

PYSÄYTÄ UHAT JO ENNEN TIETOKONETTA:

Entistäkin turvallisempi reititin

Tänä päivänä myytävissä uusimman sukupolven reitittimissä on sisäänrakennettu suojaus hakkereita, viruksia ja muita uhkia vastaan. Jokainen niihin liitetty laite on siis suojattu oletuksena.



Toimittaja
Henning Rasmussen

Arvaan, että olet vuosia suojautunut haitallisilta verkkosivustoilta, valheellisilta mainoksilta, viruksilta ja tietojenkalasteluhyökkäyksiltä tietokoneeseen asennetulla tietoturvaohjelmistolla. Hiljattain fyysisten verkkolaitteiden valmistajat ovat alkaneet rakentaa myös langattomiin reitittimiinsä tehostettua suojausta – usein yhteistyössä tunnetun tietoturvayhtiön kanssa ja ilman lisäkustannuksia.

Hieman kalliimman hintaluokan TP-Link -merkkisen reitittimen ostaja saa nyt kaupan päälle HomeCare-turvapaketin. Se on virustorjuntayhtiö Trend Micron tarjoama paketti, johon kuuluu mahdollisuus lapsilukkoon, virustorjunta ja suojaus useimpia

verkkouhkia vastaan. HomeCare on reititintä ostaessa maksettu koko tuotteen käyttöä varten.

Teknologiavalmistaja ASUS kutsuu omien reitittimiensä lisäturvaa AIProtectioniksi, ja tämänkin palvelun tuottaa Trend Micro. Palvelu sisältyy tuotteiden hintaan ja kuuluu esimerkiksi RT-AX5400-reititinmalliin, jonka saa noin 150 eurolla.

Tulossa palveluntarjoajilta

Internetyhteyksien palveluntarjoajat välittävät usein Netgearin reitittimiä. Niihin saa yleensä liitettyä Bitdefenderin Armor-turvapaketin. Armor suojaa kaikki laitteesi viruksilta, vakoilu- ja kiristysohjelmilta sekä vaarallisilta linkeiltä. Se sisältää lisäksi VPN-palvelun, jonka kiintiö on tosin vain kaksisataa megatavua päivässä. Palveluntar-

joajilla ei ole varaa jättää uutta reititinturvallisuuden trendiä huomiotta, ja yhä useammat nettiyhteyksien myyjät mainostavat modeemiensa ja reitittimiensä tuomaa lisäturvaa.

Muissa Pohjoismaissa palveluntarjoajat ovat lisänneet reitittimiinsä integroitua suojausta vuodesta 2023 lähtien. Esimerkiksi tanskalainen YouSee on tehnyt yhteistyötä suomalaisen F-Securen kanssa ja rakentanut reitittimeen pilvipalvelulla ohjattavan ohjelmiston, jota käyttäjä voi hallita puhelimen sovelluksella. Ohjelmiston myötä reitittimessä on selain-, seuranta- ja IoT-suojaus, ja kaikki siihen liitetyt laitteet on suojattu. Toistaiseksi kotimaiset palveluntarjoajat keskittyvät vielä erillisten tietoturvaratkaisujen myyntiin, joten huipputurvallista reititintä kaipaavan täytyy hankkia sellainen erikseen.



ASIAANTUNTIJA:

Tietokone kannattaa edelleen suojata

Uuden reitittimen tietoturvaa saatetaan mainostaa kirjoittamalla, ettei tietokoneelle enää tarvitse asentaa tietoturvaohjelmaa, koska tietoliikenne on suojattu jo ennen kuin se saavuttaa laitteen. Yksi maailman johtavista tietoturva-asiantuntijoista ei kuitenkaan kannata ajatusta. David Jacobylla, joka toimii suurissa tietoturvayhtiöissä neuvonantajana ja on hakkeroinut kaikenlaista tulostimista Mac-tietokoneisiin, on aiheesta omakohtaista kokemusta. Hän on tehnyt yhteistyötä ruotsalaisen internetpalveluntarjoajan kanssa.

Jacoby sanoo, että idea sisäänrakennetusta suojauksesta on periaatteessa hyvä, mutta asiakkaiden on ymmärrettävä tarkkaan, miltä he ovat turvassa ja miltä eivät. Hän kertoo, että reitittimen on mahdollista tarjota samaa suojaa kuin jos tietoturvaohjelma asennetaan suoraan tietokoneeseen. Siksi tietokoneen suojaamisesta ei kannata tinkiä, vaikka reitittimessäkin olisi suojaus. Hän neuvoo olemaan varovainen verkossa ja ottamaan käyttöön kaksivaiheisen tunnistautumisen, sillä suojatut reitittimetkään eivät suojaa kaikelta.



