

Sådan gør du dine internet-ting sikre

My Router: Nighthawk RAX80

English

BASIC ADVANCED

ADVANCED Home

VLAN / Bridge Settings

☒ Enable VLAN / Bridge Setup

☒ By bridge group

Wireless



Zyberdata
11-03-2022
Randi Mortensen

VEJLEDNING

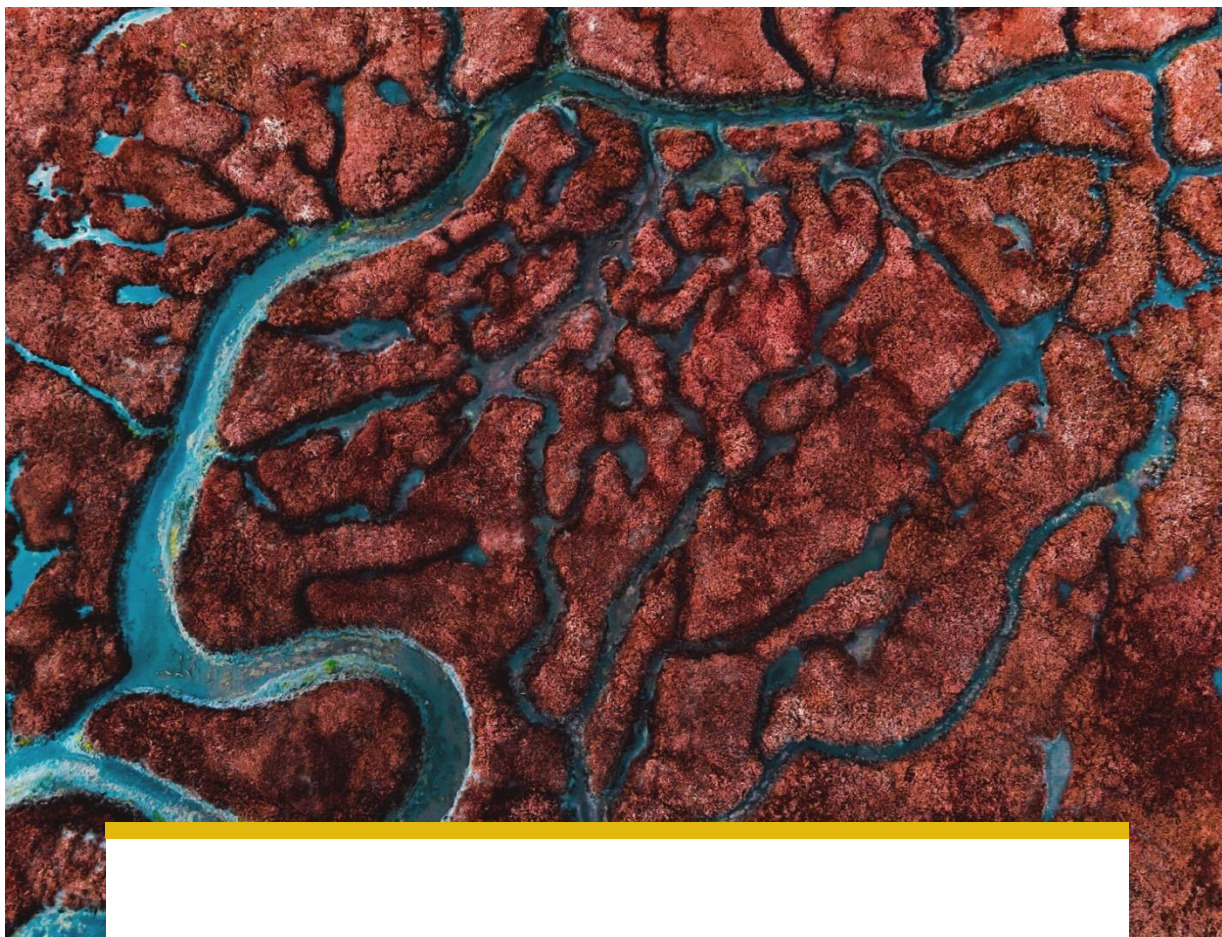
Internet Ting

Flere og flere af vores ting er tilsluttet internet. Det kan være alt fra overvågningskameraer over højttalere til termostater. Dermed er de udsat for at blive hackede. Læs her hvordan du beskytter dem

...

