Retro-fitting FTICKS to FreeRADIUS

IN PROGRESS

For a brief explanation of FTICKS and why they're useful.

What we're trying to achieve is for an RFO to send us logs of just the successful authentications happening between your registerted organisations (i.e. not the ones proxies to and from the Jisc NRPS).

To do this there are a few stages.

1. Modify the client stanzas to include an 'operator=<realm>' line which will set the internal 'operator' variable to identify the organisation from which the request originates. e.g:

```
client somesite {
        secret = something
        ipaddr = 192.168.0.1
        operator = "somesite.nhs.uk"

}
```

2. Modify the client stanzas to identify all the Jisc NRPS as 'operator=NRPS', as above. e.g:

```
client roaming0 {
        secret = something
        ipaddr = 192.168.0.1
        operator = "NRPS"

}

#Govroam server configuration
home_server roaming0 {
    ipaddr = roaming0.govroam.uk
    port = 1812
    type = auth
    secret = something
    operator = "NRPS"

}
```

3. Ensure that the Operator-Name variable is being set to the right value, or a suitable default e.g:

```
update request {
                        Operator-Name = "%{%{client:operator}:-1nhs.uk}"
                }
```

4. Add a log section for FTICKS which sends the logs to syslog. e.g:

```
# F-TICKS
```

```
linelog f_ticks {
        filename = syslog
        format = ""
        reference = "f_ticks.%{%{reply:Packet-Type}:-format}"
        f_ticks {
              Access-Accept ="F-
TICKS/govroam/1.0#REALM=%{Realm}#VISCOUNTRY=GB#VISINST=%{Operator-
Name}#CSI=%{Calling-Station-Id}#RESULT=OK#FEDID=XX#" # Replace XX with your
supplied ID, or remove FEDID=XX if you're not a Regional Federation
Operator.

        }
```

5. Modify the post-auth stanza to use the above log section only where the source and destination aren't 'NRPS'. e.g:

```
                # Only send F-TICKS to Jisc when proxying between sites.
        if ( "%{home_server:operator}" != "NRPS" && "%{client:operator}" !=
"NRPS") {
          f_ticks
        }
```

6. Configure a syslog server to proxy to the FTICKS syslog to the Jisc syslog server. Example for syslog-ng:

```
destination d_jisc {
  syslog("utilities.govroam.uk" transport("tcp") port("514"));
};

filter f_fticks {
        facility(local0) and match ("F-TICKS", value ("MESSAGE"));
};

log {
        source(s_src);
        filter(f_fticks);
        destination(d_jisc);
};
```

From:
https://wiki.govroam.uk/dokuwiki/ - **Govroam**

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=public:retro-fitting_fticks_logging_to_freeradius&rev=1710837421

Last update: **2024/03/19 08:37**