

UTM-brannmurer for de små

I dag kan du få en avansert brannmur til under 10 000 kroner. Men hvordan er det egentlig med ytelsen, og hvor enkelt er det å sette opp disse brannmurene?

Av MARTIN AGFORS, Techworld

■ Rimelige brannmurer pleier ikke å stoppe avanserte angrepsforsøk, virus, spam eller trafikk med upassende innhold. Men de siste årene har brannmurer med såkalt UTM-beskyttelse kommet ned på et svært hyggelig prisnivå. UTM står for unified threat management og er et vagt definert begrep.

Grovt sett handler det om å ta et helhetsgrep om beskyttelsen mot alskens forferdeligheter og samle dette på ett sted.

Alle brannmurene i denne testen har angrepsbeskyttelse som gjerne går under navnet IPS eller IDP. Mens en klassisk enkel pakkefiltrerende SPI-brannmur kun inspiserer på pakkenivå i trafikken, ser IPS/IDP på applikasjonsnivå.

Dermed kan sistnevnte se avvikelser i trafikken som de enklere brannmurene går glipp av, og således hindre ulike angrep og innbruddsforsøk som er integrert i tilsynelatende normal og legitim trafikk. IPS/IDP baserer seg i de fleste tilfellene på signaturer, men kan også arbeide på andre måter.

Alle brannmurene i testen, bortsett fra Cisco SA520, kan utføre sanntids-skanning etter virus i trafikken som passerer. Cisco arbeider på en annen måte med virusbeskyttelse, hvor brannmuren i stedet holder styr på virusbeskyttelsen på klientmaskinene.

Kun klienter med oppdatert virusbeskyttelse får tillatelse til å motta trafikk. Det innebærer at ytelsesmålingene for Cisco SA520 ikke kan sammenlignes direkte med de øvrige. Resultatet viser at sanntidsskanning

ofte koster mye ytelse i forhold til hva det gir i sikkerhet. Vi anser at viruskanning i brannmuren i de fleste miljøer neppe kan erstatte lokal



virusbeskyttelse i hver klient. Ikke så lenge det finnes bærbare maskiner som brukes både innenfor og utenfor brannmurens beskyttelse. Det er ellers verdt å notere at også Zyxel USG-100 kan holde orden på klientenes virusbeskyttelse.

Søk i sanntid har poenger

Selv om sanntidssøk ikke innebærer at man kan ta bort lokal virusbeskyttelse i klientmaskiner, anser vi at det kan ha sine poenger. Mange bedrifter har ikke raskere internettforbindelser enn at flere av brannmurene i testen faktisk kan virusskanne trafikken uten at ytelsen reduseres nevneverdig. Selv om man også har virusbeskyttelse lokalt i klientene, føles det ekstra trygt å ikke unødvendig slippe skadelig kode inn i nettverket. De fleste brannmurene i testen tilbyr også ulike former for søppelstfiltrering og filtrering av innhold. Førstnevnte kan være en god hjelp, men også kronglete hvis du vil ha full kontroll om hvilken type søppelst som ankommer. Hvis brannmuren kaster mistenkelig spam, mister du den informasjonen. Innholdsfiltrering er vi temmelig skeptiske til – den har ofte tendens til å sile mygg og svelge kameler.

Vi har i denne testen konsentrert oss om de to mest interessante formene for beskyttelse. Dette er innbruddsbeskyttelse og virusbeskyttelse.



Vi har sett nærmere på hvor enkelt det er å komme i gang med disse forsvarsverkene og hvordan det påvirker ytelsen.

Cisco Systems – Small Business Pro SA520

Cisco Small Business Pro SA520 oppfyller egentlig ikke kravene for å delta i denne testen. Den har innbruddsbeskyttelse, men ingen sanntidsskanning etter virus direkte i brannmuren. Den bruker i stedet en modell hvor brannmuren kun slipper gjennom trafikk fra klienter som har den nyeste virusbeskyttelsen.

Cisco mener at dette er en bedre modell ettersom sanntidskontroll koster mye form av ytelse. Dessuten må man ofte uansett ha virusbeskyttelse i klientene, spesielt for bærbare klienter som befinner seg utenfor det beskyttede miljøet og arbeidsplassen. Vi kan forstå Ciscos resonnement, men samtidig viser måleresultatene fra for eksempel Cyberoam at virusbeskyttelse kan kombineres med bra ytelse.

Cisco Small Business Pro SA520 har en WAN-port, fire LAN-porter og en port som kan ha valgfri rolle.

Cisco leverer veldig bra ytelse til en lav innkjøpspris, og har et raskt brukergrensesnitt det er enkelt å jobbe med. Men løsningen har altså ingen sanntidsbeskyttelse mot virus.

Fakta

Produsent: Cisco Systems.

Kontakt: www.cisco.com.

