

Virksomhedens

En firewall kan antage mange former. En af dem er såkaldte appliances, en hardware-enhed med integreret firewall-software. Vi har kigget syv sådanne firewall-appliances til større virksomheder efter i sømmene

AF ANDREAS OTT
andreas.ott@altomnet.dk

Markedet for firewalls er nærmest eksploderet over de seneste år. Det er der god grund til, for risikoen ved at være koblet op til Internet er reel nok. En firewall er og har derfor altid været en af grundpillerne i virksomheders sikkerhedsinfrastruktur. Vi har i tidens løb gentagne gange skrevet om firewalls – både fra en teknologisk synsvinkel og i form af produktanmeldelser.

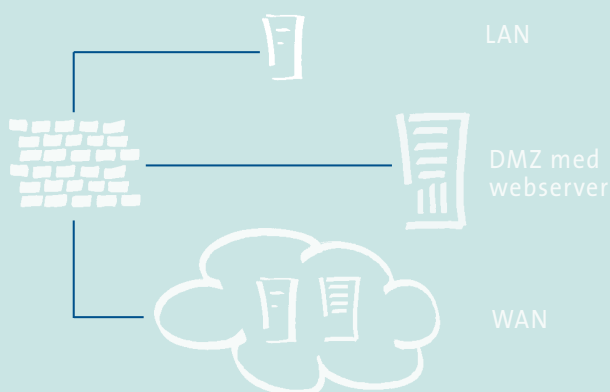
For nogle år siden var en firewall næsten altid et stykke software, der skulle installeres på en særskilt server med UNIX eller Windows NT som styresystem. Mens disse software-baserede firewalls stadig kan fås, er en forholdsvis ny produktgruppe hurtigt blevet populær. Firewalls som appliance, der ofte kun kræver en grundkonfiguration for at virke, kan fås i mange forskellige størrelser og prislæg. Vi har til denne artikel samlet seks firewall-appliances, som er beregnet til mellemstore og større virksomheder, og testet dem med henblik på sikkerhed og brugervenlighed. Derudover har vi sammenlignet, hvad de ellers har at byde på.

De indbudte

Målet har været at teste firewalls, der er beregnet til virksomheder med op til 1000 medarbejdere. Desuden skulle



brandmur



Figur 1: Testopsætningen bestod af en pc på firewall'ens inderside, en DMZ med en webserver og et simuleret WAN med en klient og en webserver.

firewall'en understøtte Virtual Private Netværk (VPN), således at virksomhedens mobile medarbejdere har mulighed for at etablere sikre forbindelser til kontoret. Endelig skulle firewall'en være i stand til at håndtere en såkaldt demilitariseret zone (DMZ), hvor virksomhedens web- og/eller mailservers kan placeres i et særskilt netværkssegment.

I testen deltog 3Com SuperStack 3 Firewall, stillet til rådighed af 3Com Danmark, GNAT Box GB-1000, venligst udlånt af distributøren RanTek Aps, og Lucent Brick 80, stillet til rådighed af producentens danske afdeling. Endvidere stillede Tempest A/S både en SonicWall PRO-VX og en Symantec Velociraptor V1.1 til rådighed, og SEC Datacom lånte os en WatchGuard Firebox 1000.

Vi takker i den anledning alle involverede producenter og distributører for udlån af enheder og velvillig assistance. Vi ville også gerne have haft PDS-appliance fra Intrusion.com med, men den danske distributør, Swanholm, takkede nej, ligesom vi heller ikke kunne bevæge Cisco Systems Danmark til at låne os et af deres passende firewall-produkter – som f.eks. Secure PIX Firewall 501 eller 525.

Testen blev udført i november måned. I testopsætningen indgik desuden to test-pc'er fra Alt om NET & PC PROs

testcenter samt diverse andet udstyr. En særlig tak til VIGILANTE som stillede deres sikkerhedsscanner SecureScan NX til rådighed og ligeledes bistod med teknisk assistance.

Sådan testede vi

Som nævnt indledningsvis gik testen dels ud på at få et indtryk af produkternes betjening og brugervenlighed, dels skulle sikkerheden afprøves. Alle firewalls blev installeret i en trebenet testopstilling som skitseret i figur 1. Samtlige produkter er grundlæggende udstyret med tre eller fire Ethernet-porte. Hos nogle produkter er portene fast konfigureret som indersiden, ydersiden og DMZ. Andre firewalls har kun det ydre interface fast konfigureret, og den sidste gruppe er frit konfigurerbar på alle porte.

Under opsætning af den skitserede testopstilling lærte vi produkterne at kende og kunne dermed bedømme graden af kompleksitet for at nå i mål. Der er i øvrigt taget højde for risikoen for at begå fejlkonfigurationer, der enten slet ikke virker, eller som åbner for utilsigtede forbindelser.

I bedømmelsen indgik kvalitet af håndbøger og skærmhjælp, idet det er vigtigt at have overblik over, hvordan

man konfigurerer sin firewall hensigtsmæssigt.

Men frem for alt skulle sikkerheden testes, og det gjorde vi med SecureScan NX fra Vigilante, som vi omtalte i Alt om NET nr. 12/2001 (se også rammen "Sikkerhedsscanning med SecureScan NX" andetsteds i artiklen).

På firewall'ens inderside havde vi en pc, som primært blev brugt til administration af firewall'en. Pc'en tjente dog også som SecureScan Agent. I DMZ'en installerede vi en webserver, der skulle være tilgængelig fra både LAN og WAN. Da webserveren var på et privat netværk, skulle der i de fleste tilfælde oprettes en adressekonvertering på firewall'en.

