

## Komentář: 95% účinnost McAfee® Network IPS

Brno 20.1. 2011

Společnost COMGUARD informuje o dalším úspěšném hodnocení řešení McAfee® Network IPS. McAfee® Network Security Platform M-8000 appliance zaznamenala nejvyšší přesnost a propustnost v posledních srovnávacích testech v NSS Labs. Výsledky odrážejí snahu McAfee teamu nabízet bezkonkurenční ochranu před hrozbami, síťovou výkonnost a provozní dokonalost. Tyto vlastnosti byly prověřeny nezávislými recenzenty, laboratořemi, analytiky, a co je nejdůležitější, zákazníky v praxi.

**Při zkouškách byla zaznamenána bezprecedentní 92% účinnost výchozího nastavení bezpečnostních pravidel (DEFAULT).** Na rozdíl od jiných IPS (Intrusion Prevention Systems) řešení, tyto výsledky svědčí o tom, že s McAfee IPS mohou organizace dosáhnout extrémně vysoké úrovně ochrany bez složitého konfigurování a „ladění“. Pro Vaši představu - v průměru se tato účinnost IPS obvykle pohybuje pod 50 procenty. Proto je McAfee® Network IPS řešení výhodné především pro organizace a společnosti, které nejsou schopny investovat nespočetné hodiny do doladování svých IPS politik, aby dosáhly účinné ochrany sítě.

V druhé fázi testování, kdy došlo k nastavení konfigurace bezpečnostními odborníky, dosáhlo řešení McAfee IPS opět **nejlepší účinnosti** ze všech testovaných řešení - **95 %**. Zákazníci McAfee také výrazně oceňují zamezení falešným poplachům (tzv. false positive), které zbytečně zahlučují administrátory, a tím blokují hlášení o skutečných hrozbách, a výrazně tak snižují reakční čas potřebný k zásahu při napadení.

Dalším z důvodů úspěchu IPS společnosti McAfee je důraz na ochranu proti tzv. „Evasion techniques“ v síťových protokolech na úrovních 3, 4 (tedy hlavně IP, TCP, UDP) a 7 (aplikační protokoly, jako např. HTTP). Ochrana proti těmto technikám je jeden ze stavebních pilířů celého řešení. Útočníci často zkoušejí obejít IPS manipulací s hlavičkou paketu (např. manipulace s TTL), segmentací a řazením paketů (útočník může pakety „rozsekát“ a posílat v nelogickém pořadí; protokoly TCP/IP si s tímto porádí, ale nekvalitní IPS nemusí odhalit takto skrytý útok) nebo maskování dat na úrovni aplikační vrstvy (např. zakódování URL, viz. jednoduchý příklad).

Originální URL:

<http://www.comguard.cz/produkty/mcafee-network-defense/mcafee-network-security-platform-intrushield/>

Zakódované URL:

<http://www.comguard.cz/%70rodu%6b%74y/%6dc%61fe%65-n%65%74w%6f%72%6b-def%65%6es%65/m%63%61%66e%65-%6ee%74%77%6frk-%73e%63%75%72%69%74y-%70%6catfo%72m-%69n%74%72us%68%69eld/>

**NSS Labs naměřily úspěšnost proti „Evasion techniques“ 100%**, byly tedy detekovány všechny pokusy o obejítí IPS. Tato vlastnost společně s kvalitními výchozími pravidly a extrémní propustností (nejvyšší model je certifikován na rychlost 10Gbps) vysvětlují, proč daly laboratoře, nebo i společnost Gartner, McAfee takový náskok před konkurencí. McAfee řešení tímto úspěchem totiž navazuje na 1. místo v [Leader Magic Quadrantu pro Network IPS v prosincové zprávě výzkumné společnosti Gartner](#).

[Více o McAfee Network IPS naleznete na stránkách společnosti COMGUARD](#), výhradního distributora pro Českou republiku a Slovensko.

### ***NSS Labs***

*NSS Labs podporuje mnoha milionové výzkumy a testování zařízení, a to v Austinu v Texasu. Testování v laboratoři možné 24 x 7, laboratoř poskytuje údaje v rámci všech testovaných výrobků. Základním cílem laboratoře je výzkum rozsáhlých síťových hrozeb. Tato globální výzkumná síť zachytí internetové hrozby a trendy, pokud se vyskytnou. Hrozby jsou umístěny do komplexní databáze zranitelností, exploitů, malwaru a phishing URL. In-house bezpečnostní analytici kombinují znalosti hackerů a vědních oborů pro vývoj a zavádění nejpřísnějších testovacích metodik. Více na <http://www.nsslabs.com/>.*

Robert Šefr, IT Security Consultant, COMGUARD, a.s.