Sådan får du et sikkert hjemmenetværk

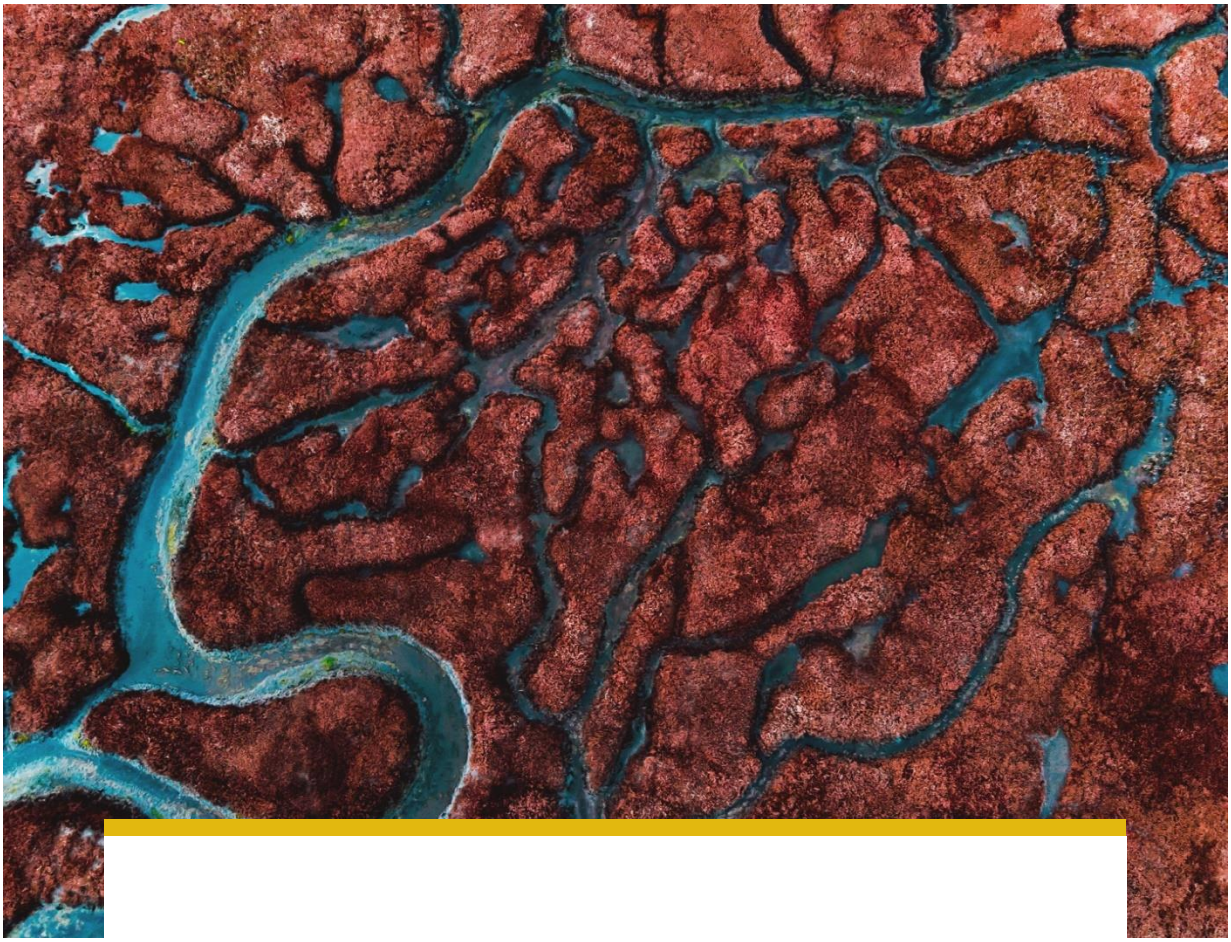
Zyberdata
11-03-2022
Randi Mortensen

VEJLEDNING

OVERSKRIFT

Vi gør en masse for at sikre vores computere og andre enheder. Men selve netværket skal også være sikkert. Her får du den komplette guide, der holder hackerne på afstand

Hvor sikkert er dit hjemmenetværk?



Sådan får du et sikkert hjemmenetværk

Vi gør en masse for at sikre vores computere og andre enheder. Men selve netværket skal også være sikkert. Her får du den komplette guide, der holder hackerne på afstand

Hvor sikkert er dit hjemmenetværk? Det er en afgørende del af vores dagligdag, fordi det forbinder alle vores hjemmeenheder med hinanden og med hele internettet. Men det er også mål for hackere og andre ondsindede typer. Det er normalt, at den router eller modemrouter, man bruger, er arrangeret med tanke på bekvemmelighed snarere end sikkerhed, og det indebærer en risiko for at blive angrebet.

Dit netværk er især sårbart over for angreb fra to sider: Den første er en fysisk indtrængen fra nogle inden for rækkevidde af dit Wi-Fi-net. Dets rækkevidde vil overraske dig – prøv at gå udenfor og se, hvor nemt det er for dit net at række ind i naboens have eller kælder eller ud på fortovet. Hvis dit netværk ikke er beskyttet af stærk kryptering (og en endnu stærkere adgangskode), risikerer du i bedste fald at dele din internetforbindelse med en nasser, og i værste fald åbner du dit netværk for spioner og hackere.

Den anden side er angreb fra nogle uden for dit netværk. Vidste du, at din router som standard er konfigureret til at blive tilgået på afstand? Hvis du ikke har ændret det kodeord, der fulgte med den, er det ikke usandsynligt, at den allerede er blevet invaderet af en forbipasserende hacker, der scanner ip-adresser og porte og søger sårbarheder. Det kan føre til, at malware såsom trojanske heste kommer ind i dit system og forærer hackere en åben dør til dit netværk og dine ressourcer.

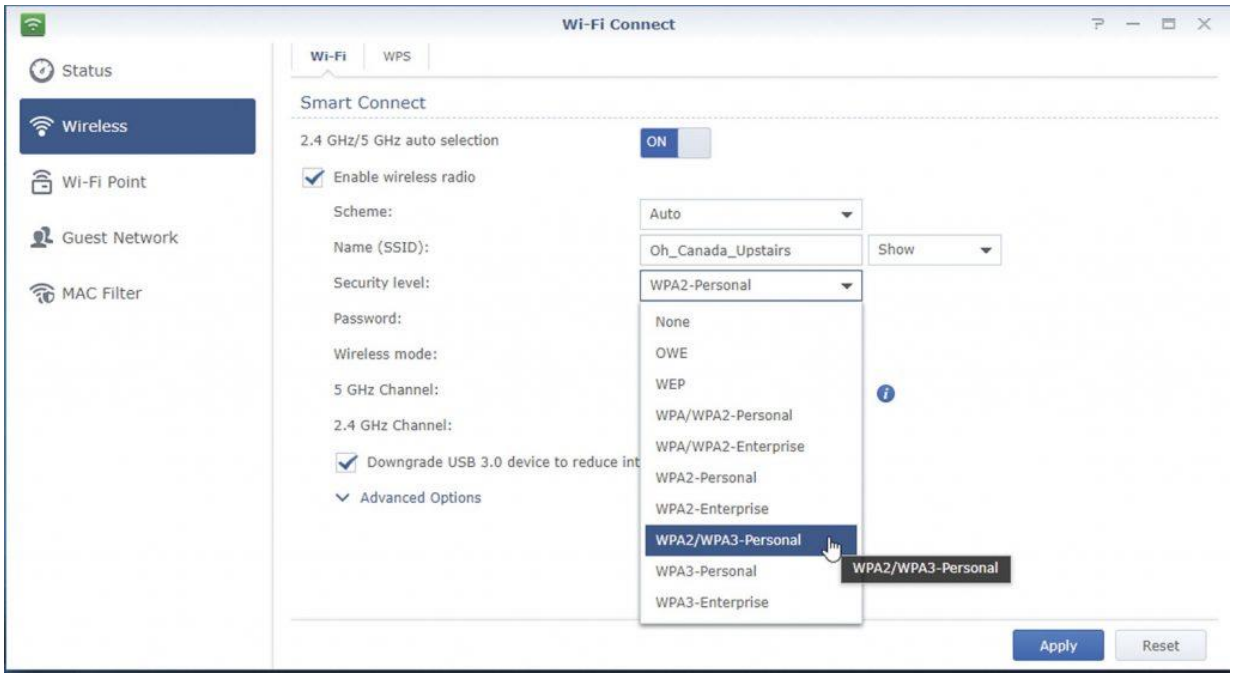
Heldigvis kan du med de rigtige redskaber og teknikker låse dit netværk mod angreb både udefra og indefra. I denne artikel fokuserer vi på at låse din adgang til internettet, nemlig din router. Vi hjælper dig med at beslutte, om tiden er inde til at anskaffe en ny model, og vi viser dig, hvilke indstillinger der tilfører ekstra lag af sikkerhed og lægger et væld af hindringer i vejen for eventuelle hackere.

