

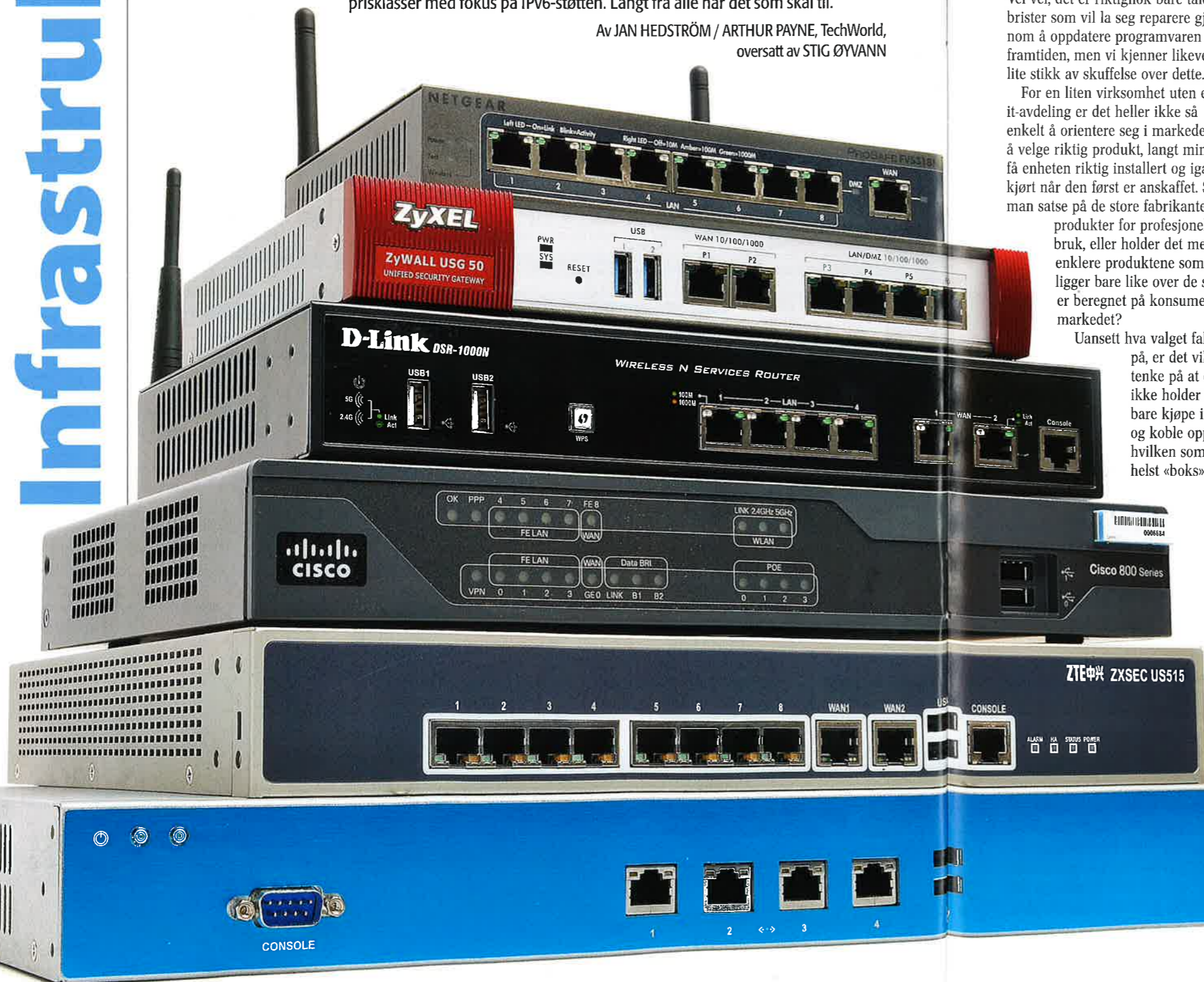


Seks for IPv6

Cisco – D-Link – Halon – Netgear – ZTE - Zyxel

TEST: Dersom du ønsker å bruke IPv6 mot internett, trenger du før eller siden en ruter/brannmur som klarer jobben. Vi har testet seks produkter i forskjellige prisklasser med fokus på IPv6-støtten. Langt fra alle har det som skal til.