Også på webserveren installerede vi en SecureScan Agent. Det simulerede WAN eller Internet bestod af en klient-pc, hvorfra SecureScan NX Console blev kørt, samt en ekstern webserver for at kontrollere, at der var "hul igennem ud af huset". Når denne testopsætning fungerede tilfredsstillende, kørte vi sikkerhedsscanningen uden at implementere yderligere forholdsregler. Resultaterne af sikkerhedstesten fremgår i skemaet, hvor der oplyses, hvor mange sårbarheder der blev fundet i risikokategorierne høj, mellem og lav. >

3Com SuperStack 3 Firewall



Den hvide SuperStack 3 Firewall i 3Coms velkendte design er udstyret med tre deciderede porte til henholdsvis WAN, LAN og DMZ. Alle tre porte er forsynet med Uplink/Normal-omskiftere, således at der både kan kobles enkelte maskiner eller en hub/switch til. Enheden, der både kan monteres i rack eller stå på et bord, er desuden udstyret med en "Redundant Power Socket" (RPS), dvs. mulighed for at tilslutte en redundant strømforsyning.

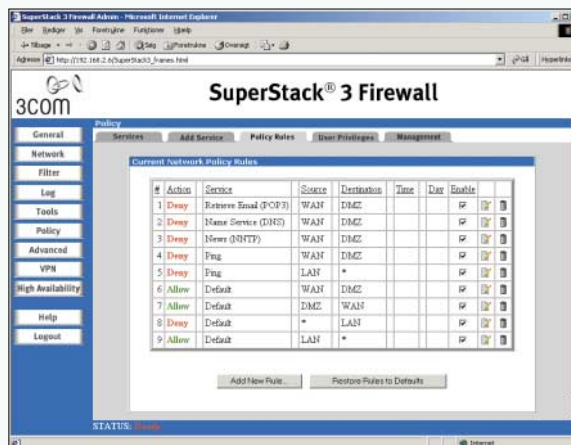
Opsætningen af 3Com SuperStack 3 Firewall er enkel. Fra fabrikken er den på indersiden konfigureret til adressen 192.168.1.254, således at den straks er tilgængelig fra en pc, der er på samme netværk. Konfigurationen finder sted i en browser, men de grundlæggende parametre kan også indtastes ved hjælp af en JavaScript-baseret wizard. Den HTML-baserede administrationsmenu er den samme, som findes i 3Coms mindre firewalls samt SonicWall-produkter. Det er da også SonicWall, der står bag softwaren, som nu videreudvikles af de to virksomheder i et samarbejde.

Menuen er enkel og ligetil, således at man for de fleste funktioners vedkommende ikke behøver at fordybe sig i manualer og håndbøger. De fleste menupunkter til venstre har en række underpunkter, der er symboliseret ved faneblade. Overordnet er opdelingen logisk, selv om få punkter måske forventes placeret et andet sted, end hvor

de befinder sig. Firewall-regler sættes op under menupunktet Policy. Som udgangspunkt er SuperStack 3 Firewall åben for udgående trafik og lukket for al indgående trafik. Dertil kommer eventuelt regler, der automatisk genereres ud fra indstillingerne til eksempelvis DMZ. Man har desuden mulighed for at tilpasse og oprette egne regler på ganske uproblematisk vis. Ud over de gængse applikationer og tjenester kan man oprette egne, protokolbaserede tjenester, som kan indgå i regelsættet. Trafikken kan desuden reguleres samlet for et netværksinterface eller særskilt for henholdsvis en IP-adresse eller et adresserum. Ved hjælp af en simpel brugerstyring kan man oprette privilegerede brugere, som eksempelvis gives tilladelse til at omgå reglerne.

En af SuperStack 3 Firewalls særlige funktioner er filtering af uønsket indhold. Dels kan man med et abonnement hos CyberNOT valgfrit frasortere nøgenhed, vold, grimt sprog og de andre velkendte kategorier, dels kan man generelt blokere for Java, ActiveX eller andre web-teknologier.

Endelig kan man ved hjælp af en række indstillinger under "High Availability" koordinere to SuperStack 3 Firewalls, således at man får en redundant opsætning med automatisk fail-over.



En enkel og intuitiv webbrugerflade finder man hos 3Com SuperStack 3 Firewall, der bygger på softwaren fra SonicWall.



SonicWall PRO-VX

SonicWall PRO-VX vil næppe vinde en designpris. Enheden er tydeligvis beregnet til at blive monteret i et rack. Men når det er sagt, så er denne firewall faktisk meget nem at have med at gøre. Ligesom 3Coms firewall er også SonicWall PRO-VX udstyret med tre dedikerede porte til henholdsvis WAN, LAN og DMZ. Ulig SuperStack 3 Firewall finder man her desuden en seriel konsolport.

Takket være softwaren, som 3Com som nævnt har licensieret, minder betjeningen af SonicWall PRO-VX og 3Com SuperStack 3 Firewall utrolig meget om hinanden. Opsætningen af SonicWall PRO-VX foregår derfor også på lignende vis.

Firewall'en er konfigureret med 192.168.168.168 som LAN-adresse. En pc, der er indstillet med en adresse på samme netværk, kan kobles til LAN-porten, hvorefter en opsætningsguide indsamler de nødvendige oplysninger. Alternativt må opsætningen også kunne gennemføres ved hjælp af konsolporten, men denne fremgangsmåde er desværre ikke beskrevet i dokumentationen.

Når grundkonfigurationen er på plads, kan man logge på administrationsbrugerfladen ved hjælp af en browser. Som nævnt er administrationsmenuen bygget op på samme vis som i 3Com SuperStack 3 Firewall. Men små forskelle er der alligevel. Til at begynde med tilbyder SonicWall i samarbejde med McAfee en virusbeskyttelse, som

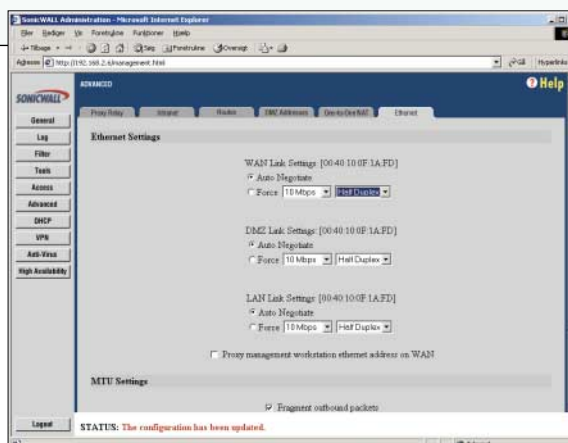
er integreret i firewall'en. Det kræver et abonnement, men køb af en SonicWall PRO-VX berettiger til en gratis forsøgsperiode.

