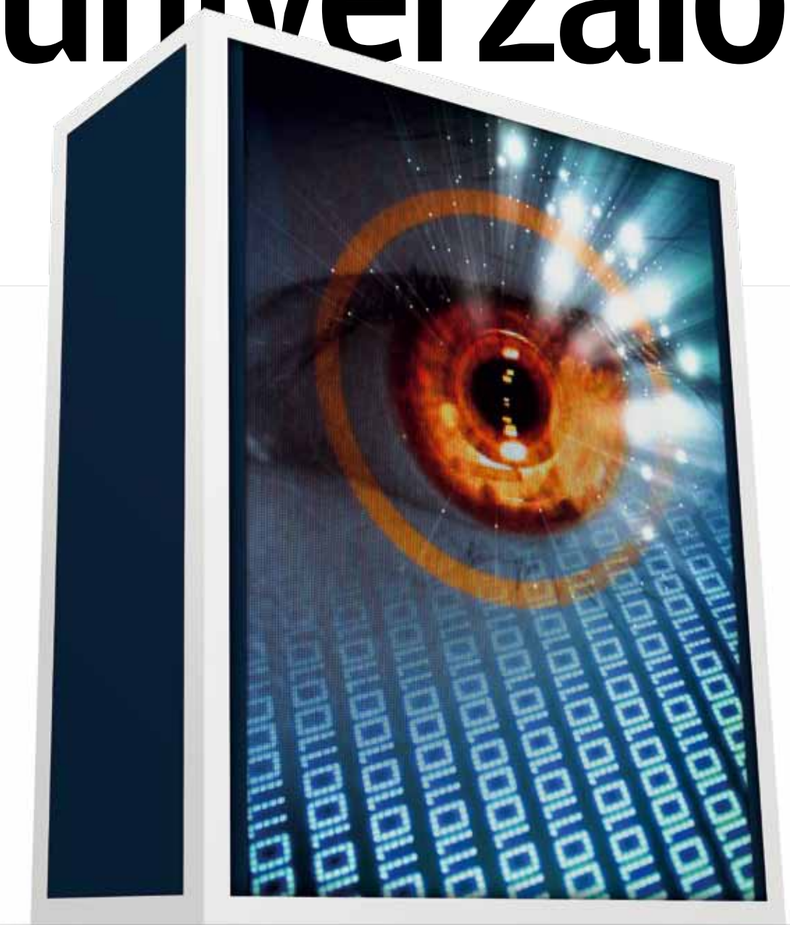
Výkonní univerzálové

se širokým záběrem



Všestranné zabezpečení firemní sítě prostřednictvím sjednocené správy hrozeb UTM (Unified Threat Management) představuje zejména pro střední firmy ekonomickou a zároveň výkonnou alternativu. Hardware typu vše v jednom lze snadno instalovat a konfigurovat; jednoduché bývají i následná správa a administrace.

VÍT PETRJANOŠ

Na rozdíl od softwarových řešení jsou zařízení pro UTM nabízena jako kompletní hardwarové řešení s výkonem a vybavením odpovídajícím všem (nebo téměř všem) potřebám firem z hlediska bezpečnosti výpočetního prostředí.

Většina výrobců v současnosti do základní ceny zahrnuje firewall, ochranu před průniky IPS a virtuální privátní síť VPN, avšak další funkcionalitu pro sjednocenou správu hrozeb je potřeba dokoupit formou příslušné licence. Zpravidla jde o licence pro neomezený počet uživatelů, jejich konkrétní počty limituje dodávaný hardware. Podobně jako u softwarových bezpečnostních produktů je nutné počítat s tím, že licence se obvykle vždy po roce obnovují.

Specifickým případem je zajištění vysoké dostupnosti – někteří výrobci dovolují provozovat dvě zařízení v redundantním režimu aktivní/pasivní bez nutnosti nákupu licencí pro obě řešení. Dá se tak ušetřit část nákladů.

Pestrá nabídka

Pro dnešní srovnání jsme vybrali třináct zařízení, která podle svých dodavatelů vyhoví jedinému kritériu – jsou vhodná pro české firmy s 50 až 500 uživateli. Z cenového i funkčního hlediska jde o velmi pestrou nabídku firem Barracuda, Cisco, Cyberoam, Fortinet, Check Point, Juniper, Kerio Technologies, TNS, McAfee, NetGear, SonicWALL, Sophos (dříve Astaro), WatchGuard a ZyXel.

