základní DLP analýzu.

Především v korporátních sítích uvítají uživatelé streaming proxy pro zpracování multimediálního obsahu. McAfee se rozhodl pro využití Helix proxy od společnosti Real Networks umožňující zákazníkům snížení nutné přenosové ka-



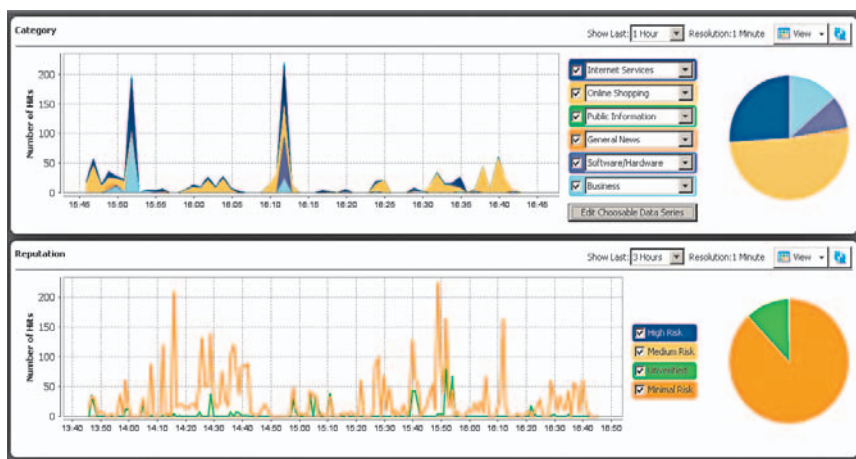
Uživatel již nemůže bezmyšlenkovitě přijímat podvržené, expirované, samopodepsané, případně jiné problémové certifikáty.

Tradiční proxy cache byla v MWG7 přepracována s ohledem na maximální bezpečnost a efektivitu. K jednotlivým objektům je zde přidán

případně jako prvek spolupracující s produkty společnosti Cisco pomocí protokolu WCCP. Zákazníci hledající transparentní proxy si mohou vybrat ze dvou režimů, kdy se proxy může chovat jako router a směřovat provoz, nebo být v bridge módu a z pohledu sítě plně transparentní.

Ve všech těchto režimech je podporována možnost zajištění plně redundance pomocí clusterů, kdy lze výkonnost jednoduše navyšovat přidáváním dalších zařízení v režimu skenovacích nodů. O distribuci konfigurace mezi jednotlivými zařízeními se stará propracovaný centrální management, kdy již nemusíme mít na všech zařízeních identickou konfiguraci, ale je možné specifikovat různé skupiny zařízení vzájemně sdílející svoje nastavení s možností určení způsobu aktualizace antimalwaru a kategorizačního enginu, čímž můžeme výrazně ušetřit přenosové kapacity internetových linek.

Pokud tedy hledáte komplexní bezpečnostní bránu pro filtraci HTTP/S provozu reagující na aktuální hrozby, můžete si být jisti, že toto zařízení splní veškerá vaše očekávání. Zákazníci využívající více produktů společnosti McAfee také jistě ocení integraci do systému centrální správy ePolicy Orchestrator. ■



pacitě ukládáním obsahu do cache, případně distribuci obsahu z jednoho zdroje více uživatelům. Pro zajištění garantované a maximální šířky pásma multimediálních toků umožňuje proxy nastavení limitů. Pro zvýšení bezpečnosti je též implementována autentizace.

Slepým místem při filtraci webového provozu je pro velké množství zařízení SSL provoz. Možnosti pro zneužití takto šifrovaného toku jsou obrovské, a proto není možné je nechat bez povšimnutí. McAfee nabízí již řadu let možnost HTTPS dešifrace s následnou šifrací, díky které je možné využít veškeré funkční možnosti zařízení pro skenování HTTP provozu včetně antimalwarové kontroly. Neméně důležitou funkcí je kontrola SSL certifikátů, kdy již uživateli nemusí být dovoleno přijímat data ze serverů, které nelze ověřit, případně jejichž certifikát nesplňuje požadovaná kritéria.

údaj, jaká verze AV enginu byla pro jejich kontrolu použita, a v případě aktualizace AV dojde pouze k opětovnému proskenování starých dat, aniž by objekt v cache musel být znovu stahován. Při načítání dat z cache mohou být tedy uplatněny pouze rychlé proaktivní filtry se zjištěním aktuální reputační úrovně, čímž se výkonnost zařízení výrazně zvyšuje. Samozřejmostí webových proxy serverů jsou široké možnosti autentizace, kdy MWG7 nabízí nově mimo standardních metod, jako jsou NTLM, LDAP nebo Radius, podporu Kerberosu verze 5. Zákazníci požadující využití transparentní proxy mohou využít integrovaný autentizační server.

Z hlediska implementace v sítích zákazníků je možné MWG7 nasadit klasicky jako běžnou netransparentní proxy. Pro využití obsahové kontroly proxy serverů jiných výrobců může běžet v režimu samostatného ICAP serveru,

Autor působí jako IT security consultant společnosti COMGUARD a.s.