En anden særlig funktion, som ikke findes i 3Com SuperStack 3 Firewall, er ViewPoint logserveren. Selve serversoftwaren, som skal installeres på en Windows 2000 eller Windows NT 4.0 Server, kan hentes gratis på SonicWalls hjemmeside. Efter installation af serveren kan SonicWall PRO-VX konfigureres til at sende loginformationer via syslog-protokollen til serveren, hvor de præsenteres. ViewPoint-systemet er dermed et værdifuldt supplement til firewall'ens indbyggede logfunktion.

Endelig er der en række andre små ekstrafunktioner, som eksempelvis indstilling af Ethernet-porte, mulighed for at lave rapporter over brugsmønstre samt understøttelse af SNMP. Desuden kan man konstatere, at funktionerne overordnet er mere logisk placeret i administrationsmenuen, end det er tilfældet ved 3Com SuperStack 3 Firewall.

Med hensyn til sikkerhed ligger SonicWall PRO-VX på samme måde som 3Com SuperStack 3 Firewall og WatchGuard Firebox 1000 i absolut topklasse, hvor SecureScan NX ikke var i stand til at finde svagheder.

På trods af samarbejdsaftalen mellem 3Com og SonicWall er SonicWalls egen software både nyere og omfatter flere funktioner.



VelociRaptor-modellerne stammer fra opkøbet af Axent Technologies, som Symantec købte for lidt over et år siden. Men også Axent Technologies købte i sin tid firewall-producenten Raptor, således at VelociRaptor indirekte har en lang historie bag sig.



Den citrongule VelociRaptor V1.1 kan monteres i et rack, på væggen eller stilles på et bord. Men selv om designet og muligheden for frontbetjening kunne antyde noget andet, hører denne firewall nok mest til i et serverrum. VelociRaptor V1.1 er udstyret med en hørbar blæser, der dog ikke er helt så støjende som nogle af de andre produkter.

Ud over et eksternt og et internt interface rummer VelociRaptor to yderligere Ethernet-porte, som frit kan konfigureres. Dertil kommer to serielle porte, hvoraf den ene er beregnet til en konsolforbindelse og den anden til styring af en UPS-enhed.

På frontsidens finder vi et LCD-display og en række knapper. Ved hjælp af disse kan man under grundkonfigurationen indtaste en IP-adresse for VelociRaptor. I den daglige drift kan man desuden se statusoplysninger, boote eller slukke enheden, samt genetablere fabriksindstillingerne. Står VelociRaptor et sted, hvor uvedkommende har adgang, kan betjening via frontpanelet dog også slås fra.

Når IP-adressen er indtastet på frontpanelet får man udleveret adgangskoden til Symantec Raptor Management Console (SRMC). Endvidere får man adgangskoder til Secure Remote Login (SRL) samt root-adgang. Der er altså en del adgangskoder at holde styr på – heldigvis kan de foreslåede kryptiske koder senere hen ændres til noget, man kan huske.

Efter overstået grundkonfiguration skal man installere SRMC, som automatisk integreres i Microsoft Management Console (MMC) under Windows 2000. Første gang man etablerer forbindelse til firewall'en gennemgår man en guide, hvor man skal indtaste licensnøgle, værtsnavn og andre informationer. Desuden har man mulighed for at konfigurere de øvrige porte. Endelig kan guiden automatisk oprette en regel, der giver det interne net tilladelse til at bruge eksterne web- og FTP-servere, ligesom guiden også klarer opsætning af regler for en intern mailserver.

Til den videre konfiguration er man dog i høj grad overladt til sig selv. Den medfølgende håndbog dækker

kun betjening af de egentlige funktioner, uden at komme nærmere ind på hvordan og til hvilket formål de bruges. Lidt bedre er skærnhjælpen til de enkelte dialogvinduer. Alligevel tog det sin tid at gennemføre den ønskede konfiguration. Der er mange parametre og muligheder for konfiguration af firewall'en. Det giver naturligvis stor fleksibilitet, men når dokumentationen er så sparsom, er der ikke meget andet at gøre end at prøve sig frem eller søge eksternt hjælp.

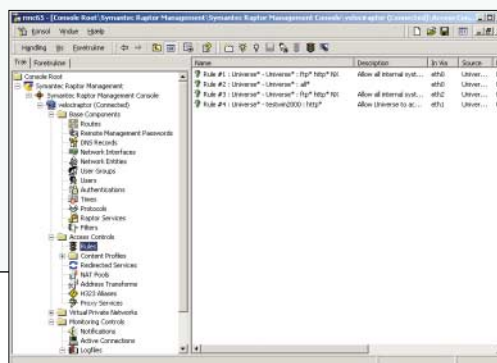
Alle funktioner er som nævnt integreret i SRMC. Dog har man mulighed for at gennemse eller rette konfigurationsfilerne direkte på VelociRaptor, der i øvrigt er baseret på et hærdet Linux 2.2-system. Endvidere har man mulighed for at logge sig på, idet SRMC har terminalprogrammet TeraTerm indbygget – til brug for en Secure Remote Login. En SRL er den eneste måde at bruge programmer som eksempelvis ping og traceroute på.

I sikkerhedstesten har SecureScan NX fundet tre højt prioriterede sårbarheder, tre mellem og en lavt prioriteret sårbarhed. Dermed ligger VelociRaptor i bunden af vore sikkerhedsmålinger. Dertil skal dog siges, at i hvert fald nogle af sårbarhederne er rent teoretiske og skyldes, at VelociRaptor som proxy-firewall automatisk svarer på forespørgsler via en del porte.

