Malformed EAP packets: investigation and analysis

Josh Howlett (Federated Solutions / Internet2)

josh@federated-solutions.com

9th June, 2023

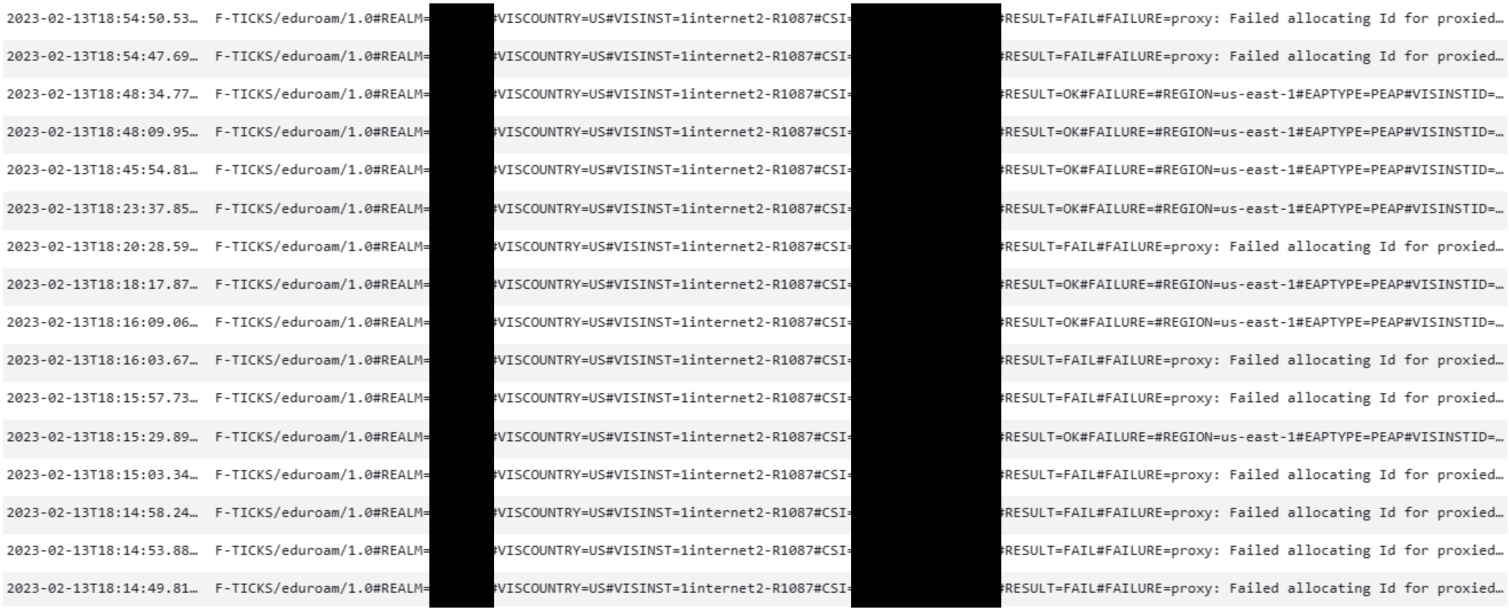
Introduction

- This presentation summarises an issue that has effected the Internet2 eduroam service since early 2023
- We have identified the root cause and taken steps to reduce its impact
- However, the issue is widespread across the eduroam network, so it is important that NROs (and RADIUS proxy operators in general) are aware
- The Internet2 eduroam service was probably first effected because of the size of the US federation
- The goals of this presentation are to
    - socialise the issue among eduroam NROs, and other RADIUS proxy operators
    - describe how we discovered the cause
    - explain how Internet2 is mitigating the impact, and
    - pose some broader questions raised by this issue

Initial reports from Service Providers

- The first indication of an issue were two tickets raised by two Service Providers on February 14th

- Both institutions reported a very similar issue: visitors were frequently unable to authenticate for a period of a few hours