TV tilsluttet nettet





Sikre Internet Ting

Flere og flere af vores ting er tilsluttet internet. Det kan være alt fra overvågningskameraer over højttalere til termostater. Dermed er de udsat for at blive hackede. Læs her hvordan du beskytter dem ...



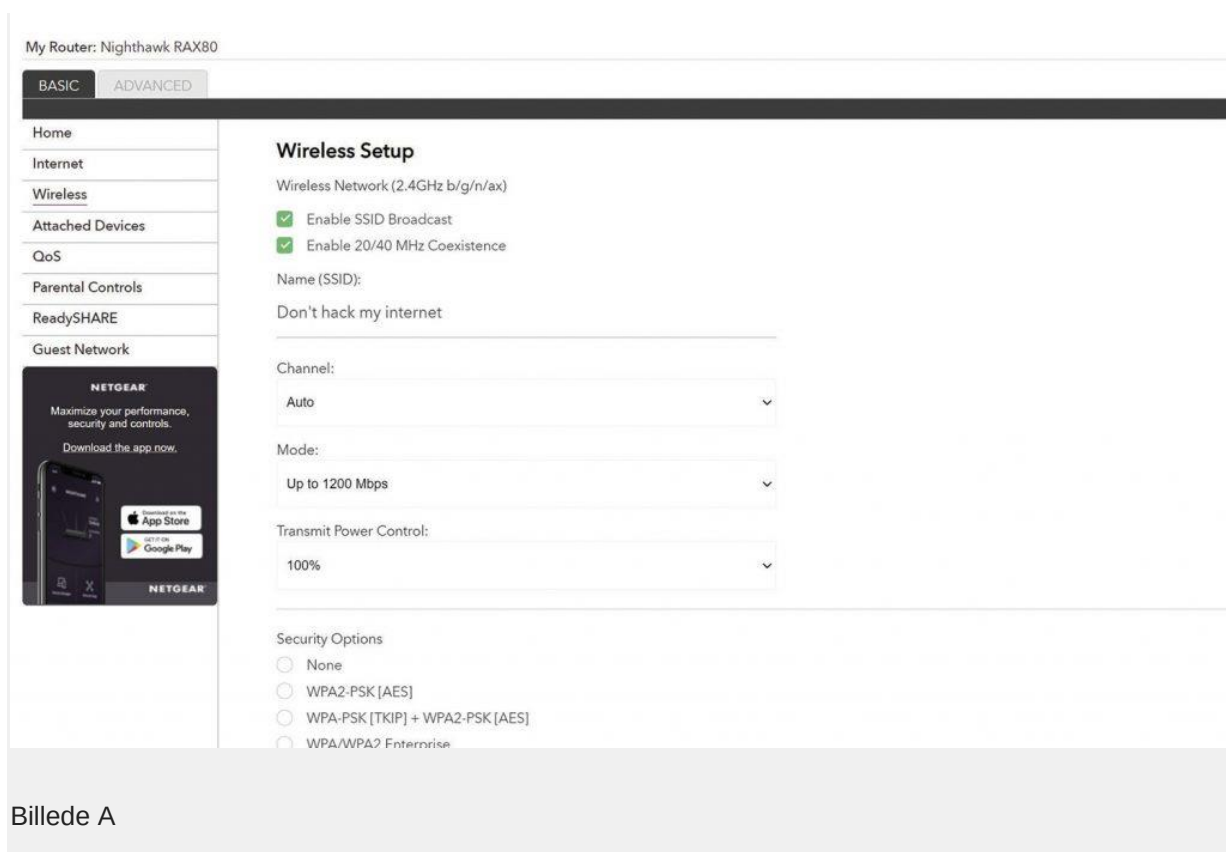
Mange af disse IoT-enheder er usikre fra det øjeblik, man installerer dem på sit hjemmenet og giver dem ubegrænset adgang til både det og selve internettet. Basale sikkerhedsproblemer såsom generiske kodeord og fjernadgang tilsluttet som standard er relativt nemme at ordne. Men der er også nogle ting, man kan gøre på sin router for at være med til at øge sikkerheden.

