Fixing Zombie Issues

(link to zombie text)

There are several reasons why zombies might happen.

1. Requests are being dropped between Jisc and your RADIUS server. Firewalls might be configured to block RADIUS traffic on port 1812 (unlikely) or might be configured to drop fragmented packets (more likely). RADIUS packets can be fragmented when they exceed the MTU size. This can happen when EAP-TLS contains too many/too big certificates. Even if you're not using EAP-TLS it doesn't stop users from trying (not that likely). Check firewall logs to identify such issues.

2. The RADIUS server configuration decides to drop the requests. Some rule sets are configured to match requests with attributes that don't exist. Just because your local wireless system includes NAS-Port-Type or Called-Station-ID with an SSID appended, doesn't mean that all incoming requests from Jisc will. Minimise the rules and/or create ones specifically for requests coming from outside. Look in RADIUS logs for any sign of requests being dropped.

3. If you're a Federation then the above might apply to your members too. You'll proxy a request to them that isn't responded to. You'll need to check your RADIUS logs for evidence of a lack of response from certain sites and take action to help them sort out their issues. Check RADIUS logs for signs that sites are being marked as down/zombies.

Checking FreeRADIUS logs for zombies

Checking RadSecProxy logs for zombies

Checking RADIATOR logs for zombies

Checking NPS logs for zombies

Checking Clearpass logs for zombies

Checking ISE logs for zombies

Checking FortiAuthentictor logs for zombies