Når din router er sikret, fortæller vi, hvordan du hurtigt tjekker, om alle dine enheder er sikre, og vi viser, hvordan du sikkert kan få forbindelse til dit hjemmenet, når du er på farten, som om du sad derhjemme. Læn dig tilbage, og forbered dig på at give enhver håbefuld hacker og nasser en ubehagelig overraskelse.

Det første skridt, når det gælder om at styrke dit hjemmenets sikkerhed, er at afgøre, om din router stadig lever op til kravene. Hvis den er over seks eller syv år gammel, er tiden inde til at overveje en opgradering til noget, der er mere robust, og som understøtter de nyeste sikkerhedsprotokoller.

I tekstboksen på side 47 kan du læse, hvad du skal søge efter i en ny router – den Synology RT2600ac, som vi her fremhæver, er en af to routere, vi har testet i forbindelse med denne artikel. Den anden er den ældre og mere forbrugerorienterede TP-Link Archer VR900 modemrouter. En anden løsning er at læse boksen om DD-WRT på side 48 for at se, om det er muligt at give din eksisterende model en ny chance.

Uanset om man har tænkt sig at investere i en ny router, eller man blot vil gennemføre en undersøgelse af netværkssikkerheden med den aktuelle model, består det første skridt i at logge på routerens styringsværktøjer, og det foregår typisk via ens webbrowser.



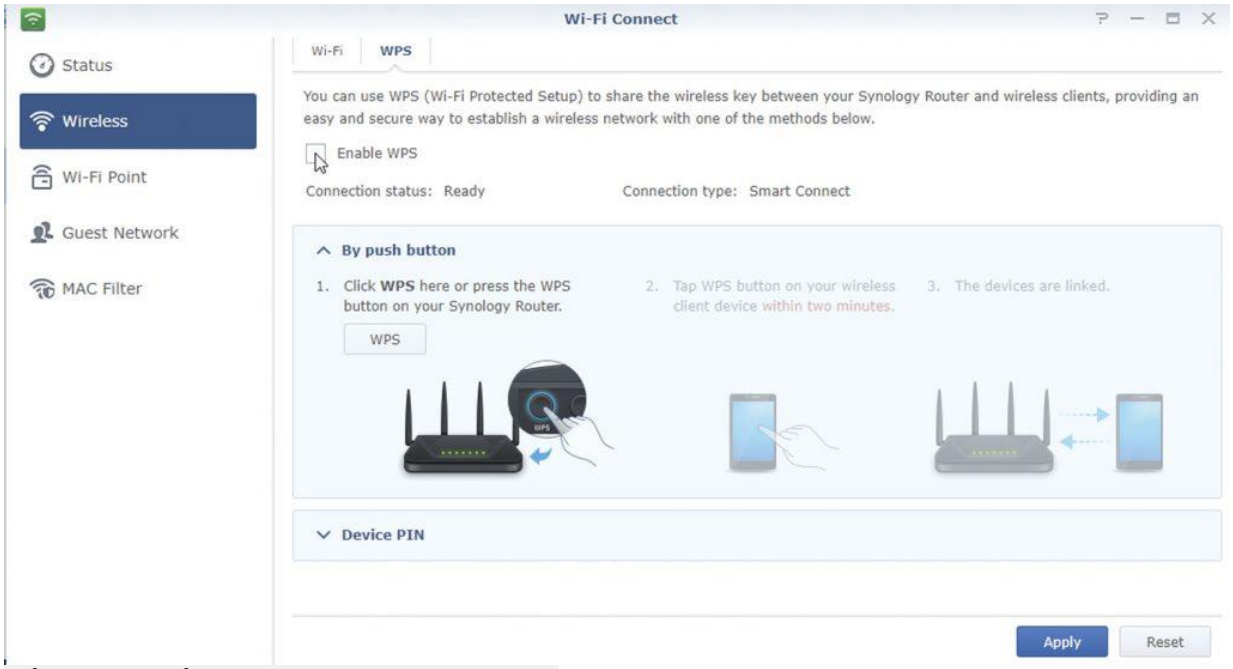
Hvis du vælger WPA2/WPA3 til Wi-Fi-kryptering, får du bagudkompatibilitet.

Alt, hvad du skal gøre, er at skrive din routers ip-adresse i browseren og trykke Enter. Hvis du er i i tvivl om, hvad ip-adressen er, åbner du i Windows 11 Indstillinger > Netværk og internet og klikker på “Egenskaber”. Din routers ip-adresse vil fremkomme ud for din IPv4-adresse.

Du bliver bedt om at logge ind, typisk med et brugernavn og et kodeord, men somme tider blot med et kodeord. Hvis du aldrig har gjort det før, skal du slå op i din routers manual. Du vil opdage, at standard-loginet ikke er sikkert, og det er her, du bør foretage din første justering. Skift det til noget, der er meget sværere at komme forbi.

Led efter en administrationssektion i din routers styringsfunktion. Brugere af Archer skal gå til Advanced > System Tools > Administration for at ændre indstillingerne til noget mere sikkert; Synology-brugere foretager ændringerne under den første opsætning eller senere under Control Panel > User. Synologys tilgang scorer points, fordi den anvender en multibruger-model, således at potentielle hackere er nødt til at gætte både brugernavn og kodeord for at få adgang.

Vi anbefaler brugen af en kodeordsmanager som den, Bitwarden tilbyder, til at oprette dit nye kodeord – noget vilkårligt, der indeholder en blanding af mindst 14 bogstaver, tal og specialtegn for at få beskyttelse mod angreb. Naturligvis skal koden gemmes i din kodeordsmanager eller skrives ned et sikkert sted.



Slå WPS fra, når funktionen ikke er nødvendig.

Mens du er i administrationssektionen, skal du søge efter en mulighed for at administrere din router på afstand – med andre ord uden for dit lokale netværk over internettet. Hvis du slår denne funktion fra, forhindrer du forbipasserende hackere i at prøve at logge ind.

Hvis du mener, at du kan få brug for denne funktion, bør du styrke din konto yderligere. Når det gælder Synology-routere, kan du indføre totrinsbekræftelse via en 2FA-kode og tilføje et ekstra lag af sikkerhed. Prøv at lade det blive en vane at lade denne funktion være frakoblet, undtaget når du har brug for den (for eksempel under rejse). Det vil minimere din eksponering til internettet.

Skift dit netværks subnet

Dette er også et godt tidspunkt til at overveje at ændre dit netværks standardsubnet. De fleste routere har som standard 192.168.0 eller 192.168.1 til deres subnet og tildeler sig selv en indlysende adresse såsom 192.168.1.1 ved samme lejlighed.

Det gør det nemmere for hackere at gætte ip-adresser, også efter at man har fravalgt den automatiske tildeling af ip-adresser til nye enheder via DHCP (det vender vi tilbage til). Hvorfor ikke vælge noget mindre indlysende – for eksempel 192.168.42 som subnet og 192.168.42.187 til routerens ip-adresse?

Men pas på: Hvis du allerede har tildelt manuelle ip-adresser på routerens subnet til bestemte enheder af den ene eller den anden grund, mister de netværksadgang, så snart ændringen bliver indført. Derfor skal man midlertidigt skifte dem tilbage til automatisk/DHCP.

Hvis du for eksempel ser på din Windows 11-pc, kan du gøre det i Indstillinger > Netværk og internet. Klik på din netværksadapter (Wi-Fi eller Ethernet) efterfulgt af Rediger under IP-indstillinger for at gå tilbage til Automatisk (DHCP).

Når det er gjort, foretager du ændringen: For eksempel skal brugere af Synology gå til Network Center > Local Network > General tab, hvor man kan se sin routers aktuelle ip-adresse under Local IP. Skift den til den ønskede erstatning, og lad subnet mask være indstillet til 255.255.255.0. Husk også at opdatere DHCP-indstillingerne under dette punkt.

Efter at du har klikket Apply, mister du midlertidigt din forbindelse, men når den vender tilbage, bør du kunne logge på din router igen via dens nye ip-adresse og fortsætte med at øge sikkerheden.

opgrader din router

Hvis du mener, at din router trænger til opgradering, er dette tidspunkt ideelt til at lade sikkerheden få indflydelse på din indkøbsbeslutning. Det betyder, at du skal se videre end forbrugerroutere og finde noget, der er bedre egnet til et hjemmekontor (SOHO).

Disse former for routere modtager regelmæssige opdateringer (mange andre modtager ingen), der lukker smuthuller i sikkerheden og af og til leverer nye funktioner. De har desuden ekstra fordele såsom indbyggede VPN-servere, mere omfattende forældrestyring og firewalls.