1 Netværkssikkerhed

Du kan gøre mange ting med din router for at forhindre, at ubudne gæster skaffer sig adgang til dit hjemmenetværk. Den første består i at ændre navnet på ens SSID til noget, der ikke angiver routerens producent.

Husk, at det navn, du vælger, bliver rundsendt til naboernes boliger. Derfor bør man afgjort undgå navne som "Overvågningsvogn fra PET" eller "Nummer 42: Vi hader din skodmusik", hvis man går ind for godt naboskab. Prøv at undgå at inddrage personlig information i navnet. Altså ikke "Dette er familien Johansens Netgear-router" [Billede A].

Hvis du kan leve med et skjult SSID, er det endnu bedre. Dit trådløse net bliver nemlig ikke nær så synligt for folk med en laptop, der bugner af hackerværktøj og med en hang til skarnsstreger. Det er imidlertid ikke alle, der er villige til at leve med den løsning, og derfor er det næste, du skal undersøge, om du bruger den bedste krypteringsprotokol, som din router kan mønstre.



Billede A

Nye enheder skal understøtte WPA3 for at få deres Wi-Fi-certificering, men WPA2 med dens obligatoriske AES-kryptering er stadig en anvendelig mulighed. Hvis man bruger WPA eller endda WEP

og går op i sikkerhed, bør anskaffelse af en ny router stå øverst på ens huskeseddel. Og hvis man har en ældre enhed, der ikke kan få adgang til et WPA2-netværk, er det bedre at opgradere den end at løbe en sikkerhedsrisiko.

2 Separer dine bånd

De fleste IoT-enheder bliver forbundet ved 2,4 GHz, og man kan derfor flytte enheder til 5 GHz-båndet, hvis ens router understøtter det, uden nogen sikkerhedsproblemer. 2,4 GHz-netværket har bedre række-

vidde, men lavere hastighed, og det kan derfor potentielt opfange overvågningskameraer og Wi-Fi-lamper længere væk uden behov for en booster.

Det betyder, at det hurtigere 5 GHz-netværk uhindret kan betjene ens telefon, tablet og pc. Man får en hurtigere og mere stabil forbindelse via Ethernet, og derfor kan man tilslutte faste enheder som smart-tv, desktop-pc'er, NAS-bokse og medieservere og dermed lette presset på ens Wi-Fi-bånd.

Tæt på indstillingerne

My Router: Nighthawk RAX80

BASIC	ADVANCED
ADVANCED Home	
Setup Wizard	
WPS Wizard	
Setup	—
Internet Setup	
Wireless Setup	
WAN Setup	
LAN Setup	
QoS Setup	
Guest Network	
USB Functions	+
Security	+
Administration	+
Advanced Setup	+

1

2

3

Wireless Settings (2.4GHz)

Wireless AP
On

Broadcast Name
On

Wi-Fi Protected Setup
Configured

Guest Network (2.4 GHz)

Wireless AP
Off

Broadcast Name
Off

ASUS RT-AX88U Powered by Asuswrt-Merlin Logout

Operation Mode: **Wireless router** Firmware Version: **386.3_2** SS

Quick Internet Setup

General WPS WDS Wireless MAC Filter RADIUS Setting

Wireless - Professional

Wireless Professional Setting allows you to set up additional parameters

* Reminder: The System time zone is different from your locale setting.