David Jacoby on hakkeri ja tunnettu turvallisuusasiantuntija.

Uuden sukupolven reititin suojaa sinua

Kotireitittimesi suojaa sinua todennäköisesti jo yleisimmiltä uhilta, mutta uusimmissa reitittimissä tietoturva on viety uudelle tasolle.

Turvallisuusnormi	Nykyinen reitittimesi	Uusi reititin
Palomuuuri	Kyllä	Kyllä
Suojausavain	Kyllä	Kyllä
WPA3- ja WPS -salaus	Kyllä	Kyllä
NAT eli osoitteenmuunnos	Kyllä	Kyllä
VPN	Ehkä	Kyllä
Lapsilukko	Ei	Kyllä
Puhelinsovellus	Ei	Kyllä
Virustorjunta	Ei	Kyllä
Suojaus vaarallisia sivustoja vastaan	Ei	Kyllä
Laiteohjelmiston automaattipäivitys	Ehkä	Kyllä
DNS-esto	Ei	Kyllä

Uudet reitittimet ovat turvallisia kuin Fort Knox

Kaikissa reitittimissä on sisäänrakennettu palomuuuri ja verkossa olevien laitteiden välisen liikenteen salausta, mutta uuden sukupolven reitittimien parannettu tietoturva tuo laajan valikoiman muita turvallisuusominaisuuksia.

Suojausavain (salasana)

Uudempiin reitittimiin voi asettaa pitkän ja turvallisen salasanan, joka voi olla yli kymmenen merkkiä pitkä ja koostua niin kirjaimista, numeroista kuin merkeistäkin. Hankalat salasanat suojaavat reititintä sellaisilta asetusten muutoksilta, jotka voivat vaarantaa turvallisuutesi.

Palomuuuri

Reitittimen sisäänrakennettu palomuuuri estää yhteydet internetistä lähiverkossasi oleviin laitteisiin. Tämän ominaisuuden ansiosta hakkeri ei pääse käsiksi NAS-verkkoläpypalvelimeesi tai kotonasi olevaan verkkokameraan.

WPA3 ja WPS -salaus

Viimeisin WPA3-suojausprotokolla salaa reitittimen ja laitteiden välisen tietoliikenteen, jotta luvattomat osapuolet eivät voi siepata tietoja. Sisäänrakennetulla WPS-toiminnolla taas on helppo luoda suojattu yhteys verkkoon painamalla painiketta tulostimessa, toistimessa tai muussa verkkolaitteessa.

NAT

Reitittimessäsi on ominaisuus nimeltä NAT eli Network Address Translation, joka tarkoittaa verkko-osoitteiden kääntämistä. Se piilottaa lähiverkkosi laitteiden IP-osoitteet, kun ne ovat yhteydessä internetin eri palvelimiin.

Virustorjunta

Reititinvalmistajat ja palveluntarjoajat tarjoavat nykyään yhteistyössä F-Securen, Trend Micron, Aviran ja Bitdefenderin kaltaisten turvallisuusyhtiöiden kanssa myös virustorjuntaa reitittimiin. Vaaralliset tiedostot pysäytetään ennen kuin ne pääsevät laitteille. Tämä suojaa esimerkiksi tulostimia ja NAS-asemia.



VPN

VPN-toiminnolla reitittimesi voi muodostaa salatun yhteyden internetissä olevaan palvelimeen ja reitittää kaiken tietoliikenteesi tämän palvelimen kautta. Verkkosivustoilla vieraillessasi käytät tämän palvelimen osoitetta todellisen internetpalveluntarjoajalta saamasi IP-osoitteen sijaan.

Suojaus vaarallisilta verkkosivustoilta

Uusissa reitittimissä on jonkin tunnetun tietoturvayhtiön pilvipalvelu, johon kuuluu jatkuvasti päivittyvä lista vaarallisista verkkosivustoista, jotka reititin sitten estää. Mikäli yrität vierailla selaimellasi reitittimen estämällä verkkosivustolla, tietokoneesi ilmoittaa, ettei sivustolle pääse. Siten et altistu verkkosivujen sisältämille tietojenkaistelu- ja haittaohjelmille.