SOHO-routere er ikke billige, men de behøver ikke at koste en formue. Synologys RT2600ac (ovenfor) koster omkring 1900 kroner, og selvom den ikke er den hurtigste, er den afgjort langt mere sikker end nogen forbrugerrouter, og den er en af de billigste routere, der understøtter WPA3-kryptering.

Som de fleste andre SOHO-routere har RT2600ac intet indbygget modem. Hvis du tidligere har brugt en modemrouter, kan du beholde den som modem fremover. Opsætningen er relativt ligetil: Læs i instruktionerne om placering af din eksisterende modemrouter i ren modemtilstand (hvis det ikke findes, må du undersøge muligheden for at arrangere den i bridgetilstand).

Forbind dens WAN-port til routerens WAN-port, således at de bliver linket sammen. SOHO-routere er traditionelt mere komplekse i opsætning og brug, og det er endnu en grund til, at RT2600ac er et godt valg. Den kører sit eget dedikerede operativsystem, Synology Router Manager (SRM), der modtager løbende opdateringer og leverer et relativt enkelt peg og klik-interface, og det tillader adgang via en mobil-app.

Man kan også udvide SRM via applikationer, som man downloader og installerer fra internettet, herunder Security Advisor, der er en app, som scanner din routers sikkerhedsindstillinger, afslører svage punkter og foreslår forbedringer. Det er os en fornøjelse at kunne meddele, at efter at vi havde fulgt rådene i denne guide, fik vi sikkerhedskarakteren “Good” fra vores RT2600ac på test af både hjemme- og arbejdssituationer.

Sikkert Wi-Fi-netværk

Mens routerens egen administra-tionsportal er lukket ned, er tiden inde til at fokusere på dit fysiske netværk. Vi skal med andre ord sikre både dens trådløse og kablede forbindelser for at forhindre, at hackere i nabolaget kan få adgang.

Lad os begynde med dit Wi-Fi-netværk. Gå til dets Wireless-indstillinger for at se, hvilken kryptering du bruger. Som et absolut minimum bør den omfatte WPA2-PSK med support af AES (undgå den mere sårbare TKIP-kryptering). Sørg for, at WPA2-PSK/AES er tilvalgt, hvis det er tilfældet.

Moderne routere understøtter den nyere WPA3-standard. Synology understøtter standarden med en firmwareopdatering, men det gælder ikke alle dine netværksenheder. WPA3-support er påkrævet på både hardware- og styresystemniveau, og selvom din computers Wi-Fi-adapter understøtter WPA3, er du derfor nødt til at køre Windows 10/11 eller Ubuntu 20.04 (eller nyere). Kompatible Apple-enheder omfatter iPhone 7, iPad 5, Watch 3, Apple TV 4K og Mac fra 2013 med 802.11ac-support eller nyere. Android-enheder skal køre Android 10 eller nyere.

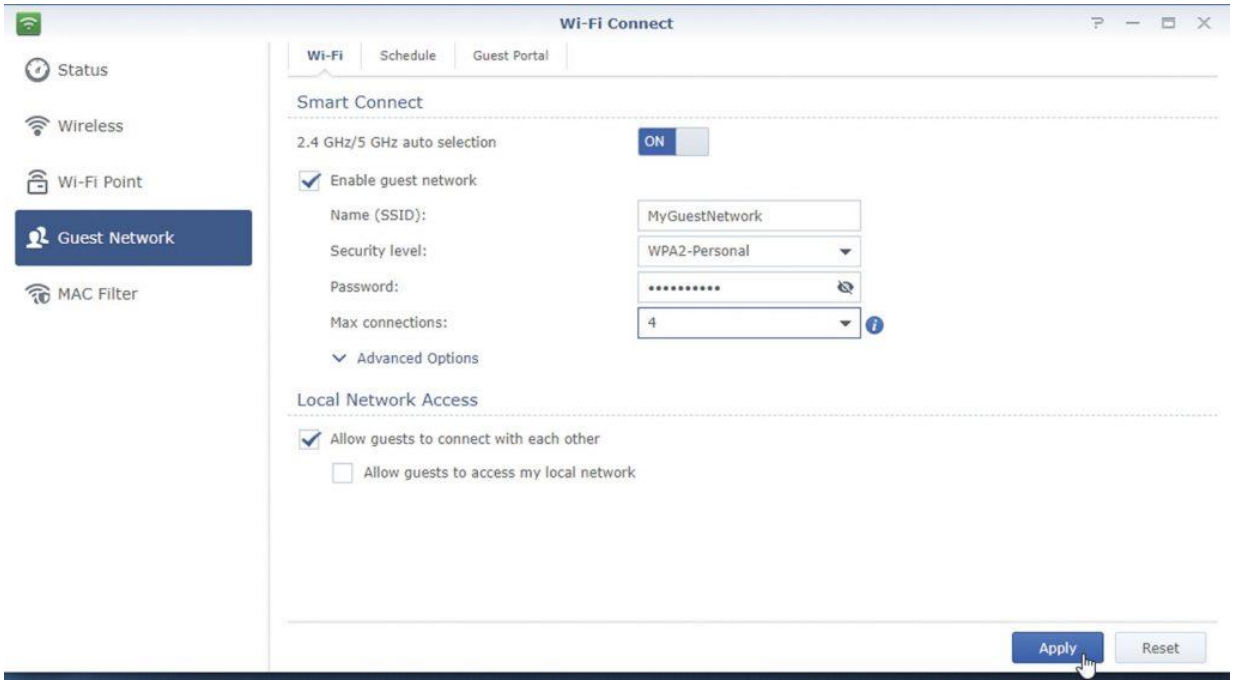
Du må heller ikke glemme alle dine trådløse enheder: tv, konsoller, tv-bokse og så videre. Du kan sandsynligvis ikke skifte udelukkende til WPA3, men med det in mente bør din WPA3-kompatible router tilbyde en bagudkompatibel indstilling, der giver WPA3 til de enheder, som understøtter denne kryptering, og WPA2-PSK/AES til dem, der ikke gør det. Når det gælder Synology, skal det konfigureres via Wi-Fi Connect > Wireless > Wi-Fi section. Vælg WPA2/WPA3-Personal fra rullemenuen.

Skift og skjul dit SSID

Dit netværk meddeler sig til andre ved hjælp af sit SSID, og der er to måder, hvorpå man kan styrke denne del af netværket. Først skal man ændre SSID-navnet. Standard-navnet omfatter som regel routerens model eller producent, og disse oplysninger kan hjælpe en determineret hacker til at opnå adgang til ens system ved at afsløre, hvilken hardware hackeren står over for. Man kan gøre det fra Wireless-sektionen af routerens konfigurationsfunktion.

Man kan gå videre og forhindre netværket i at meddele sin tilstede-værelse ved at frakoble SSID-broad-castsignalet (det er en simpel tjek-boks med “Hide SSID” på Archer VR900). Det forhindrer netværket i

at dukke op, når folk i nærheden scanner efter Wi-Fi-netværk, de kan koble sig til. Folk, der ønsker at få forbindelse til dit netværk første gang, skal manuelt indskrive SSID'et (derefter bliver de automatisk forbundet som sædvanlig).



Sørg for, at gæsteenheder er isoleret fra dit netværk.

Det er ingen perfekt løsning, eftersom hackere stadig nemt kan sniffe sig vej til SSID'et ved hjælp af legitime værktøjer som inSSIDer (www.metageek.com/products/inssider), men det afskrækker tilfældige forbipasserende. Vi tror, at det ekstra lag af sikkerhed opvejer det ubekvemme ved manuelt at skulle indtaste SSID'et, hver gang man skal forbinde en ny enhed til netværket.

Begræns gæsteadgang

Alle moderne routere tilbyder et separat trådløst gæstenetværk til besøgende og andre uregelmæssige brugere, og det er noget, som vi varmt vil anbefale, at du gør brug af, idet du igen bør bruge den bedste kryptering, din router understøtter, og med et stærkt kodeord.

