

Wash  
ME!

# VYPERTE SI WEB

## Centrální filtr pro HTTP s podporou SSL

**Společnost COMGUARD nám zapůjčila produkt Webwasher (McAfee Web Gateway). Jedná se o komplexní řešení pro kontrolu a řízení komunikace po vybraných internetových protokolech.**

**W**ebwasher kontroluje a řídí provoz nejdůležitějších aplikačních protokolů používaných ve firemním prostředí. Prvním takovým protokolem je HTTP pro přístup k webovým stránkám a jeho varianta šifrovaná pomocí TLS/SSL, HTTPS. Druhým klíčovým protokolem firemních sítí je SMTP pro odesílání a doručování e-mailů. Kromě těchto základních protokolů podporuje Webwasher i souborové přenosy po protokolu FTP.

### Co je zač?

Zařízení a jeho kvalita nás zajímaly už proto, že Gartner řadí Webwasher do leader části Magic kvadrantu. Přístroj jsme dostali ve formě předinstalovaného serveru rackového formátu 1U. Konfigurace zařízení probíhá pomocí přehledného webového rozhraní, komunikujícího anglicky, nicméně veškerá uživatelská hlášení mohou být lokalizována.

Předinstalovaný Webwasher běží na variantě operačního systému na linuxovém jádře. V rámci základní licence je poskytnuta předinstalovaná appliance, reportovací nástroj Web reporter doplněný o moduly proxy, cache, URL filtrace dle kategorií i reputací, McAfee Antivirus, SSL scanner a obsahové kontroly DLP včetně „Document inspector“. Podle informací na webu lze Webwasher instalovat na vlastní hardware s Linuxem, nebo dokonce i Windows, nicméně předinstalovaná varianta má své nesporné výhody. Z papírové dokumentace bylo možné zjistit i administrátorské heslo

pro interaktivní linuxový shell (heslo bylo odvozené od MAC adresy). Pro konfiguraci zařízení ale nebylo vůbec potřeba ho používat.

### Způsob zapojení

Konfigurace síťových rozhraní a adres byla přímočará. Možnost nakonfigurovat dvě síťová rozhraní serveru navádí k zapojení zařízení mezi uživatelské počítače a přístupový bod do internetu. Součástí konfigurace není DHCP server, ale ten by zde využil málokdo.

Mimoto je možné zapojit jen jedno rozhraní do místního routeru nebo firewallu. Z Webwasheru se tak stává samostatná zóna nebo je zařazen do stávající DMZ.

Nastavení síťových rozhraní, směrování a aktualizace času tvoří podsektory Appliance sekce Configuration webového rozhraní. Umístění není úplně dobře odhadnutelné, ale po prvních pokusech už si ho člověk zapamatuje. Dále je v této sekci zařazena možnost stroj restartovat nebo vypnout.

### HTTP proxy

Po dokončení síťového nastavení přichází na řadu sekce Proxies. Webová proxy je přednastavena na port 9090 a nechybí možnost vyladit její parametry. Například je možné povolit posílání hlavičky „X-Forwarded-For“ webovému serveru. Rovněž lze upřesnit timeouty Webwasheru nebo zapnout ochranu proti timeoutům webových prohlížečů.

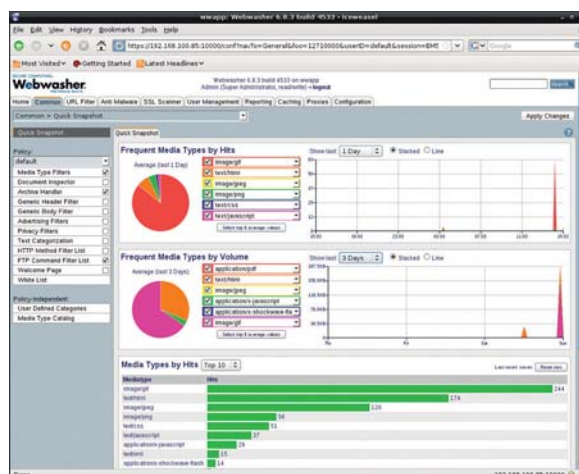
Dalším krokem je konfigurace webových prohlížečů uživatelů. Prohlížeče je potřeba nastavit, aby používaly webovou proxy pro HTTP i HTTPS spojení. Bez další konfigurace můžeme využívat výhod proxy serveru pro nešifrované HTTP a jeho statistik. Statistiku rozlišují typy dokumentů a zobrazují se podle nastavené délky časového úseku (například hodina, půl roku, rok).