Laiteohjelmiston automaattipäivitys

Harva meistä kirjautuu säännöllisesti reitittimen ohjaussivuille ja tarkistaa reitittimen sisäänrakennetun laiteohjelmiston uusimmat päivitykset. Siksi on tärkeää, että reititin osaa tarkistaa ja päivittää ohjelmiston itse, kun uusi versio on saatavilla. Samalla äskettäin löydetty tietoturva-aukot tukitaan mahdollisimman nopeasti.

Lapsilukko

Uusimmissa reitittimissä on myös lapsilukko, eli niihin voi muun muassa asettaa käyttörajoituksia lasten puhelimille ja tableteille sekä estää lapsilta sopimatonta sisältöä sisältävät verkkosivustot.

DNS-esto

DNS on palvelu, joka muuntaa verkkosivustojen osoitteet numeerisiksi IP-osoitteiksi, ja sitä käytetään joissakin maissa myös ei-toivottujen verkkosivustojen sensurointiin. Uudemmissa reitittimissä DNS:ää voidaan käyttää estämään haittaohjelmia ja tietojenkalastelutoimintoja sisältäviä tai muuten haitallisia verkkosivustoja.

Puhelinsovellus

Reitittimen suojauksen määrittäminen on huomattavasti helpompaa, kun sen voi tehdä puhelimen sovelluksessa vaikkapa tietokoneen selaimessa seikkailemisen sijaan. Uusissa reitittimissä sekä tietoturvaa että uutta lapsilukko-ominaisuutta voi ohjata suoraan puhelimen sovelluksella. Tämän toiminnon ansiosta sinun ei tarvitse muistaa reitittimen hankalaa osoitetta säätääksesi sen tietoturvaominaisuuksia. Sovellus on yhteydessä suoraan reitittimeen, ja uudet asetukset astuvat voimaan välittömästi.

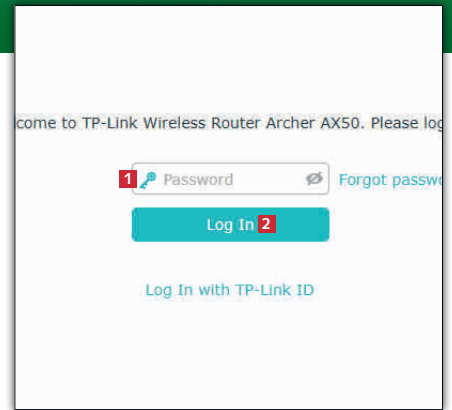
Näin suojaat jo olemassa olevan reitittimesi



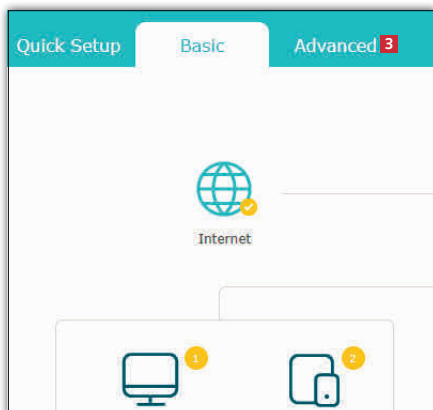
TARKISTA REITITTIMESI SUOJAUS

Lukitse avoimet portit

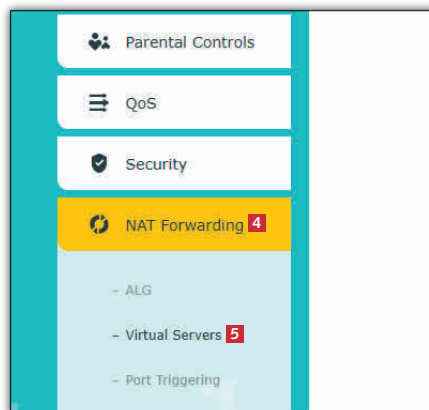
Voit parantaa verkkosi turvallisuutta, vaikka et omistaisikaan uutta ja erityisen hyvin suojattua reititintä. Kaikki reitittimet kommunikoivat porttien kautta, ja sellaisten porttien sulkeminen, joita et itse ole avannut, parantaa turvallisuuttasi internetissä. Esimerkissä käytämme TP-Linkin reititintä, mutta prosessi näyttää kutakuinkin samalta myös muissa reitittimissä.



