Dealing with packet fragmentation with EAP-TLS

Symptoms

- If you're receiving reports from end users of authentication failing and you can't see anything in your logs.
- If you're using EAP-TLS
- If you're seeing firewall reports of potential packet fragmentation attacks from RADIUS servers.

Cause

MTU size on network interfaces is around 1500 bytes. If the RADIUS UDP packet exceeds this size then they packets will be split up. UDP packets are normally quite small so this isn't common. EAP-PEAP packets tend to be small because PEAP just uses certificates at one end and username/password at the other. On the other hand, EAP-TLS use certificates in both directions. Certificates are much bigger than a username and password so more likely to exceed the MTU size.

If a firewall is configured to be suspicious of packet fragmentation (often used as way of hacking organisations) then it could block these authentication attempts. We've only really heard of this happening with EAP-TLS for the reasons above.

The configuration of the client and servers with the certificate chain is an important factor. At a bare minimum the server needs a Root CA and a client needs a client certificate. In this simple case the packet size isn't likely to cause fragmentation. However, the certificate chain might contain one or more intermediate CAs and where these are deployed is critical. The key is to have as much of the chain as possible installed on the server and for the client to send as little as possible with each auth request.

The same applies to EAP-PEAP for the TTLS part - the client should have as much of the chain as possible and the server with just the server cert.

Doing this means that during an authentication the minimum (one server cert and one client cert) are passed around rather than a number of client, server and intermediates. However, the number of certificates, and thus size of packet, is quite dependent on the PKI. A private CA can have a very short chain, whilst a public CA could have a long one.

The key length used to encrypt the certificates can impact the certificate sizes. So using 4096 results in a file bigger than if using 2048. There are arguments for and against using 4096 over 2048. If there are certificate size issues then you're not compromising security by running 2048 rather than 4096 and the smaller key lengths have much less impact on CPU.

Solutions

These are not exclusive.

- Disable packet fragmentation checks/blocks on the firewall (just for the NRPS and any other known RADIUS servers)
- Ensure only the minimum number of certs are sent in the auth and that as much of the chain as possible is installed on the client and server.
- Change from a public CA to a private CA and just have a Root and client/server certificate rather than multiple intermediates
- Use 2048 rather than 4096 for the key length
- Set Framed-MTU to 1100

The last option is somewhat of a last resort because it's not universally respected by RADIUS servers. However, what it does do is to pass a hint to a RADIUS server to request that the RADIUS server use a maximum of 1100 bytes for the RADIUS packet. This would mean that, with the additional headers provided by the TCP stack that the packets should never be fragmented.

The caveat is, as stated, that different RADIUS servers react differently to seeing Framed-MTU and all servers in the path would have to respect it. It certainly can't be relied on as the solution.

Cisco ISE has a maximum MTU size of 1002 bytes, this can not be changed and ISE doesn't take any notice of the Framed-MTU attribute.

Aruba Clearpass has a default maximum MTU size of 1100, which should be fine. The value can be changed. Clearpass will send a Framed-MTU attribute out to authentication servers.

Microsoft NPS has a default MTU size of 1500, which is too big, and does not respond to the Framed-MTU if it receives it. You can add a Framed-MTU attribute and set its value via the Network Policy that is handling the authentication of your users - and that Framed-MTU will be used by NPS to manage the size of the packets sent back to your remote user. We suggest setting it to 1100.

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

Permanent link:
https://wiki.govroam.uk/doku.php?id=public:how_to_deal_with_fragmentation_of_eap_packets

Last update: **2022/12/06 11:02**