

STOPPA HOTEN INNAN DE NÅR DATORN

Nu blir din router ännu säkrare

Den senaste generationen routrar som finns i butikerna har ofta ett direkt skydd mot hackare, virus, nätfiske och andra hot, så att alla enheter i nätverket skyddas.



Journalist
Henning Rasmussen

I årtal har det främsta skyddet mot skadliga webbplatser, virus, falska annonser och nätfiskeattacker varit de säkerhetsprogram som installerats på datorn. Nu har allt fler tillverkare av fysisk nätverksutrustning börjat bygga in förbättrad säkerhet i sina trådlösa routrar, ofta i samarbete med ett något erkänt säkerhetsföretag.

Om du köper en router av märket TP-Link i den dyrare prisklassen kan det inkludera ett säkerhetspaket som heter HomeCare. Det tillhandahålls av antivirusstillverkaren Trend Micro och ger dig föräldrakontroll, antivirus och ett skydd mot de flesta onlinehot. Säkerhetspaketet HomeCare köps och betalas tillsammans med routern för

produktens hela livstid. Tillverkaren Asus lösning kallas AiProtection, som även den kommer från Trend Micro. Tjänsten ingår i priset och finns till exempel i modellen RT-AX5400, som finns tillgänglig för cirka 2 000 kronor.

Allt fler tillverkare hakar på

Netgear har routrar som inkluderar ett säkerhetspaket som tillhandahålls av Bitdefender. Lösningen kallas för Armor och den skyddar alla typer av enheter som ansluts till nätverket mot hot som virus, spyware, ransomware och farliga länkar. Den har även en inbyggd VPN-tjänst, även om du bara får använda 200 megabyte per dag. Den nya trenden med säkerhet som är inbyggd i routrar har även börjat leta sig fram till internetleverantörer som vill kunna skryta med att kunna erbjuda den extra säkerhet du får med

deras modem och routrar. Om du har en internetleverantör som levererat en Sagemcom-router av modellen FAST380v2 eller FAST380v3, kan du ha haft inbyggd säkerhet sedan 2023.

Det är främst två stora fördelar med en säkerhetslösning i en routern. En är att routern blir ett extra lager av skydd mot internet som hot måste forcera innan de ens når enheterna på nätverket och deras respektive skydd.

En annan fördel är att, eftersom all trafik går genom routern och därmed måste passera det skyddslagret, så skyddas alla enheter i nätverket. Det spelar ingen roll om det är Windows-datorer, Android-enheter, Iphone eller ett smart kylskåp.

Att ha skydd inbyggt i routern tar dock inte bort behovet av vanliga säkerhetsprogram. Routerskyddet är ett komplement, inte en ersättare.





Så skyddas du av den nya generationens routrar

Du har förmodligen redan ett grundläggande skydd i din router, men med de senaste routrarna har säkerheten nått en ny nivå.

Säkerhet	Tidigare routrar	Nya routrar
Brandvägg	Ja	Ja
Säkra lösenord	Ja	Ja
Kryptering med WPA3 och WPS	Ja	Ja
NAT-skydd	Ja	Ja
VPN	Kanske	Ja
Föräldrakontroll	Nej	Ja
Smart app till mobilen	Nej	Ja
Antivirus	Nej	Ja
Skydd mot farliga webbplatser	Nej	Ja
Automatisk uppdatering av firmware	Kanske	Ja
DNS-blockering	Nej	Ja

EXPERT:

Du behöver fortfarande skydd för din dator

När tillverkare pratar om den nya routersäkerheten får de det ofta att låta som att du med lösningen inte behöver installera ett säkerhetsprogram på datorn eftersom du är skyddad redan innan datatrafiken når dina enheter. En av världens ledande säkerhetsexperten tycker dock att det är en dålig idé. David Jacoby, som är rådgivare till ett antal stora säkerhetsföretag och som har hackat allt från skrivare till Mac-datorer, har erfarenhet av området från ett samarbete med en svensk internetleverantör.