Většina modelů je navíc jen jedním zástupcem širšího portfolia jednotlivých výrobců, kteří nabízejí celou škálu produktů v různě výkonných variantách a pro firmy rozličných velikostí, od nejmenších až po velké podniky a rozsáhlé sítě. Je potěšitelné, že mezi nabízenými modely se neztrácejí ani zařízení od firem s českými kořeny.

Všechny modely až na výjimky disponují základními funkcemi – firewallem, VPN se SSL i IPSec, antivirovým, antispywarovým a antispamovým softwarem, nástroji IPS a IDS pro detekci a obranu před záškodnickými průniky, webovým a aplikačním filtrem a ochranou komunikace přes instantní messengery a P2P. Propustnost se u firewallu pohybuje v širokém rozpětí od 350 Mb/s po 3 Gb/s, podobně široké rozpětí

Fortinet FortiGate 80C v bezdrátové verzi

Odchytávání packetů v Cisco ASA 5200

najdeme i u propustnosti nástrojů pro IPS a u VPN.

Každé zařízení je vybaveno minimálně čtyřmi síťovými porty, přičemž vždy alespoň dva jsou určeny pro gigabitový Ethernet. Přeborníkem v tomto směru je Kerio Control Box 3110, které v základním provedení nabízí hned osm gigabitových portů. Vůbec nejvíc (deset) portů najdeme u Fortinetu Fortigate 80C, osm z nich je ovšem určeno pouze pro Fast Ethernet.

Velká většina systémů je schopná pracovat v režimu vysoké dostupnosti; tam, kde tomu tak není, bývá možné přikoupit tuto volbu za příplatek. Naproti tomu u podpory 3G a Wimaxu přes USB port už nejsou údaje tak jednoznačné, i když alespoň jedním USB portem jsou vybaveny všechny modely.

Grafy síťové komunikace v Kerio Control

U zhruba poloviny bez ohledu na cenu modelů najdeme i možnost virtualizace jejich provozu. Naproti tomu vybavení nástroji pro forenzní analýzu nebo korelaci událostí se stavem sítě či činností uživatelů je spíše slabší. Ani tady cena nerozhoduje.

Ceny uvedených softwarových licencí jsou spíše orientační a obvykle závisejí na konfiguraci UTM funkcí pro konkrétního zákazníka. U dražších systémů bývá software v ceně celého zařízení.

Na některá řešení z doprovodné tabulky se podíváme podrobněji.

Kerio Control Box 3110

Box s poutavým designem a velikostí odpovídající racku 1 U prodává firma Kerio Technologies za 34 000 korun včetně licencí pro pět uživatelů. Součástí licence jsou softwarová aplikace Kerio Control, antivirová ochrana Sophos, statistické a reportovací nástroje Kerio StaR a dále Kerio Web Filter a VPN server. Zařízení je vybaveno osmi porty pro gigabitový Ethernet a paměťovou kartou Compact Flash s kapacitou 8 GB. O „pohon" se stará procesor Intel Dual Core s frekvencí 2,6 GHz, který má k dispozici 2GB operační paměť.

Základem zařízení je aplikace Kerio Control, která zvládá všechny běžné funkce ochrany sítě včetně sledování síťových spojení (SPI), omezování počtu spojení, ochrany proti falšování zdrojových adres (antispoofing) či inspekce protokolů. Detekce a prevence útoků (IDS/IPS) založená na systému Snort využívá databázi signatur útoků, autorizovanou společností Kerio Technologies, a umožňuje vytvářet seznamy zakázaných IP adres.

K dispozici je i mnoho funkcí pro filtrování obsahu, od omezování časové platnosti a eliminace sítí P2P přes kategorizaci webových stránek až k možnosti vytvářet skupiny URL adres či zakázaných slov (včetně výjimek) a pravidla pro FTP.

Kerio Control podporuje neomezený počet VPN tunelů a jeho klientská aplikace poběží jak na MS Windows (a to i jako služba), tak na Mac OS X a Linuxu. Pro Windows je k dispozici i webové rozhraní SSL-VPN.

Zařízení umožňuje provoz více internetových linek najednou, směrování podle pravidel a implicitní zálohování připojení. Správci sítě mohou rozkládat zátěž sítě a v průvodci pro nastavení řízení šířky pásma a QoS snadno nastavovat kvalitu služeb.

