



Cyberoam CR100ia

Astaro oproti jiným výrobcům nabízí – celý bezpečnostní systém si lze fakticky stáhnout z webu ve formě softwarové appliance, kterou lze nainstalovat na běžný počítač mj. i za účelem časově omezeného zkušebního provozu či nekomerčního bezplatného využití. Stejně tak lze díky tomu snadno provádět upgrady zařízení po vydání nové verze a reinstalace v případě poruchy hardwaru. Vedle toho výrobce nabízí také tzv. virtual appliance, tedy verzi připravenou pro běh ve virtuálním prostředí. U ASG-120 jde jinak o běžné řešení se čtyřmi ethernetovými porty podporujícími, stejně jako většina testovaných produktů, rychlosti do 100 Mb/s.

Základní blok bezpečnostních funkcí tvoří trojlístek firewall, IPS, VPN (IPSec i SSL) a optimalizace šířky pásma, které přicházejí v ceně základního zařízení, přičemž zde není žádné omezení jak z hlediska počtu uživatelů, tak z hlediska počtu tunelů IPSec či SSL VPN – jediným limitem je tedy výkon hardwaru. IPS využívá celkem 7 500 signatur pro odhalení a zastavení pokusů o napadení. Tyto bezpečnostní funkce jsou postaveny na open

source technologiích Netfilter a Snort. Podobný přístup výrobce uplatňuje také v dalším bloku funkcí, kde na místě antiviru/antimalwaru využívá dnes již poměrně populární ClamAV a Avira (ten vystřídal dříve používaný engine Authentium), a ten doplňují technologie pro filtrování webového (Trusted Source, IP a P2P (Astaro Flow Classifier) provozu, stejně jako kontrola přístupu na web s možností časového omezení. Mechanismus filtrování si přitom v poslední verzi softwaru poradí také se šifrovaným provozem přes HTTPS. Uvedenou funkcionalitu je již třeba licencovat dodatečně v rámci balíku Web Security, samozřejmě bez omezení počtu uživatelů. Totéž platí i o další skupině funkcí, jejíž označení Email Security poukazuje, že je zaměřena specificky na elektronickou poštu. Sem kromě antiviru se dvěma skenovacími enginy spadá ještě ochrana proti spamu a phishingu a zajímavá je především podpora šifrování pošty, což ocení firmy, které touto cestou distribuují cenné či citlivé informace. Při provozu dvou zařízení v režimu vysoké dostupnosti aktivní/pasivní (kdy je

druhé zařízení nasazeno pouze jako záložní) platíte licence pouze jedenkrát.

Podstatné je, že výrobce dobře zvládl svoji hlavní úlohu – povedlo se mu integrovat všechny zmíněné funkce a open source komponenty do dobře fungujícího celku, který je zastřešen v rámci efektivně navržené správy prostřednictvím webového rozhraní. Už jen vzhledem k rozsahu funkcí nemusejí být první krůčky v něm úplně nejsnazší, ale po chvíli práce jsme zjistili, že jsme byli schopni všechny požadované funkce snadno rychle nakonfigurovat podle požadavků bez zbytečných ne-

problémy během správy velmi snadno vyřešit. Celkově je tak užitná hodnota tohoto zařízení, a to i s ohledem na výkon, který během testování vykazovalo, na velmi dobré úrovni. Co se týká podpory, je možné volit ze dvou úrovní (Gold, Platinum), v jejichž rámci můžete kromě aktualizací softwaru na nové verze a e-mailové či telefonické podpory v češtině očekávat také rychlou výměnu hardwaru v případě poruchy.