Han säger att idén med den nya inbyggda säkerheten i grunden är bra, men att användarna måste förstå exakt var de är skyddade och var de inte är det. Han säger att det är omöjligt att få samma skydd från routern som man får när säkerheten installeras direkt på datorn. Därför ska man inte kompromissa med säkerheten på datorn, även om man har skydd i routern. Hans råd är att man ska vara mycket försiktig på nätet och att ha tvåstegsverifiering där det går, eftersom säkra routrar inte ger dig fullständigt skydd.



David Jacoby är hackare och en erkänd säkerhetsexpert.

Nya routrar är säkra som Fort Knox

Alla routrar har inbyggd brandvägg och kryptering av trafiken mellan varje enhet i nätverket, men med den förbättrade säkerheten som finns i den nya generationens routrar får du ett stort utbud av ytterligare säkerhetsfunktioner.

Säkra lösenord

Nyare routrar låter dig använda ett långt och säkert lösenord som kan vara betydligt mer än tio tecken långt och innehålla bokstäver, siffror och tecken. Dessa omständliga lösenorden skyddar routern från ändringar i inställningarna som i sin tur skulle kunna äventyra din säkerhet.

Brandvägg

Routerns inbyggda brandvägg blockerar otillåtna anslutningar från internet till enheter i det lokala nätverket. Tack vare brandväggen kan en hackare inte komma åt enheter som din nätverkshårddisk eller en dina nätverkskameror.

Kryptering med WPA3 och WPS

Med det senaste säkerhetsprotokollet WPA3 krypteras trafiken mellan routern och dina enheter så att data inte kan fångas upp av obehöriga. Dessutom hjälper den inbyggda WPS-funktionen dig att skapa en säker anslutning till nätverket genom att bara trycka på en knapp på en skrivare, en repeater eller någon annan nätverksenhet.

NAT-skydd

Din router innehåller en funktion som kallas NAT, en förkortning för Network Address Translation. Den funktionen ser bland annat till att maskera IP-adresser för enheter i nätverket när de kommunicerar med servrar på Internet.

Antivirus

Genom att samarbeta med säkerhetsföretag som F-Secure, Trend Micro, Avira och Bitdefender kan routertillverkare erbjuda virussökning direkt i routern, vilket blockerar farliga filer innan de når din dator eller andra enheter. Det är också användbart för enheter som skrivare och nätverkshårddiskar.



VPN

Med VPN-funktionen kan din router skapa en krypterad anslutning till en server på internet och sedan dirigera all din trafik genom den servern. När du besöker webbplatser kommer du att ha den servern som avsändaradress istället för din riktiga IP-adress hos internetleverantören.

Skydd mot farliga webbplatser

I de nya routrarna ingår en så kallad molnlösning från ett erkänt säkerhetsföretag som tillhandahåller en ständigt uppdaterad lista över farliga webbadresser, som sedan blockeras av routern. På din dator får du veta att en webbplats är otillgänglig när du försöker besöka den i din webbläsare om den är blockerad av routern. På så sätt skyddas du mot nätfiske eller skadlig kod från webbplatsen.

Automatisk uppdatering av firmware

Det är få personer som regelbundet loggar in i sin router för att se om det finns nya uppdateringar av routerns inbyggda programvara. Därför är det viktigt att routern på egen hand kan kontrollera och uppdatera sin firmware när en ny version finns tillgänglig. På så sätt säkerställs att nylupptäckta säkerhetshål täpps till så snabbt som möjligt.

Föräldrakontroll

På de senaste routrarna finns det föräldrakontroll som hjälper dig att sätta upp regler för dina barns mobiler och surfplattor. Det kan handla om surf-tider och att blockera webbplatser som har osmakligt innehåll.