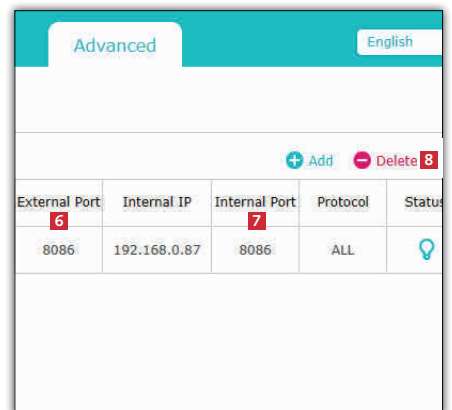
1 Avaa selain ja kirjoita siihen reitittimesi osoite. Se lukee ohjekirjasta. Kirjoita reitittimen salasana **1** ja valitse **Log In** **2**. Myös reitittimen oletussalasana lukee käyttöoppaassa.



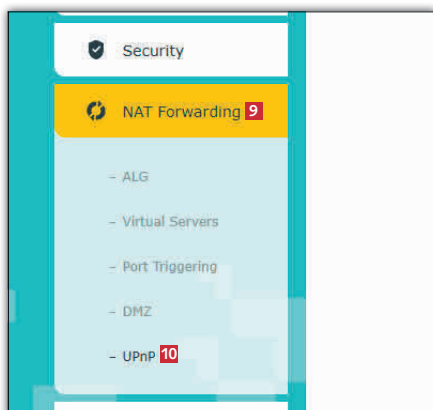
2 Siirry reitittimen yksityiskohtaisempiin asetuksiin napsauttamalla kohtaa **Advanced** **3**.



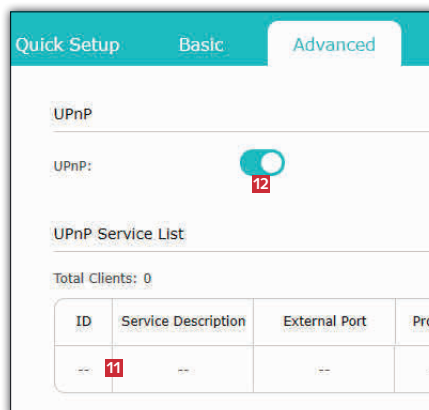
3 Etsi sitten kohta nimeltä **NAT Forwarding** **4**, Port Forwarding tai vastaava. Napsauta sitä. Tässä valitaan sen jälkeen vaihtoehto **Virtual Servers** **5**.



4 Tarkista, onko porttien edelleenlähetykselle sääntöjä **6**. Jos tässä kohdassa on listattuna portteja **7**, poista ne merkitsemällä ja napsauttamalla sitten painiketta **Delete** **8**.



5 Kohdan **NAT Forwarding** **9** alla on yleensä myös kohta **UPnP** **10**, joka sallii automaattisen pääsyn verkkoon laitteille, jotka toimivat sen kanssa.



6 Mikäli luettelossa ei näy laitteita, jotka aktiivisesti käyttävät UPnP-toimintoa **11**, kannattaa se turvallisuuden takaamiseksi kytkeä kokonaan pois päältä **12**.

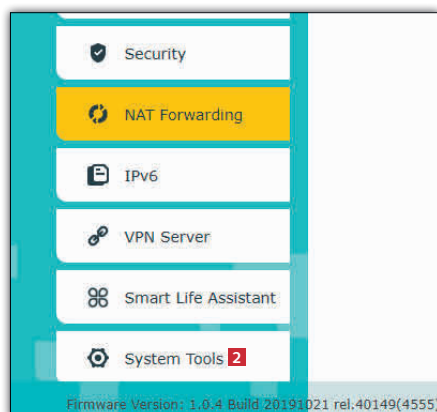
Muista virustorjunta!

Riippumatta reitittimestäsi suosittelemme asentamaan ensiluokkaisen virustorjuntaohjelman Avast One Essentialin. Voit ladata sen osoitteesta [kotimikro.fi/2505](https://www.kotimikro.fi/2505). Samassa osoitteessa on kattava ohje ohjelmiston käyttöön.

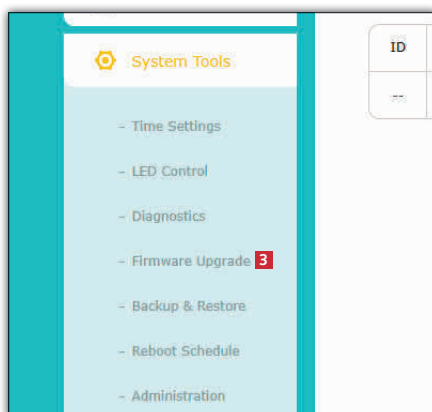


Onko reitittimelle saatavilla päivityksiä?