Av JAN HEDSTRÖM / ARTHUR PAYNE, TechWorld, oversatt av STIG ØYVANN



Ti år etter at IPv6 ble spesifisert og standardisert, og ett år etter at adresserommet til IPv4 gikk tomt, er det på tide at enhetene vi setter opp mot internett også klarer den nye protokollen. Da vi satte i gang med denne testen viste det seg imidlertid at «støtte for IPv6» fremdeles er et ganske fleksibelt begrep når fabrikantene tar det i bruk. Hva skal man for eksempel si om at et par av de testete produktene ikke hadde fungerende brannmurer for IPv6-trafikk? Vel vel, det er riktignok bare tale om brister som vil la seg reparere gjennom å oppdatere programvaren i fremtiden, men vi kjenner likevel et lite stikk av skuffelse over dette.

For en liten virksomhet uten egen it-avdeling er det heller ikke så enkelt å orientere seg i markedet for å velge riktig produkt, langt mindre få enheten riktig installert og igangkjørt når den først er anskaffet. Skal man satse på de store fabrikantenes produkter for profesjonell bruk, eller holder det med de enklere produktene som ligger bare like over de som er beregnet på konsumentmarkedet?

Uansett hva valget faller på, er det viktig å tenke på at det ikke holder å bare kjøpe inn og koble opp hvilken som helst «boks».

Nettverk og sikkerhet er en kompleks materie, og et enkelt kryss i feil rute kan åpne for at inntrengere får en mulighet til å ta seg inn på it-systemene dine. Dette er definitivt ett av de tilfellene der det er ekstra smart å leie inn en konsulent som har de rette kunnskapene.

Cisco 829F-K9

Først ut i denne testen er Cisco. Ikke bare fordi selskapets navn er det første når vi ordner dem i alfabetisk rekkefølge, men også fordi at dette er uten tvil den største og viktigste leverandøren i nettverksmarkedet.

På baksiden av ruterer finner vi åtte interne porter, og to tilkoblinger mot omverdenen, den ene holder gigabit hastighet. Noensteds der inne finnes det en vifte, men den er svært stillegående. Boksen skal skrues opp på en vegg, men ettersom denne modellen ikke har trådløst nettverk innebygd, kan den like gjerne stappes inn sammen med resten av bedriftens it-utstyr. Helhetsinntrykket av maskinvaren er svært tillitsvekkende.

Dessverre har Cisco lagd grunnkonfigurasjonen av produktet svært og unødvendig komplisert. I stedet for et innebygd web-basert konfigurasjonsverktøy følger det med en egne applikasjon som heter «Configuration Professional» (CP). Denne javabaserte programvaren kan bare installeres på Windows. Hvorfor, Cisco, hvorfor?

Vanskelig konfigurering

Nåvel, hjelpetekster finnes nesten overalt i CP og vi finner inntrengingsbeskyttelse (IPS - «Intrusion Protection System») med cirka 20 forhåndsdefinerte profiler. Men så forsøker vi å sette opp grunninnstillingene for IPv6 i CP. Det går overhodet ikke. Til alt hell finnes det kommandolinjebaserte brukergrensesnittet til Cisco. Her kan man konfigurere IPv6-adresser, brannmurregler, DHCPv6-server, ja - alt. Kommandolinjen i Cisco IOS er et svært kraftig og anvendelig verktøy, forutsatt at man finner fram den riktige manualen. Men den er til stadig-

het bare en kommandolinje, noe som den it-ansvarlige i vårt scenario kanskje ikke engang vet at finnes. Kjære Cisco, bygg inn bedre IPv6-støtte i CP!

HALON

Scenario

En liten virksomhet med 20 ansatte trenger ny brannvegg. Selskapet har ingen egen it-avdeling, men bruker en lokal it-konsulent ved behov. Nå skal bedriften stramme opp sikkerheten på sitt interne nettverk, og trenger en DMZ («Demilitarized Zone») med et par servere i tillegg.

Personellet trenger å koble seg til ved hjelp av VPN iblant, og ettersom selskapet har mange kontakter i Asia blir det stadig viktigere å kunne bruke IPv6. Sikkerhetsfunksjoner for e-post og webtrafikk er også et pluss.

