FreeRADIUS Realm Filtering

In your **proxy.conf** file:

```
# Blackhole (REJECT) where the realm is missing.

realm NULL {
}

# Realms that don't match any other listed send to the pool of govroam
servers
realm "~^[^@.]([a-zA-Z0-9-]+\.)+[a-zA-Z]{2,6}$" {
    auth_pool = govroam
    nostrip
}
```

How to stop proxying your own realm when handling both eduroam and govroam on the same server

There's a particular case where this is handy. If a RADIUS server is being used for both eduroam and govroam traffic then the rule logic becomes a bit harder.

Stepping back a bit: if a RADIUS server that just handles eduroam then the rules are easy:

1. If realm matches our own, authenticate locally.
2. Proxy all other valid realms to Jisc.
3. Reject the rest.

When you add govroam then you need to keep the traffic separate so that eduroam traffic goes to the Jisc eduroam NRPS and the govroam traffic goes to the Jisc govroam NRPS/Federation Operator. The way to do this is to match the SSID portion of the CSI for 'eduroam' or 'govroam' and include this in the rules. Thus, for the case of a University adding govroam:

1. If realm matches our own and SSID is 'eduroam' then authenticate locally.
2. If realm is valid and SSID is 'eduroam' then proxy to Jisc eduroam NRPS.
3. If realm is valid and SSID is 'govroam' then proxy to Jisc govroam NRPS/Federation ORPS.
4. Reject the rest.

However, here you can see a case that's inappropriate: if the realm is their own and the SSID is 'govroam' then the traffic is proxied to the Jisc govroam NRPS. So, for a site 'camford.ac.uk', users such as 'fred@camford.ac.uk' who use the govroam SSID by mistake have their traffic sent to the Jisc govroam NRPS. It's risky (and specifically banned in the Tech Spec) if sites are sending their own user traffic to Jisc. We're not likely to try to send it back because such sites are Visited Only for govroam but stopping it would eliminate any risks. It would also help sites to spot patterns of behaviour with their users.

If the RADIUS server is capable of doing explicit rejects then a rule can be added that says:

- If the SSID is 'govroam' and the realm is ours then Reject

otherwise the third rule becomes:

- If realm is valid, is not our own and the SSID is 'govroam' then proxy to Jisc govroam NPRS.

which means that, in the above case, inappropriate auths are now rejected by default.