No pasarán aneb Štábní kultura od Keria

Kerio WinRoute Firewall 5.0 (dále jen KWF) firmy Kerio Technologies vychází z osvědčeného WinRoute Pro 4.x. (WRP). První ostrá verze KWF 5.0 byla zpřístupněna koncem února, zatím jen pro OS Windows. Partnerská aplikace Kerio MailServer existuje i ve verzích pro Linux a Mac OS X. K dispozici je však speciální verze s integrovaným antivirem McAfee.

V nástupci WRP se tvůrci rozhodli vyčlenit služby poštovního serveru do produktu s názvem Kerio MailServer (KMS), jenž má mnohem větší rozsah funkcí než poštovní služba původního WRP, a v KWF ponechat všechny zbývající služby předchůdce, které ovšem dále rozšířili o mnoho dalších. Původní produkt s novým názvem Kerio WinRoute Pro 4.2 je nadále nabízen těm firmám, jimž jeho možnosti plně vyhovují. Pro větší či náročnější společnosti je tu kombinace KWF a KMS.

Instalace

Instalace pomocí průvodce je jednoduchá. Pokud provádíme upgrade, je prvním krokem výzva k ukončení WRP. Instalační program detekuje kolizní software (např. sdílení internetového připojení Windows), který je třeba vypnout. Po odsouhlasení licence a cesty pro uložení souborů následuje výběr mezi typickou nebo kompaktní instalací. Volbu Custom využijeme při instalování administrační konzoly a plug-inu do ní na počítač administrátora, tj tam, kde WinRoute engine nepotřebujeme.

Je-li detekována starší verze, nabídne průvodce import nastavení z WRP a jeho odinstalaci. Původní konfigurace WRP se uchová, takže se později můžeme jednoduše vrátit k původnímu WRP. Provádíme-li import staré konfigurace, uvidíme v průvodci také výsledek importu (report - kolik bylo importováno uživatelů a skupin, výsledek importu konfigurace DNS, DHCP, proxy serveru, HTTP cache, skupin IP adres, časových intervalů, definic URL atd.). Na uživateli pak záleží, chce-li po odinstalaci smazat logy staré aplikace. Po dokončení instalace následuje restart serveru. Můžeme se také rozhodnout neimportovat a začít "od čistého stolu".

Po instalaci se v oblasti systray usídlí ikona umožňující spuštění a zastavení služby KWF, nastavení automatického spuštění služby a monitoru služby a v neposlední řadě také ukončení samotného monitoru a spuštění administrace.

Konzola

Nyní můžeme spustit administrační konzolu a konfigurovat pro nás potřebné služby. Grafika administrační konzoly je proti WRP zcela přepracovaná. Je založena na knihovně Qt a je společná i pro další produkty firmy Kerio Technologies. Pro pohodlnou práci je třeba rozlišení alespoň 1024 x 768. Nižší nestačí, protože některé panely jsou příliš široké a neustálé posouvání horizontální lištou zdržuje.

V konzole s výhodou použijeme záložky, do nichž uložíme nastavení připojení jednotlivých aplikací, třeba i včetně přístupových hesel. Přístup k záložkám je chráněn zvláštním heslem (passphrase). Místo ručního zadávání údajů (jména či IP adresy serveru, jména a hesla oprávněného uživatele) zvolíme konkrétní připojení z menu nebo z nástrojové lišty myší. V pruhu nástrojů konzoly jsou jen tlačítka pro odpojení a připojení a případné záložky.

V otevřeném administračním okně vidíme v levém sloupci strom položek, vpravo jednotlivé volby. Vpravo dole lze tlačítkem potvrdit nově zadané údaje nebo je stornovat. Nad volbami ve tvaru tabulek lze přes pravé tlačítko myši nastavit, které informace (sloupce) chcete či nechcete zobrazovat, a lze i měnit jejich pořadí. Komunikace s KWF je šifrovaná a běží na stejném portu jako u WRP (44333).

