Rejected authentication requests

This is one diagnosed by Hans Litteck from the University of London.

He'd noticed that attempts to authenticate a test user were failing and worked with Camden Council to figure it out. Thanks to all involved.

The exective summary is that Microsoft NPS was configured to reject any request that wasn't formatted like:

```
Called-Station-ID =~ :govroam$
```

i.e. the Called-Station-ID should have a suffix of ':govroam' after the address of the device.

To quote Hans:

> I'm aware RFC 3580 states the Called-Station-ID SHOULD append the SSID. However,
>
> 1. Not everything does; ArubaOS below 6.4 doesn't allow you to add this to the RADIUS client configuration.
>
> 2. The default pre-proxy attribute filter in FreeRADIUS, if turned on, will remove Called-Station-ID from a proxy request.
>
> So the policy condition is a bit strict for a 'federated' environment.
>
> I've update our FreeRADIUS configuration to add the missing SSID if not supplied by the NAS client and I can now authenticate via Camden's RADIUS server.

Further to this Hans has looked into the attribute filters and determined that NPS should be configured not to filter out the following from a proxied request:

```
NAS-IP-Address
NAS-Identifier
NAS-Port
NAS-Port-Type
```

> My interpretation is it that a RADIUS server will always see those if the request comes direct from a NAS client (AP, wireless controller, edge switch, …) but not necessarily for a proxy request especially of the visited site uses filtering.

What isn't know at the moment is if this standard NPS policy or a configuration being placed on NPS by administrators.

A general note about attributes and filtering

The Govroam tech spec talks about attributes and what should be in the various packets and what shouldn't. The key things to note, relevant to the above, are in section 2.4.1.13:

```
The following RADIUS attributes MUST be forwarded unaltered by participants’
ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept
or Access-Reject messages.
13.1. User-Name
13.2. Reply-Message
13.3. State
13.4. Class
13.5. Message-Authenticator
13.6. Proxy-State
13.7. EAP-Message
13.8. MS-MPPE-Send-Key
13.9. MS-MPPE-Recv-Key
13.10. Calling-Station-Id
13.11. Operator-Name
13.12. Chargeable-User-Identity
Participants’ ORPSs MUST log all RADIUS authentication requests exchanged
```

which is fine but if RADIUS servers are expecting OTHER attributes, such as NAS-*, and rejecting if they're not there then it'll cause a problem, as seen above. The discussion section 2.4.3 says:

> The inclusion of spurious RADIUS attributes in packets exchanged between organisations can have unexpected effects and result in problems. It is therefore best practice to filter out unnecessary attributes. It is however essential that the key attributes detailed in this specification are not filtered and must be retained in forwarded packets.

So the solution to the problem of failed authentications is to NOT filter out certain attributes and the spec says that they ought to be. Which is correct? The best advice is to filter out these attributes when proxing outwards but if there are any authentication issues with remote sites that you're struggling to fix then consider removing the filter to see what happens.

At the same time ensure that your RADIUS is NOT configured to expect these extra attributes. It WILL be possible to run a service with just the key attributes mentioned in the spec.

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

Permanent link:
https://wiki.govroam.uk/dokuwiki/doku.php?id=siteadmin:radius_troubleshooting&rev=1507630555

Last update: **2017/10/10 10:15**