ClearPass FTICKS

There are a number of steps required to set up FTICKS logging.

Configure Clearpass to send logs in the right format to a syslog server.

```
SELECT
        concat(
substring(user name,2,100)||'#VISCOUNTRY=UK#VISINST='||attr value||'#CSI='||
end host id||'#RESULT=0K#FEDID=0X000')
AS "F-TICKS/govroam/1.0#REALM"
FROM public.tips radius session log, public.tips session log details
WHERE public.tips radius session log.id =
public.tips session log details.session id
AND public.tips session_log_details.attr_name = 'Radius:IETF:Operator-Name'
AND public.tips radius session log.timestamp > --START-TIME--
AND public.tips radius session log.timestamp <= --END-TIME--
AND public.tips_radius_session_log.auth_method='PROXY'
AND public.tips radius session log.service name not like '%NRPS%'
AND public.tips radius session log.request status = 1
ORDER BY public.tips radius session log.timestamp asc
```

The line "public.tips radius session log.service name not like '%NRPS%'" is where the authentications to/from the NRPS are filtered out. The names of the services which proxy to/from the NRPS needs to have a name which could be matched by an SQL guery. The example here must have 'NRPS' in the name.

The line "AND public.tips radius session log.request status = 1" ensures that only logs of successful authentications are pass on.

There might need to be othe lines in there to ensure that the only logs sent to lisc are ones that match a proxy between two sites specifically for govroam, rather than all proxied logs for nongovroam services.

Set up a syslog server

From: https://wiki.govroam.uk/ - Govroam Permanent link: https://wiki.govroam.uk/doku.php?id=siteadmin:clearpass_fticks&rev=171575942



Last update: 2024/05/15 07:50