Det finnes en rekke med tilleggs-lisenser som man kan kjøpe til dette produktet. Visst er det bra at man ikke er nødt til å betale for funksjonalitet som man ikke har til hensikt å bruke, men samtidig er det kanskje litt for enkelt å kjøpe unødvendig mange lisenser «for sikkerhets skyld».

D-Link DSR-1000N

D-Link har vært flinke nok til å lage en strømgjerrig enhet som er absolutt stillegående, og som derfor uten videre kan plasseres ute blant folk i selv et stille kontor.

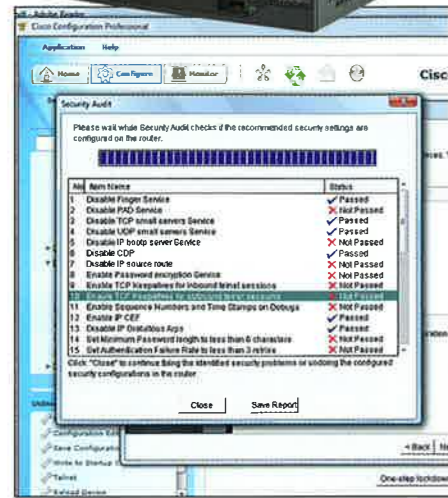
Denne ruterer har to WAN-porter der den ene kan brukes for å koble til en reservelinje mot internett, eller som en DMZ-port. Dessuten kan man få en ekstra reservetilkobling dersom vi kobler til et 3G-modem via enhetens USB-port. Da gjelder det imidlertid å sørge for at man bruker en mobiloperatør som håndterer IPv6.

DSR-1000N har også trådløst nettverk. Vi kan definere opptil fire forskjellige virtuelle aksesspunkter, og VLAN gjør det enkelt å holde bedriftens egen interne trafikk adskilt fra gjestetrafikk fra besøkende. Gjester og andre brukere kan styres til en inngangsportal før de får tilgangen sin på nettverket.

Trist, men brukbart grensesnitt

Webgrensesnittet på denne enheten er ganske enkelt og smått gråtrist, men det tilbyr relativt mange innstillingsmuligheter. Tidssynkronisering ved hjelp av NTP og inntrengerdeteksjon (IDS/IPS) finnes også i enheten.

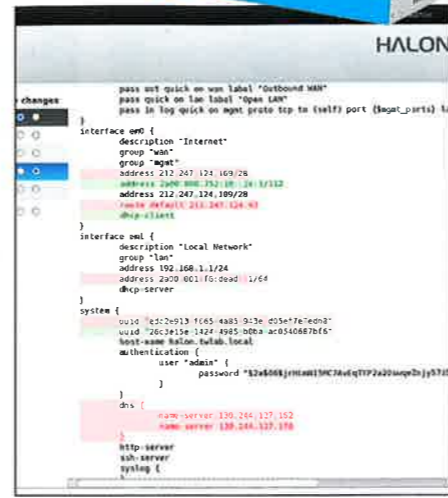
IPv6-innstillingene finner vi under fanen «Advanced». Der kan vi velge det nødvendige: statiske eller dynamiske adresser, ruter-annonsering og ruting. Webgrensesnittet er det kun mulig å nå ved hjelp av IPv4, men vi kan bruke telnet over IPv6 for å konfigurere ruterer med kommandolinje-



Cisco har et vidunderlig verktøy som heter Security Audit, en innebygget funksjon for å analysere konfigurasjonen og finne potensielle sikkerhetsproblemer.



D-Links pakkefilter tillater ikke å konfigureres for IPv6-adresser. Til og med når vi velger å blokkere all trafikk som kommer inn på WAN-porten, så slipper IPv6 gjennom!



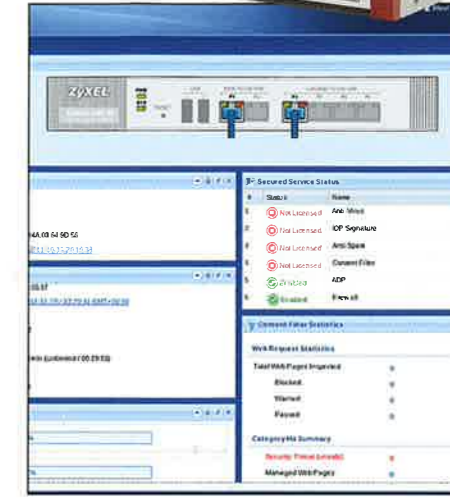
Halons versjonshåndtering forteller når innstillingene har blitt endret og viser elegant alt som skiller to forskjellige versjoner.