App till mobilen

Det är mycket enklare att hantera säkerheten i routern när du kan göra det med en app i mobilen istället för att gå den vanliga vägen via webbläsaren i datorn. Med de nya routrarna kan du både anpassa säkerheten och ställa in den nya funktionen för föräldrakontroll direkt från appen i mobilen. Med det här alternativet behöver du inte komma ihåg en besvärlig adress för att ansluta till routern. Appen är kopplad direkt till routern och när du ändrar inställningar börjar de gälla direkt.

DNS-blockering

DNS är en tjänst som översätter webbadresser till numeriska IP-adresser, och den används också i somliga länder för att censurera och blockera oönskade webbplatser. På nyare routrar kan du använda DNS för att blockera oönskade webbplatser eller webbplatser som innehåller skadlig kod och nätfiskeförsök.

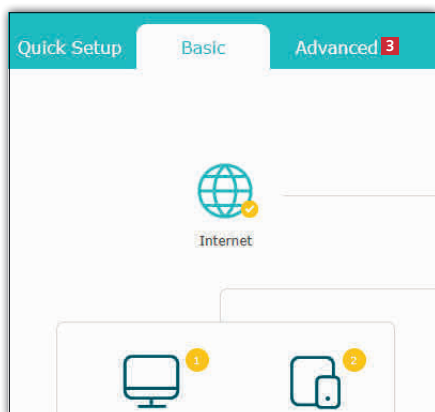
Så skyddar du routern du redan har



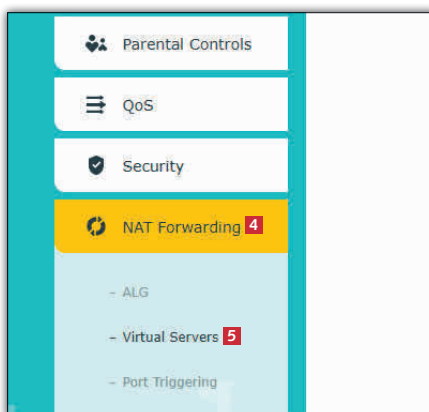
KONTROLLERA SÄKERHETEN I DIN ROUTER

Stäng portar i routern

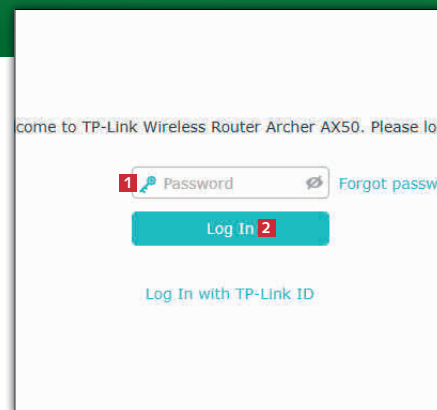
Även om du inte äger en av de nya och säkrare routrarna kan du förbättra säkerheten i ditt nätverk. Routrar kommunicerar via portar, och du bör stänga portar som du inte själv öppnat för att göra ditt skydd starkare. Här visar vi det i en router från TP-Link, men det ser ungefär likadant ut i andra routrar.



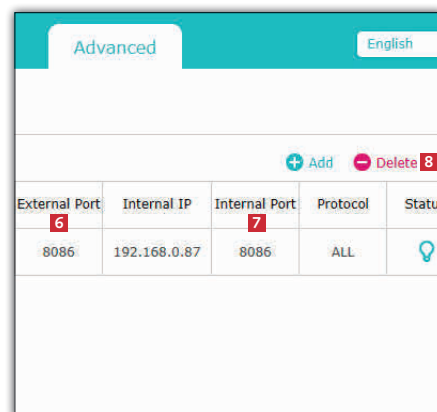
2 Klicka på **Advanced** **3** för att komma åt routerns avancerade inställningar.