Aplikace je bohatě vybavena funkcemi pro reporting. Lze vytvářet reporty o využití internetu jednotlivými uživateli, skupinami nebo celou sítí, podrobné reporty o aktivitách uživatelů

Inzerce

Řešení koncentrující nejlepší světové technologie
VAD distribuce www.comguard.cz

McAfee®
An Intel Company

Některá zařízení pro sjednocenou správu hrozeb dostupná na českém trhu

														
Produkt	**Barracuda NG Firewall F300**	**Cisco ASA 5520-BUN-K9**	**Cyberoam CR100ia**	**Fortinet FortiGate 80C**	**Check Point 4210 Appliance**	**Juniper SRX 100**	**Kerio Control Box 3110**	**Kernun UTM 150**	**McAfee Firewall Enterprise S1104**	**NetGear ProSecure UTM150**	**SonicWALL NSA 250M**	**Sophos UTM 120**	**WatchGuard XTM 510**	**ZyXel ZyWALL USG 1000**
Dodavatel, kontakt	Gesto Communications, *www.gestocomm.cz*	Alef Nula, *www.alefnula.cz*	Comguard, *www.comguard.cz*	Skynet, *www.skynet.cz*	Check Point, *www.checkpoint.com*	DNS, *www.dns.cz*	Kerio Technologies, *www.kerio.cz*	Trusted Network Solutions, *www.tns.cz*	Comguard, *www.comguard.cz*	NetGear, *www.netgear.cz*	Comguard, *www.comguard.cz*	Annex Net, *www.annexnet.cz*	Permanence, *www.itsczech.cz*	ZyXEL Communications Czech, *www.zyxel.cz*
Firewall (SPI)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VPN se SSL | IPSec	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✗	✓|✗	✓|✓	✗|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓
Antivirus | antispyware	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✗	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓
Antispam	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
IPS | IDS	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✦|✦	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓
Webový filtr | ochrana IM a P2P	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✦|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓
Aplikační filtr	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Propustnost FW | IPS | VPN	350 M | 84 M | 160 M	450 M | 225 M | 225 M	1 G | 300 M | 80 M	500 M | 350 M | 100 M	min. 3 G | 2 G | 400 M	700 M | 60 M | 65 M	1 G | cca 600 M | 250 M	1 G | 600 M | 200 M	750 M | 250 M | 60 M	900 M | 130 M | 400 M	700 M | 250 M | 200 M	2,2 G | 640 M | 490 M	1,4 G | 400 M | 350 M	400 M | 100 M | 180 M
Počet uživatelů	neomezen	neomezen	neomezen	100	neuvádí	neomezen	1 000 až 1 500 podle zátěže	150	neomezen	neomezen	neomezen	neomezen, doporučeno 50	neomezen	doporučeno do 200 uživatelů