### Kategorizace webů

Webwasher obsahuje filtr, který rozděluje weby a tím pádem i webové adresy (URL) na kategorie. Používá k tomu centrální databázi, kterou si umí automaticky aktualizovat, obsah stránek a lokální databázi.

V sekci URL Filter najdete statistiky podle kategorií. To vám umožňuje odlišit přístupy k webovým adresám, u nichž je kategorie známa. Kategorie a podkategorie jemně rozlišují různé oblasti lidské činnosti od obchodních a vzdělávacích až po pornografii.

Podle kategorií je možné v této sekci nastavit i konkrétní akce, které se mají při pokusu o přístup provést. Umožní vám to blokovat weby, o kterých je známo, že patří k některé z kategorií. Kategorizace samozřej-



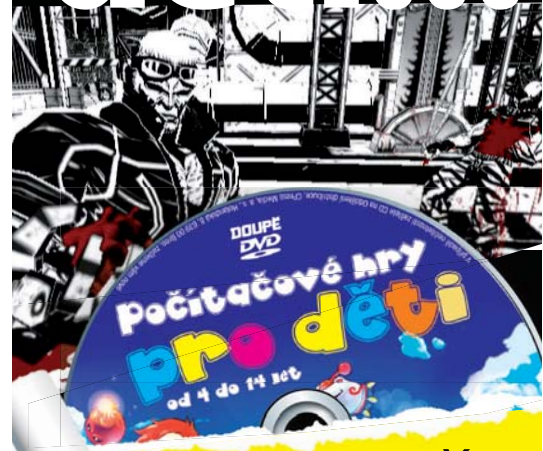
Webwasher komunikuje v angličtině, ale lze jej lokalizovat.

AUTOR

**Pavel Šimerda**

Externí spolupracovník redakce.