Modell: Small Business Pro SA520.

Cirkapris: 2990 kroner.

Garanti: 12 måneder, 90 dagers programvaregaranti.

Tilkoblinger: 1 WAN, 4 LAN, 1 valgfri.

UTM-kostnadsmodell: Årlige separate lisenser for IPS og beskyttelse av klienter.

UTM-priser: ProtectLink Gateway: ca 1200 kroner i året, ProtectLink

Endpoint: ca 1250 kroner i året, IPS: ca 1000 kroner i året.

VPN-trafikkapasitet: 65 Mbps.

VPN-kostnad for klienter: IPsec kostnadsfritt, to SSL-lisenser inngår, 25 ekstra SSL-lisenser koster ca 1000 kroner.

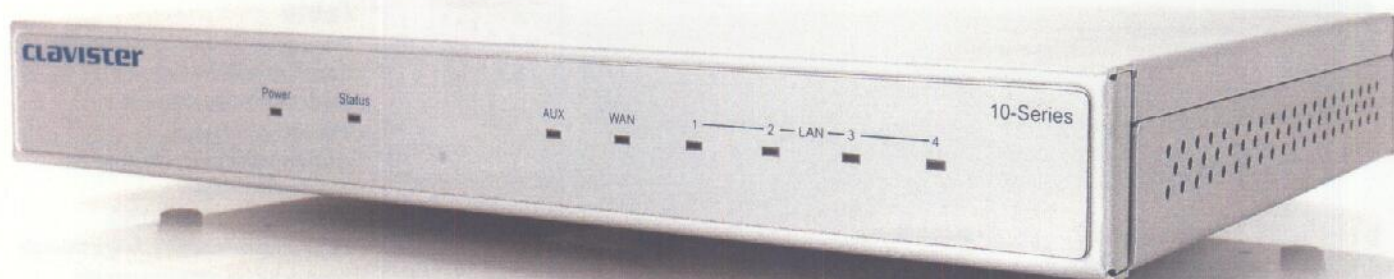
Slik testet vi

■ Testen tar i hovedsak for seg ytelsesmålinger med og uten UTM-funksjonalitet, samt vurdering av grensesnittene.

Ytelsesmålingene bestod i å kjøre FTP-trafikk gjennom brannmurene. Som FTP-server kjørte vi Freeftpd, og som klient brukte vi Filezilla. Våre testdata var et stort katalogtre med litt over 200 MB. Her var det en mengde underkataloger og totalt rundt 300 små og store filer inkludert noen zip-filer.

Dette innebærer mange TCP-sesjoner som skal åpnes og lukkes, viruskanning av mange filer pluss oppakning av zip-arkiv. Rutingkonfigurasjonen som vi gjorde, var å angi adresser for de ulike grensesnittene (WAN, test-LAN og admin-LAN). Vi gikk også gjennom aktivisering av innbrudds- og virusbeskyttelse samt hvordan man oppretter brannmurregler eller port forwarding for HTTP-trafikk til en tenkt webserver i en DMZ.





Fakta

Produsent: Clavister.

Kontakt: www.clavister.com.

Modell: SG 15.

Cirka pris: 5200 kroner.

Garanti: 24 måneders garanti, bytte av maskinvare i løpet av 24 timer, kan forlenges.

Tilkoblinger: 1 WAN, 4 LAN, 1 valgfri, 1 serieport.

UTM-kostnadsmodell:

Årlige separate lisenser for ulike vern.

UTM-priser: Samtlige tjenester koster rundt 1000 kroner i året.

UTM-leverandør av antivirus: Kaspersky.

VPN-trafikkapasitet: 25 Mbps.

VPN-kostnad for klienter: Kostnadsfritt.

VPN-antall samtidige tunneler: 5.

Clavister SG 15 har en WAN-port, fire LAN-porter, en port som kan ha valgfri rolle pluss en serieport.