Konfigurace

Nemáme-li importovánu konfiguraci z WRP, nabídne se při prvním spuštění konzoly průvodce konfigurací (můžeme jej samozřejmě inicializovat i později). Dokončení práce s průvodcem má za následek přepis původní konfigurace!

V průvodci vybíráme, zda máme internetové připojení přímé (Ethernet, DSL, KTV), nebo vytáčené (dial-up, ISDN), a v dalším kroku zadáváme, které vytáčené připojení k internetu se má používat, resp. která síťová karta vede do internetu. Dále definujeme, které služby internetu chceme uživatelům zpřístupnit a které servery ve vnitřní síti a služby na nich běžící mají být naopak dostupné z internetu.

Nakonec povolíme NAT (překlad síťových adres) a aktivujeme svou konfiguraci firewallu. Stejné kroky má i průvodce v rámci instalace produktu.

Pravidla můžeme následně (ale i hned od počátku) upravovat ručně. Nejlepší však je nejprve přejmenovat jednotlivá rozhraní na LAN a Internet (příp. DMZ) - zlepšuje to přehlednost v nastavení komunikačních pravidel. U malých firem, které mají všechny služby nebo většinu služeb na jednom serveru, je výhodné vyčlenit rozhraní lokální sítě (LAN) z dohledu firewallu. Umožňuje to vyšší výkon souborového nebo databázového serveru, na němž je KWF instalován. Konfigurace funkcí paketového filtru, NAT a mapovaných portů byla sloučena do jediné tabulky nastavení s názvem Komunikační pravidla. Každé pravidlo lze dočasně deaktivovat a pro přehlednost zvolit barvu pozadí každého řádku.

Při ručním zadávání volíme stručný název pravidla, zdroj a cíl paketu, typ služby nebo protokol a rozsah portů. Službu vybíráme z rozsáhlého seznamu sahajícího od ICMP přes například MS-SQL a PC Anywhere až po VNC nebo WINS, a nic nám nebrání definovat si službu vlastní. Pakety vyhovující tomuto pravidlu můžeme povolit, zakázat nebo zahodit. Dále je k dispozici záznam paketů anebo odpovídajících spojení a také překlad na jiný cíl a port. Nakonec pro pravidlo můžeme vymyslet vlastní delší popis. Jako zdroj či cíl můžeme vybrat počítač (jednu IP adresu), rozsah IP adres, definovanou skupinu adres, síť s maskou a všechny sítě připojené k danému rozhraní. Zvláštní skupinou zdrojových paketů a jejich cílů jsou Firewall a Libovolný.

Zdrojem však mohou být i vybraní uživatelé nebo skupiny - omezíme tak přístup ke službám internetu nepřihlášeným uživatelům, musíme však pro ně mít omezující pravidlo. U služby HTTP jsou nepřihlášení automaticky přesměrováni na přihlašovací stránku. U jiných protokolů (např. FTP) musí uživatel nejprve pomocí WWW prohlížeče jít na přihlašovací stránku a tam se autentizovat. S IE 5.0 a vyšším lze v doméně provést přihlašování na pozadí protokolem NTLM (NTLanMan).

Funkce

Pěkná je funkce převedení DNS jména počítače na jeho IP adresu. Lze ji využít u definice zdroje a cíle paketů, ne u cílového počítače pro mapování portů. Pravidla se procházejí shora dolů a na konci všech pravidel je vždy tzv. implicitní pravidlo, které zakazuje veškerou komunikaci a které nelze zrušit. Zde je možné pakety jen zakázat nebo zahodit a případně logovat.

Nejdůležitější funkcí KWF je filtrování obsahu. Celá strategie je založena na neanonymním přístupu ke službám internetu. U přihlášených uživatelů se do logu zapisuje jejich jméno a IP adresa, u ostatních jen IP adresa. Zápis jména PC, jak tomu bylo u WRP, již není možný.