# Některé hry nejsou pro děti...



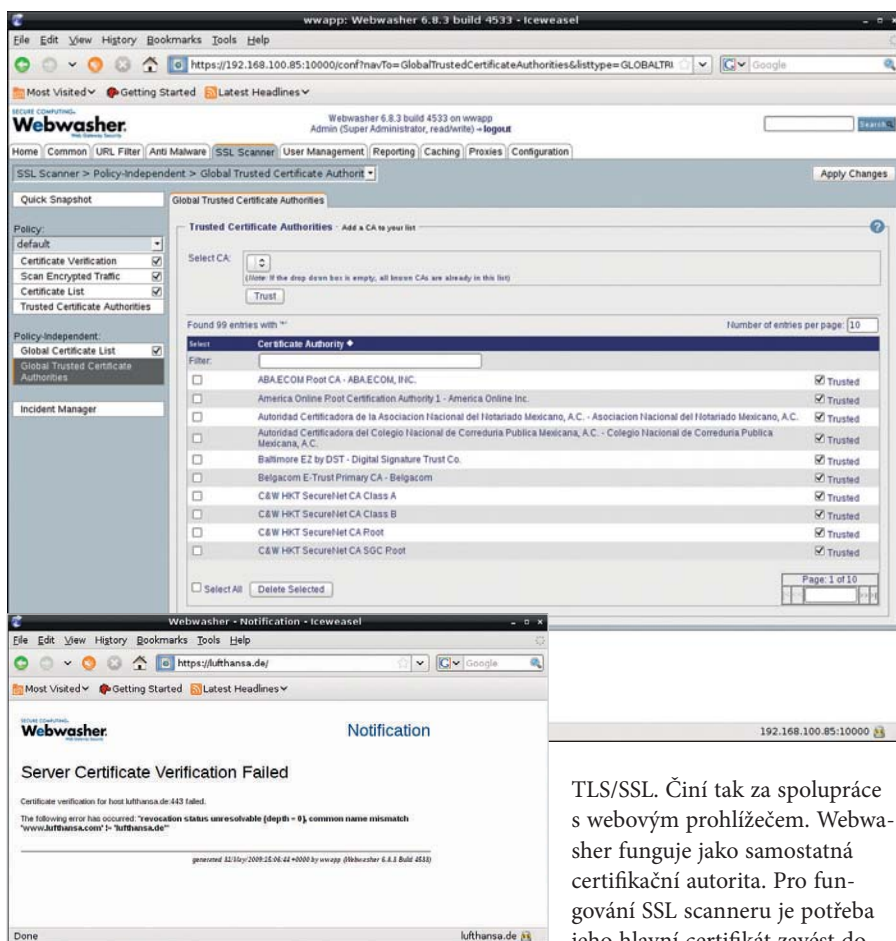
...ty naše

# ANO!

**200 nejlepších her**  
NÍZKÉ NÁROKY NA POČÍTAČ

HRY BEZ NÁSILÍ  
ROZVÍJÍ MÝŠLENÍ  
ZRYCHLUJÍ REFLEXY  
TRÉNUJÍ PAMĚŤ  
PROCVIČUJÍ MOTORIKU

# DVD PŘÁVĚ V PRODEJI!



Ve webovém rozhraní se pak nastavuje celá bezpečnostní politika certifikátů a certifikačních autorit.

mě nemusí být přesná a je jen na vás, jakou přístupovou politiku zvolíte.

## Antimalware

Ochrana proti různým druhům škodlivého software je společná pro všechny protokoly. Objekty (soubory, přílohy) podstupují reaktivní i proaktivní opatření. Reaktivní opatření spočívají ve vyhledávání signatur známých škodlivých kódů. Proaktivní navíc zkoumají podezřelé chování a blokují na základě heuristiky.

Navíc umožňuje Webwasher definovat pravidla pro nakládání s objekty odkazovanými z HTML stránek včetně javascriptů, ActiveX prvků a spustitelných souborů. Můžete definovat i filtry namířené proti reklamním objektům a spamu.

Detailněji jde nastavit filtrování komunikace podle HTTP/SMTP hlaviček a samozřejmě i podle těla zpráv a webových stránek. Tato vlastnost ještě více zdůrazňuje podobnost mezi komunikací HTTP a SMTP. Filtry jsou rozloženy mezi několik konfiguračních sekcí a ne vždy je lehké uhadnout, ve které z nich hledat. Toť snad jediná výtka.

## Fitrování SSL

Klíčovou technologií Webwasheru je SSL scanner, který umožňuje monitorovat webovou komunikaci šifrovanou pomocí

TLS/SSL. Činí tak za spolupráce s webovým prohlížečem. Webwasher funguje jako samostatná certifikační autorita. Pro fungování SSL scanneru je potřeba jeho hlavní certifikát zavést do prohlížeče a převést tím odpovědnost za uznávání SSL certifikátů na Webwasher.

Ve webovém rozhraní se pak nastavuje celá bezpečnostní politika certifikátů a certifikačních autorit. Vedle seznamu certifikačních autorit a výjimek tu najdete i detailní nastavení skenování SSL. Máte možnost určit, které certifikáty serverů se jen kontrolují na správnost a které spouští mechanismus přešifrování novým klíčem.

V případě přešifrovávání funguje Webwasher jako legitimní man-in-the-middle (muž uprostřed, prostředník). Obvykle se tento pojem spíše spojuje s útokem proti bezpečnosti šifrovaného spojení, kdy je prostředník s přístupem k datům nežádoucí.

Webwasher představuje komplexní webovou proxy bránu s pokročilými možnostmi zabezpečení uživatelů uvnitř sítě. Využit lze řízení uživatelů za účelem zvýšení produktivity práce, caching pro optimalizaci spotřeby šířky pásma, ale umožňuje zejména postihnout velmi dobře aktuální hrozby šířené cíleně pomocí skriptů a aktivních kódů vložených hackery využitím technologií WEB 2.0 na zranitelné byť důvěryhodné weby. Komplexnost je dotažena možností postihnout tyto hrozby i v šifrovaném https provozu. Nicméně je určen spíše pro střední a větší organizace s bezpečnostními IT odborníky. □