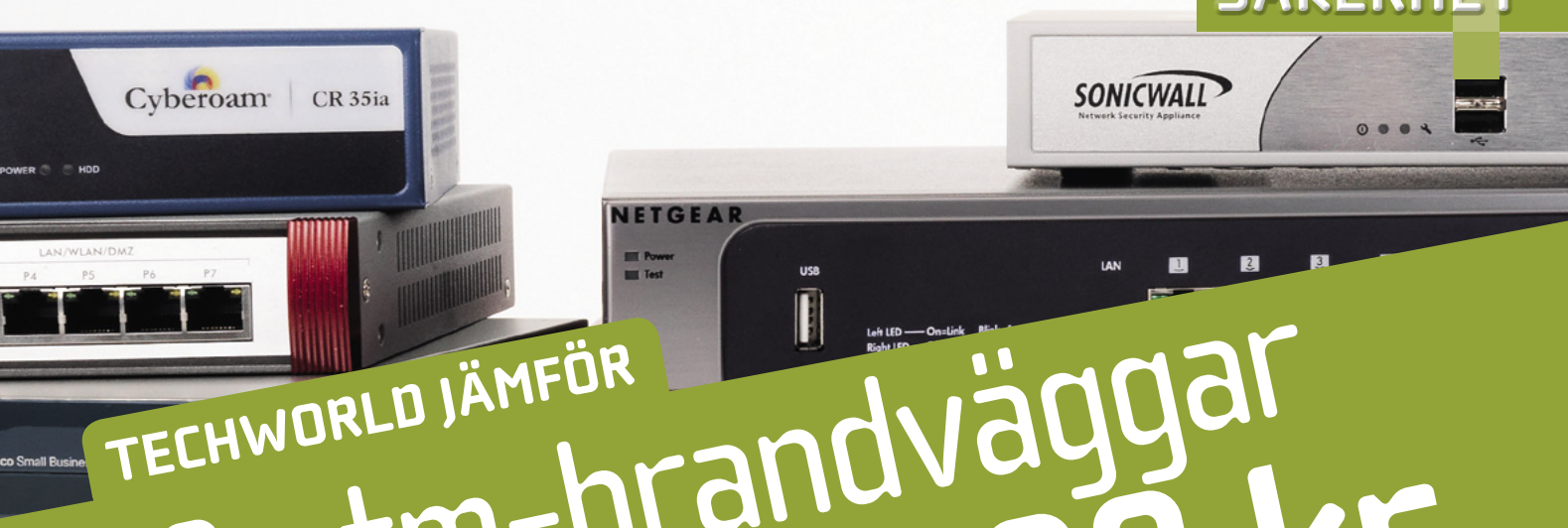
Särtryck ur
TechWorld nr 7-2010

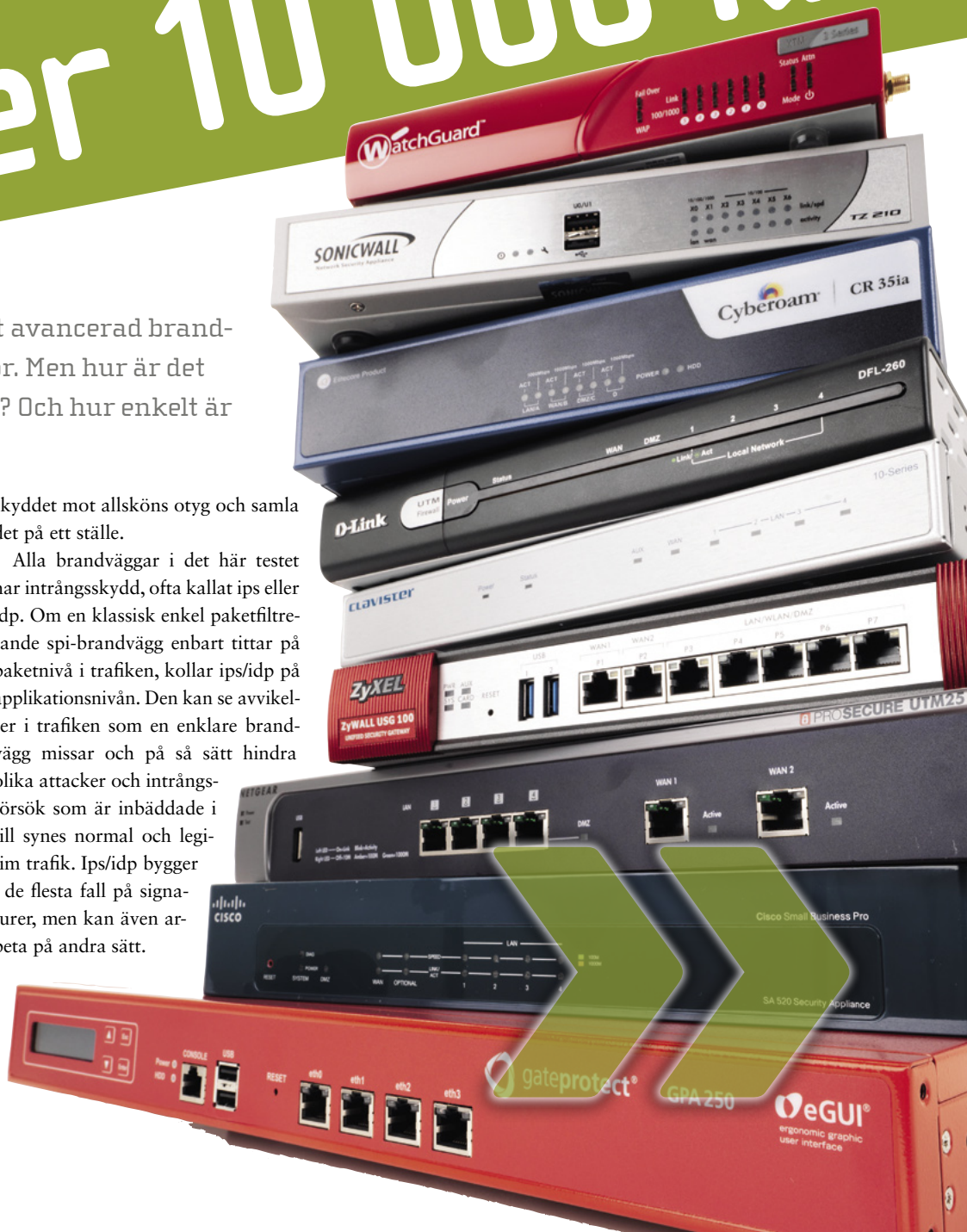
Publikation är utgiven av IDG
– världens största mediehus
inom IT/teknik, miljö och affärer

SÄKERHET



TECHWORLD JÄMFÖR

10 utm-brandväggar under 10 000 kr



Numera kan du få en riktigt avancerad brandvägg för under 10 000 kronor. Men hur är det egentligen med prestandan? Och hur enkelt är det att sätta upp väggen?

Billiga brandväggar brukar varken kunna stoppa avancerade intrångsförsök, virus, spam eller trafik med olämpligt innehåll. Men sedan några år har brandväggar med så kallat utm-skydd sjunkit till riktigt trevliga prisnivåer. Utm står för unified threat management och är ett mycket vagt definierat begrepp. I sin vidaste mening handlar det om att ta ett helhetsgrepp om skyddet mot allsköns otyg och samla det på ett ställe.

Alla brandväggar i det här testet har intrångsskydd, ofta kallat ips eller idp. Om en klassisk enkel paketfiltrerande spi-brandvägg enbart tittar på paketnivå i trafiken, kollar ips/idp på applikationsnivån. Den kan se avvikelser i trafiken som en enklare brandvägg missar och på så sätt hindra olika attacker och intrångsförsök som är inbäddade i till synes normal och legitim trafik. Ips/idp bygger i de flesta fall på signaturer, men kan även arbeta på andra sätt.