Symantec VelociRaptor findes i tre størrelser, model 500, model 700 og model 1000. Selv om vi til testen lånte en model 1000, er prisen beregnet ud fra model 700, der i de tekniske specifikationer bedst svarer til de øvrige produkter. I prisen er indregnet 27.923 kroner for VPN-opgradering, der ikke er med som standard. Til gengæld kan VelociRaptor 700 arbejde med et ubegrænset antal VPN-tunneler, ligesom antallet af almindelige sessioner heller ikke er begrænset.

Symantec VelociRaptor V1.1

Symantec Raptor Management Console (SRMC) integreres fuldt i Microsoft Management Console.





GTA GNAT Box GB-1000

Global Technology Associates (GTA) producerer firewall-produktet GNAT Box, som kan fås som software-løsning, som flash-kort eller i form af to appliances, hvoraf vi lånte den ene til testen. Set forfra er GB-1000 en forholdsvis kedelig kasse, men indeni gemmer der sig en diskløs pc med et styresystem, der har sine rødder i FreeBSD. GB-1000 er udstyret med fire frit konfigurerbare netværksporte, en konsolport, samt en USB og en parallelport, som dog er reserverede og ikke umiddelbart kan anvendes til eksterne enheder. Til gengæld er firewall'en udstyret med en ekstra serielport, hvor man ved hjælp af et modem kan indrette en pager-funktion. Når man tænder for GB-1000 kan man ikke undgå at lægge mærke til den kraftfulde blæser, som holder enheden kølig, men som samtidig larmer så meget, at man næppe kan placere enheden andet steds end i et serverrum.

Grundkonfigurationen foregår ved at tilslutte en pc til GB-1000's første Ethernet-port, der er indstillet på adressen 192.168.71.254. Alternativt kan man også konfigurere firewall'en ved hjælp af en konsolforbindelse. På grund af en velkendt fejl i Windows' terminalprogram HyperTerminal fungerer enhedens menu-styrede terminalapplikation dog ikke optimalt i dette program. Ønsker man at konfigurere GNAT Box fra konsollen, er det derfor bedre at bruge sharewareprogrammet TeraTerm, som følger med på GNAT Box'ens cd-rom.

Ellers er der både en web-baseret administrations-menu samt en Windows-applikation til administration af GNAT Box, så der er frit valg på alle hylde. På trods af de tre forskellige menuer, er betjeningen kon-

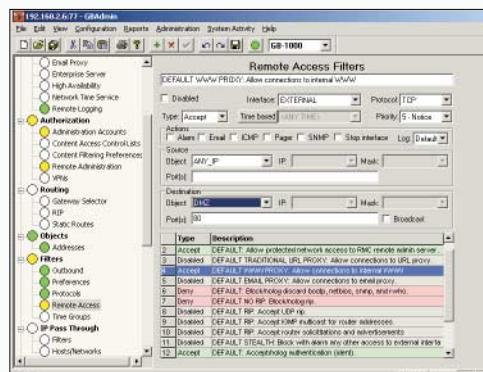
sistent og forholdsvis intuitiv. Mens GB-1000 principielt kan konfigureres ved hjælp af alle tre værktøjer, giver Windows-applikationen GBAdmin størst betjeningskomfort. GBAdmin er et managementsystem, som godt kan tåle sammenligning med store og dyre systemer.

På trods af den forholdsvis enkle betjening er der mange parametre at holde styr på. Det giver på den ene side en uhyre stor fleksibilitet i opsætning af firewall'en, på den anden side kræver det lidt viden om regler, routning og protokoller. Uden den viden – eller viljen til at læse sig til den – er der fare for, at man sætter boksen forkert op og lukker op for utilsigtede tjenester. For at undgå de værste brølere har GNAT Box en valideringsfunktion, hvor man kan få vist fejl og advarsler ved fejlagtige konfigurationer.

Desuden har man ved hjælp af en detaljeret logføring mulighed for at følge med i, hvordan firewall'en reagerer. Logdata kan i øvrigt ved hjælp af syslog-protokollen også sendes til en anden maskine på lokalnettet.

Endelig kan flere GB-1000-enheder sættes sammen til en High Availability-klynge, hvor man ved hjælp af et redundant backup-system kan sikre sig mod driftsudfald.

Sikkerhedsmæssigt er der ikke meget at komme efter. Målingen viste to mindre svagheder i grundkonfigurationen, som uden videre kan fjernes ved at ændre konfigurationen tilsvarende. Hvis man skulle kritisere noget, kunne man ønske sig en papirudgave af betjeningsvejledningen. Med i leveringsomfanget er blot en opstartsguide, mens den egentlige håndbog er temmelig godt gemt på den medfølgende cd-rom.



GNAT Box' administrationsværktøj GBAdmin kan ved første øjesyn virke lidt overlæst. Men programmet gemmer på mange nyttige og brugervenlige funktioner.



WatchGuard Firebox 1000

Den røde kasse med det futuristiske display er en fryd for øjet, og hvis det ikke var for dens lidt højlydte blæser, kunne man fint have Firebox 1000 stående på skrivebordet. Men firewall'en hører til kategorien diskløs pc, som bortset fra harddisken er udstyret med pc-komponenter, heriblandt en AMD K6-II processor, der kræver køling.

På bagsiden finder man tre Ethernet-porte til henholdsvis det eksterne og det interne netværk, samt en tredje, frit konfigurerbar port. Endvidere er der en seriel port til en konsolforbindelse og en PCI-baseret udvidelsesslot.