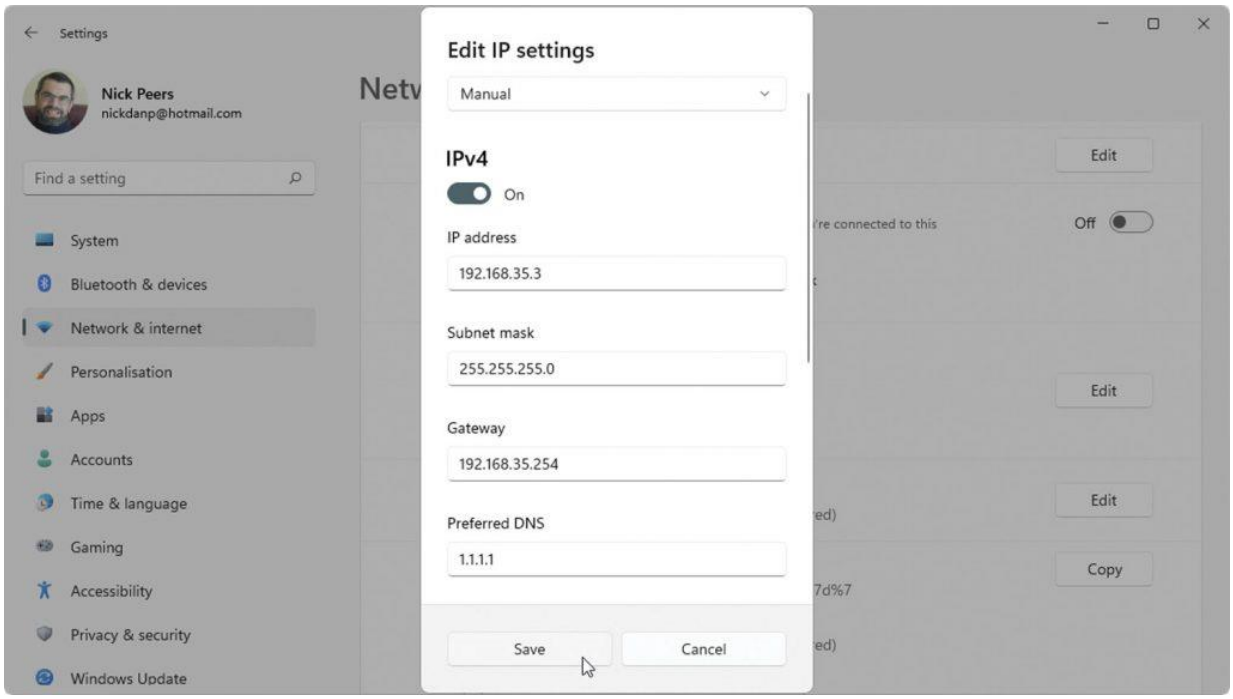
Som standard bør gæstenetværket forblive isoleret fra resten af dit netværk, således at mens gæster kan besøge internettet, kan de ikke bruge netværksressourcer såsom delte mapper eller printere eller kigge ind i delte mapper.

Alt afhængigt af din router kan du vælge at lade gæster se hinanden på gæstenetværket uden at give dem adgang til dit hovednetværk, og du kan trække en grænse for antallet af enheder, som kan være forbundet samtidig – overvej at reducere tallet til en eller to afhængigt af dem, der kommer på besøg. Synology-brugere kan også oprette en gæsteportal, som man kan bruge til at angive tidsbegrænsning for gæsternes brug af netværket.

Filtrering af MAC-adresser

En anden udbredt metode til at begrænse det, som enheder kan få adgang til, består i at oprette filtrering af MAC-adresser. Hver enhed bliver identificeret ved hjælp af en unik MAC-adresse – seks tocifrede heksa-decimale koder som for eksempel 00:0a:95:9d:68:16 – når den bliver forbundet til dit netværk.

Et MAC-adressefilter giver mulighed for at opsætte en liste over tilladte enheder baseret på deres MAC-adresser, hvilket i teorien forhindrer andre enheder i at få adgang til dit netværk eller internettet, også selvom de er korrekt forbundet til dit Wi-Fi-netværk. Indstillingerne er som regel nemme at finde. Brugere af Archer VR900 skal for eksempel gå til Advanced > Wireless > MAC Filtering. Vælg “Allow wireless access only from the devices in the list below”, og klik så Add for at aktivere dem en efter en.



Tildel ip-adresser manuelt, og slå din DHCP-server fra.

Din router bør allerede have registreret, hvilke enheder der er forbundet til dit netværk, således at du kan identificere dem ved navn og tildelt ip-adresse. Hvis det ikke er tilfældet, kan du bruge et gratis program ved navn Advanced IP Scanner (www.advanced-ip-scanner.com) til at lave en komplet liste.

MAC-filtrering er ikke skudsikkert, idet det er muligt for enheder at sløre deres MAC-adresser, men hvis hackere skal få adgang, skal de vide, hvilke MAC-adresser der er blevet hvidlistet og bruge et redskab som Technitium MAC Address Changer (https://technitium.com/tmac). Det er måske ikke en ideel løsning, men filtrering af MAC-adresser er alligevel en mulighed, man kan overveje.

Fravælg DHCP

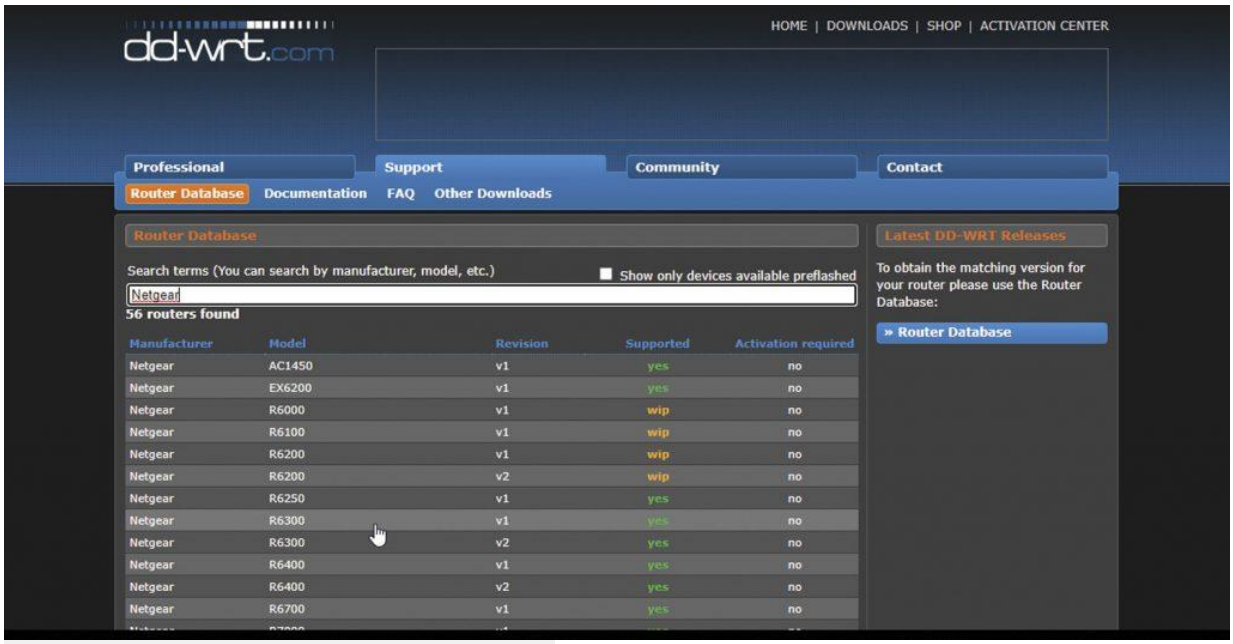
En lignende fremgangsmåde består i at fravælge din routers DHCP-server, som er ansvarlig for tildeling af ip-adresser til enheder, når de bliver forbundet til dit netværk.

DHCP svarer omtrent til at rulle den røde løber ud, og selvom det er praktisk, kan man overveje, om det er en bedre idé helt at fravælge denne protokol og satse på, at enhederne bliver manuelt konfigureret med de tre vigtige ting, du skal bruge: Din routers ip-adresse som gateway, subnet mask (255.255.255.0) og en unik ip-adresse, der bygger på samme subnet som din router, altså 192.168.x.y, hvor "x" svarer til routerens, og "y" er et tal mellem 0 og 255, der ikke er tildelt nogen anden enhed.

Hvis du vælger denne fremgangsmåde, er det en god idé at lave en liste over alle sine forbundne enheder (her kan Advanced IP Scanner være en hjælp) og derefter allokere ip-adresser til hver af dem, før du aktiverer dem efter tur. Hvis vi tager din Windows 11-pc som eksempel, skal du gå til Indstillinger > Netværk og internet og klikke Wi-Fi eller Ethernet (ved kablede forbindelser) efterfulgt af Rediger ved "IP-tildeling".

Skift til "Manuel", og skriv de krævede oplysninger. Hvis du vil tilsidesætte din routers DNS-adgang, kan du også gøre det her, før du klikker "Gem". Vi anbefaler, at du allokerer manuelle IP-adresser til alle dine enheder, før du til sidst fravælger DHCP Server (Synology-brugere kan for eksempel finde den under Network Center > Local Network > General tab).

Avanceret sikkerhedstrick



DD-WRT fungerer med en lang række routere.

Hvis din router er en ældre sag, og du ikke vil opgradere den, kan du gå ind på DD-WRT-websiden på https://dd-wrt.com/support/router-database, og se, om din routermodel er anført som kompatibel med den gratis alternative DD-WRT-firmware. Ellers kan du overveje at købe en billig router som TP-Link Archer C7 (cirka 500 kroner), som man kan gøre mere sikker med hjælp fra DD-WRT.