Počet současných spojení	70 000	130 000	400 000	400 000	min. 1,2 milionu	32 000	45 000 (LAN-LAN)	4 500	200 000	65 000	110 000	300 000	50 000	500 000
Počet nových spojení za vteřinu	2 500	9 000	10 000	10 000	neuvádí	2 000	až 1 500	500	5 000	neuvádí	3 000	6 400	neuvádí	12 000
Síťové porty a další rozhraní	8× FE, 2× USB	3× FE, 2× GbE, 2× USB	6× GbE, 2× USB	8× FE, 2× GbE	4× GbE, 2× USB	8× FE, 1× USB	8× GbE, 2× USB, 1× SP	6× GbE, 2× USB, 1× SP	4× GbE, 4× USB	4×/4× GbE*, 1× USB	5× GbE, 2× USB	4× GbE, 1× USB	1× FE, 6× GbE, 2× USB, 1× SP	5× GbE, 2× USB, 1× SP
Vysoká dostupnost A-A | A-P	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✓|✓	✗|✗	✦|✦	✓|✓	✓|✗	✗|✓	✓|✓	✓|✓	✓|✓
Podpora 3G | Wimax přes USB port	✓|✗	✗|✗	✓|✓	✓|✗	✗|✗	✓|✓	✗|✗	✗|✗	✗|✗	✗|✗	✓|✗	✓|✗	✗|✗	✓|✗
Optimalizace šířky pásma	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Rozkládání zátěže sítě	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓
Monitoring událostí	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Korelace událostí se stavem sítě	✓	✗	✗	✓	✦	✦	✓	✦	✦	✗	✗	✗	✓	✓
Korelace událostí s činností uživatelů	✓	✗	✗	✓	✦	✦	✓	✦	✦	✗	✗	✗	✓	✓
Forenzní analýza	✓	✓	✗	✦	✦	✦	✗	✓	✗	✗	✗	✗	✗	✓
Analýza trendů	✓	✓	✓	✦	✦	✓	✗	✦	✦	✗	✓	✗	✗	✓
Geolokace	✗	✦	✓	✓	✓	✗	✗	✦	✓	✗	✓	✗	✗	✗
Vizualizace konfliktů | korelací | aktivit	✓|✓|✓	✓|✗|✓	✗|✗|✓	✓|✓|✓	✦|✦|✦	✦|✦|✦	✗|✗|✓	✗|✦|✓	✦|✗|✓	✗|✗|✗	✗|✗|✓	✗|✗|✗	✓|✓|✓	✓|✓|✓
Analýza a simulace pravidel	✓	✓	✗	✗	✦	✗	✗	✓	✦	✗	✗	✗	✓	✗
Reporting využívání internetu	✓	✓	✓	✓	✦	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reporting uživatelských aktivit	✓	✓	✓	✦	✦	✓	✓	✓	✓	✓	✓	✓	✓	✓
Systém výstrah	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtualizace zařízení	✓	✓	✗	✓	✦	✗	✓	✓	✗	✗	✗	✓	✗	✗
Lokalizace rozhraní do češtiny	částečně	✓	✗	✗	✓	✗	✓	částečně	✗	✗	✗	částečně	✗	✗
Základní záruka na hardware (měs.)	12	podle zakoupené podpory	podle zakoupené podpory	12	12	12	12 (možno rozšířit na 36)	36	podle zakoupené podpory	24	podle zakoupené podpory	po dobu platnosti licence	12	60
Cena zařízení (bez DPH)	90 800 Kč	7 995 dolarů (cca 152 000 Kč)	cca 51 000 Kč	1 295 eur (cca 32 400 Kč)	5 500 dolarů (cca 104 500 Kč)	949 dolarů (cca 18 000 Kč)	34 000 Kč (lic. pro 5 uživ.)	125 000 Kč	cca 52 000 Kč	31 000 Kč	cca 35 000 Kč	11 379 Kč	3 318 dolarů (cca 63 000 Kč)	2 534 eur (cca 63 400 Kč)
Cena licencí na rok (bez DPH)	od 16 500 Kč	v ceně	cca 24 000 Kč	403 eur (cca 10 000 Kč)	Softwarové blady v ceně	617 dolarů (cca 11 700 Kč)	234 Kč/uživ. (sw maintenance)	v ceně	cca 10 000 Kč	7 000 Kč	cca 30 000 Kč	24 289 Kč	1 749 dolarů (cca 33 200 Kč)	1 125 eur (cca 28 100 Kč)