Scenario

Ett litet företag med 12 anställda behöver ny brandvägg. Företaget har en person som sköter it-strukturen, som består av fyra servrar plus de anställdas datorer. Man vill köra utm-skydd för att minimera arbetet med att säkra av enskilda datorer, och man behöver två vpn-tunnlar. Budgeten för brandväggen ligger på 10 000 kronor för inköpsåret.

Alla brandväggar i testet utom en, Cisco SA520, kan göra realtidsskanning efter virus i trafiken som passerar. Cisco arbetar på ett annat sätt med virusskydd, där brandväggen i stället håller koll på virusskyddet i klientdatorerna. Endast klienter med uppdaterat virusskydd tillåts ta emot trafik. Det här innebär att prestandamätningarna för Cisco SA520 inte riktigt kan jämföras med de övriga, men resultaten visar ändå på en poäng i Ciscos arbetssätt: realtidsskanning kostar ofta väldigt mycket prestanda i förhållande till vad det ger i säkerhet. Vi anser att virusskanning i brandväggen i de flesta miljöer knappast kan ersätta lokalt virusskydd i varje klient, inte så länge det finns bärbara datorer som både används innanför och utanför brandväggens skydd. Värt att notera är att även Zyxel USG-100 kan hålla koll på klienternas virusskydd.