Under opsætningen, der kan foregå ved hjælp af en Windows-baseret QuickSetup-guide eller via konsolforbindelsen, kan man tage stilling til, om Firebox 1000 skal køre i såkaldt Drop in-mode eller Routed mode. Drop in-mode er en bridgeforbindelse, hvor firewallen er transparent, mens Routed mode svarer til den almindelige opsætning, hvor et privat adresserum skjules fra det offentlige netværk. QuickSetup-guiden hører til de mest brugervenlige opsætningssystemer i denne testrunde. Man indtaster IP-adresserne for hvert netværkssegment, definerer en adgangskode og rebooter Firebox 1000. Således er det ikke nødvendigt at skifte IP-adresse på administrations-pc'en, som det er tilfældet ved mange af de andre produkter. Meget positiv er også, at man allerede i QuickSetup-guiden kan angive web-, mail- eller andre servere, der skal være tilgængelige fra det eksterne netværk. Guiden opretter dermed allerede de nødvendige regler, som herefter kun skal finindstilles.

Efter grundkonfigurationen står et væld af administrationsmuligheder til rådighed. En smart detalje er, at WatchGuards kontrolcenter arbejder med to adgangskoder. Den ene giver kun adgang til at læse, således at man eksempelvis kan uddelegere overvågning af logfiler og forbindelser til en medarbejder, men kun administratoren har ret til at ændre i konfigurationen.

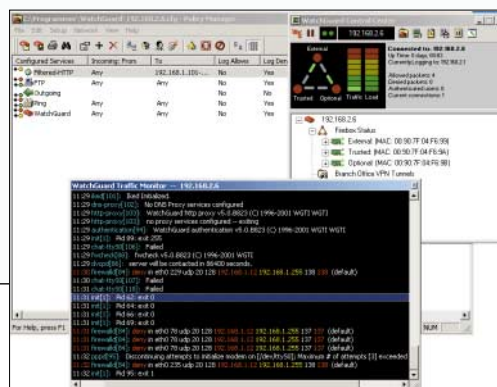
WatchGuard Control Center (t.h.) med Policy Manager i baggrunden og Traffic Monitor forrest.

Blandt de mange applikationer, som kontrolcentret omfatter, er en af de vigtigste Policy Manager, hvor regler opsættes. Firebox 1000 kan konfigureres med pakkebaserede eller proxy-baserede regler. Det kan i første omgang synes forvirrende, men når man først har vænnet sig til princippet, kan man generere meget overskuelige retningslinier. Kontrolcentret indeholder også et statusvindue, hvor der løbende vises loginformationer. Disse sendes til administrations-pc'en ved hjælp af en proprietær protokol, men syslog-protokollen understøttes også.

En anden smart applikation i kontrolsuiten er HostWatch, hvor ind- og udgående forbindelser vises både som liste og i et grafisk diagram. Naturligvis omfatter Firebox 1000s administrationsmuligheder også firewall'ens indbyggede webfilter og styring af VPN. Til sidstnævnte har WatchGuard i øvrigt udviklet en dynamisk VPN-konfigurationsprotokol (DVCP), som letter opsætningen af VPN-klienter.

Ved hjælp af en API kan tredjepartsleverandører udvikle tjenester, der arbejder sammen med firewall'en, som eksempelvis den allerede eksisterende integration med et Intrusion Detection System (IDS). Endelig har WatchGuard Firebox 1000 også en antivirusfunktion samt mulighed for at indgå i en High Availability-klynge.

Sikkerheden er også i denne firewall i top, eftersom SecureScan NX ikke kunne afsløre nogle sikkerhedsbrister.



Lucent Brick 80



Brick-serien fra Lucent omfatter en række modeller fra Brick 20 til mindre virksomheder til Brick 1000 til Internet-udbydere og datacentre. I midten finder vi Brick 80, en appliance i desktop-chassis, hvis specifikationer ligger tæt op ad den rack-baserede Brick 201.

Lucent's Brick er i bogstavelig forstand en brik i spillet. Enheden kan nemlig fungere som transparent bridge, som router eller som firewall. De fire indbyggede Ethernet-porte kan konfigureres fuldt efter behov og uafhængigt af hinanden.

Til opsætning af Brick-enhederne leveres Lucent Security Management Server (LSMS), som består af en Java-baseret brugerflade og en række systemtjenester under Windows NT/2000. Grundkonfigurationen oprettes ved i LSMS at generere et objekt, der repræsenterer Brick 80. Her indtaster man basisoplysninger som IP-adresse, navn, gateway-adresse og en række andre parametre. Disse indstillinger skrives herefter til en floppydisk, som Brick 80 skal boote med for at den kan komme i kontakt med LSMS.

Det eksterne floppydrev, som skulle have været med Brick 80, manglede imidlertid, og Lucent nåede desværre ikke at fremsende et drev inden den redaktionelle deadline. Af den grund var det ikke muligt at afprøve Brick 80 i praksis. Enheden er alligevel opført i testens featureskema, da det kan være relevant på den vis at sammenligne Brick 80 med de andre fire-

walls. Men i den egentlige test indgår Brick 80 med andre ord ikke.

Løsningen med et eksternt floppydrev virker umiddelbart lidt omstændelig, og i de større Brick-modeller er der da også et indbygget drev. På den anden side giver et eksternt drev mulighed for at sætte flere enheder op i forskellige afdelinger, hvorefter drevet lægges til side. Den således konfigurerede Brick 80 er dermed temmelig godt sikret mod uautoriserede indgreb.

Alligevel kan det undre, at Brick 80, der er udstyret med både serial port - og endda stik til en skærm og et tastatur - ikke kan konfigureres på anden vis end med en gammeldags floppydisk. Brick 80 adskiller sig også på en række andre punkter fra de øvrige kombattanter. Den lille brik er mere end nogen anden enhed gearret til at være del af en større opsætning med forskellige afdelingskontorer, hvor der er behov for central administration. I den henseende kan Brick 80 faktisk nærmere sammenlignes med enheder som Nokia IP71, som vi vil kigge på i et af de næste numre.