Pravidla obsahu HTTP umožňují zakázat všem nebo jen určitým uživatelům přístup ke konkrétním stránkám na základě jejich URL. Oproti WRP však pravidlo v KWF může platit i jen v určitém čase (po pracovní době povoleno) a jen pro konkrétní MIME typ objektu (třeba jen pro obrázky). Správce může definovat text zákazu zobrazující se místo požadované stránky a kromě globálního omezení je možné pro každé jednotlivé URL definovat zakázané HTML objekty jako ActiveX, Java applety apod. V pravidlech je možné využít předdefinovaných skupin URL (reklamy a bannery) a vytvářet vlastní. Při zakoupení licence na integrovaného klienta obsahového filtru Cobion, jehož databáze obsahuje několik miliard internetových stránek, můžeme omezit přístup uživatelů ke stránkám s nevhodným obsahem (pornografie, warez apod.). Pokud je odpověď systému Cobion kladná, je uživateli přístup na danou stránku odepřen. Určití uživatelé mohou mít povoleno některé zákazy odemknout. Odemknutí bude zaznamenáno do logu Security, platí jen 10 minut a jeden uživatel může odemknout maximálně 10 zákazů najednou. V neposlední řadě umožňuje KWF zamezit přístup na WWW stránky na základě zakázaných slov. V seznamu má každé tzv. zakázané slovo přiřazenu hodnotu a při překročení limitu počtu zakázaných slov na stránce je tato stránka nepřístupná. Správce může limit měnit a seznam libovolně upravovat.

Další inovací je transparentní proxy. V prohlížeči uživatelů není nutno definovat žádnou proxy, přesto je veškerá komunikace kontrolována a zaznamenána. Přes DHCP server KWF lze provádět automatickou konfiguraci "browserů". Obsažen je i klasický proxy server, který ovšem nepodporuje protokol FTP. Pro tento protokol, pokud není definován nadřízený proxy server (jenž FTP proxy umí), je možné použít jen transparentní proxy. Velikost společné cache obou proxy může být až 8 GB (pokud to souborový systém dovolí).

V části Pravidla FTP jsou předdefinována pravidla pro zákaz stahování hudebních souborů formátu MP3, zákaz stahování videa (AVI) a zákaz uploadu pro zabránění úniku dat z firmy. Implicitně je však zapnuto jen pravidlo zakazující pokračování ve stahování FTP po jeho přerušení (REST) kvůli antivirové kontrole. Inspekční modul pro tento protokol umožňuje používat FTP v aktivním modu. Správce není nikterak omezen v definici vlastních pravidel. Může omezit přístup na konkrétní FTP servery nebo zakázat libovolnou skupinu FTP příkazů. Může též omezit pravidlo v čase, na konkrétní uživatele a jména přenášených souborů (např. *.EXE).

Další význačnou novinkou je antivirová kontrola, která se provádí nad protokoly HTTP a FTP. Kromě verze produktu s integrovaným antivirem McAfee si můžeme vybrat mezi produkty šesti jiných firem - od

Grisoftu po Symantec. Standardně se kontrolují spustitelné soubory, archivy, applety, dokumenty MS Office, soubory VBS a soubory MIME typu "application/*".

KWF poskytuje také služby DNS forwarderu a nového, plnohodnotného DHCP serveru, umožňujícího přidělovat adresy i klientům BOOTP a RAS. Klientům DHCP umí kromě IP adres předávat další konfigurační parametry. KWF podporuje i protokoly H.323, SIP a SCCP (vše VoIP), IPsec a UPnP. Dalším méně důležitým vylepšením je zanořování skupin IP adres do sebe (firma = lokální síť centrály + pobočky).

U vytáčení na žádost lze definovat, na které URL požadavky se má spojení vytvořit a které požadavky se mají ignorovat. Dial-up se konfiguruje (kdy vytočit, kdy držet, zavěsit, zda připojení trvale držet) v definici rozhraní. Směrovací tabulka nám umožňuje zkontrolovat hodnoty v systému a definovat vlastní statické cesty. Konfiguraci antispoofingu získává KWF z routovacích tabulek a již není nutno jako u WRP explicitně určovat, jaké adresy se na daném rozhraní smějí vyskytovat.