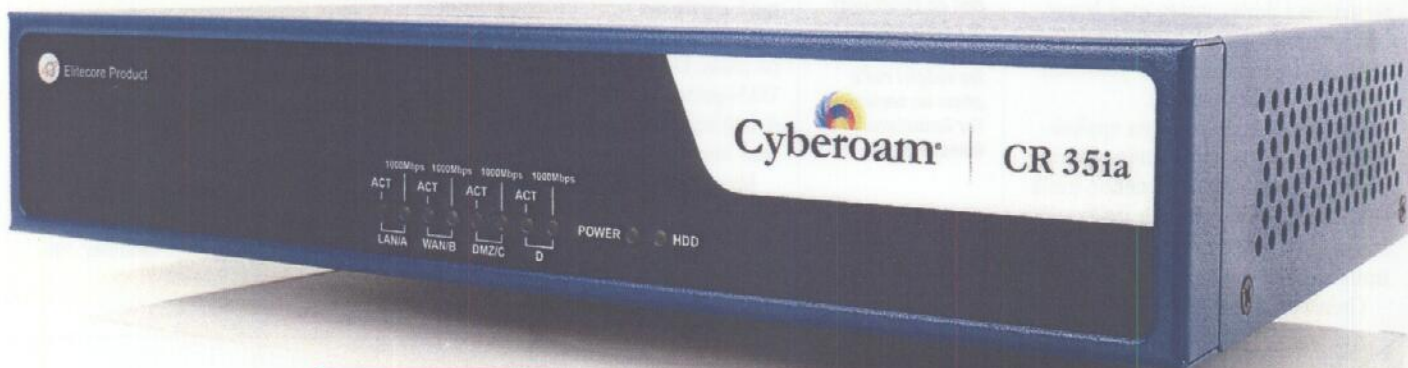
Clavister – SG 15

Å komme i gang med Clavister SG 15 føles som et studiebesøk på nittitallet. Det er bra for avanserte administratører å ha mulighet til å kjøre et raskt kommandogrensesnitt via en seriellport, men med Clavister er det faktisk den eneste måten å få i gang enheten. Det er temmelig umoderne i dag.

Når du har fått i gang enheten, skjer resten av administrasjonen via programmet Clavister Finetune. Dette

byr på et supersmidig grensesnitt som er raskt å jobbe i. Men det krevdes en del leting og lesing i håndbøkene før vi klarte å definere og koble sammen reglene som krevdes for å aktivere innbrudds- og virusbeskyttelsen.

Ytelsen er bra og årskostnaden for UTM-funksjonene er overkommelig. Men konfigurasjonen burde vært enklere.



Fakta

Produsent: Cyberoam.

Kontakt: www.cyberoam.com.

Modell: CR35ia.

Cirka pris: 8550 kroner.

Garanti: 12 måneders garanti.

Tilkoblinger: 1 WAN, LAN, DMZ, 1 valgfri, 1 USB, 1 konsollport for rj-45.

UTM-kostnadsmodell: Årlige separate lisenser for IPS, antivirus, spambeskyttelse samt web- og applikasjonsfilter.

UTM-priser: Hele beskyttelsespakken pluss support koster 3538 kroner i året. De ulike delene kan også kjøpes separat.

UTM-leverandør av antivirus: Kaspersky.

VPN-trafikkapasitet: 80 Mbps.

VPN-kostnad for klienter: Kostnadsfritt.

VPN-antall samtidige tunneler: 50.

BEST i TEST
Nettverk
& KOMMUNIKASJON

Cyberoam CR35ia har en WAN-port, en LAN-port, en DMZ-port, en port som kan ha valgfri rolle pluss en konsollport for rj-45-kontakt samt en USB-port.

Cyberoam – CR35ia

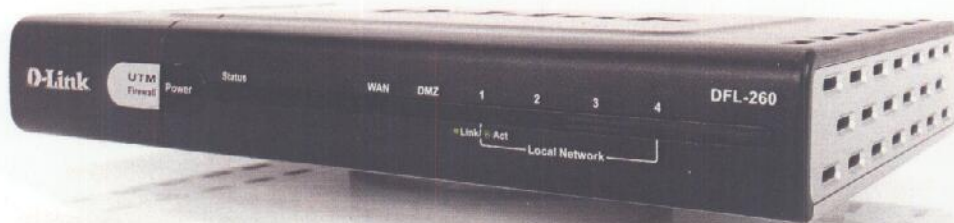
Cyberoam CR35ia er sammen med Watchguard de dyreste i dette startfeltet, både i innkjøp og i årskostnad. Men du får mye ytelse for pengene. I målingene for gjennomstrømning fikk vi over 100 Mbps med aktivert UTM-beskyttelse – fantastisk i denne prisklassen.

Webgrensesnittet er tydelig og intuitivt, noe som gjør administrasjonen enkel. Det tok oss mindre enn fem minutter å finne ut hvordan innbrudds- og virusbeskyttelsen ble akti-

vert, og da leste vi ikke i instruksjonene i det hele tatt.

En fin detalj å notere er at Cyberoam har mange standardinnstillinger som sendes med ved levering. Dette er for eksempel ferdige regeloppsett for IPSec-VPN.

Cyberoam CR35ia blir her best-i-test takket være en kombinasjon av bra ytelse og en enkel og intuitiv administrasjon. Den er et dyrt men veldig godt valg.



D-Link – DFL-260 NetDefend

Å komme i gang med DFL-260 NetDefend er enkelt og smidig takket være en gjennomtenkt startguide. Men å gå videre og få i gang virus- og innbruddsbeskyttelse er litt vanskeligere. Konfigurasjonen er regelbasert, noe som innebærer litt av en opplærings terskel for de som ikke er vant med dette. Nå har D-Link heldigvis en tydelig og bra dokumentasjon på web. Da vi først fant riktig avsnitt i dokumenta-

D-Link DFL-260 NetDefend har to WAN-porter og to LAN-porter.

sjonen, gikk det raskt å konfigurere.