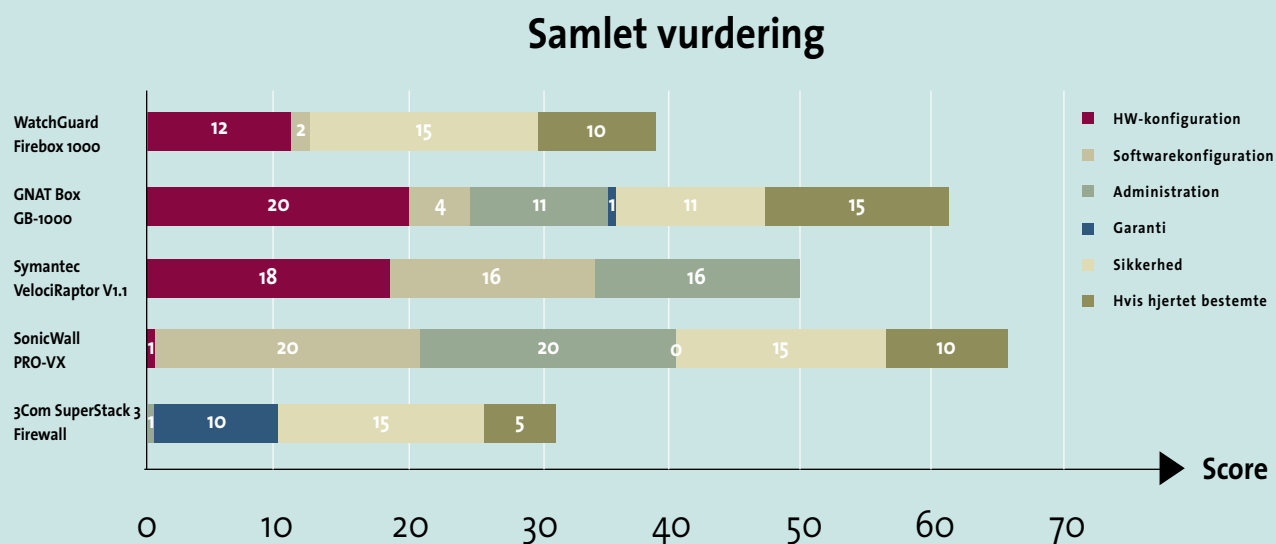
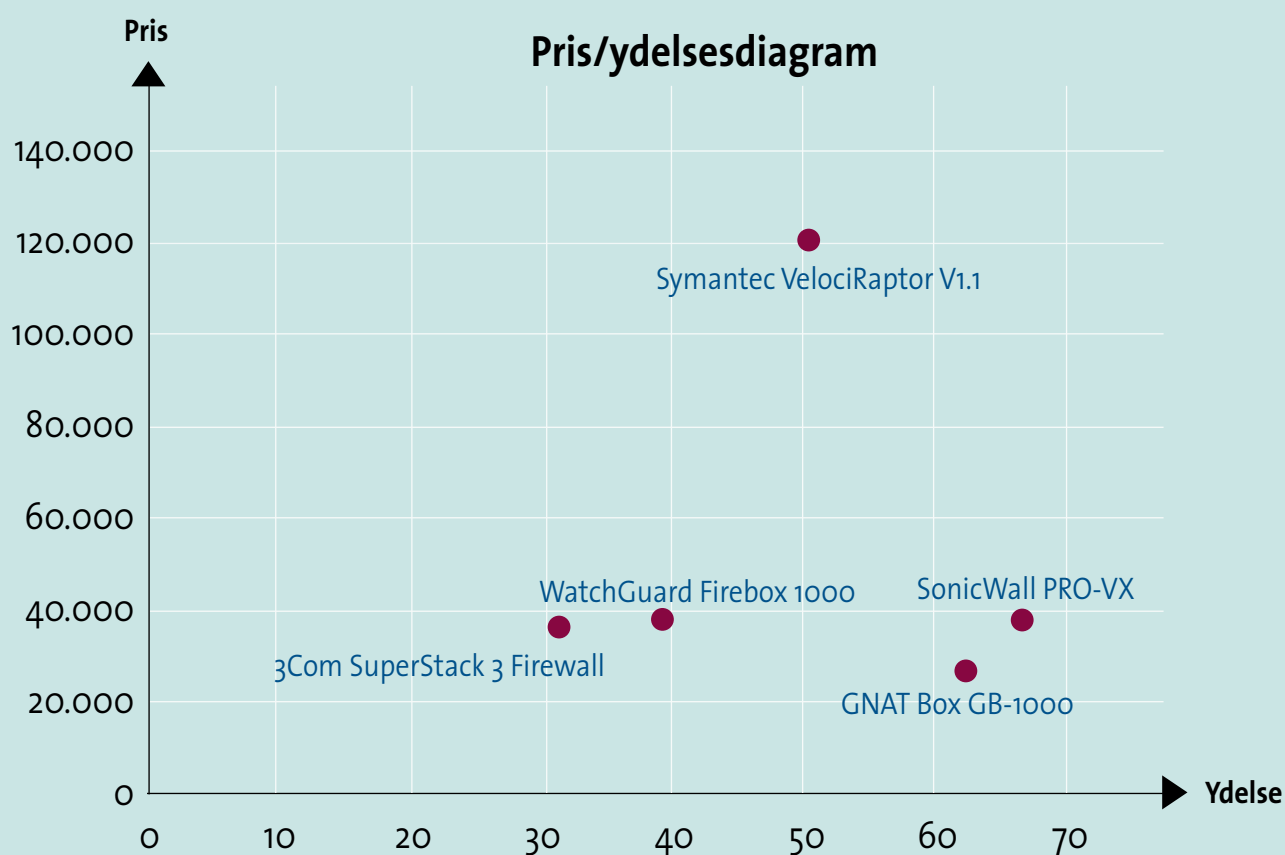
Brick 80's fleksibilitet, som desværre ikke afspejler sig i opsætningen, åbner op for et hav af muligheder, heriblandt kan Brick 80 partitioneres i op til 100 virtuelle firewalls, som alle kan have individuelle indstillinger for hvert deres virtuelle netværk (VLAN).