FE - Fast Ethernet (10/100Base-T), GbE - gigabitový Ethernet (10/100/1000Base-T), SP - sériový port G = Gb/s, M = Mb/s * 4× GbE pro WAN + 4× GbE pro LAN ✦ - doplněk za příplatek

Zdroj: příslušní dodavatelé, Computerworld

a statistiky využití internetového připojení, filtrování webového obsahu a webových stránek či činnosti jednotlivých uživatelů ve webovém prohlížeči. K dispozici jsou i funkce pro historickou analýzu.

Software dále podporuje multihoming, umožňuje úpravy směrovací tabulky a vytváření různých úrovní přístupových práv ke správě. Uživatelské rozhraní je lokalizováno do patnácti světových jazyků, mezi nimiž nechybí ani čeština. Ověřování uživatelů může probíhat přes Kerberos, Active Directory i Open Directory.

Kernun UTM 150

Srdcem zařízení vyráběného českou firmou Trusted Network Solutions v designu obvyklém pro racková provedení 1 U je procesor Intel Pentium s frekvencí 2,6 GHz, využívající 4GB paměť a 160GB pevný disk. Uživatelé mohou využít šest gigabitových síťových portů a dva USB porty.

Základem Kernun UTM jsou aplikační proxy firewall, antivirová a antispamová ochrana a zabezpečení DNS. Systém je standardně dodáván s antivirem Dr.Web; kromě toho umí pracovat s řadou jiných antivirových systémů podporujících ICAP protokol (McAffe, Symantec, AVG či NOD32).

Proxy pro protokoly elektronické pošty umožňují kontrolovat obsah přenášených zpráv a přítomnost spamu. V kombinaci s antivirovou kontrolou tak lze vystavět velmi robustní systém pro zajištění čistoty e-mailových schránek.

Mezi další funkce Kernun UTM 150 patří autentizace uživatelů pomocí hardwarových předmětů nebo šifrovaný přístup do vnitřní sítě prostřednictvím VPN s flexibilními možnostmi nastavení. Zařízení pracuje s protokoly IPsec/IKE a OpenVPN – druhý je vhodný jak pro připojení klienta k síti (point-to-multipoint), tak pro propojování sítí (point-to-point).

Kernun UTM 150 dále obsahuje paketový filtr s možnostmi detekce vzdáleného operačního systému, umožňuje řízení šířky pásma a ochrany proti útokům DoS a disponuje i funkcemi pro obousměrný překlad adres, normalizaci síťového provozu a logování komunikace.

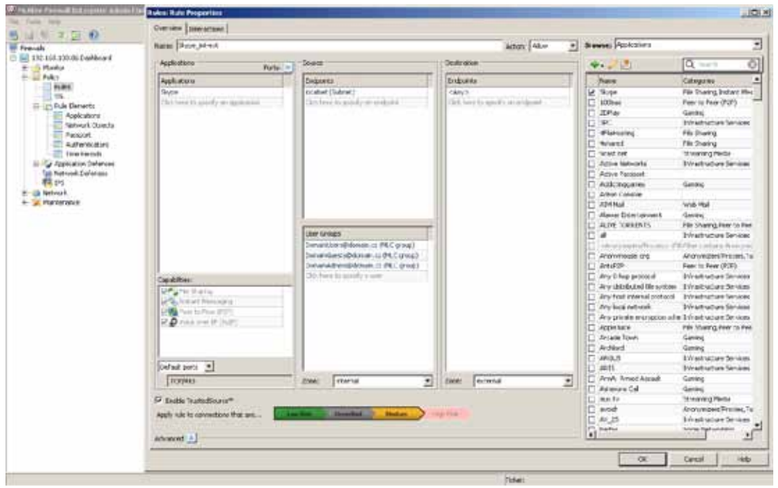
V základní verzi systému uživatel najde i funkce pro filtrování obsahu, detekci typu souboru podle obsahu, garanci autorizované DNS odpovědi, ochranu proti DNS poisoningu, kontrolu obsahu HTTPS spojení, monitoring provozu v reálném čase a virtuální privátní síť pro cestující uživatele.

Grafy síťového provozu v Kernun UTM

Dvojice zařízení Kernun UTM 150 při provozu ▶

Kernun UTM 150 lze volitelně doplnit o webfiltr Kernun Clear Web s katalogem webových serverů a URL adres. Databáze obsahuje průběžně aktualizované záznamy tříděné lidskými kategorizátory podle tematického obsahu. Podle údajů výrobce dosahuje tento filtr u českých zákazníků více než 90% úspěšnosti kategorizace webového provozu.

Uživatelé mohou zařízení za příplatek provozovat i v režimu vysoké dostupnosti – dvě nebo více vzájemně se zálohujících hardwarových zařízení je pak spojeno do tzv. hot stand-by clusteru. Ten také umožňuje připojení k více internetovým providerům a rozložení zátěže linky mezi ně.



Správa bezpečnostních pravidel v McAfee Firewall Enterprise

McAfee Firewall Enterprise S1104

Další zařízení určené do racku (výška 1 U) se spartánským designem je vybaveno operačním systémem SecureOS a firewallem s firemní technologií AppPrism pro detekci, kontrolu, vizualizaci a ochranu aplikací a s architekturou plnohodnotných aplikačních proxy bran, kde je provoz kontrolován do hloubky, ne jen pomocí jednoduchých pravidel na základě IP a portů.

V základní verzi uživatel dostane i funkce pro vysokou dostupnost a optimalizaci šířky pásma. Soubor nástrojů obsahuje i engine pro IPS doplněný více než 10 000 signaturami ve 170 kategoriích a jedenácti předdefinovaných skupinách. Pro filtrování provozu instantních messengerů a P2P je k dispozici dalších více než 500 signatur. K dispozici je i prohlížeč s možností procházet popisy nebo vypínat signatury.