Netgears programvare har ikke tilstrekkelig støtte for IPv6. Vi håper at den biten blir rettet på til neste versjon, for ruterens maskinvare er helt klart godkjent og prisen på produktet er svært konkurransedyktig.



Spoofingbeskyttelse virker kun på IPv4, men ellers har ZTE lagt inn støtte for å håndtere en mengde protokoller i brannmurens pakkefilter. Nærmere 100 er forhåndsdefinerte og de støtter til og med IPv6-trafikk.



ZyXel har det mest grafiske administrasjonsgrensesnittet i vår test. Det synes allerede på statussiden som gir deg et overblikk over hva som skjer på systemet.

grensesnittet. Det er i og for seg en bagatell, men det som er verre er at brannmuren, altså pakkefilteret, ikke blokkerer IPv6.

Det er svært enkelt å ta en sikkerhetskopiering av innstillingene, da logger man inn i grensesnittet og klikker på en knapp. Vi klarer imidlertid ikke å opprette en automatisert kopieringsrutine til en ekstern server – det hadde vært greit å slippe å huske på å alltid lage en backup etter at man har endret på oppsett og innstillinger.

I programvaren til D-Link finnes det også en DHCPv6-server som vi kan bruke i lokalnettet vårt. DHCP gir flere muligheter til å styre adressetildelingen enn vanlige ruter-annonseringer, for eksempel kan man logge hvilke adresser som faktisk har blitt reservert av tilkoblede maskiner. Dessverre har likevel ikke DHCPv6-serveren fått like mange funksjoner som den for IPv4. Fremfor alt savner

vi muligheten til å permanent knytte en IPv6-adresse til en bestemt MAC-adresse, altså til en spesifikk maskin i nettverket.

Halon SX-150

Også svenske Halon har en ny generasjon produkter på beddingen, i denne testen har vi vært nødt til å teste nesten ferdig programvare på eldre maskinvare.

Ruteren SX-150 er en relativt stor og omfangsrik boks som helt tydelig er tenkt å monteres i et rack eller stativ i et datarom.

Det finnes ingen dedikerte WAN- eller DMZ-porter, bruken av portene på denne enheten styres fritt og helt og holdent av konfigurasjonen. Halon hevder stolt at enheten skal holde tritt med gigabit-hastighet trafikk, selv med brannmuren aktiv.

Halons webgrensesnitt ligner ikke på noe annet vi har sett på en ruter. Det er avskallet, med færre funksjoner men med mer lettnavigerte menyer enn de fleste andre. Følelsen av et «hjemmesnekrete» webgrensesnitt trenger seg iblant på, men i perioden vi har testet, har Halon fintrimmet flere grafiske detaljer.

Fantastisk for feilsøking

All konfigurasjon kan presenteres i tekstformat, og nye konfigurasjoner testes i 30 sekunder og ruller deretter

automatisk tilbake om noe gikk galt. Denne programvaren er fantastisk bra når man feilsøker eller eksperimenterer med konfigurasjonen.

Halon har bygd inn støtte for IPv6 fra grunnen av, men alt er ikke på plass ennå. Noen DHCPv6-server finner vi for eksempel ikke i betaversjonen, men ifølge Halon skal den være på plass når produktet offisielt lanseres.

Fra kommandolinjen har vi verktøy tilgjengelig for all mulig konfigurasjon og feilsøking i nettverket. Webgrensesnittet kunne ikke i vår versjon av programvaren håndtere inntrengerdeteksjon, klynger eller lastbalansering, men de funksjonene skal dukke opp i neste versjon.

For en it-tekniker som er dyktig i nettverksteknologi vil halon oppleves som et bra og annerledes alternativ. Det finnes nok en risiko for at vår scenariedrift vil bli frustrert og Halons programvare, men om de leier inn en kompetent nettverkskonsulent som alt-i-ett-support og «husnisse», er det og grunn til å se nærmere på denne ruteren.