Söka i realtid har poänger

Även om realtidsskanning inte innebär att man kan ta bort lokalt virusskydd i klientdatorer, anser vi att det kan ha sina poänger. Många företag har inte snabbare internetuppkoppling än att flera av brandväggarna i testet faktiskt kan virusskanna trafiken utan att sänka prestanda nämnvärt. Även om man också har ett virusskydd lokalt i klienterna känns det extra tryggt att inte i onödan släppa in skadlig kod i nätverket.

"Vi har koncentrerat oss på de två mest intressanta formerna av skydd: intrångs- och virusskydd."

De flesta av brandväggarna i testet erbjuder även olika former av skräpfiltrering och innehållsfiltrering. Det förstanämnda kan vara en bra hjälp, men också vara lurigt om du vill ha full koll på vilken typ av skräp det är du får. Slänger brandväggen bort misstänkt spam tappar du den informationen. Innehållsfiltrering är vi tämligen skeptiska mot – den har ofta en tendens att sila mygg och svälja kameler.

Vi har i det här testet koncentrerat oss på de två, i våra ögon, mest intressanta formerna av skydd: intrångsskydd och virusskydd. Vi har tittat på hur enkelt det är att komma igång med de skydden och hur det påverkar prestanda.

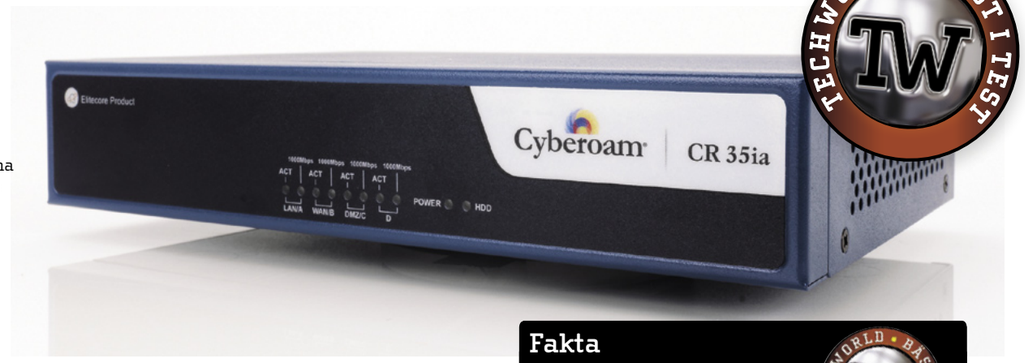
Så gjorde vi testet

Testet avser främst prestandamätningar med och utan utm-funktioner plus bedömning av gränssnitten.

Prestandamätningarna bestod i att köra ftp-trafik genom brandväggarna. Som ftp-server körde vi Freeftpd, som klient Filezilla. Våra testdata var ett stort katalogträd på drygt 200 megabyte med en mängd underkataloger och totalt runt 300 små och stora filer, varav några zip-filer.

Det här innebär en massa tcp-sessioner att öppna och stänga, virusskanning av många filer plus uppackning av zip-arkiv.

Rutininställningarna som vi gjorde var att ange adresser för de olika gränssnitten (wan, test-lan och admin-lan). Vi gick även igenom aktivering av intrångs- och virusskydd samt hur det går till att skapa brandväggsgregler eller portforwarding för http-trafik till en tänkt webbserver i en dmz.



Cyberoam CR35ia har en wan-port, en lan-port, en dmz-port, en port som kan ha valfri roll plus en konsolport för rj-45-konktakt samt en usb-port.

Cyberoam – CR35ia

Cyberoam CR35ia är tillsammans med Watchguard dyrast i vårt startfält, både i inköp och i årskostnad. Men du får rejält med prestanda för pengarna. I genomströmningsmätningen fick vi över 100 megabit/sekund med utm-skydd aktivt – fantastiskt i den här prisklassen.

Webbgränssnittet är tydligt och intuitivt vilket gör administrationen enkel. Det tog oss mindre än fem minuter att lista ut hur intrångs- och virusskydd aktiveras, och då tittade vi inte i instruktionerna alls. En trevlig detalj att notera är att Cyberoam har gott om användbara standardinställningar som skickas med vid leverans, som färdiga regeluppsättningar för ipsec-vpn.

Cyberoam CR35ia blir bäst i test tack vare en kombination av bra prestanda och en rättfram och intuitiv administration. Den är ett dyrt men mycket bra val.

