

Technologické novinky

pojďme se podívat na možnosti virtualizace

Analýza společnosti Gartner opět i na konci roku 2008 umístila bezpečnostní technologie Check Point Technologies do magického kvadrantu vedoucích hráčů na trhu – a to jak v oblasti podnikových firewallů, tak i v oblasti ochrany dat na mobilních zařízeních.



Virtualizace VPN-1 VE

Slovo virtualizace se dnes skloňuje mnoha způsoby. Při nasazení mnoha virtuálních serverů na jednom fyzickém železe s běžícím hypervisorem stojí firma před problémem, jak bezpečně ochránit např. virtuální databázový server od zbytku systémů běžících na stejném železe. Check Point VPN-1 VE (Virtual Edition) je bezpečnostní brána certifikovaná společností VMware pro ochranu virtuálních strojů. VPN-1 v sobě obsahuje především firewall a VPN, ale také antivirus, anti-spyware, URL filtering, anti-spam, QOS, IPS atd.

VE je obdoba software Check Point VPN-1, optimalizovaná pro běh ve virtuálním prostředí a licencovaná dle počtu chráněných virtuálních serverů.

Virtualizace VSX-1

Společnost Check Point nabízí řadu dedikovaných hardware platform pro zajištění bezpečnosti. Kromě modelů UTM-1, Power-1, IPS-1, SSL VPN Connectra a dalších, přichází nyní se zařízením VSX-1.

Celkem tři modely zařízení VSX-1 nabízejí propustnost firewallu od 4,5Gb/s až po 27Gb/s. Umožňují na jednom fyzickém zařízení běh až 150ti oddělených VPN-1 bran současně. Mezi virtuálními bránami je možné vytvářet virtuální infrastrukturu (zařízení ty-

pu switch/router) a vytvořit tak levnou, rychlou a bezpečnou platformu pro velké firmy o mnoha pobočkách, poskytovatele internetu, či telekomunikační operátory. Typicky tak do jednoho zařízení VSX-1 vedou VLANy různých poboček, či zákazníků. VSX-1 v sobě tyto VLANy propojuje virtuální infrastrukturou a každá pobočka/zákazník má svoji politiku, spravovanou jinými administrátory apod.

Pokud by byl zapotřebí vyšší počet virtuálních strojů (až 250), je možné zakoupit **software VSX** a nasadit ho na hardware třetí strany

Nová verze R70 bezpečnostních bran

Produkt VPN-1 v této verzi (ať již na hardware Check Point, či jako software na železe jiných výrobců – např. Crossbeam, Nokia, SUN, apod.) doznal značných změn.

Software Blades – novinkou jsou zásuvné moduly, které lze samostatně zakoupit. Zcela nezávislé licence tak umožňují kupovat jen ty moduly, které si zákazník vyžádá (IPS, Antivir a Anti malware, VPN, URL filtering, Messaging security apod).

Nový blade **Provisioning** slouží pro snazší správu mnoho bran najednou. Jen pomocí vytvoření profilu můžete nastavovat centrálně pro všechny brány route tabulky, hostname, IP adresy vybraných rozhraní, DNS



záznamy, či nastavení zálohování. Centrálně tak lze určit, na kterých branách se bude dělat pravidelná záloha konfigurace, frekvenci opakování, místo uložení zálohy (lokálně na branách, SCP nebo TFTP server), nebo zda budou v záloze konfigurace ukládány i log soubory (ty jsou standardně ukládány také na log serverech – buď samostatných serverech určených jen pro ukládání logů, nebo na management serveru).

Kromě řady vylepšení pro VoIP, nabízí verze R70 především nový blade IPS, který v sobě zahrnuje to nejlepší z interního IPS systému (dříve SmartDefense) – zabudovaného jako funkcionality firewallu a z externího systému IPS-1, který byl získán akvizicí společnosti NFR. Dle předpovědi společnosti Gartner bude trh interních IPS systémů na-

dále růst a dohánět tak zatím stále značný náskok externích IPS zařízení.

UTM (Unified Threat Management)

Jsou k dispozici tři základní modelové řady UTM boxů:

- 1) Model **UTM-1 Edge** (aktuálně verze 8.0) určený pro SOHO trh (wi-fi router, ADSL port, Radius server pro 802.1X, print server, terminal server pro RS232 apod.)
- 2) Nyní celkem 6 modelů **UTM-1** určených pro střední firmy s propustností firewallu od 400Mb/s až po 4,5Gb/s.
- 3) Celkem pět modelů **Power-1** a **IAS** určených pro velké firmy s propustností firewallu od 4,5Gb/s až po 14Gb/s. Tyto modely obsahují v ceně i funkcionality typu QOS, dynamický routing, redundantní napájecí zdroje,

RAID pole dvou disků a další nadstandardní vlastnosti.

Produkt Endpoint Security v sobě zahrnuje personální firewall, antivirus, anti-spyware, šifrování disku a médií, ochranu portů, NAC a IPSec/SSL VPN klienta. Novinkou ve verzi R71 je možnost šifrovat CD/DVD disky přímo z průvodce Windows XP/Vista. Byla přidána možnost zakázat zápis na šifrované externí disky. Mazání zálohy se nyní při šifrování výměnného média provádí bezpečným algoritmem (tzv. skartace dat) a média se šifrují silným 256bitovým šifrováním algoritmu AES.

Produkty pro šifrování dat mají bezpečnostní certifikace FIPS [2] a Common Criteria a lze s nimi šifrovat celou řadu mobilních zařízení: pevné disky s různými operačními systémy Windows/Linux/Mac OS, externí pevné disky, USB flash, CD/DVD, či mobilní zařízení s operačními systémy Palm OS, Windows Mobile, či Symbian.

Více informací naleznete na www.checkpoint.com/services/techsupport/hcl/vsx.html
www.nist.org