Firewall kombinuje kontroly lokální s globálním reputačním systémem TrustedSource, který celosvětově monitoruje činnost jednotlivých IP adres a následně vyhodnocuje jejich škodlivost.

Systém nabízí i bohaté možnosti autentizace – administrátoři mohou vytvářet pravidla přímo pro uživatele či skupiny uživatelů a při řešení problémů mohou využít návaznost na uživatelské jméno, nikoli pouze na IP adresu, která v některých případech nemusí být dostatečně popisná. Lze využít autentizace přes LDAP/AD/RADIUS a řadu dalších.

Soubor nástrojů doplňují analytické funkce umožňující intuitivní zobrazení konfliktů, pravidel a korelací aplikačních aktivit v reálném čase podle identity uživatele, umístění (geolokace) či úrovně oprávnění. Pomocí nástroje Firewall Reporter, který centrálně monitoruje provoz a generuje korelovaná upozornění a hlášení, lze vytvářet a měnit proudy dat do informací přímo použitelných pro účely auditu.

Zdarma je také možné využít reporting využití webového provozu McAfee Web Reporter. Druhý zmiňovaný využívá výstupy SmartFilteru. Tato komponenta na firewallu nám umožňuje regulovat využití webového provozu, a to na základě 90 kategorií obsahujících desítky milionů kategorizovaných stránek, tak příslušnosti do skupin nebo denní doby.

Zařízení se pyšní certifikací Common Criteria EAL4+ pro aplikační kontroly a filtruje šifrovaný provoz do hloubky – dešifruje zabezpečené protokoly (jako HTTPS, SSH, SCP a SFTP), uplatní antivirovou ochranu, IPS a aplikační filtraci a poté provoz opět šifruje a odesílá na cílový server. Systém dále neumožňuje oklamání firewallu tunelováním jiných protokolů, poskytuje plnohodnotné skrytí vnitřní sítě (network cloaking) a disponuje virtuální technologií „black hole“ pro odražení útoků. ■

Virtualizace firewallů

V počítačovém odvětví se stále zřetelněji prosazuje trend přesunout stavové firewally v rámci IT prostředí blíže k serverům.

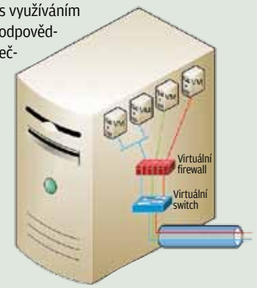
Díky virtualizaci a konsolidaci serverů můžeme provozovat na jednom fyzickém serveru několik virtuálních serverů s rozdílnými úrovněmi důvěryhodnosti. Základní (core) firewally a firewally na perimetru už nejsou těmto serverům dostatečně blízko. Firewall blízko fyzického serveru může lépe zabezpečit každý virtuální server a umožňuje serverům komunikaci s dalšími servery odlišných úrovní důvěryhodnosti pouze přes stavový firewall. Takový firewall provozovaný na vrstvě hypervizoru či serverové virtualizace zabraňuje nežádoucí komunikaci mezi servery.

Na obrázku je znázorněn provoz několika virtuálních počítačů na jednom fyzickém stroji. Každý z nich může mít odlišnou úroveň důvěryhodnosti nebo klasifikace dat, s nimiž pracuje. Pro oddělení komunikace jednotlivých virtuálních strojů a zajištění jejich bezpečnosti je proto potřeba zajistit stavovou filtraci paketů v rámci virtuálního prostředí. Taková filtrace na dané architektonické úrovni může být někdy vyžadována i pro účely zajištění souladu s legislativou.

Současným trendem je posun směrem k hostovaným firewallům. Stále více organizací se poohlíží po využití propracovanějších firewallů na úrovni hypervizoru. V současnosti už tyto typy virtualizovaných produktů nabízí celá řada dodavatelů jako Cisco, Juniper, Check Point, Fortinet či Sophos (dříve Astaro).

Další otázkou, která v mnoha organizacích přichází na přetřes v souvislosti s využíváním virtuálního firewallu, je, kdo má tento virtualizovaný firewall spravovat. Bude odpovědnost za konfiguraci a správu virtuálního firewallu ležet na bedrech síťařů, bezpečnostního týmu nebo systémových administrátorů? Otázka je ještě naléhavější v případech, kdy do virtualizační vrstvy se přesunují celá zařízení pro UTM.