Fakta

Tillverkare: Cyberoam
Kontakt: www.cyberoam.com
Modell: CR35ia
Cirkapris: 8 550 kr
Garanti: 12 månaders garanti
Anslutningar: 1 wan, lan, dmz, 1 valfri roll, 1 usb, 1 konsolport för rj-45-konktakt
UTM - Kostnadsmodell: Årliga separata licenser för ips, virusskydd, spamskydd samt webb- och applikationsfilter
UTM - Priser: Hela skyddspaketet plus support 3538 kr/år. De olika delarna går även att köpas separat.
UTM - Leverantör av virusskydd: Kaspersky
VPN - Trafikkapacitet: 80 Mbit/sek
VPN - Kostnad för klienter: Kostnadsfritt
VPN - Antal samtidiga tunnlar: 50

Mätningar

Tillverkare		Cisco Systems	Clavister	Cyberoam	D-Link	Draytek	Gateprotect	Netgear	Sonicwall	Watchguard	Zyxel
Modell		Small Business Pro SA520	SG 15	CR35ia	DFL-260 NetDefend	Vigor Pro 5300	GPA 250	ProSecure UTM25	TZ210	XTM 22	Zywall USG-100
Genomströmning											
Många sessioner utan utm	Mbit/sek	131,73	68,84	119,22	66,69	44,93	129,34	85,36	94,85	58,47	71,13
Många sessioner med utm	Mbit/sek	32,02	28,64	37,44	27,36	7,79	8,52	13,72	15,19	37,44	22,7
Maxfart utan utm	Mbit/sek	234,51	58,47	194	52,69	45,89	237,12	90,81	105,39	46,9	65,66
Maxfart med utm	Mbit/sek	93,37	34,2	103,2	31,12	19,74	0	15,01	14,74	59,42	22,98
Energiförbrukning											
Drift	watt	12,4	6	24,8	9,6	6,8	30,3	12,9	7,3	10,5	11,2

Obs! Mätvärdena för Cisco SA520 bör inte rakt av jämföras med övriga i och med att de saknar virusskanning.

Techworlds slutsats

Prisnivåerna i vårt startfält är klart trevliga. Draytek ger med ett inköpspris under 3000 kronor det överlägset billigaste skyddet och klarar sig trots detta med hedern i behåll i prestandamätningarna. Fyra deltagare, Clavister, D-link, Netgear och Zyxel, ligger runt 5000 kronor i inköpspris, och av dem är det Zyxel som sticker ut positivt med riktigt bra prestanda, enkel administration och en låg årskostnad.

Årskostnaderna varierar annars en hel del och du bör ställa dig frågan hur mycket realtidsskydd du vill betala för. Intrångsskydd ska du ha, det är ett bra skydd som är värt varenda krona. Virusskanning kan vara mer tveksamt om budgeten är snäv. Du kommer ändå att behöva någon form av virusskydd i klienterna, i synnerhet om du har bärbara datorer som ibland befinner sig utanför brandväggen. Fördelen med skydd även i brandväggen är att den automatiskt hålls bra uppdaterad och tar bort problem redan innan de släppts in i nätverket.

Testvinnaren Cyberoam CR35ia är dyr, både att köpa och i årskostnad, men ger mycket för pengarna och är överraskande enkel att använda. Detsamma kan sägas om Watchguard XTM 22 som är en hårsmån från att ta utmärkelsen från Cyberoam. Dessutom utmärker sig Zyxel Zywall USG-100 genom att vara enkel att använda och ge mycket bra prestanda, men ändå ha låga kostnader både för inköp och för uppdateringar. Fast det riktiga budgetvalet är ändå den långsammare men otroligt billiga Draytek Vigor Pro 5100.

Betyg

Tillverkare		Cisco Systems	Clavister	Cyberoam	D-Link		Draytek	Gateprotect	Netgear	Sonicwall	Watchguard	Zyxel
Modell		Small Business Pro SA520	SG 15	CR35ia	DFL-260 NetDefend		Vigor Pro 5300	GPA 250	Pro Secure UTM25	TZ210	XTM 22	Zywall USG-100
Prestanda	30	22	22	27	21		12	14	14	15	25	17
Funktioner & finesser	20	8	15	15	15		17	16	15	16	18	16
Uppstart	30	22	10	24	16		24	20	25	20	22	24
Administration	20	15	8	14	8		14	12	15	12	12	14
Totalt	**100**	**67**	**55**	**80**	**60**		**67**	**62**	**69**	**63**	**77**	**71**
Fördelar		Inköpspriset, prestanda	Årskostnaden	Prestanda, lätt att komma igång	Ångra-funktion i gränssnittet, årskostnaden		Inköpspriset, årskostnaden, snabbt gränssnitt	Trevligt gränssnitt	Lätt att komma igång, snabbt gränssnitt	Flera konfigurationsguider	Prestanda, wi-fi	Inköpspriset, årskostnaden
Nackdelar		Ingen virusskanning	Bökig uppstart, krävande konfiguration	Dyr i inköp, hög årskostnad	Krävande konfiguration		Prestanda	Oklar årskostnad, prestandaproblem	Prestanda	Prestanda	Segt gränssnitt, hög årskostnad	Inga särskilda