Band	2.4 GHz
Enable Radio	☒ Yes ☐ No
Enable wireless scheduler	☐ Yes ☒ No
Set AP Isolated	☐ Yes ☒ No
Roaming assistant	Enable Disconnect
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Disable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	3
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable

General

Network Map

AiMesh

Guest Network

AiProtection

Adaptive QoS

Traffic Analyzer

Game

Open NAT

USB Application

AiCloud 2.0

Tools

Advanced Settings

Wireless

LAN

WAN

Alexa & IFTTT

IPv6

1. Advanced

Det er her i Netgear-routeren, de interessante redskaber er. Se også sikkerhedsfunktioner under Basic.

2. Guest Network

Både vores Netgear- og Asus-router (til højre, med Merlin-firmware) gør det nemt at indstille gæstenetværk.

3. Advanced setup

Her finder man VLAN-indstillinger, og dem bør man læse op på, før man går i gang.

4. Asus

General Settings Gæstenetværket står højt placeret på Asus' liste, og her er der tre netværk mod blot et hos Netgear.

5. Wireless

Settings Her finder vi sikkerhed, filtrering, en blokeringsliste og avancerede Wi-Fi-indstillinger samlet på ét sted.

6. AP Isolated

En nyttig indstilling, som kan afskære et adgangspunkt fra resten af netværket.

3 Gæstenetværk

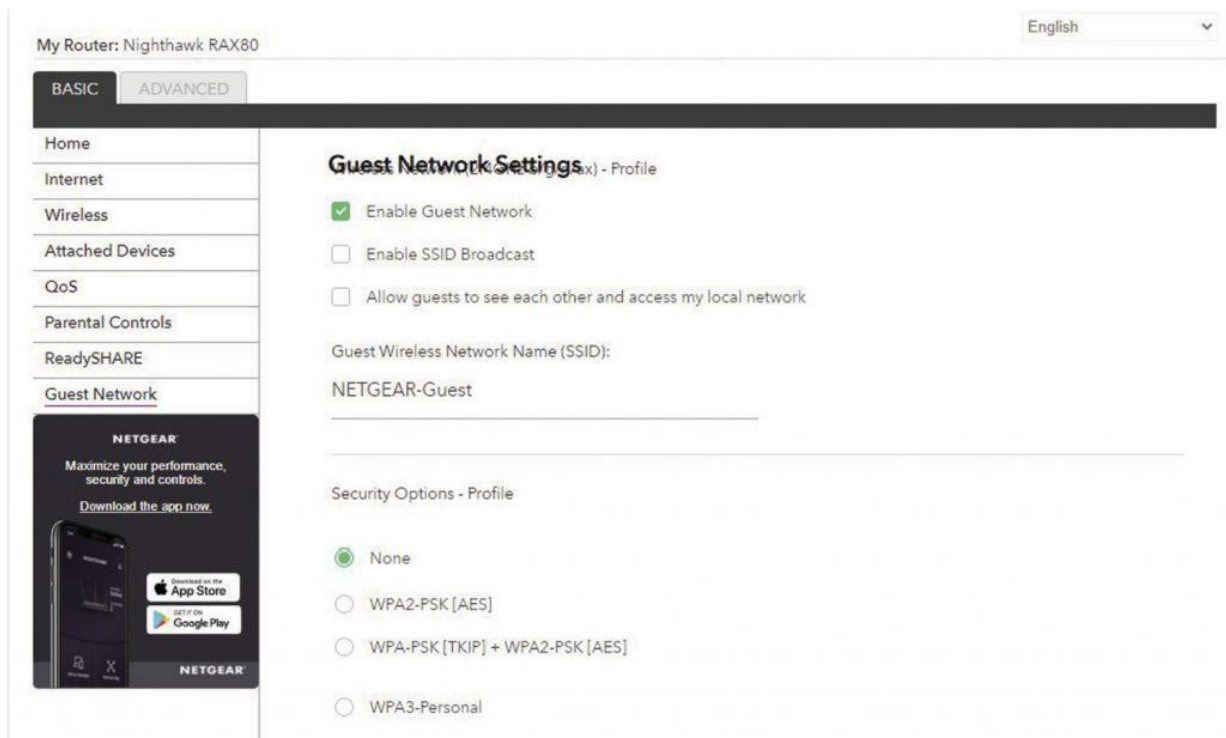
Mange routere understøtter et ekstra virtuelt "gæstenetværk", der er adskilt fra det primære net. Det er ikke tænkt som en sikkerhedsforanstaltning, men som noget man kan tænde for, når familien er på besøg, og man nødt vil udlevere sit kodeord.

