Fixing Zombie Issues

The text we send explaining the nature of a 'Zombie' is below.

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

Zombie explanation email

We're seeing that one or more of your RADIUS servers is not responding to all the EAP authentication requests that we're proxying to them, so our RADIUS servers are marking them as unavailable. This could have a significant impact on your users' ability to authenticate. Once our RADIUS servers have no more available servers to try they will automatically reject further authentication attempts for a period of five minutes.

Since it only takes one failure to respond to trigger this 'zombie' status, if your server frequently fails to respond then your site could be marked as unavailable for a considerable proportion of the day.

Our monitoring system show the status of your servers:

https://utilities.govroam.uk/livestatus/livestatus/list

As such, it's absolutely critical that every single EAP authentication request received is responded to. It doesn't matter if it's for an EAP type not in use or a test message or for a disabled user. Any failure to respond to a proxied auth attempt with trigger the zombie status.

More detail:

Each type of RADIUS server has their own idiosyncrasies but the basic process is below. RADIUS is UDP based so, unlike TCP systems, can't rely on the connection status to know if there is a server at the other end receiving requests. As such it uses timeouts: it expects a response and if it doesn't receive one in a set period then it assumes that the remote server is not working.

The process for our NRPS:

1. receive an auth request and figure out which site to send to

2. pick an available server from the pool of servers

3. proxy the request to that server

4. if no response is received with 30s mark the server as down and removed from the pool

(during that 30s period other requests could have been proxied to the same server, including retries)

5. a timer is set for that server for 5 minutes

We have four NRPS and the load across them is generally balanced and they operate independently of each other. So, say, there are three remote RADIUS then there are twelve possible combinations. It could take as few as twelve failures to respond before all NRPS had remove all remote servers from their pools.

If there are no available servers in the pool then the NRPS send a Reject immediately.

There are ways to mitigate this but ultimately failure to respond to a request will cause problems to someone somewhere. Some RADIUS servers implement the Status-Server message which is, effectively, a RADIUS 'ping'. If configured, the sending RADIUS server will use Status-Server to check the state of the remote RADIUS server if the zombie status kicks in. If the server responds to the Status-Server check then the server will be returned to the pool. Status-Server isn't supported by Microsoft NPS or Cisco ISE. FreeRADIUS, RadSecProxy, RADIATOR and Aruba Clearpass do support it.

However, this is not a panacea. The Visited site from which the request originated will not see a response from Jisc's NRPS and could mark those as down. Or if a member of a Federation, mark the Federation RADIUS server as down. There is a knock on effect no matter what.

It's worth checking firewall logs to ensure that there aren't problems with fragmentation or other issues with the packets actually being received by the RADIUS server.

As such it really is absolutely critical that all EAP auth requests are responded to.

It is the individual organisations responsibility to ensure that their servers are correctly configured to respond to all requests.