DD-WRT føjer nyttig funktionalitet til billige hjemmeroutere, herunder yderligere sikkerhedsredskaber som en firewall, VLAN-support og en VPN-server. Den bliver også regelmæssigt opdateret, således at din router er up to date. Det er ikke alle funktioner, der er til rådighed på hver enhed; efter at have bekræftet kompatibiliteten kan du prøve at google dit modelnummer og "dd-wrt" for at se, hvordan andre har båret sig ad.

Selvom hoved-DD-WRT- interfacet er enkelt nok at bevæge sig rundt i, er der nogle funktioner, som kræver et element af teknisk viden, og derfor bør du dykke dybt ned i DD-WRT-wikien (klik https://forum.dd-wrt.com/wiki/, og vælg “Tutorials”) for at se, hvad visse funktioner kræver af kompleksitet – OpenVPN-server er et sådant eksempel. Hertil kommer, at installation af DD-WRT potentielt kan stoppe din router.

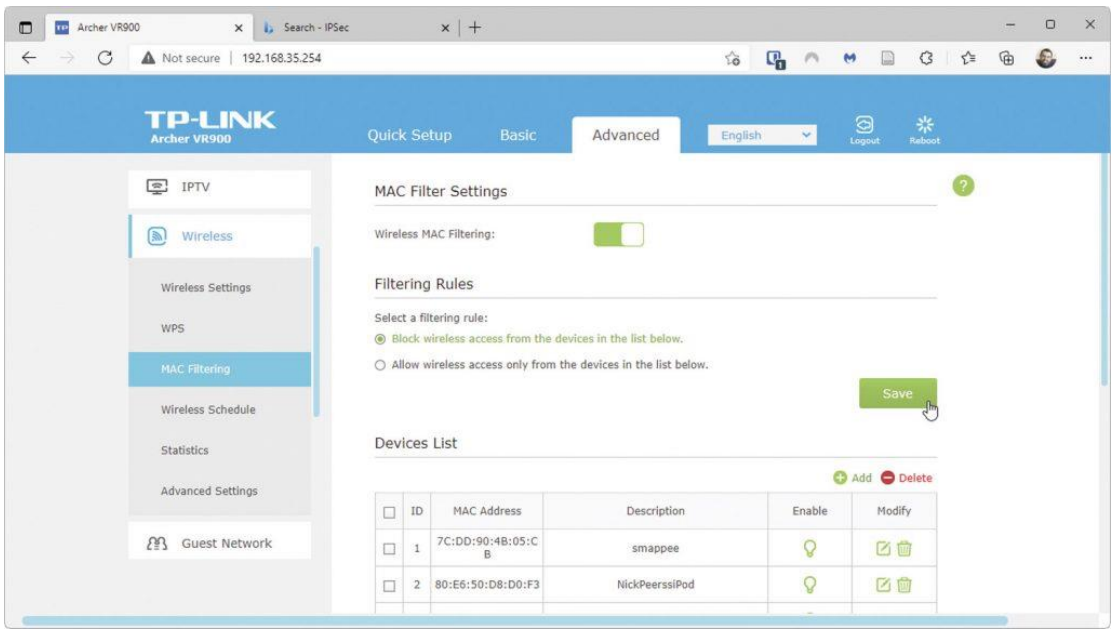
Derfor bør du sørge for, at du er fortrolig med proceduren. Giv dig tid, og download først et eksemplar af producentens firmware for det tilfældes skyld, at noget går galt. Hvis din router går i stå, kan du måske være i stand til at gendanne den via en hård nulstilling eller ved at bruge TFTP til at gendanne din oprindelige firmware.

Du kan få adgang til en TFTP-klient i Windows 11 via værktøjet “Turn Windows features on or off”. På https://forum.dd-wrt.com/wiki/index.php/Recover_from_a_Bad_Flash kan du finde oplysninger om gendannelsesprocedurer, hvis du får brug for dem. Husk, at hvis du beslutter dig for at installere DD-WRT på din router, gør du det helt og holdent på eget ansvar.

Sluk for WPS

Der er endnu et gabende sikkerhedshul, som skal lukkes, og det er WPS (Wi-Fi Protected Setup). WPS’ formål er at forenkle tilføjelse af kompatible enheder til dit netværk – man skal enten definere en pin eller trykke på en knap, der sætter din router i WPS-scanningtilstand. Når du trykker på den relevante knap på enheden, bliver den automatisk forbundet med dit Wi-Fi-netværk uden videre dikkedarer.

WPS er nyttig, når det gælder om at spare tid, men man bør ikke komme i vane med at lade den være aktiv, fordi enhver med pin-koden eller adgang til WPS-knappen på routeren kan bruge den til i smug at forbinde en enhed. Her kan man overveje at bruge indstillingerne til at frakoble begge funktioner, når de ikke er i brug. Se under Advanced > Wireless > WPS på en Archer-router, eller åbn Wi-Fi Connect, og gå til Wireless > WPS tab på en Synology-model, for eksempel.



Tjek dine porte

Nu, da dit netværk er lukket over for potentielle forsøg på fysisk indtrængen, er tiden inde til at beskytte dig selv mod angreb, der foregår online. Det er en god begyndelse at frakoble fjernadministration og ændre din routers kodeord, men lad os gå lidt længere end det.

Med henblik på at kommunikere med andre netværksenheder og tilgå tjenester over internettet er din router nødt til at åbne porte og give trafik mulighed for at bevæge sig frit fra et sted til et andet. Porte gør det nemt for trafik at nå frem til den korrekte destination, og nogle er velkendte, for eksempel 80 til http-webtrafik, 20 og 21 til FTP og 25 til at åbne en ukrypteret SMTP-forbindelse med henblik på at sende mail.

Der er teoretisk 65.535 porte til rådighed, men det antal, der kan bruges af tjenester, er tættere på 49.000. Enhver aktivitet, der involverer en server, uanset om den er hos-tet lokalt eller over internettet, gør brug af disse porte. Nogle af dem er officielle såsom 32.400 til Plex, mens andre er mere frie.

Før fremkomsten af Universal Plug ‘n’ Play (UPnP) var man nødt til at gå ind i sin router og arrangere disse porte manuelt, specificere portnummeret, dens protokol (TCP og/eller UDP) og dens destination på ens netværk (ip-adressen på serveren eller enhedstrafik på den port skulle omdirigeres eller routes).

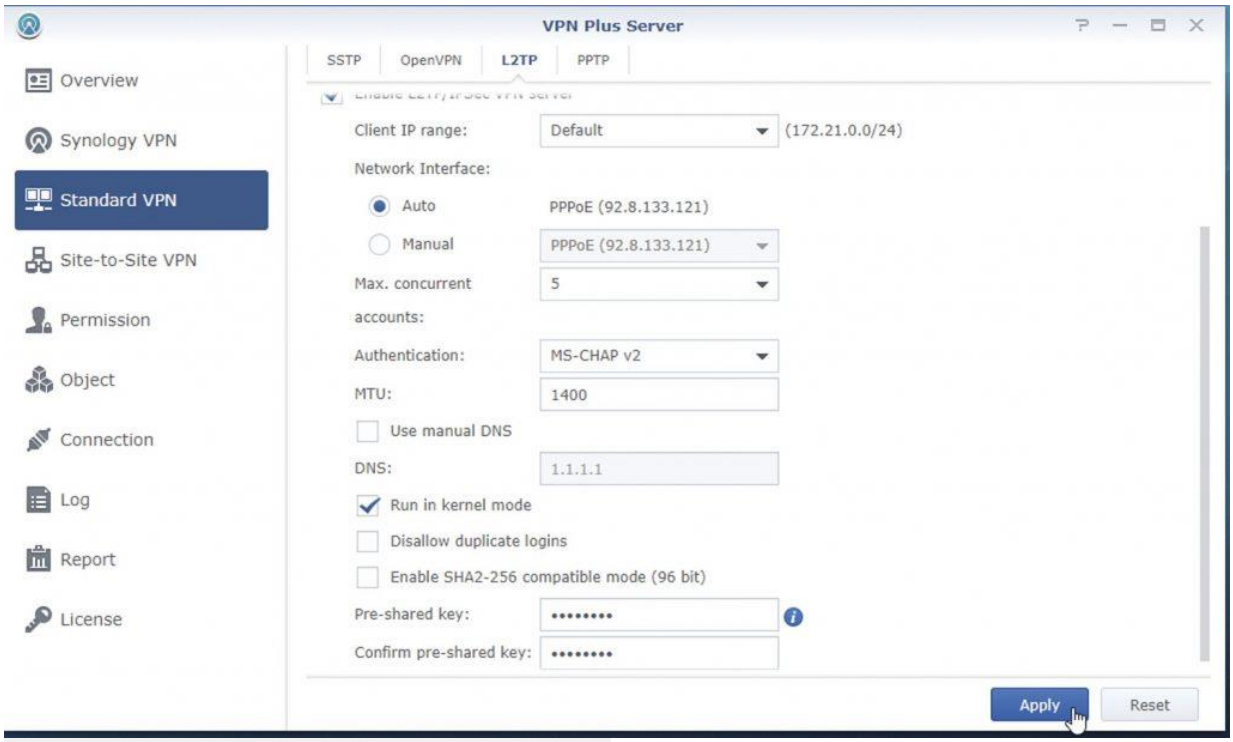
UPnP er en netværksprotokol, der er beregnet til at give samarbejdende enheder mulighed for selv at indstille disse regler – når en enhed anmoder om adgang til en specificeret port, bliver reglerne automatisk arrangeret. Det er glimrende for mageligheden, men ikke for sikkerheden.