### Cyberoam CR100ia

Šíře nabídky společnosti Elitecore Technologies, která na trh dodává UTM firewall značky Cyberoam, sa-



D-Link Netdefend DFL-860

příjemných překvapení. Počáteční nasazení maximálně zjednodušuje průvodce a pro správu uživatelů nyní Astaro využívá podobné rozhraní, na jaké jste zvyklí z prostředí Active Directory. Pochvalu si zaslouží také možnosti reportingu. Za zmínku také stojí velmi dobře zpracovaná dokumentace, s jejíž využitím lze jakékoliv

há od produktů pro nejmenší firmy až po výkonná zařízení, přičemž model CR100ia, byť vyhovuje základní orientační specifikaci našeho testu pro síť s řádově desítkami uživatelů, představuje jednoznačně nejvýkonnější produkt zařazený do tohoto testu se základní propustností firewallu 1 000 Mb/s, resp. s výkonem 160 Mb/s při

## UTM firewally pro malé a střední firmy

Produkt	Firewall (SPI)	IPSec/SSL VPN	IPS/IDS	Antivirus/antispware	Web filtering/IM a P2P ochrana	Antispam	Propustnost	Současná sessions	Porty	Vysoká dostupnost A-P/A-A
Astaro Security Gateway 120	✓	✓/✓	✓	✓/✓	✓/✓	✓	200 (FW)/80 (IPS)/60 (VPN) Mb/s	90 000	4× Ethernet, 2× USB, COM, RS-232	✓/✓
Cyberoam CR100ia	✓	✓/✓	✓	✓/✓	✓/✓	✓	1 000 (FW)/300 (IPS)/200 (AV)/160 (UTM)/80 (3DES VPN) Mb/s	400 000	6× Ethernet, 2× USB, COM	✓/✓
D-Link Netdefend DFL-860	✓	✓/✗	✓	✓/✗	✓/✓	✗	150 (FW), 60 (VPN) Mb/s	25 000	10× Ethernet, 1× RS-232	✓/✓
Fortinet FortiGate-60B	✓	✓/✓	✓	✓/✓	✓/✓	✓	100 (FW)/70 (IPS)/20 (AV)/64 (3DES VPN) Mb/s	70 000	9× Ethernet, 2× USB, modem, PC Card	✓/✓
Juniper SSG5-SH	✓	✓/✗	✓	✓/✓	✓/✓	✓	160 (FW)/90 (IMIX FW)/40 (VPN) Mb/s	8 000	7× Ethernet, Console, Aux	✓/✓
McAfee Secure Firewall (Sidewinder) 210F	✓	✓/✗	✓	✓/✓	✓/✓	✓	170 (FW)/140 (filtering)/80 (VPN) Mb/s	150 000	4× Ethernet, Console	✓/✓
SonicWall NSA 240	✓	✓/✓	✓	✓/✓	✓/✗	✓	600 (FW)/195 (IPS)/110 (UTM)/150 (VPN) Mb/s	25 000	3× Gigabit Ethernet, 6× Fast Ethernet, 2× USB, Console	✓/✓
ZyXel ZyWall USG 100	✓	✓/✓	✓	✓/✓	✓/✓	✓	100 (FW)/24 (UTM)/50 (VPN) Mb/s	20 000	7× Gigabit Ethernet	✓/✗

plném zabezpečení prostřednictvím funkcí UTM. Koresponduje s tím také vyšší pořizovací cena, která ale těmto možnostem odpovídá – oproti tomu, pokud si vystačíte s nižšími hodnotami uvedených parametrů, v nabídce jsou i levnější varianty, které končí u modelu CR25i a CR15i s propustností firewallu 100 a 90 Mb/s.