Det er også nyttigt, hvis man har en butik og vil tilbyde kunderne internetadgang. På grund af dette nets isolation fra resten af nettet har det dog sikkerhedsgevinster – så længe denne isolation er slået til. I nogle routere er det slået til som standard, med andre skal man klikke i en boks. Nogle går endnu videre og isolerer enheder på gæstenetværket fra hinanden.

Det er godt nok, men det virker begge veje. Hvis man har isoleret en enhed, således at den ikke kan hoppe på ens hovednet, kan man heller ikke få adgang til den fra dette net. Heldigvis tilgår apps som Alexa ikke ens enhed direkte over netværket, men både appen og enheden taler til den samme server i et datacenter et eller andet sted.

Hvis man har brug for at gå direkte til ip-adressen for den enhed, der er i den interne pulje, som bliver styret af routerens DHCP-server, skal man enten reducere sikkerheden eller slutte den til 2,4 GHz-netværket.

Vores Netgear AX-router til hjemmebrugere har kun begrænsede valgmuligheder og viser kun i ringe grad gæstenetværket [Billede B]. Vi kan oprette et gæste-netværk på enten 2,4 GHz- eller 5 GHz-båndene, vise eller skjule SSID'et og vælge, om der skal tilføjes sikkerhed eller ej.



Billede B

Det vigtigste er, at der er en tjekboks, som kan forhindre, at gæsteenheder ser hinanden på hovednettet. Til IoT-enheder bør denne boks være markeret. Bemærk, at Google-routere slet ikke tilbyder dette sikkerhedsniveau og i stedet tillader gæsteenheder at blande sig med andre.

4 Gæstenetværk og Pi-holes

Hvis man bruger programmet Pi-hole til at blokere reklamer, skal man tillade disse gæsteenheder at få adgang til det, fordi det fungerer som netværkets DNS-server og dermed som porten til det globale internet. Det er et spørgsmål om ens routerfirmware.

Man skal tilføje ens Pi-holes ip-adresse. Den funktion figurerer ikke i indstillingerne for vores Netgear-router, og det samme gælder for nogle få andre mærker, herunder Apple og TP-Link.

De eneste muligheder synes at være at tillade gæsteenheder at se hinanden og hovednetværket, hvilket går stik imod intentionerne, eller at finde en særlig routerfirmware, som ikke åbner en række andre sikkerhedshuller undervejs.

Tip: Opsæt en ekstra router

Man kan udvide sit netværk ved at føje en gammel eller ubrugt router til nettet og opnå ekstra Wi-Fi-net, hvis hovedenheden ikke tilbyder mere end to. Det er dog klogt at sikre sig, at den sekundære enhed ikke er for gammel – er den det, kan den blive en sikkerhedsrisiko.

Man skal først sætte den sekundære router i access point-tilstand, og det kan variere fra producent til producent, hvordan det gøres. På vores Netgear-router fandt vi det under Advanced > Advanced Setup > Wireless AP, men andre modeller kan have andre metoder. AP-tilstand slukker for routerens modemfunktioner og underkaster den DHCP-tjenesten, som kører på hovedenheden.

