Näin toimii YKSITYINEN VPN

Kaikkea verkossa tekemäämme seurataan tarkasti. Siitä ovat kiinnostuneet niin viranomaiset, mainostajat kuin rikollisetkin. Tämä on synnyttänyt markkinaraon palveluille, joilla yksityishenkilö voi peittää jälkensä.

TEKSTI: **TERO LEHTO** | KUVITUS: **TIMO PENNANEN**

Yksityisyyden suojaaminen kiinnostaa monia jo sen takia, että useat kaupalliset sivustot seuraavat käyttäjää koko ajan tarkemmin. Siirtymiset mediatalon tai sosiaalisen median sivustojen välillä tallentuvat evästeiden avulla.

Vielä kriittisemmäksi suojauksen merkitys tulee, jos asuu internetin käyttöä rajoittavassa maassa. Esimerkiksi Kiinassa maan johdolle kriittisten verkkopalvelujen toiminta yritetään estää kokonaan tai tehdä ainakin niiden käytöstä turhauttavan hidasta.

Ongelman voi ratkaista salaamalla käyttäjän koneelta lähtevän liikenteen niin, että se pääsee omassa ”putkessaan” mahdollisten rajoitteiden ja seurantajärjestelmien ohi. Tällaista suojatun putken muodostavia tekniikoita kutsutaan virtuaalisiksi yksityisiksi verkoiksi eli vpn:iksi (virtual private network).

Vpn suojaa yhteyden ja käyttäjän sijainnin.

Tyypillisesti vpn-yhteys muodostetaan yrityksen työntekijän kotona käyttämän koneen ja yrityksen palvelimen välille. Yhteyden voi muodostaa jonkin vpn-tarjoajan palvelimelle (ja sieltä edelleen avoimeen internetiin). Yksi tällainen palvelu on suomalaisen F-Securen Freedome. Muita vastaavantyyppisiä palveluja ovat esimerkiksi Hotspot Shield, Private Internet Access ja Pure VPN.

VALITSE KOTIMAASI

Freedome tarjoaa hajautetun vpn-verkon, jossa pääsee internetiin 17 eri puolella maailmaan sijaitsevien palvelinten kautta. Kun Freedome-sovellus on asennettu ja aktivoitu mobiililaitteessa tai tietokoneessa, ohjautuu kaikki koneelta ulos lähtevä liikenne salattuna ensin F-Securen palveluun (”tietoturvapilvi”) valitussa maassa ja vasta sieltä eteenpäin julkiseen internetiin.

F-Securen tietoturvapilvellä on liittymäpisteitä pääasiassa Euroopassa, Suomen lisäksi esimerkiksi Britanniassa, Espanjassa Ruotsissa ja Saksassa. Lisäksi palvelimia on Aasiassa, Australiassa sekä Yhdysvalloissa itä- ja länsirannikoilla.

Monissa yksityiskäyttöön suunnatuissa vpn-palveluissa yhteyspisteet sijaitsevat fyysisesti yhdessä tai muutamissa pisteissä, ja palveluntarjoaja on vain ostanut internetin ip-osoitteita eri maiden verkkoavaruuksista.

Freedomen yhteyspisteet taas sijaitsevat aidosti eri maissa. Tämän etu on, että käyttäjä näkyy internetiin päin eli käyttämilleen palveluille ikään kuin hän olisi oikeasti valitsemassaan paikassa. Ja kun vpn-tunneli on aktivoitu, reitittyy kaikki verkkoliikenne automaattisesti sen kautta.