Navíc se dá předpokládat, že se do této vrstvy přesunou i virtualizované verze nástrojů SLB (Server Load Balancer) pro vyrovnávání zátěže serverů a systémů ADC (Application Delivery Controller) pro řízení aplikačních zdrojů. Tradiční fyzické hranice se tak budou stírat stále více a místo dříve využívaných centralizovaných firewallů se budou ve stále větší míře nasazovat firewally distribuované.



Virtualizace firewallu v rámci virtuálního výpočetního prostředí

Inzerce

Partnerský příspěvek

Osobní strážce internetu

Filtr webového provozu Kernun Clear Web

Kernun

Devadesát procent. Přesně tolik z internetového provozu typické organizace představuje webová komunikace. A pokud budeme souhlasit s tvrzením, že internet znamená jeden z nejrizikovějších faktorů pro naši bezpečnost (a asi není důvod s ním nesouhlasit), pak je nabíledni, že ošetření tohoto provozu musíme dát odpovídající důraz.

Bezkonkurenční znalost terénu

Dvě až čtyři procenta webového obsahu představují riziko (pro zajímavost: mezi placenými odkazy je to šest až deset procent!). Průměrný web je díky absenci nejnovějších záplat nebo špatně zvoleným programátorským postupům nebezpečný svému okolí až devět měsíců v roce! O nárůstu internetových podvodů (podle některých statistik meziročně o 8 tisíc procent) ani nemluvě.

Se všemi těmito výzvami si přitom dokáže poradit Kernun Clear Web: řešení pro filtrování webového provozu. Jeho hlavní předností je skutečnost, že se zaměřuje na prostředí „českého internetu“. To pochopitelně není technický pojem, ale je zapotřebí si uvědomit, že čeští uživatelé navštěvují jiné stránky než například Američané (jimž je většina řešení „šitá na míru“) a že mají jiné profily chování. Argument „je jen jeden internet“ je sice pravdivý, ale v daném případě neobstojí. Svědčí o tom i to, že Kernun Clear Web má v českém prostředí úspěšnost převyšující 98 procent – konkurenční produkty ze zahraničí se typicky pohybují mezi šedesáti a sedmdesáti procenty.

Filtr pro dvacet tisíc uživatelů

Důležitost filtrování webového provozu si uvědomilo i Ministerstvo práce a sociálních věcí ČR, které zaměstnává téměř 20 tisíc osob s přístupem na internet: a to v mnoha lokalitách a s rozličnými právy nebo bezpečnostními režimy. Ministerstvo donedávna používalo pro správu sítě a filtrování webů řešení, které bylo závislé na spolupráci několika webových proxy. Tento systém se ovšem nedal jednoduše aktualizovat, udržovat v chodu – a o nějaké centralizaci nebylo možné ani uvažovat.

Kromě vytvoření přehledné a bezpečné počítačové sítě bylo zároveň potřeba vyřešit další dva navazující problémy. Za prvé provést transparentní opatření, aby zaměstnanci využívali internet co nejefektivněji a zároveň síť zbytečně nezatěžovali. Za druhé zvýšit efektivitu práce. Tzn. zamezit tomu, aby zaměstnanci ministerstva využívali svou pracovní dobu k nepracovním aktivitám. Ze všech nabízených řešení si nakonec ministerstvo vybralo právě řešení Kernun Clear Web. Ostatně o jeho možnostech se můžete přesvědčit sami na stránkách *www.kernun.cz/demo*.

Testováno na lidech

Pokud bychom měli nechat promluvit suchou řeč statistik, pak z měřitelných parametrů po nasazení řešení Kernun Clear Web poklesl počet virových nákaz na klientských stanicích ministerstva o plnou třetinu (což je ohromný úspěch vzhledem k tomu, že Kernun není primárně antivirovým systémem) a využívání internetu pro soukromé potřeby kleslo o 69 procent. A to nemluvíme o nepřímých efektech: produktivitě práce, lepším využití hardwaru apod. Kernun Clear Web zkrátka ukázal, že se na něj lze při filtrování webového provozu stoprocentně spolehnout. Více informací lze také najít v případové studii MPSV ČR na stránkách *www.kernun.cz*.