Netgear Prosafe FVS318N

Netgear har den aller minste ruter/brannvegg-enheten i denne testen, en diskret liten boks med et par antenner på baksiden. Den kan skrues fast på veggen, og kommer ikke til å gi

det minste pip fra seg der. Dette er den eneste testdeltakeren som ikke har mulighet til redundant internett-tilkobling, men til gjengjeld fungerer den også som et trådløst aksesspunkt som støtter 802.11b, g og n. Dette er også testens billigste produkt, men det har likevel svært gode tilkoblingsmuligheter og støtte for alle grunnleggende funksjoner.

Akkurat som alle de andre rutene i testen kan Netgear tunnelere IPv6 til andre lokale nettverk, selv om internettforbindelsen vår kun støtter IPv4. En innebygd DHCPv6-server for å holde orden på hvilke klienter som får koble seg til og hvilke IPv6-adresser de får, finnes.

Ingen brannmur for IPv6

Så langt er alt fryd og gammen, men lengre enn dette strekker ikke støtten for den nye nettverksprotokollen seg. Når vi studerer brannmurfunksjonen oppdager vi at pakkefilteret ikke har støtte for annet enn IPv4, og på DMZ-nettet går det ikke engang å konfigurere IPv6-adresser. Ifølge produktseksjonen hos Netgear skal brannmuren få støtte for IPv6 ved hjelp av en programvareoppdatering som skal være tilgjengelig i løpet av våren 2012.

VPN-støtten er i det minste bra, så lenge vi holder oss til IPv4. L2TP og opptil tolv samtidige IPsec-tunneler støttes, og man kan til og med konfi-

gurere en portal for SSL-VPN med opptil fem samtidige sesjoner. Slett ikke dårlig, men kjære Netgear: Gi oss støtte for VPN via IPv6 snart!

Netgears webgrensesnitt er pyntelig og lettnavigert, men det er så alt for tregt i responsen sin. Brukerne kan autentiseres med en rekke protokoller, blant annet mot Active Directory og LDAP. IPv6-konfigurasjonen er for en stor del adskilt fra IPv4-konfigurasjonen, og det finnes en del uklarheter i grensesnittet når deg kommer til IPv6.

All konfigurasjon kan lagres i en tekstfil som både er enkel å forstå og lett å tilpasse. Her finner vi til og med en del innstillinger som ikke er å finne i webgrensesnittet.

I skrivende stund (januar 2012) er ikke dette produktet et særlig godt valg for vårt scenario, men med de

Halon fornyer

Halon har en ny generasjon rutere som ikke hadde kommet på markedet da denne testen ble gjennomført. Vi fikk altså teste en nesten ferdig betaversjon av programvaren på eldre maskinvare. Den kommende modellen HSR-2006 kommer til å få bedre ytelse og seks gigabit Ethernet-porter i stedet for fire, men ifølge Halon blir prisen likevel halvert til knappe SEK 10 000.

oppdateringene som Netgear har lovt, så virker det lovende.

ZTE Zxsec US 515

Den kinesiske fabrikanten ZTE har den klart dyreste ruteren. Dette er en bastant boks med åtte 100 megabit/sekund porter for beskyttede nettverk, og to WAN-porter på 1 gigabit/sekund. I tillegg kan et 3G-modem kobles til en av USB-portene som reserveløsning.

Maskinvaren har eksistert i et par år allerede, noe som blant annet vises ved at enheten er den i testen som trekker mest strøm. Tilbehør for å montere ruteren i rack følger med, og det trenges fordi denne ruteren også har testens mest støvende vifte – den låter nærmest som en liten støvsuger.

Lar deg skreddersy

ZTE lar oss skreddersy de aller fleste innstillingene. Webgrensesnittet har massevis av konfigurasjonsmuligheter, og det reagerer kjapt. Mens de andre produktene har en enkel avkryssing for å sette de to WAN-portene til å jobbe parallelt, har ZTE bygd inn muligheter for å finjustere lastfordelingen. Logger kan sendes til en syslog-tjeneste eller via ZTEs egen USLA-protokoll for fjernadministrasjon.