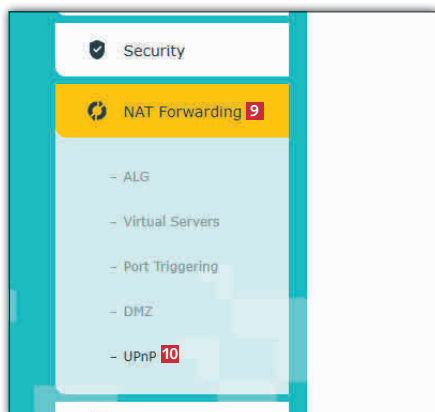
3 Leta efter ett alternativ som heter **NAT Forwarding** **4**, Port Forwarding eller liknande. På just den här modellen ska du sedan klicka på inställningen **Virtual Servers** **5**.



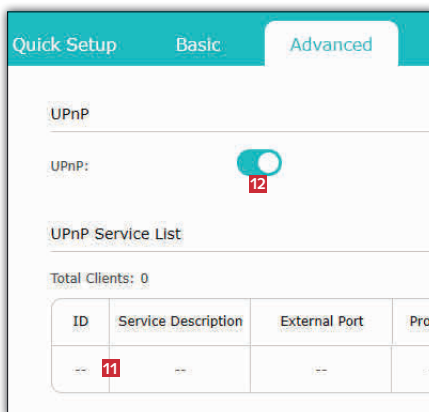
1 Öppna din webbläsare och skriv in adressen till din router. Den finns i manualen. Skriv in lösenordet **1** och klicka på **Log In** **2**. Även routerns standardlösenord finns i manualen.



4 Kontrollera om det redan finns sparade regler vidarebefordran av portar **6**. Om det finns **7**, som här, bör du radera dem genom att markera regeln och klicka på **Delete** **8**.



5 Under **NAT Forwarding** **9** finns som regel även alternativet **UPnP** **10**, som ger automatisk åtkomst till nätverket för alla enheter som är kompatibla med funktionen.



6 Om det inte finns några anslutna enheter i listan som använder UPnP-funktionen **11** är det säkrast att stänga av funktionen **12** för att göra nätverket säkrare.

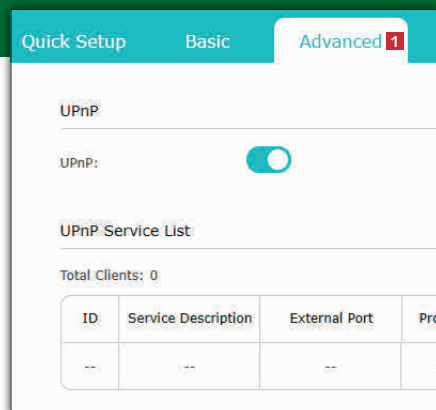
Kom ihåg antivirus

Oavsett om du har en ny router eller inte rekommenderar vi att du installerar antivirusprogrammet Avast One Essential, som du kan hämta på pctidningen.se/2505. Där hittar du också vår stora guide till programmet.

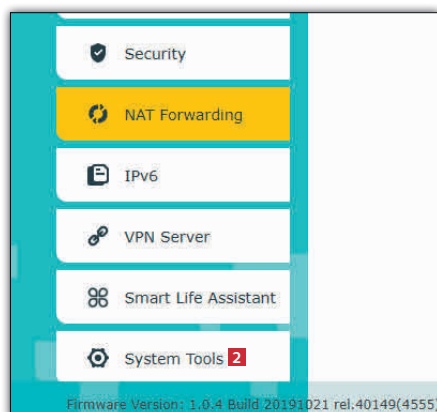


Kontrollera om det finns uppdateringar

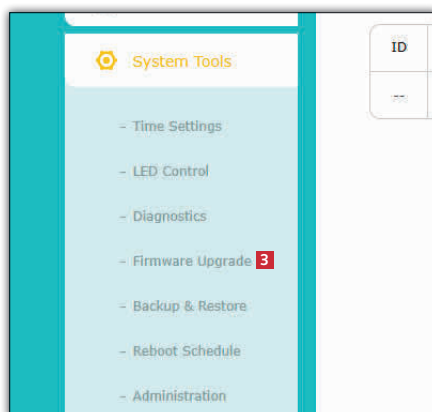
Operativsystemet i din dator uppdateras automatiskt av Microsoft när det upptäcks nya säkerhetshål och andra faror. Detsamma gäller inte nödvändigtvis för din router. Därför bör du regelbundet kontrollera om det finns uppdateringar av routerns firmware. Här visar vi dig hur det går till i en TP-Link-router.