Når disse porte bliver åbnet, kan de nemlig bruges til både ondsindede og legitime formål. Endnu værre er det, at selvom UPnP kun svarer på anmodninger om adgang fra ens lokale netværk, antager den, at disse anmodninger er legitime, og hvis der kommer malware på ens pc, kan den derfor åbne porte uden videre.

Den enkleste løsning består i helt at fravælge UPnP, men før man gør det, bør man danne sig et overblik over, hvilke porte der er blevet åbnet. Hvis man genkender dem, skal man manuelt oprette regler, der dækker dem. På en Archer går man til Advanced > NAT Forwarding > UPnP. Skriv ned, hvad der er på UPnP’s Service List: beskrivelse, ekstern port, protokol, intern ip-adresse og intern port. Det bør hjælpe dig med at identificere, hvad der er tale om.

Gå til sektionen Virtual Servers, og klik på “Add” for at tilføje dem en ad gangen. Service Name kan være hvad som helst, der kan hjælpe dig med at identificere det i fremtiden. Men husk at kopiere den anden information, nøjagtig som den er angivet. Når det er gjort, klikker du “OK” og går videre til den næste. Når alle dine tjenester er blevet arrangeret, vender du tilbage til UPnP og slår kontakten fra.

Ring sikkert hjem



Synology tilbyder en række VPN-servermuligheder.

Har du nogensinde været på farten og har haft brug for at tilgå dit hjemmenetværk, for eksempel for at kopiere filer til eller fra en delt mappe eller for at sende noget til din hjemmeprinter, så det kunne vente på dig derhjemme?

Hvis du bruger en VPN-server, kan du tilføje den funktionalitet uden at blotte dit netværk for angreb. VPN-serverer kræver opsætning af eksisterende hardware i dit hjemmenetværk. Det kan være på din SOHO-router (VPN Plus er en del af Synologys SRM-software), eller du kan føje den til din server: PiVPN (https://pivpn.io/) virker for eksempel med en ekstra Raspberry Pi, eller du kan finde support i dyrere NAS-drev fra for eksempel Qnap og Synology.

Du kan endda oprette en VPN-server på din Windows-pc, men så ville du skulle lade den være tændt og forbundet, mens du var væk, for at opnå adgang – Helpdesk Geek (https://helpdeskgeek.com/windows-10/how-to-set-up-the-windows-10-built-in-vpn-service/) er et eksempel på en praktisk guide. Når det drejer sig om forbindelse gennem en tredjeparts-VPN-tjeneste, anbefaler vi brugen af L2TP/IPSec-protokollen af hensyn til kompatibiliteten.

Husk at aktivere funktionen “Pre-shared key” for at tvinge brugere til at levere yderligere verifikation, før de får forbindelse. Du er nødt til at konfigurere din laptop for at få adgang til VPN-serveren, når du er ude på farten. I Windows 11 går du til Indstillinger> Netværk og internet > VPN og klikker på “Tilføj en VPN-forbindelse”.

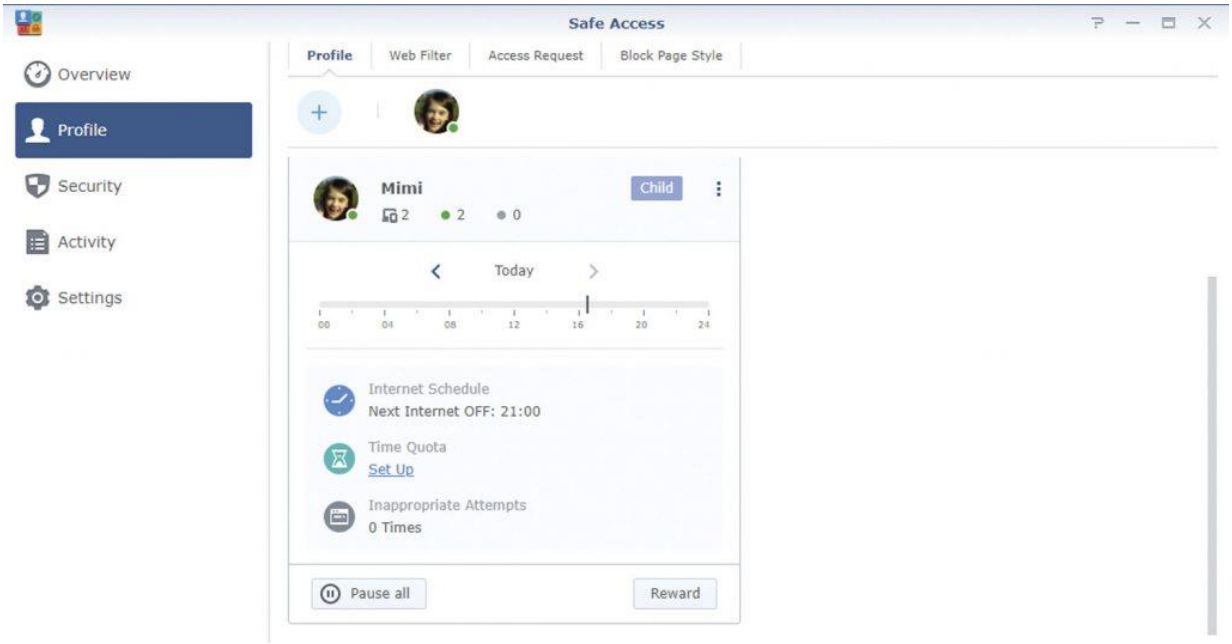
Vælg “Windows (indbygget)” som VPN-udbyder, giv din forbindelse et beskrivende navn, og udfyld felterne med de krævede oplysninger: servernavn eller adresse, der strengt taget er din offentlige ip-adresse (se www.whatsmyip.com), eller domæne eller dynamisk værtsnavn, hvis du har oprettet et.

Fortsæt med delt nøgle plus brugernavn og kodeord (se Permission-fanen på VPN Plus Server på din Synology-enhed). Og det er så det. Nu kan du få forbindelse til dit lokale netværk, når du er væk hjemmefra.

Overvej UPnP

Hvis du synes, at du ikke kan leve uden UPnP, kan du overveje dette kompromis: Indstil en reminder til en gang om ugen at tjekke for nye tjenester. Når de er godkendt, gentager du processen med at konvertere dem til virtuelle servere, hvorefter du igen slår UPnP fra for dermed at rydde listen.

Processen er lidt anderledes hos vores andet routereksempel, den mere avancerede fra Synology. Alting er praktisk placeret i et enkelt skærmbillede (Network Center > Port Forwarding > Port Forwarding tab), og man kan kombinere flere porte i en enkelt port-forwarding-regel (hvis du gør det, skal du imidlertid lade feltet “Private port” stå tomt – det vil automatisk vælge alle de porte, du har defineret under “Public port”).