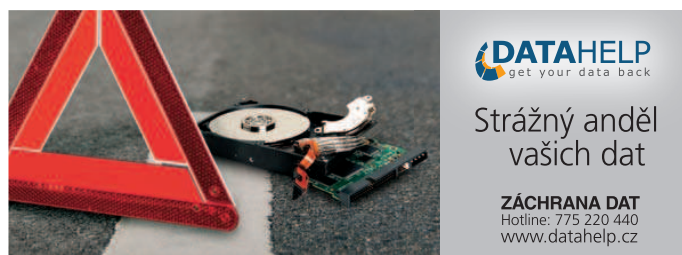
Těmto parametrům odpovídá také to, že produkt disponuje šestíci konfigurovatelných portů pro Gigabit Ethernet, a nutno dodat, že v rámci tohoto testu, byť se uvedeny standard stává stále běžnějším, se jedná o jeden z mála firewallů, které gigabitové rychlosti podporují. (Na druhé straně u většiny ostatních to s ohledem na propustnost není nijak citelným problémem.) Opět můžete použít konfiguraci s podporou fail-overu pro více internetových připojení, což ocení zákazníci nároční na dostupnost připojení.

Klíčovou vlastností je možnost integrace s Active Directory nebo LDAP/Radius databází a schopnost kontrolovat provoz a řídit vynucování politik na základě identity uživatele – zatímco běžné přístupy jsou založeny na IP adresách. Ta činí produkty této značky ideálními pro firmy, jež využívají síťové adresářové služby, jejichž správčům tento přístup značně usnadní život. Pravidla a kontroly pak lze můžete aplikovat na již existující skupiny uživatelů či jednotlivce a ověřování

probíhá přes protokol LDAP. Pro možnost kontroly uživatelů, kteří se v adresáři nenacházejí, lze využít klientské agenty (pro Windows nebo Linux), kteří autentizaci na základě identity umožní. Tento způsob kontroly může poskytnout dodatečnou úroveň ochrany i přesnější možnosti sledování aktivit uživatelů. Cyberoam ale samozřejmě podporuje i standardní kontrolu bez autentizace.

Kromě toho Cyberoam nabízí veškeré očekávané funkce včetně IPSec a SSL VPN, antivirový engine (Kaspersky), antispam (Comm-touch), flexibilní filtrování URL/obsahu a řízení šířky pásma. Zařízení nabízí předdefinované kategorie webových stránek a lze aplikovat i časová omezení. Nadprůměrné jsou možnosti reportingu, díky nimž můžete sledovat bezpečnostní incidenty i aktivitu uživatelů podle různých kritérií, a to i pomocí grafů.

Možnosti licencování jsou velmi pružné, počínaje platbou za jednotlivé funkce UTM, zvýhodněné balíčky Antivirus + Antispam případně Antivirus + IPS + Web & Application Filter až po kompletní UTM balík se všemi dostupnými funkcemi. Při nasazení dvou zařízení pak dochází ke zvýhodnění licencí v obou z nich, což je dobrou motivací pro



INZERCE

jejich nasazení v režimu aktivní/aktivní. Podpora zahrnuje technický support 8/5, přístup ke znalostní bázi, záruku na hardware a upgrady OS, signatur atd., nebo také vzdálenou diagnostiku při potížích. Nutno přitom konstatovat, že uváděná cena konfiguraci i možnostem tohoto UTM firewallu zcela odpovídá, můžete však sáhnout i po podstatně levnějších variantách.

k dispozici DMZ a sedm LAN portů, gigabitových rychlostí se zde však nedočkáte. Základní propustnost firewallu činí 150 Mb/s, u 3DES/AES VPN je to 60 Mb/s. Alespoň s ohledem na doporučenou cenu je nutno konstatovat, že výkonnostní parametry nijak závažně nejsou, nicméně akcelerace IPS se při našem testování projevovala velmi pozitivně. Řízení šířky pásma dovoluje prioritizovat provoz, definovat maximální či garantovat potřebnou šířku pásma pro určité typy provozu.