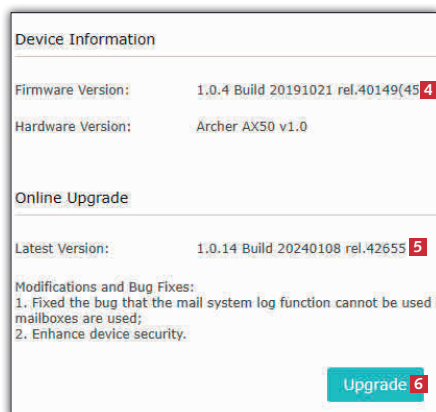
1 Klicka på **Advanced** **1** i routerns administrations-sidor för att komma åt de avancerade inställningarna.



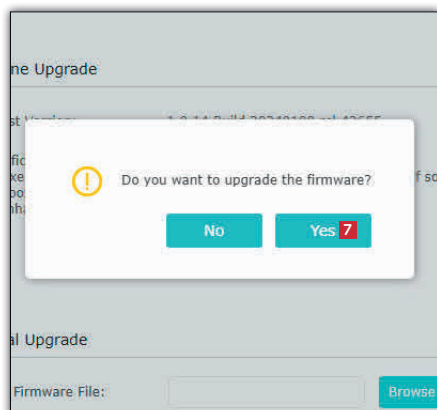
2 Klicka på **System Tools** **2** eller liknande i menyn.



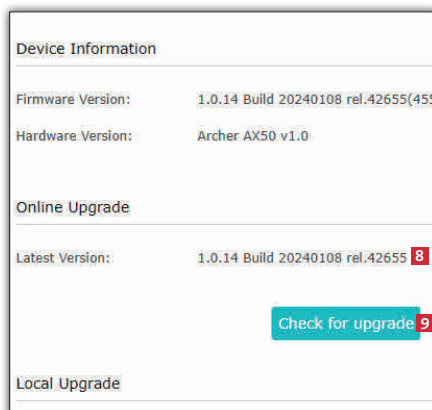
3 Välj alternativet **Firmware Upgrade** **3** i undermenyn.



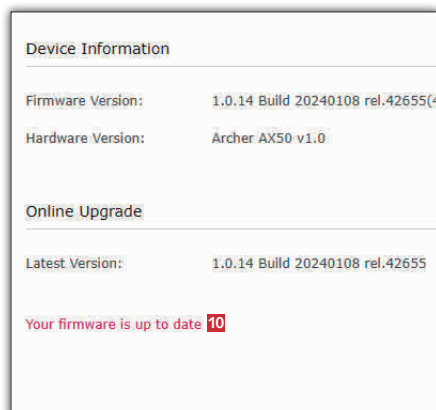
4 Här ser du om den installerade programvaran **4** kan bytas ut till en nyare version **5**. Klicka på **Upgrade** **6** för att uppdatera routern.



5 Klicka på **Yes** **7** för att fortsätta. Rör inte routern medan uppdateringen pågår. Din dator kommer att kopplas bort från nätverket under processen.



6 Logga in på nätverket efter 5-10 minuter. Nu är programvaran uppdaterad **8**. Du kan klicka på **Check for upgrade** **9** igen för att dubbelkolla om det finns mer.



7 Du får ett meddelande om att routerns firmware är den senaste tillgängliga **10**. Nu har du de senaste säkerhetsuppdateringarna installerade.