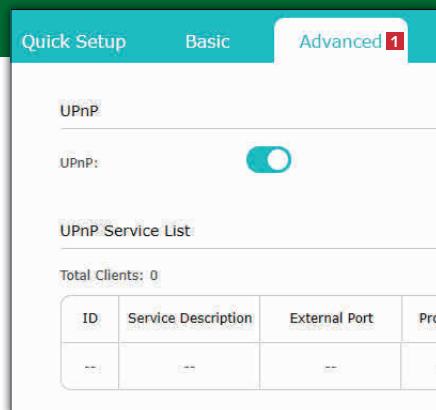
Microsoft päivittää tietokoneesi käyttöjärjestelmää jatkuvasti, kun uusia tietoturva-aukkoja ja muita vaa-roja löydetään. Sama ei välttämättä päde reitittimeesi, ja siksi sinun on tarkistettava säännöllisesti, onko sen laiteohjelmistoon saatavilla päivityksiä. Tässä näytämme, miten se tehdään TP-Link-reitittimellä.



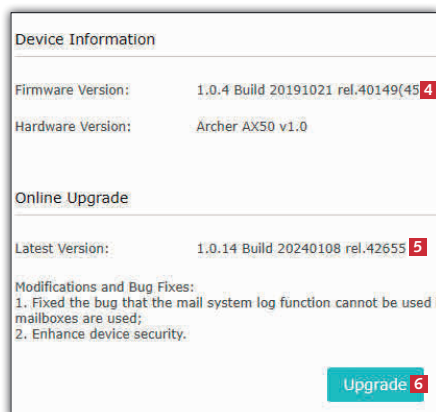
2 Napsauta sitten valikon kohtaa **System Tools** **2** tai vastaavaa.



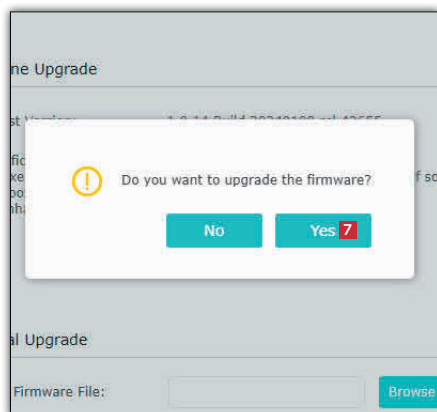
3 Valitse alavalikosta seuraavaksi **Firmware Upgrade** **3**.



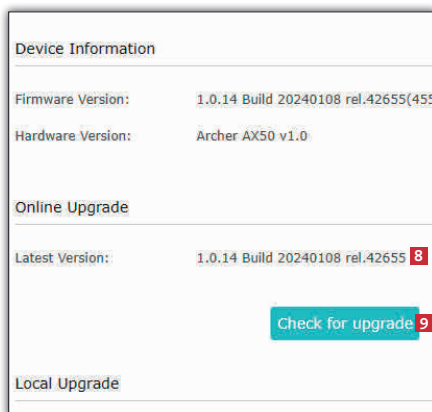
1 Siirry reitittimen lisäasetuksiin napsauttamalla reitittimen ohjaussivulla kohtaa **Advanced** **1**.



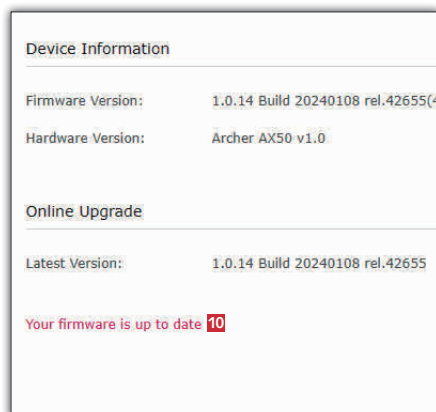
4 Tästä näet, voiko nykyisen laiteohjelmiston **4** päivittää uudempaan **5**. Päivitä reitittimen ohjelmisto napsauttamalla painiketta **Upgrade** **6**.



5 Jatka valitsemalla **Yes** **7**. Älä koske reitittimeen päivityksen aikana. Tietokoneesi irrotetaan verkosta päivityksen edetessä.



6 Kirjautu verkkoon 5–10 minuutin kuluttua ja päivitä sivu **F5**-näppäimellä. Laiteohjelmisto on nyt päivitetty **8**. Voit vielä varmistaa asian valitsemalla **Check for upgrade** **9**.



7 Saat vielä ilmoituksen siitä, että järjestelmäversio on viimeisin mahdollinen **10**. Valmistajan uusimmat tietoturvaominaisuudet on nyt asennettu reitittimeesi.