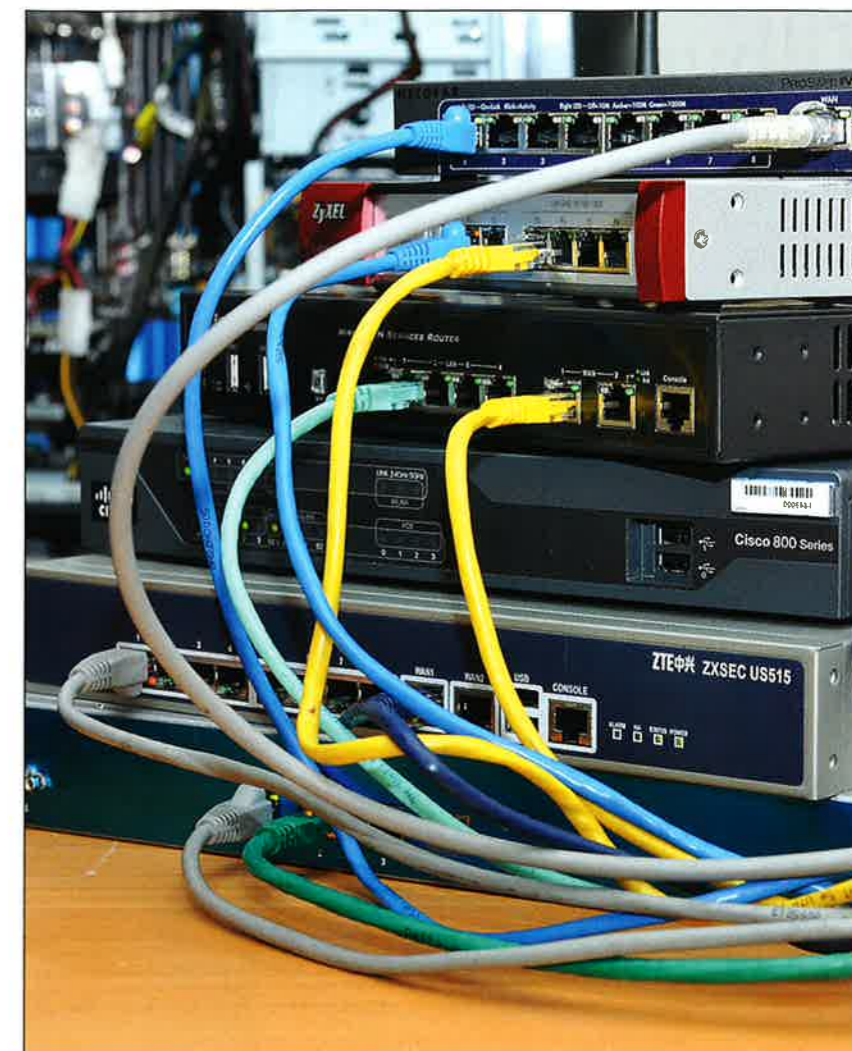
Brannmuren har støtte for IPv6, men adresser og regler må konfigu-

Slik testet vi

Vi satte opp noen enkle nettverkskonfigurasjoner på hver ruter, dels mot internett med adresser tildelt via ruter-annonsering og DHCPv6, og dels i et isolert nettverk med statiske IPv6-adresser. Vi testet først og fremst hvilke av brannmurfunksjonene som virkelig ble støttet med IPv6-trafikk.