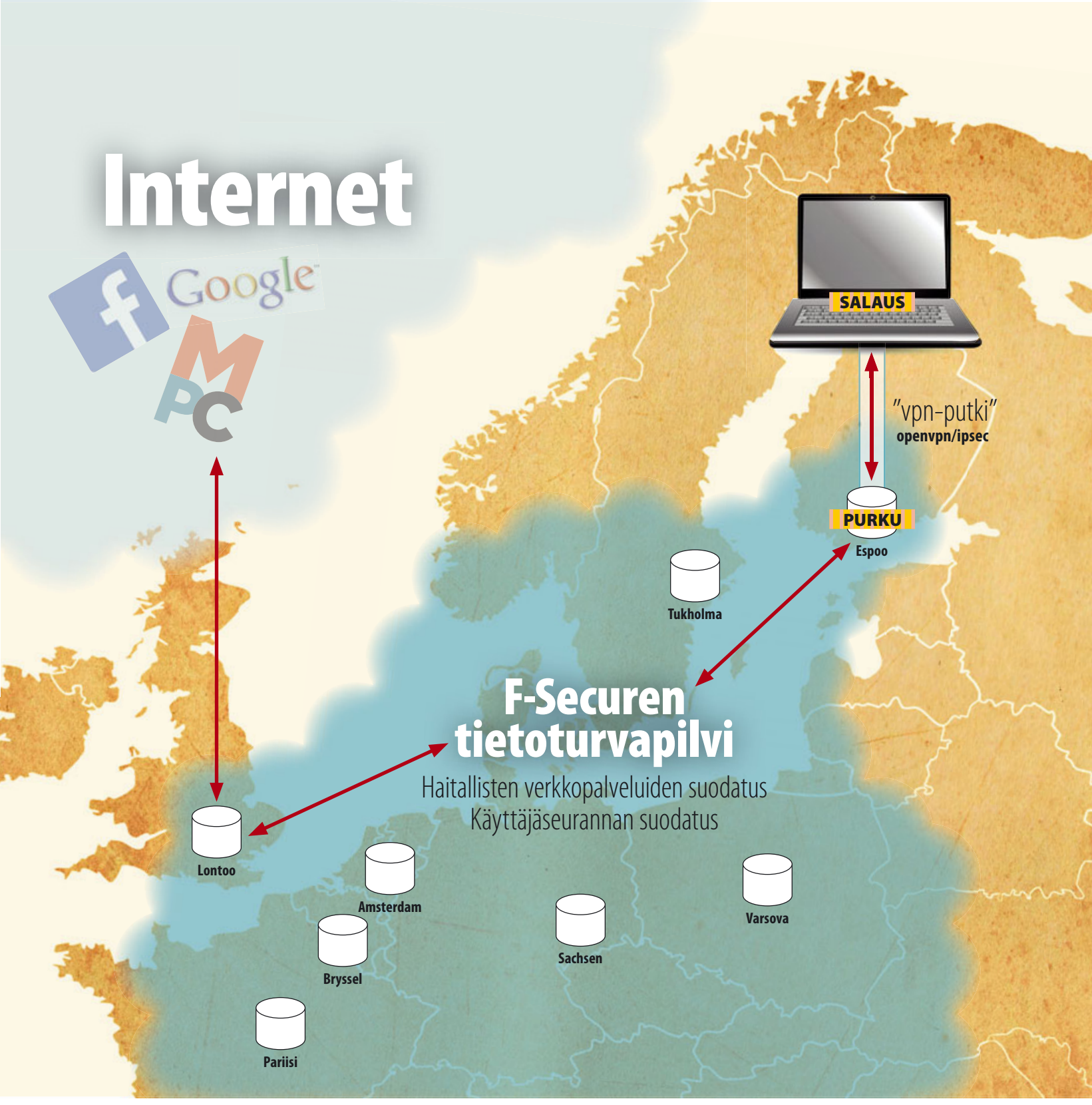
Kussakin Freedomen yhteyspisteessä on toistakymmentä ulosmenoporttia tarjoavaa palvelinta, ja yhteensä ip-osoitteita on kussakin kymmeniä. Tästä seuraa, että yhteyspistettä vaihtavaa käyttäjää on hyvin vaikea seurata, koska ip-osoite voi vaihdella satojen osoitteiden välillä. Näin käyttäjiä on siis vaikea tunnistaa ja estää palvelun käyttöä.

Sijainnin hämärtämisestä on monia etuja. Sen ansiosta voi välttää verkkopalveluiden maarajoitukset, eli esimerkiksi yleisradioyhtiö BBC:n sisältöjä voi katsoa myös Suomesta, kun reitittää yhteytensä Britannian kautta. Vastaavasti suomalaisten kanavien sisältöjä voi katsoa myös Suomen ulkopuolelta. Kiinassa taas pääsee valtiollisen palomuurin rajoitusten ohi.

Moni käyttää Freedomea katsoakseen Suomessa esimerkiksi Netflix-palvelun Yhdysvalloissa tarjoamaa sisältöä.

PAINOSTUS KASVAA

Yhdysvalloissa on käyty jo keskustelua siitä, että media- ja viihdeyritykset yrittäisivät rajoittaa palveluidensa



käyttöä vpn-palveluiden kautta. Toistaiseksi tämä ei näytä iskeneen ainakaan Freedomeen.

F-Secure on taipunut viranomaisten vaatimuksiin siinä määrin, että maasta riippuen torrent-vertaisverkkoliikennettä on joko hidastettu tai estetty kokonaan.

F-Secure on valinnut vpn-yhteydelleen avoimen lähdekoodin openvpn-protokollan, koska se on havaittu hyvin yhteensopivaksi useimpien sovellusten ja verkkojen kanssa. Poikkeus on ohjelman iOS-versio iPadille ja iPhonelle, joka perustuu ipsec-protokollaan.

Applen mobiilialusta ei vielä tue muita vpn-toteutuksia. Tämä toteutus on verkkoyhteyksien suhteen nirsompi.

Applen iOS-käyttöjärjestelmän vpn-yhteyksien rajoitusten takia Freedomen käyttö iPad-tableteilla ja iPhone-puhelimilla on myös hankalampaa kuin Android-mobiililaitteissa tai OS X- ja Windows-koneissa. Käyttöliittymän logiikka sinänsä on samanlainen.

Salatun yhdyskäytävän lisäksi palvelun ominaisuuksiin kuuluu epäluotettavista verkkopalveluista varoittaminen, jos käyttäjä yrittää mennä haitalliseksi tiedettyyn verkko-osoitteeseen. Osoitelistaa päivitetään yhtiön turvaohjelmienkin käyttämästä pilvipalvelusta. ◁