Det webbaserte grensesnittet er hierarkisk oppbygd på samme måte som Utforsker-modellen, smidig og bra, men med tanke på målgruppen hadde vi gjerne sett veivisere for å få i gang UTM-funksjonene.

Både innkjøpspris og ytelse havner omtrent på gjennomsnittet, mens årskostnaden for UTM-beskyttelse er hyggelig lav.

Fakta

Produsent: D-Link.
Kontakt: www.dlink.no.
Modell: DFL-260 NetDefend.
Cirkapris: 5550 kroner.
Garanti: Livstidsgaranti med next business day service.
Tilkoblinger: 2 WAN, 2 LAN.
UTM-kostnadsmodell: Årlige separate lisenser for IPS, antivirus og webfiltrering.
UTM-priser: Innbrudds- og virusbeskyttelse pluss webfiltrering koster 1225 kroner i året.
UTM-leverandør av antivirus: Kaspersky.
VPN-trafikkapasitet: 25 Mbps.
VPN-kostnad for klienter: Kostnadsfritt.
VPN-antall samtidige tunneler: 100.



Draytek – Vigor Pro 5300

Draytek Vigor Pro 5300 er budsjettalternativet i denne testen med lavest innkjøpspris og lavest årskostnad. Ikke overraskende er også ytelsestallene blant de helt laveste.

Men dersom man har en oppkobling på 10 Mbps eller mindre, så vil Draytek kunne håndtere denne trafikken. Husk på at vår måling med mange sesjoner tilsvarer en svært høy trafikkbelastning.

Grensesnittet er raskt å arbeide

Vigor Pro 5300 har en WAN-port, fire LAN-porter, en port som kan ha valgfri rolle pluss en serieport for kommandokonsoll.

med, og finesser som lastbalansering og failover mellom WAN-portene er på plass. Du kan også benytte doble WAN-porter for VPN-sammenkobling (trunking), som er smart hvis man skal kjøre tung trafikk over VPN.

Men glem ikke å sette ytelsestallene i relasjon til hvor rask oppkoblingen er. Draytek viser at det er mulig å få god UTM-ytelse til en svært lav pris.

Fakta

Produsent: Draytek.
Kontakt: www.draytek.no.
Modell: Vigor Pro 5300.
Cirkapris: 2400 kroner.
Garanti: 24 måneder.
Tilkoblinger: 1 WAN, 4 LAN, 1 valgfri, 1 serieport.
UTM-kostnadsmodell: Årlig lisens.
UTM-priser: Med Kaspersky AV: 1300 kroner i året, med Draytek AV: 700 kroner i året.
UTM-leverandør av antivirus: Kaspersky eller Draytek.
VPN-trafikkapasitet: 50 Mbps.
VPN-kostnad for klienter: Kostnadsfritt.
VPN-antall samtidige tunneler: 100.

Fakta

Produsent: Gateprotect.
Kontakt: www.gateprotect.com.
Modell: GPA 250.
Cirkapris: 8650 kroner.
Garanti: Ingen opplysning.
Tilkoblinger: 4 valgfrie roller, 1 konsollport for rj-45, 2 USB + liten informasjonsskjerm med styreknapper.
UTM-kostnadsmodell: UTM-beskyttelse i pakken for 12, 36 eller 60 måneder.
UTM-priser: Avhenger av driftstiden.
UTM-leverandør av antivirus: Kaspersky.
VPN-trafikkapasitet: 120 Mbps.
VPN-kostnad for klienter: Kostnadsfritt.
VPN-antall samtidige tunneler: 50.



Gateprotect – GPA 250

Gateprotect GP 250 er en påkostet brannmur med mange finesser, for eksempel en liten skjerm på enheten som viser status og adresser for de ulike portene. Administrasjonen skjer via et program man installerer, og grensesnittet er det triveligste vi har sett hos noen brannmur. Fordelene kommer best til sin rett i store nettverk, men er også smidige for den lille bedriften.

Ytelsen uten UTM-funksjonene er fantastisk, men med UTM akti-

Fire porter for valgfrie roller, en konsollport for rj-45, to USB-porter samt skjerm med styreknapper.

vert fikk vi problemer. Målingene av maksimal gjennomstrømning med en stor ZIP-fil ga ingen resultater i det hele tatt ettersom tilkoblingen ble brutt. I målingene med mange sesjoner ble ytelsen dårlig, og exe-filer på over en viss størrelse kom ikke gjennom. Vi har vært i kontakt med Gateprotect som er klare over hva som skaper disse problemene, og de skal fikse dette via oppgraderinger.