Selv om Lucent Brick 80 altså ikke er med i den egentlige test, kan denne firewall være et kig værd, hvis man skal beskytte en vidt forgrenet organisation.



Lucent Security Management Server byder på mange muligheder – vi fik dog ikke mulighed for at afprøve dem i praksis.

Samlet vurdering	Vægtning	3Com SuperStack 3 Firewall	SonicWall PRO-VX	Symantec VelociRaptor V1.1	GNAT Box GB-1000	WatchGuard Firebox 1000
HW-konfiguration	20	0	1	18	20	12
Softwarekonfiguration	20	0	20	16	4	2
Administration	20	1	20	16	11	0
Garanti	10	10	0	0	1	0
Sikkerhed	15	15	15	0	11	15
Hvis hjertet bestemte	15	5	10	0	15	10
I alt		31	66	50	62	39



Producent Produkt	Lucent Brick 80	3Com SuperStack 3 Firewall
Leveringsomfang		
Dokumentation	cd-rom	håndbog
Software	2 cd-rom'er (LSMS, IPSec)	1 cd-rom, 1 WebTrends Trial
Kabler	strøm	strøm
Hardware		
Ethernet-porte	4	3
heraf fri konfigurerbar	4	0
Seriellport	ja	nej
Statuslamper, brugervenlighed	**	*
High-Availability	option	ja
Andet	tilslutning for floppydrev, skærm og tastatur	Redundant Power Socket, Uplink/Normal-omskifter
Ydelse, klartekst	60 Mbps	100 Mbps
Ydelse, krypteret (3DES)	8 Mbps	45 Mbps
Antal sessioner	25000	30000
Software/funktioner		
Styresystem	Inferno OS	proprietær
VPN, antal tunneler	4000	1000
VPN, antal klientlicenser	50	50
DHCP-klient	nej	ja
DHCP-server	nej	ja
PPPoE	nej	ja
SNMP	ja	nej
Web-/Content filter	content filter	content filter + CyberNOT
Antivirus (kræver særskilt abonnement)	ja	nej
Administration		
Browser	nej	****
Telnet/SSH	nej	nej
Management Software	***	nej
Onlinedokumentation	**	****
Håndbog	****	*****
Frontbetjening	nej	nej
Garanti, antal år	1	livstid
Sikkerhed		
Høj risiko	ikke målt	0
Mellem risiko	ikke målt	0
Lav risiko	ikke målt	0
Yderligere oplysninger		
Producentens website	www.lucent.com	www.3com.com
Distributør	Lucent Danmark	EET Nordic, m.fl.
Telefonnummer	33 88 80 00	45 82 19 19
Website	www.lucent.dk	www.eet.dk
Pris i kr. ekskl. moms	80.324 (\$9495)	36.480

Sikkerhedsscanning med SecureScan NX

I Alt om NET nr. 12/2001 omtalte vi den distribuerede sikkerhedsscanner SecureScan NX fra dansk-amerikanske VIGILANTE. I forbindelse med nærværende stortest fik Alt om NET mulighed for at afprøve SecureScan NX i praksis. SecureScan NX kan både undersøge firewalls og host for kendte sårbarheder eller sikkerheds-

brister. Ud af sikkerhedsscannerens mange nuancerede test har vi her kun brugt dem, der vedrører firewalls. Scanneren fungerer ved, at et antal agenter, der er placeret på det lokale netværk, tager kontakt med konsollen, som befinder sig uden for firewall'en. Når agenterne har sendt informationer til konsollen om det

netværk, de er placeret i, går SecureScan NX i gang med en række test og angrebsforsøg, der udnytter kendte sikkerhedshuller. Resultaterne samles og SecureScan producerer en overskuelig rapport, hvoraf det fremgår, hvilke sårbarheder scanneren har fundet, og i mange tilfælde også hvordan de kan udbe-

SonicWall PRO-VX	Symantec VelociRaptor 1.1	GTA GnatBox GB-1000	Watchguard Firebox 1000
opstartsguide, håndbog 1 cd-rom	opstartsguide, håndbog 1 cd-rom	opstartsguide, cd-rom 1 cd-rom	opstartsguide, håndbog, cd-rom 1 cd-rom
strøm, UTP, UTP-X	-	strøm, konsol	strøm, UTP, UTP-X, konsol
3	4	4	3
o	2	4	1
ja	2 (konsol/UPS)	2 (konsol/pager)	ja
**	*****	**	****
option	nej	option	option
-	LCD-display og frontbetjening	I/O-port, USB	PCI udvidelsesslot
100 Mbps	100 Mbps	155 Mbps	185 Mbps
45 Mbps	45 Mbps	45 Mbps	55 Mbps
32000	ubegrænset	32768	12500
proprietær	Linux 2.2	FreeBSD	proprietær
1000	ubegrænset	300	1000
50	ubegrænset	1	5
ja	nej	ja	nej
ja	nej	ja	ja
ja	nej	ja	ja
ja	ja	ja	ja
content filter + CyberNOT	option	content filter	CyberPatrol
ja	nej	nej	ja
****	nej	****	nej
nej	ja	ja	ja
kun ViewPoint	****	****	****
****	***	**	*
****	**	*	****
nej	ja	nej	nej
1	1	2	1
o	3	o	o
o	3	o	o
o	1	2	o
www.sonicwall.com	www.symantec.com	www.gnatbox.com	www.watchguard.com
Tempest A/S	Tempest A/S	RanTek ApS	SEC Datacom
70 20 56 56	70 20 56 56	87 10 01 02	48 10 80 00
www.tempest.dk	www.tempest.dk	www.rantek.dk	www.secdacom.dk
37.455	120.723	26.995	37.940

dres. Sårbarhederne er desuden klassificeret i de tre risikokategorier: høj, mellem og lav.

Sikkerhedsscanneren er nem at sætte op og betjene. Takket være SecureScan NX er det derfor lykkedes os på kort tid at få et grundigt overblik over produkternes sikkerhedsformåen.