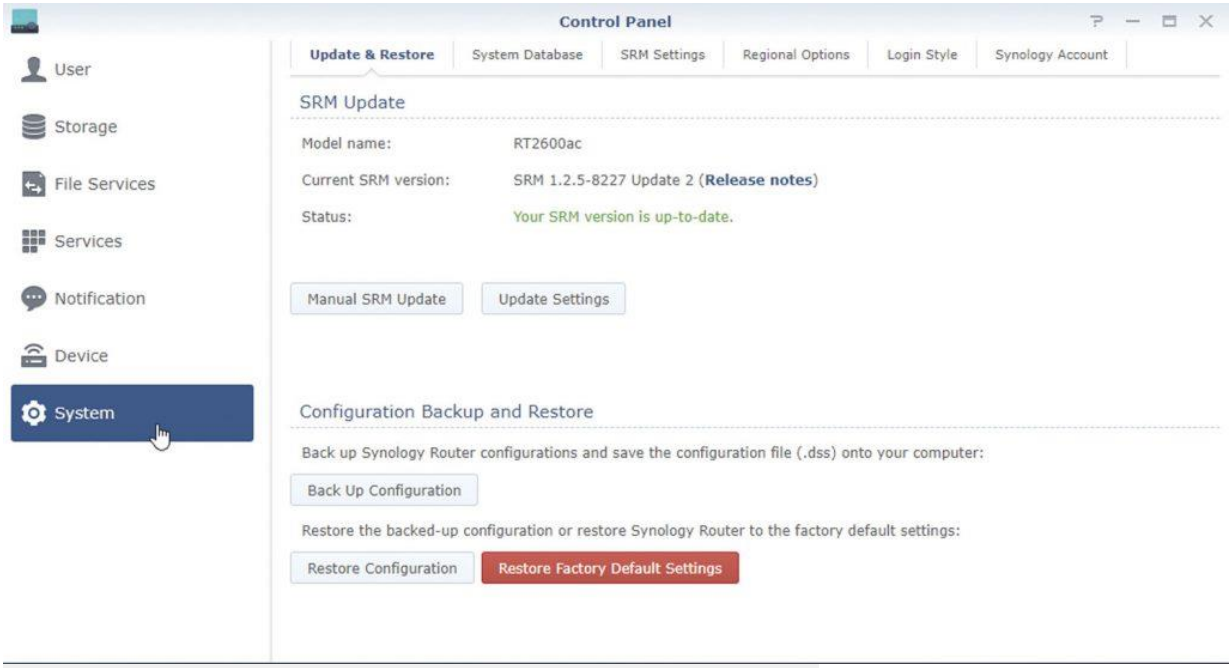
Med forældrestyring kan man beskytte bestemte medlemmer af husstanden.

Når du har oprettet en port-forwarding-regel her, forsvinder den tilsvarende UPnP-regel, men den kan komme igen, hvis en anden enhed på dit netværk prøver at tilgå den samme port. I modsætning til Archer VR900 har Synology-routeren en indbygget firewall, der scanner al trafik, når den kommer ind fra internettet.

Indstil forældrekontrol

Den er imidlertid konfigureret til automatisk at oprette regler, der giver adgang til de porte, som er blevet konfigureret her, enten manuelt eller via UPnP. Klik på knappen “Settings” for at ændre denne adfærd. Du kan eventuelt vælge at frakoble automatiske regler for UPnP-oprettede regler, men du er nødt til at huske selv at tilføje dem, når en ny tjeneste prøver at åbne en port.

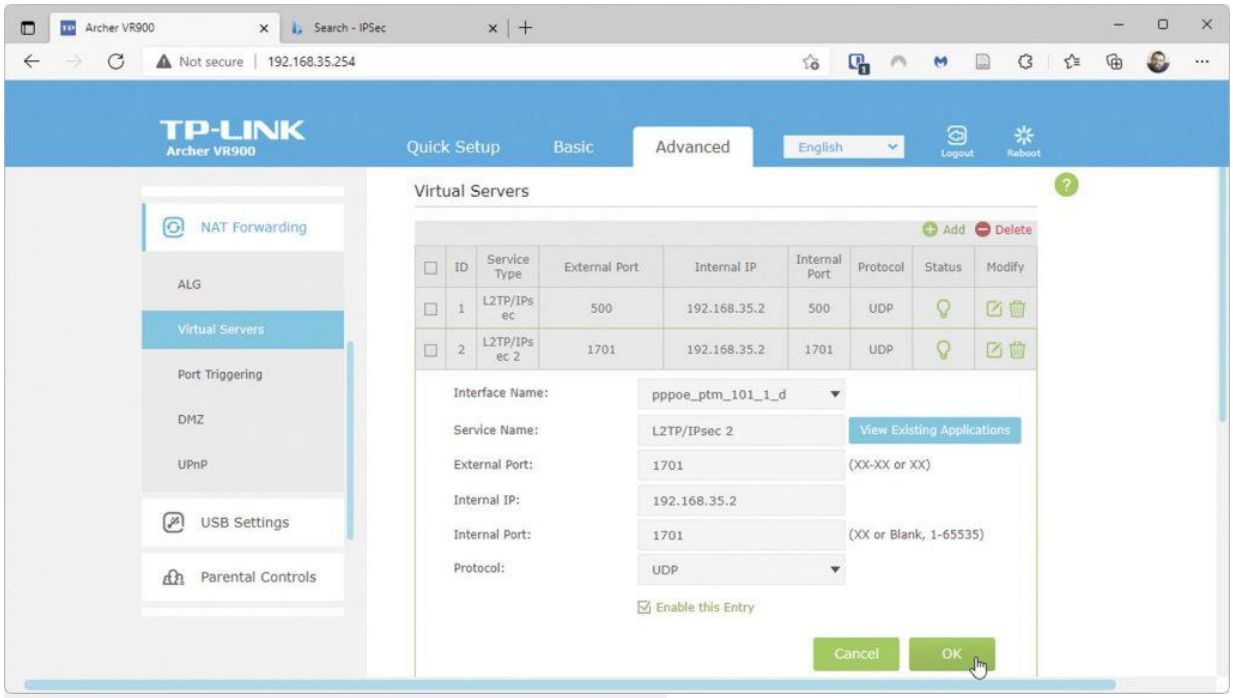
Hvis du vil slå UPnP fra på Synology-routeren, skal du skifte til sektionen Local Network, blade ned til sektionen DHCP Server og sætte menuen “Enable UPnP” til Disabled. Din router har formentlig også nogle enkle redskaber til forældrekontrol.



Luk potentielle sikkerhedshuller ved at opdatere din routers firmware.

Archer VR900 er typisk for de fleste forbruger-routere derved, at dens valgmuligheder er ret begrænsede: Man kan indstille tidsgrænser for specifikke enheder på baggrund af deres MAC-adresser, og man kan lave simple indholdsfiltre til blokering ud fra URL eller bestemte ord.

Synology scorer højest i denne henseende: Åbn Package Center, og klik “Open” ved siden af forældrestyrings-Safe Access. Reglerne bliver knyttet til profiler, der kan være personer i dit hjem (herunder alle deres enheder), alle ikketildelte enheder på dit netværk eller dit gæste-Wi-Fi.



Manuelle portforwarding-regler er mere sikre end UPnP.

Når tildelingen er foretaget, kan du begrænse brugernes adgang til internettet til specifikke tidspukter på dagen eller indstille et maksimalt tidsrum pr. dag. Ligesom i Archer-routeren er der et webfilter, som kan blokere efter kategori såvel som efter domæne. Der er skabeloner til børn, gæster, ansatte og så videre, og dem kan man selv finindstille. Og man kan endda definere et sidelayout, som brugerne ser, når de bliver fanget af filteret.

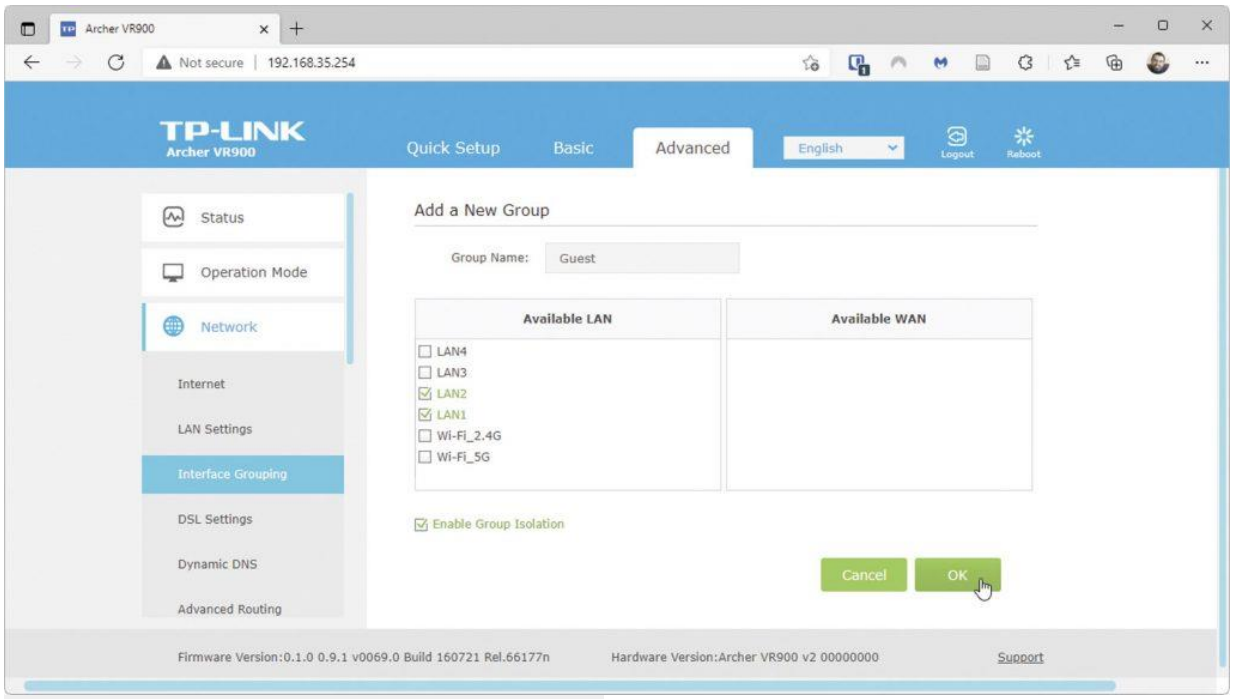
Safe Access forsyner også Synology-brugere med yderligere beskyttelse mod phishing, malware og potentielt uønsket software via Threat Intelligence-databasen og Google Safe Browsing (der kræves en API-nøgle til sidstnævnte).