Fortinet FortiGate-60B

### D-Link Netdefend DFL-860

UTM firewall D-Linku se se svou propustností pohybuje zhruba uprostřed startovního pole (nepočítáme-li dva nejvýkonnější produkty, které z něj vybočují) a nabízí poměrně ucelenou škálu funkcí. Stavový firewall DFL-860 podporuje také zabezpečení na aplikační vrstvě (ALG) a díky funkci ZoneDefense se je ve spolupráci s přepínači xStack stejného výrobce schopen zajistit izolaci infikovaných počítačů v síti – na to však mohou spoléhat pouze zákazníci navázaní čistě na síťové produkty D-Linku. Nechybí detekce a prevence průniků, která využívá hardwarový akcelerator, ani engine pro skenování virů ve streamu (Kaspersky) a filtr webového obsahu. Na straně VPN je podporován pouze protokol IPSec/PPTP/L2TP, nikoliv SSL, ale zato můžete využít až nadstandardních 300 tunelů. Podporováno je šifrování DES, 3DES, AES, Blowfish, Twofish a CAST-128 a autentizace uživatelů proti Radius serveru, LDAP, Active Directory nebo lokální databázi.

Dvojice WAN portů může být nakonfigurována pro zvýšení dostupnosti a fail-over včetně možnosti rozkládání zátěže, dále je

Tento UTM firewall bude dobrou volbou pro uživatele switchů D-Linku, kteří kombinací těchto produktů mohou získat zvýšenou úroveň zabezpečení. Mezi klady můžeme zmínit pětiletou záruku zahrnující i výměnu do druhého dne.

Antivirus, IPS i filtrování obsahu jsou licencovány zvlášť, nelze ale počítat se zvýhodněním při provozu dvou redundantních UTM. Naproti tomu však výrobce neklade žádná další licenční omezení na využití dostupných možností a pro prvních 90 dnů nabízí zmíněné licence zdarma.

### Fortinet FortiGate-60B

Fortinet patří na trhu UTM firewallů k zavedeným pojmům, přičemž model FortiGate-60B ukazuje, že ač je výrobce schopen prosadit se velmi dobře ve výkonnostních testech UTM pro podnikové prostředí, myslí také na menší zákazníky, jimž je schopen poskytnout kompletní ochranu postavenou na bázi své platformy FortiOS a hardwaru využívajícím speciální ASIC čipy. K dispozici jsou všechny potřebné prvky zabezpečení včetně stavového firewallu, IPS, IPSec i SSL VPN (podporováno je maximálně 40 tu-

Záruka na hardware	Cena zařízení (bez DPH)	Cena licencí (na rok, bez DPH)	Prodejce
2 roky	1 195 eur	Web Security 575 eur, Email Security 445 eur	Annex Net, <a href="http://www.annexnet.cz">www.annexnet.cz</a>
1 rok	54 890 Kč	UTM bundle 27 610 Kč	Comguard, <a href="http://www.comguard.cz">www.comguard.cz</a>
5 let	25 298 Kč	Antivirus 4 247 Kč, IPS 4 247 Kč, Content filtering 4 247 Kč	D-Link, <a href="http://www.dlink.cz">www.dlink.cz</a>
1 rok	626 eur	Firewall (hardware) + licenční bundle 896 eur	SkyNet, <a href="http://www.skynet.cz">www.skynet.cz</a>
1 rok	900 dolarů	UTM bundle 543 dolarů	Soft-tronik, <a href="http://www.soft-tronik.cz">www.soft-tronik.cz</a>
3 roky	59 000 Kč	Antivirus 550 Kč/uživatel (pro 101 – 250 uživatelů), IPS 21 490, URL Filtrace 1 620 Kč/ /uživatel Kč (vše perpetuální licence)	Comguard, <a href="http://www.comguard.cz">www.comguard.cz</a>
1 rok	1 231 dolarů	UTM 592 dolarů	SonicWall, <a href="http://www.sonicwall.com">www.sonicwall.com</a>
5 let	11 390 Kč	IDP 1 250 Kč, Antivir ZyXEL 1 950 Kč nebo Antivir Kaspersky 2 390 Kč, Content Filtering 1 630 Kč	ZyXel, <a href="http://www.zyxel.cz">www.zyxel.cz</a>