I testskemaet nøjes vi med at angive, hvor mange sikkerhedsrisici SecureScan NX har fundet. I den forbindelse skal det nævnes, at forskellige firewall-teknologier reagerer forskelligt på portscanninger. Mens nogle firewalls stiltiende blokerer for lukkede porte, melder andre tilbage, at porten er lukket. Grundlæggende

er begge systemer sikret, idet den pågældende port jo under alle omstændigheder er lukket. Men da også information, om at en bestemt port er lukket, kan give et fingerpeg om firewall'en, vurderes en tilbagemelding fra firewall'en alligevel som en ulempe.

PC PRO er kendt for sine omfangsrige og grundige stortest. Via et regneark på forside-cd-rom'en gav de ekstraordinært læserne mulighed for at ændre testparametrene vægtning og tilpasse produkternes priser til eventuelle aktuelle ændringer. Den tradition fortsætter vi med på det nye Alt om NET & PC PRO, men vi har valgt at skifte til et mere tidssvarende medie: Internet. På adressen www.altomnet.dk finder du derfor både resultatet af denne test og mulighed for at påvirke resultatet med din personlige vægtning af testparametrene. På websiden finder du ligeledes information om vores vægtningsprincip.

Det blev resultatet

Testkriterierne er delt op i fem kategorier. Første kategori er hardwarekonfiguration, som omfatter Ethernet-porte og andre tilslutningsmuligheder. Anden kategori, software-baserede funktioner, indeholder en række punkter, som skal være med til at vise forskellene mellem produkterne. En funktion som NAT er eksempelvis ikke taget med, fordi alle firewalls forventes at understøtte NAT. Ligeledes er VPN-understøttelsen ikke anført, da det har været et af udvalgs-kriterierne. Til gengæld er anført antallet af VPN-klientlicenser, der følger med til den oplyste pris.

Ved siden af hardware- og software-baserede kriterier, blev der også sammenlignet ydelsestal. Tallene for ydelsen er oplyst af producenten eller distributøren. Den faktiske ydelse, der er angivet i Mbps, afhænger dog i høj grad af pakkerens størrelse og protokollen. Derfor skal de oplyste værdier tages med forbehold, idet kun de færreste producenter redegør for målemetoden. Som udgangspunkt kan man dog formode, at firewall'ens maksimale evne under spidsbelastninger i de flestes tilfælde er oplyst. Endvidere skal man huske, at der naturligvis også skal være den tilsvarende båndbredde til stede før enhedens ydelsesgrænse kan nås.

Vigtigere i den sammenhæng er antal samtidige sessioner. Det gælder især for virksomheder, som agter at drive egen webserver fra hhv. DMZ'en eller det interne netværk. Er serveren godt

besøgt, og har man samtidig mange medarbejdere, der aktivt bruger Internet, har man hurtigt brug for at kunne styre en del sessioner.

I den tredje kategori bedømmer vi administrationsmulighederne og brugervenligheden. Tallet ud for det enkelte administrationsværktøj angiver bedømmelsen af brugervenligheden mellem en og fem stjerner. Står der "nej", betyder det, at det pågældende værktøj ikke er understøttet. Den fjerde kategori omhandler garanti og i den femte kategori sammenligner vi resultaterne fra sikkerhedstesten.

Såvel hovedkategorierne som de enkelte parametre blev vægtet efter PC PROs sædvanlige pointssystem. Det samlede pointtal blev herefter sat i forhold til produktets pris.

Sikkerheden er i alle produkter fuldt tilfredsstillende. Det er stort set kun Vel-

ociRaptor, der på dette punkt halter lidt bagefter, men ingen af de fundne svagheder er deciderede sikkerhedshuller, men snarere risici i forbindelse med, at en eventuel angriber indsamler informationer.

Til gengæld er der en række forskelle i firewall'enes funktioner og specifikationer. Suverænt flest point scorede SonicWall PRO-VX, men testvinder blev alligevel GNAT Box GB-1000, som ligeledes opnåede et anseeligt antal points, men derudover sælges til en yderst fordelagtig pris. Omvendt forholder det sig med Symantec VelociRaptor V1.1, der ud fra pointtallet ligger i testfeltets midte, men på grund af dens høje pris røg i bunden af skalaen. På tredjepladsen finder vi i stedet WatchGuard Firebox 1000, mens fjerdepladsen besættes af 3Com SuperStack 3 Firewall.

GNAT Box GB-1000



GNAT Box GB-1000 forener fremragende firewall-egenskaber med en konkurrenceløs lav pris. Den endnu forholdsvis ukendte firewall er produceret af Global Technology Associates med hovedsæde i Florida. Ud over GB-1000 udvikler og sælger GTA en række andre firewall-produkter, der alle sammen baserer sig på den samme software, som i øvrigt kan downloades gratis som 5-bruger-version.

GNAT Box GB-1000 er dog tæt fulgt af SonicWall PRO-VX, der endda ligger over GNAT Box GB-1000, hvis vi udelukkende sammenligner points. Men det højere pointtal skyldes først og fremmest, at SonicWall PRO-VX understøtter flere VPN-tunneler og leveres med flere VPN-klientlicenser, hvilket dog ikke helt retfærdiggør prisforskellen på godt 10.000 kroner. For man kan – i hvert fald i teorien – bruge hvilken som helst VPN-klientsoftware.

Af den grund har vi kåret GNAT Box GB-1000 til testvinder, men giver hermed også hæderfuld omtale til SonicWall PRO-VX.

HYPERSPRING

www.vigilante.com

(Vigilante, producent af SecureScan NX)

www.itsvar.dk – søg efter id3360

(Alt om NET 12/2001, Better safe than sorry – om SecureScan NX)

www.itsvar.dk – søg efter id3037

(PC PRO 9/2001, Beskyt dit netværk – stortest af hardwarebaserede SOHO-firewalls)

www.itsvar.dk – søg efter id2844

(Alt om NET 7-8/2001, Personlig sikkerhed – stortest af personlige firewalls)