Uživatele lze zadávat ručně a importovat z NT domény nebo z Active Directory. Jednotlivé uživatele integrujeme do skupin, abychom mohli přidělovat práva celým skupinám uživatelů. U každého uživatele jednotlivě lze nastavit, jaké objekty jsou pro něj v HTTP povoleny (ActiveX, pop-up windows atp.), a práva k administraci, k vytvoření komutovaného spojení a k odemykání pravidel pro URL.

Pod položkou Sledování stavu lze prohlédnout grafy vytížení jednotlivých rozhraní v následujících časových periodách: poslední 2 hodiny, 12 hodin, 1 den a 30 dní (chybí období 7 a 14 dní). Sledovat můžeme i to, kteří uživatelé a jak dlouho jsou přihlášení a kolik přenesli dat, také lze sledovat a "zabít" (násilně ukončit) některá z aktuálních spojení. Odchozí, lokální a příchozí spojení jsou odlišena barvou pozadí, barva písma indikuje aktivní a neaktivní spojení.

V záznamech můžeme sledovat zápisy změn konfigurace (včetně autora změny), jednotlivá spojení, ladicí výpisy, vytáčení, chyby, zápisy paketového filtru, HTTP požadavky, antispoofing, varovná hlášení a logování přístupu k WWW stránkám.

Během redakčního zpracování článku dokončili pracovníci firmy Kerio Technologies další upgrade systému na nyní aktuální verzi 5.0.5.

Ve verzi 5.0.5 se vývojáři rozhodli zrušit funkčnost volby "Nesledovat komunikaci s firewallem na tomto rozhraní". Ta je nadále přístupná, ale nemá vliv na chod firewallu. Produkt je standardně dodáván v elektronické verzi - uživatel dostane na papíře jen licenční kartu a vlastní produkt i manuály získá stažením z internetu, kde jej i registruje. Krabicová verze s instalačním CD a tištěným manuálem je k dispozici za příplatek.

Připomínky

Nevíce mi chybí antivirová kontrola protokolů POP3 i NNTP (NEWS) a dalších. Pro SMTP mě už tolik netrápí, máme KMS a ten má vlastní antivirovou kontrolu pošty. Zkušení uživatelé si však chtějí číst poštu i z jiných, externích serverů. Správce se může buď spoléhat na zapnutou a aktuální antivirovou kontrolu na koncové stanici, nebo komunikaci z LAN technicky zakázat a vybraným pracovníkům na vyžádání vytvořit stahování jejich pošty prostřednictvím KMS s ukládáním do jejich složky. Přitom se však musí dozvědět jejich hesla a uživatelé si nemohou stáhnout stejné zprávy ještě i doma, protože volbu "zanechat zprávy na serveru" KMS nemá.

Chybičkou je ukládání nové definice nebo pravidla až na samý konec seznamu - záležíli na pořadí, je potom nutné posunout pravidlo bočními šipkami nahoru. Vhodnější řešení je u komunikačních pravidel, kde se zařazuje nad vyznačený řádek. Také rotaci logů, adresář pro jejich ukládání a šablony uživatelů by měli vývojáři zapracovat tak, jak to udělali u KMS.

Závěr

Upgradem z WinRoute Pro nově získáte transparentní proxy, antivirovou kontrolu protokolů HTTP a FTP. Použitím KWF si můžete snadno vynutit správnou firemní bezpečnostní politiku týkající se internetu. Je jen škoda, že zatím nemohu napsat: "KWF znamená totální bezpečnost". Těším se na další verze, kde snad bude antivirová kontrola rozšířena a bude zapracována funkce detekce skenování portů a detekce útoků (IDS).

Vít Ožana

KERIO WINROUTE FIREWALL 5.0.4

Robustní podnikový firewall s integrovanou transparentní cache, DHCP, filtrováním přístupu ke stránkám s nevhodným obsahem a s antivirovou kontrolou HTTP a FTP protokolu.

Minimální požadavky CPU 300 MHz, 128 MB RAM, Windows NT/2000/XP

Poskytl/výrobce Kerio Technologies, Plzeň (www.kerio.cz)

Cena 9660 Kč včetně DPH (základní verze do 10 uživatelů)