Anonymisering av f-ticks

Anonymisering av f-ticks

Egentligen är det en anonymisering av attributet "Calling-Station-Id" i f-ticks loggen man gör. Det attributet är MAC-adressen på den anslutna enheten.
Man kan välja att anonymisera antingen hela MAC-adressen eller endast de tre sista byte'n och behålla vendor id delen intakt.
Anonymiseringen sker genom att göra en hash av MAC-adressen (antingen hela eller halva). Attributet Calling-Station-Id i en f-ticks logg kan då se ut så här (med anonymisering av
de tre sista byte'n):

00:11:22:dede55444d46e715fddad1a16b0833c2c9dc7b9f

Här följer tips på hur man kan göra i olika radiusservrar för att anonymisera.

NPS

TBD

Radiator

På sidan https://github.com/stockholmuniversity/radiator-fticks-anonymizer finns en hook till Radiator.
Beskrivning av hur den installeras och används finns på sidan.

radsecproxy

Information finns på sidan https://wiki.terena.org/display/H2eduroam/radsecproxy-flr

Freeradius

En modul till Freeradius finns att ladda ner på sidan https://www.lan.kth.se/eduroam/download/anon_fticks.pl

En beskrivning hur den används finns i filen, men nedan följer en utförligare instruktion. Modulen har testats med Freeradius vers. 2.2.3 och 3.0.4.
För att fungera krävs stöd för Perl i Freeradius. Ev. behöver man ladda ner perl extensions för Freeradius, beroende på vilken distribution man har.
Alternativt, om man kompilerar Freeradius själv, se till att nödvändiga Perl bibliotek finns. Saknas något så säger Freeradius configure till.

För vers 2.1.x behöver man syslog-ng eller rsyslog för att logga f-ticks till en specifik syslog facility. Kontakta Hans Berggren <hansb at kth.se> om information om det önskas.

Följande instruktion gäller för version 2.2.3

- Ladda hem modulen från sidan ovan.
- Flytta den till Freeradius konfigurationskatalog (vanligtvis /etc/raddb/)
- Gå till konfigurationskatalogen
- i filen dictionary, lägg till följande rader i slutet.

  ```
  ATTRIBUTE  X-Calling-Station-Id  3000  string
  ATTRIBUTE  X-Realm               3001  string
  ```

- I katalogen modules, kopiera filen perl till en ny fil med namn anon_fticks (utan suffix)
- Editera filen anon_fticks:

  Ändra raden "perl {" till "perl anon_fticks {"
  Ändra raden "module = ${confdir}/example.pl" till "module = ${confdir}/anon_fticks.pl"

- I katalogen modules, skapa modulen f_ticks enligt anvisningarna på Terenas wikisida https://wiki.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-F-Ticks
- Editera filen f_ticks:
  Efter raden "filename = syslog", lägg till raden "syslog_facility = local2 (eller den facility man vill använda. Detta för att lättare skilja ut och kunna skicka f-ticks loggen till Sunet. Möjligheten att välja facility finns inte i vers. 2.1.x)
  Ändra "%{Realm}" till "%{control:X-Realm}" och "%{Calling-Station-Id}" till "%{control:X-Calling-Station-Id}"
- Editera perlscriptet anon_fticks.pl:
  Skriv den hashnyckel ni ska använda på raden KEY. Denna nyckel måste behållas och användas "för all framtid". Om man byter nyckel kommer inte loggningarna vara unika för resp. enhet.
  Vill man anonymisera hela MAC-adressen ändrar man från 0 till 1 på raden HASH_ALL.
- I katalogen sites-enabled:
  Editera filen default. I sektionen post-auth lägg till följande rader efter reply_log

  ```
  anon_fticks
  if (ok) {
    f_ticks
  }
  ```

  Lägg samma rader i samma sektion under Post-Auth-Type REJECT

- Kolla konfigurationen med "radiusd -C -X"
- Om det är ok, start om radiusd och kolla loggen att f-ticks blir som förväntat