FAKTA	Cisco 892F-K9	D-link DSR-1000N	Halon SX-150	Netgear Prosafe FVS318N	ZTE Zxsec US 515	Zyxel Zywall USG 50
Antall WAN-porter, hastighet	1 stk 1 Gbit/s (kobber + optisk), 1 stk 100 Mbit/s	2 stk 1 Gbit/s + USB	1-3 (av 4), 1 Gbit/s	1 stk 1 Gbit/s	2 stk 1 Gbit/s + USB	1 eller 2 stk 1 Gbit/s + USB
Antall LAN- og DMZ-porter	8 stk 100 Mbit/s	4 stk 1 Gbit/s	1-3 (av 4), 1 Gbit/s	8 stk 1 Gbit/s	8 stk 100 Mbit/s	4 + 0 eller 1, 1 Gbit/s
Trådløst nettverk	Nei	Ja, 802.11 a/b/g/n	Nei	Ja, 802.11 b/g/n	Nei	Nei
DHCPv6-støtte	Klient + server	Klient + server	Klient (snart også server)	Klient + Server	Nei	Klient + server
Brannmur - pakkefilter for IPv6	Ja	Nei	Ja	Kommer i februar	Ja	Ja
Applikasjonsbrannmur for IPv6	Ja	Nei	Nei	Nei	Ja	Ja
VPN-protokoll	IPsec, SSL, easy VPN m.fl.	IPv4: IPsec, PPTP, L2TP, SSL, openvpn	IPsec, L2TP, PPTP	IPv4: IPsec, L2TP, SSL	IPsec, PPTP, SSL	IPv4: IPsec, SSL
UTM	IDS/IPS	IDS/IPS	IDS/IPS	-	Virusbeskyttelse, innholdsfiltrering, IPS mm.	Virusbeskyttelse, IPS + IDP
Brukerautentisering	Lokalt, LDAP, Radius, Tacacs+ m.fl.	Lokalt, Radius	Lokal database	Lokalt, Radius, AD, LDAP	Lokalt, LDAP, Radius, Tacacs+, AD	Lokalt, LDAP, AD, Radius, ASAS
Målt effektforbruk ved lav belastning	12 W	9 W	25 W	4 W	25 W	8 W
Cirkapris (SEK)	10 000 SEK + VPN-lisenser	2 600 SEK	19000 SEK	1 350 SEK	30 000 SEK	3 000 SEK + abonnementer
PLUSS OG MINUS						
Fordeler:	Maskinvaren, IOS-operativsystemet, protokollstøtten.	Prisen, innebygd trådløst nettverk, DHCPv6.	Verktøy for feilsøking og problemanalyse, ytelse.	Billigste og minste ruter. Trådløst nettverk, mange nettverksporter.	Avanserte funksjoner og bra webbgrensesnitt. Bra dokumentasjon.	Svært bra dokumentasjon og webbgrensesnitt. Bra støtte for IPv6 og UTM.
Ulemper:	Administrasjonsverktøyet CP Express, skjulte kostnader for lisenser.	IPv6-støtte mangler i brannmurens pakkefilter.	Færre funksjoner enn flere av konkurrentene, bare fire nettverksporter.	IPv6-støtte ikke ferdig ennå, tregt webbgrensesnitt.	Urimelig dyr. Høyt lyd nivå.	Ingen VPN med IPv6. Ekstra kostnader for abonnement på UTM og VPN.
POENGENE						
Brukergrønsnitt	8/30	11/30	18/30	12/30	22/30	25/30
VPN-støtte	16/20	12/20	12/20	8/20	15/20	12/20
IPv6-støtte	15/20	6/20	17/20	7/20	16/20	15/20
Maskinvare, form og støy	10/15	14/15	5/15	13/15	5/15	12/15
Dokumentasjon	10/15	10/15	8/15	9/15	13/15	14/15
Totalt	59 AV 100	53 AV 100	60 AV 100	49 AV 100	71 AV 100	78 AV 100



Flere porter innebærer ikke alltid høyere kapasitet. De minste ruterne har svake prosessorer, og kan ikke filtrere trafikken i full hastighet.

res en gang ekstra ved siden av IPv4-reglene. DHCP-serveren klarer dessverre også bare IPv4. For å slippe å konfigurere våre interne datamaskiners IPv6-adresser manuelt, må vi altså ta i bruk ruter-annonsering. Men bortsett fra dette finner vi god støtte for IPv6 i dette produktet.

Konfigurasjon av IPv6 gjøres i stor grad ved hjelp av webbgrensesnittet, men visse innstillinger må tas via kommandolinjen. Denne er for en gangs skyld ikke en etterligning av Cisco eller Linux, men det er likevel lett å lære og smidig å arbeide i.

Her finner vi også testens mest avanserte UTM-funksjoner («Unified Threat Management»), selv for IPv6. Antivirus, innholdsfiltere for e-post og webtrafikk og mye mer finnes her. Systemet for inntrengerdeteksjon identifiserer en mengde av forhåndsdefinerte trusler, og det er også mulig

å definere side egne, om de innebygde ikke strekker til.

