SUOMEN EDUROAM-JUURIPALVELUN UUDISTUKSET

2023-01-30 Karri Huhtanen (Radiator Software Oy)

Radiator

Alkutilanne

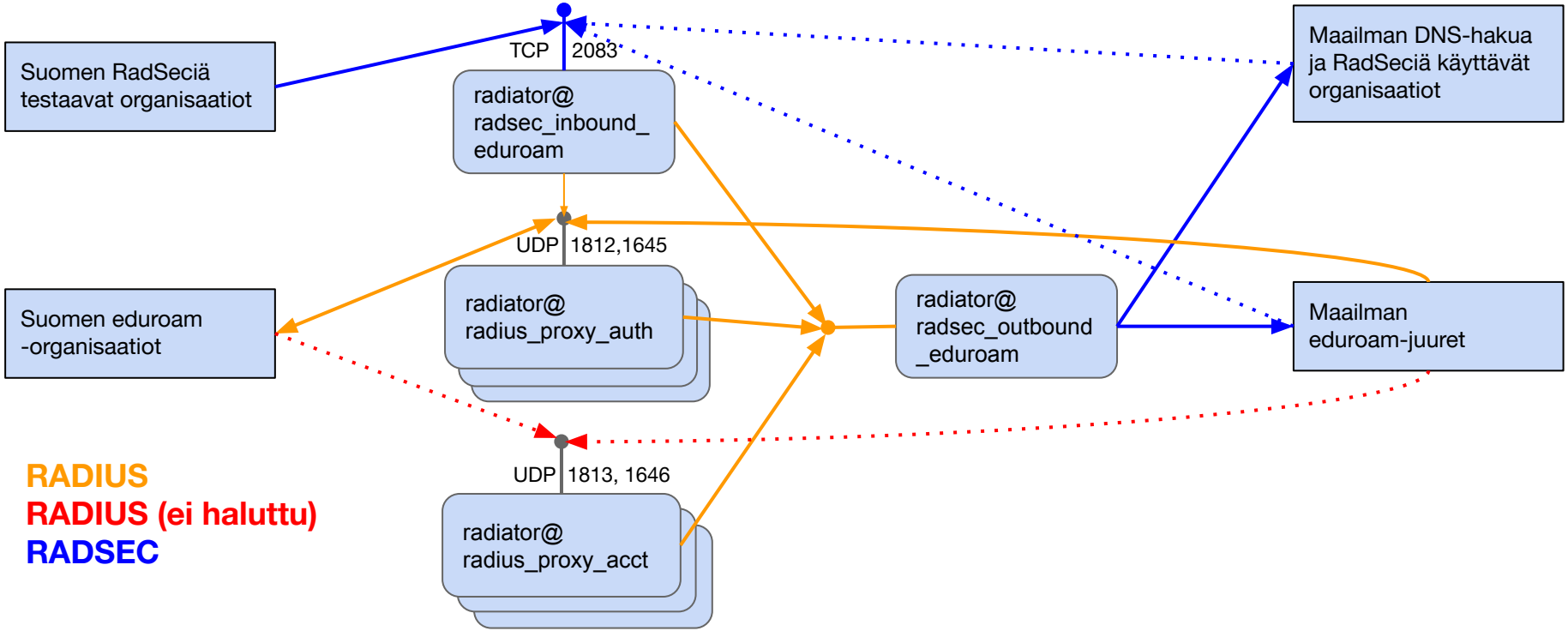
- Suomen eduroamin ja Funet-WLAN-verkkovierailun juuripalvelimen konfiguraatiota on kehitetty kokeiluista vuosina 2002-2003 ja vuodesta 2004 lähtien Arch Red Oy:n, nykyisen Radiator Softwaren palveluna CSC:lle.
- Radiatorin konfiguraatiota on muokattu lähemmäs 19 vuoden aikana, suurimmat muutokset on tehty rauta- tai virtualisointialustaa vaihtaessa.
- Konfiguraatiossa on aikojen saatossa tuettu useampia yhtäaikaisia roamausfederaatioita (Funet WLAN-verkkovierailu/eduroam), RadSecia sekä clienttien että realmien lisäämistä SQL-kannan avulla ilman katkoja.
- (Uusien) ominaisuuksien lisääminen muuttui ajan myötä haastavammaksi ja tästä syystä sovimme CSC:n kanssa juuripalvelun konfiguraation uudelleen kirjoittamisesta huomioiden nyky- ja tulevaisuuden tarpeet.

Vuodesta 2004

TTKK:n ja CSC tutkimusprojektin juuripalvelin 2004-02-11

Arch Red Oy:n toteuttama Radiator-juuripalvelin keväällä 2004

Eduroam-juuren uusi arkkitehtuuri



Uudistukset juuren toiminnallisuudessa

- Skaalautuva hajautettu rakenne mahdollistaa suorituskyvyn noston lisäämällä virtuaalikoneelle prosessoreita, muistia jne. Prosessit voidaan hajauttaa tarvittaessa vaikka eri virtuaalikoneille ja/tai kontteihin.
- Uusi kanta (sqlite3), realmien käsittely ja rakenne yhdessä mahdollistavat jatkossa juuripalvelun pystytyksen ja hallinnan esim. Ansiblella
- RadSec (TCP, Radius over TLS, RFC 6614) käytännössä millä tahansa varmenteilla
- RadSec-palvelinten DNS-etsintä (DNS discovery, DNS roaming)
- RadSecilla suojatut verkkovierailut (roaming) suoraan DNS-etsinnän kautta tai RadSecilla eduroamin maailman juuripalveluiden kautta. Mahdollisuus suomalaisten organisaatioiden verkkovierailujen suojaamiseen myös.
- RADIUS Accountingin maadoittaminen: Suomen juuri vastaanottaa ja kuittaa, mutta ei välitä eteenpäin.

Uudistukset juureen liittyneille

- Uusi rakenne mahdollistaa helpomman organisaatiokohtaisen mukautuksen:
  - Organisaation RADIUS-palvelinten tilan tarkastus onnistuu sekä RADIUS Status-Server- että RADIUS Access Request -pyynnöillä
  - Juuri pystyy hajauttamaan organisaation suuntaan tulevat pyynnöt organisaation kaikille RADIUS-palvelimille (hashbalance)
  - RadSec voidaan ottaa käyttöön organisaatioilla sitä mukaa kuin kyvykkyyttä löytyy

- Staattisia RadSec-yhteyksiä voidaan kokeilla ja ottaa käyttöön heti kun saadaan sovittua varmenteiden käytöstä – juuri tukee useamman CA:n käyttöä

- Organisaatio voi ottaa kokeiluun ja käyttöönsä myös juuren kautta tapahtuvan dynaamisen RadSec-verkkovierailun lisäämällä tarvittavat DNS-tietueet (NAPTR, SRV) omaan nimipalveluunsa.

Kiitoksia. Kysymyksiä?