Nul firmwareopdateringer

Opdateringer er en del af det at holde sig sikker online, men det er en trist kendsgerning, at de fleste forbruger-routere sjældent – hvis overhovedet – modtager firmwareopdateringer.

Hvis vi tager Archer VR900 som eksempel, findes den i tre hardwareversioner, og af dem har V2 ikke modtaget nogen firmwareopdateringer, mens V1 og V3 kun har modtaget en håndfuld. På den anden side modtager Synology-routerens SRM-operativsystem regelmæssige opdateringer og kan konfigureres til automatisk at søge efter opdateringer.

Uanset hvilken routermodel du har, bør du lede efter en mulighed for at tjekke for opdateringer i routerens konfigurationsfunktioner. Hvis der ikke er nogen, kan du læse i support-sektionen på routerens website og se, om der findes en, som du selv kan downloade manuelt og installere.



VLAN-support er indbygget i Archer VR900-serien.

Synology-routere har også en dedikeret Security-sektion under Network Center, og den er et besøg værd. Bemærk, at indstillingen “Enable DoS Protection” henvender sig mere til organisationer end til enkeltpersoner, fordi det ikke er sandsynligt, at du bliver offer, medmindre du afvikler tjenester direkte fra dit hjemmenetværk. Vi kan imidlertid anbefale brugen af fanen Auto Block, hvis du vil afværge angreb på routerens konfigurations-funktioner.

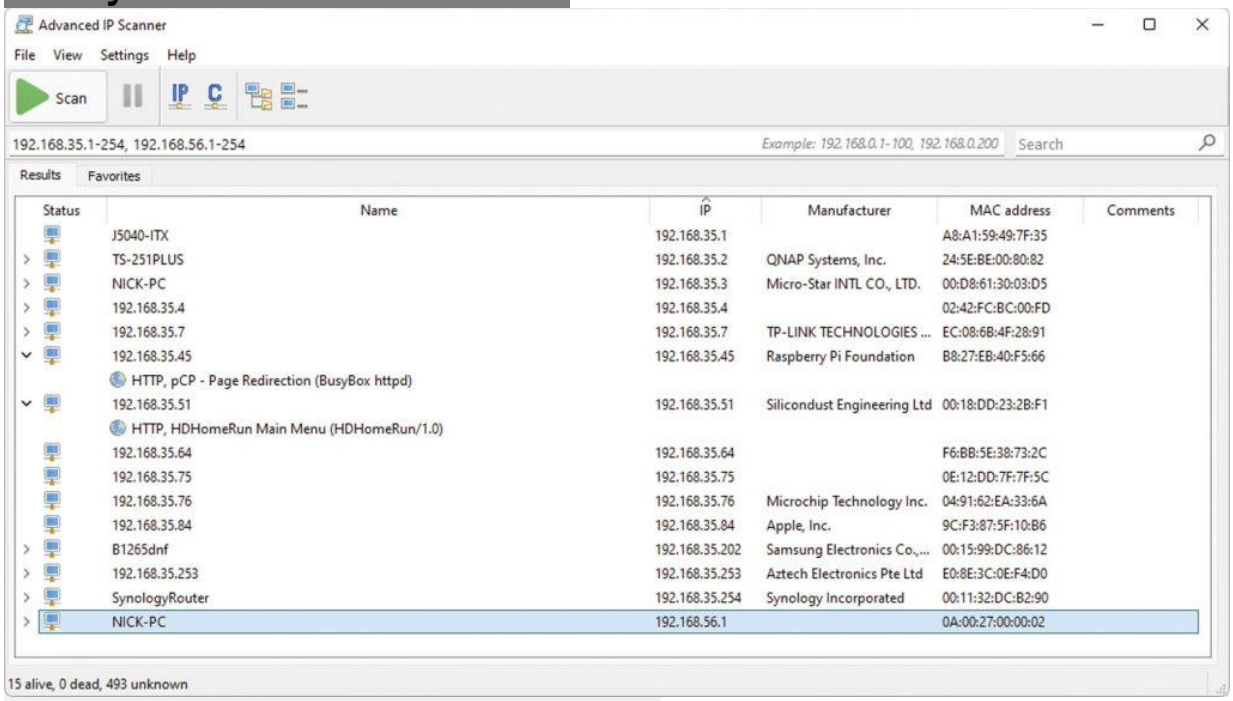
Hvis du gerne vil opdele dit netværk i “troværdige” og “utroværdige” zoner, eller du vil oprette separate og isolerede netværk, skal du undersøge, om din router understøtter VLAN. Det gør både Archers og Synologys routere; man kan separere kablet fra trådløs eller oprette separate hybride netværk (kablede eller Wi-Fi). Søg oplysningerne i din manual om den rette opsætning.

Den sidste boks afslører, hvordan man kommer sikkert ind i dit hjem ved hjælp af en VPN-serveropsætning på din router, men hvad med mere traditionelle VPN-tjenester, der gør det muligt at sløre ens sande lokation og kryptere data over utroværdige Wi-Fi-netværk?

Nogle routere, herunder den fra Synology, gør det muligt at opsætte en VPN-forbindelse på selve routeren, hvilket betyder, at alle enheder i ens hjem kan udnytte opsætningen uden at være separat forbundne.
På Synology-routeren skal du først undersøge, om din VPN-udbyder understøtter L2TP/IPSec eller OpenVPN (via konfigurationsfil) med henblik på den mest sikre forbindelse.

Gå så til Network Center > Internet, og klik på “VPN Settings” under “Primary Interface” for at arrangere forbindelsen. Husk dog, at VPN’er kan gå hårdt ud over ydelsen, og du vil derfor måske foretrække at nøjes med at beskytte individuelle enheder i stedet for at gøre hele din internetforbindelse langsommere.

Beskyt individuelle enheder



Identificer tilsluttede drev, og tjek hvert drevs sikkerhed.

Ved at sikre din router beskytter du indgangen til dit netværk, men det betyder ikke, at man kan ignorere sikkerheden i hver enkelt computer eller enhed, som du har forbundet til netværket. Husk, at dit netværk ikke er stærkere end det svageste led. Din Windows-pc vil i nogen udstrækning være beskyttet af den indbyggede Windows Security, men hvad med dine mobiler, tablets og andre forbundne enheder?

Teknisk set kræver iOS-enheder ikke sikkerhedsapps, men sørg alligevel for, at du kører den seneste version af iOS. Hvis du har installeret tredjeparts-beskyttelse på din pc, bør du finde en mobil-app som Bitdefender Mobile Security, der kan afsløre potentielle sårbarheder og give en vis e-mail- og web-beskyttelse. Android-enheder kræver antivirus ligesom din pc, og det er god praksis også at beskytte Mac-maskiner.

Tiden er måske inde til at købe en sikkerhedspakke til flere enheder fra for eksempel Eset for at dække alle dit hjems vigtigste enheder med et enkelt abonnement. Så er der elementer som dit internetforbundne tv eller som smarte enheder.

I forbindelse med disse enheder bør du sikre dig, at de er indstillet til automatisk at modtage og installere opdateringer, eller du bør give dig tid til at foretage en komplet afprøvning af dine enheder ved hjælp af Advanced IP Scanner (www.advanced-ip-scanner.com) eller et lignende værktøj.

Tjek også hver enhed manuelt for at se, om der findes opdateringer. Du kan også overveje at isolere nogle enheder fra resten af dit netværk. Undersøg, om din router understøtter VLAN – det gør VR900, både kablet og trådløs. Synology-routere skulle få denne support i den næste opdatering af SRM-operativsystemet (1.3).

Hvis der er trådløse enheder, og du vil være ekstra sikker, bør du placere dem på dit gæstenetværk, således at du sikrer dig, at dine gæster ikke har adgang til dit hoved-netværk. Det vil muligvis ikke være praktisk, hvis disse enheder kræver adgang til lokale netværksressourcer for at kunne fungere korrekt.