Zyxel Zywall USG 50

Blikkboksen fra Zyxel er ikke spesielt umfangsrik, og den er helt fri for vifter slik at vi slipper irriterende støy. Nettverksportene klarer 1 gigabits/sekund, men via brannmuren er gjennomstrømmingen i praksis begrenset til cirka 100 megabits/sekund – og bare halvparten så mye når vi bruker VPN-tunneler.

Vi testet ruterne med en betaversjon av programvaren som skal være ferdig når denne artikkelen er på trykk. I programvaren finnes massevis av funksjoner, blant annet båndbreddereservasjon der vi kan gi høyeste prioritet til telefoniprotokollen SIP og lastbalansering av både utgående og innkommende internett-trafikk.

Brannmuren kan virkelig håndtere

IPv6 på samme måte som IPv4, det finnes til og med støtte for enkelte spesielle protokoller som H.323 og SIP, men alle regler må settes opp to ganger når man bruker begge protokollene.

Håndbok på 970 sider

Det er enkelt å rulle tilbake til eldre utgaver av innstillingene, og Zyxel har bygd inn en god kommandolinjetolk som vi får tak i ved hjelp av SSH. De to manualene er på 394, respektive 970 sider, men heldigvis kommer de i PDF-format og ikke på kilovis med papir.

Zyxel har støtte for virusbeskyttelse, søppelpostfiltrering og inntrengerdetektering. Å kjøpe tilleggsabonnement for UTM og VPN kan koste flere tusenlapper per år, men det er virkelig en nyttig mulighet som hever sikkerhetsnivået betraktelig.

Zyxel har fått med støtte for SSL-VPN i USG 50, i tillegg til IPsec og L2TP. SSL-funksjonen gjør det mulig å nå inn til bedriftens interne ressurser ved hjelp av Firefox eller Internet Explorer selv fra en lånt datamaskin, men bare over IPv4! Dessuten er vi begrenset til maksimalt fem samtidige sesjoner per protokoll, og høyst får to brukere logge inn via VPN med grunnlisensen – litt i gjerrigste laget, synes vi.

Testerens etterord

Vi regnet med å kunne få prøvekjøre en lang rekke detaljer i IPv6-protokollene i denne testen. Med noen av disse enhetene rakk vi ikke mer enn å sette i gang for funksjonaliteten tok slutt. IPv6-adresser kan jo deles ut automatisk med ruter-annonsering, men den støtten finnes ikke i alle produktene, og det er absolutt ikke

selsagt at vi kan bruke DHCPv6, som er litt nyere men som gir oss bedre kontroll over nettverket. Med

Hermetikk

Allerede da vi ringte rundt til markedsledende leverandører for å be dem stille opp i en test med fokus på IPv6, trakk flere svært kjente nettverksleverandører seg tilbake, og vegret seg for å låne ut utstyr. De sa rett ut at de ikke støttet IPv6 ennå. Vi tolker det dithen at de ønsker å konservere den gamle IPv4-verdenen i sine produkter.

Men seks modige leverandører vågde å stille opp, selv om noen av dem bare er i ferd med å bygge inn støtte for IPv6 nå, til tross for at protokollen er over ti år gammel. De seks produktene i testen som alle har en eller annen form for støtte av IPv6, følger ikke engang spesifikasjonene. For eksempel går det ikke å bruke IPsec over IPv6 – til tross for at IPsec ble utviklet for IPv6, og spesifikasjonene krever at IPsec skal støttes!

flere av brannmurene er det heller ikke mulig å bruke VPN, virusbeskyttelse og andre nyttige funksjoner over IPv6.

Som kunde gjelder det altså fortsatt å være forsiktig og heller stille et spørsmål for mye enn å risikere å kjøpe en enhet som ikke holder mål. Vi konstaterer at den gamle sannheten «du får det du betaler for» til stadighet gjelder, ikke minst når det kommer til hvilken ytelse man får når man bruker avanserte funksjoner som VPN eller brannveggfunksjonaliteten.

Men en av de billigste ruterne, den fra Zyxel, imponerte stort. Den har nesten like avanserte funksjoner som de langt dyrere enhetene fra Cisco og ZTE. I vårt scenario blir det faktisk bedre å kjøpe Zyxels ruter, og bruke litt av de pengene man sparer på konsulenthjelp som sørger for å utnytte alle funksjonene optimalt.