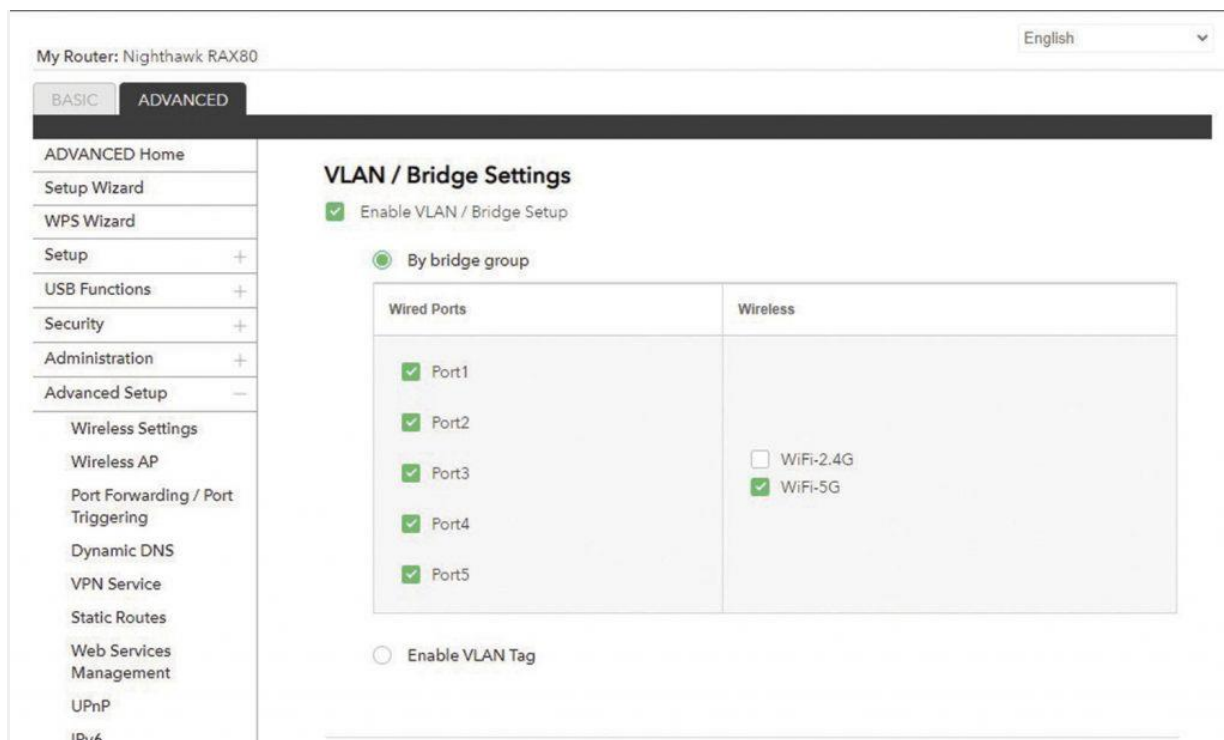
Den bliver ved med at lede efter de trådløse net, den kan vise – typisk et på 2,4 GHz og et på 5 GHz, men man behøver ikke at bruge dem begge – og fører al trafik gennem hovedrouteren til hovednettet eller internettet. Der er stadig ingen mulighed på Netgear-firmwaren for at isolere en sekundær router fra resten af netværket, men man kan bruge et VLAN til at adskille dem fra hinanden.

5 VLAN

Et Virtual LAN svarer til et forstærket gæsternetværk. Routersecurity.org sammenligner et VLAN med et akvarium. Hvis man har to akvarier, kan fiskene i det ene ikke interagere med fiskene i det andet. Anbring et forhæng (eller et VLAN) mellem akvarierne, og så kan de heller ikke se hinanden.

Forkert konfiguration af et VLAN kan betyde tab af internetforbindelse, mange routergenstarter og generel irritation for enhver på netværket. Man skal være forsigtig. På vores Netgear-router er det den sidste valgmulighed i Advanced > Advanced Setup.

Anbring dine Ethernet-porte og dit 5 GHz-Wi-Fi-netværk i ét VLAN, og læg 2,4 GHz-netværket i et andet. Begge har adgang til internettet – enheder på 5 GHz-Wi-Fi og Ethernet kan tale med hinanden, men enheder på 2,4 GHz kan ikke interagere [Billede C].



Billede C