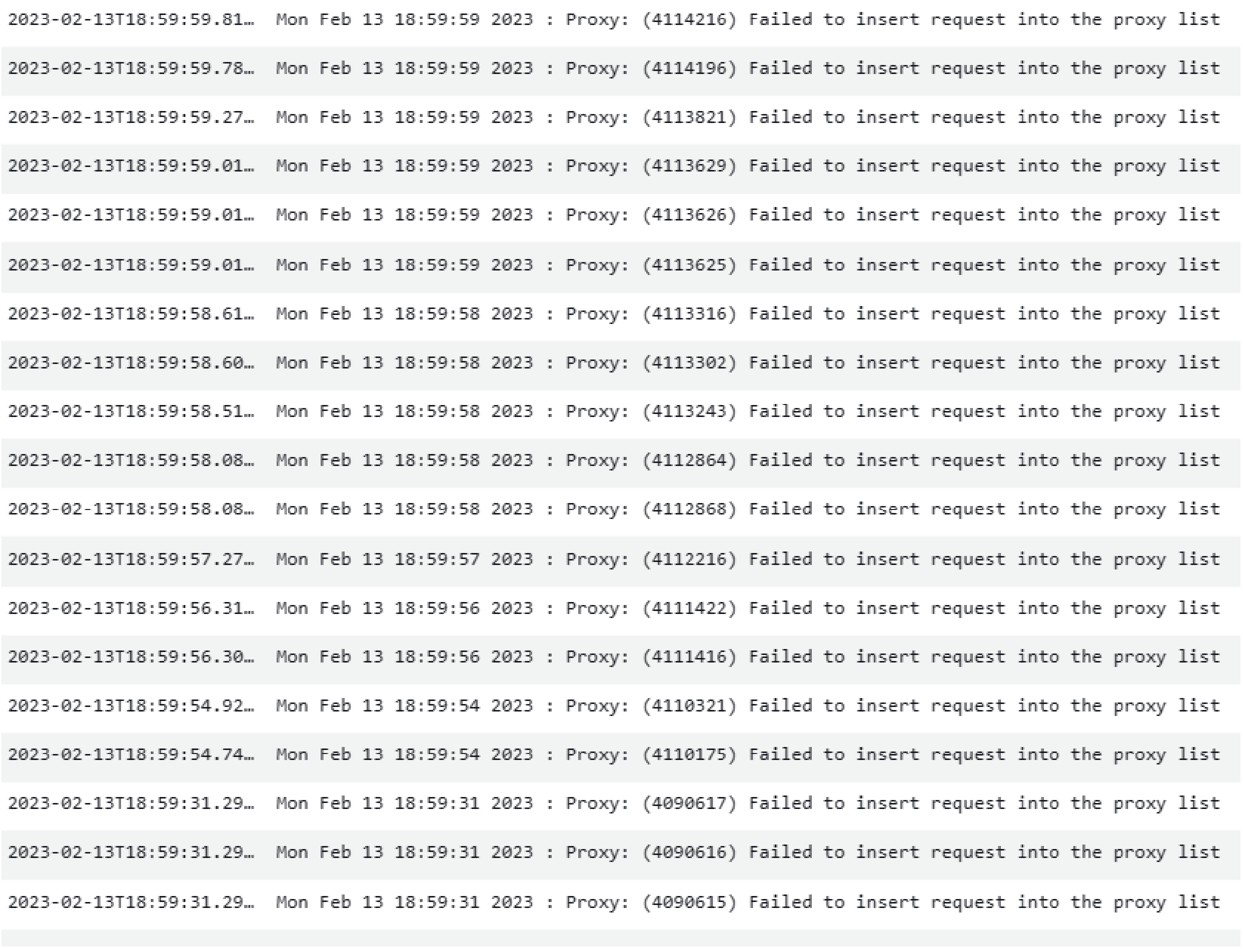
```
2023-02-13T18:54:50.53…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:54:47.69…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:48:34.77…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:48:09.95…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:45:54.81…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:23:37.85…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:20:28.59…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:18:17.87…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:16:09.06…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:16:03.67…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:15:57.73…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:15:29.89…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=OK#FAILURE=#REGION=us-east-1#EAPTYPE=PEAP#VISINSTID=…
2023-02-13T18:15:03.34…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:14:58.24…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:14:53.88…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
2023-02-13T18:14:49.81…  F-TICKS/eduroam/1.0#REALM=[redacted]VISCOUNTRY=US#VISINST=1internet2-R1087#CSI=[redacted]RESULT=FAIL#FAILURE=proxy: Failed allocating Id for proxied…
```

- Our FreeRADIUS logs showed an error of “Failed allocating Id for proxied request”

Mysterious proxy error

- There are multiple instances of a second error message “Failed to insert request into the proxy list” in our proxy logs

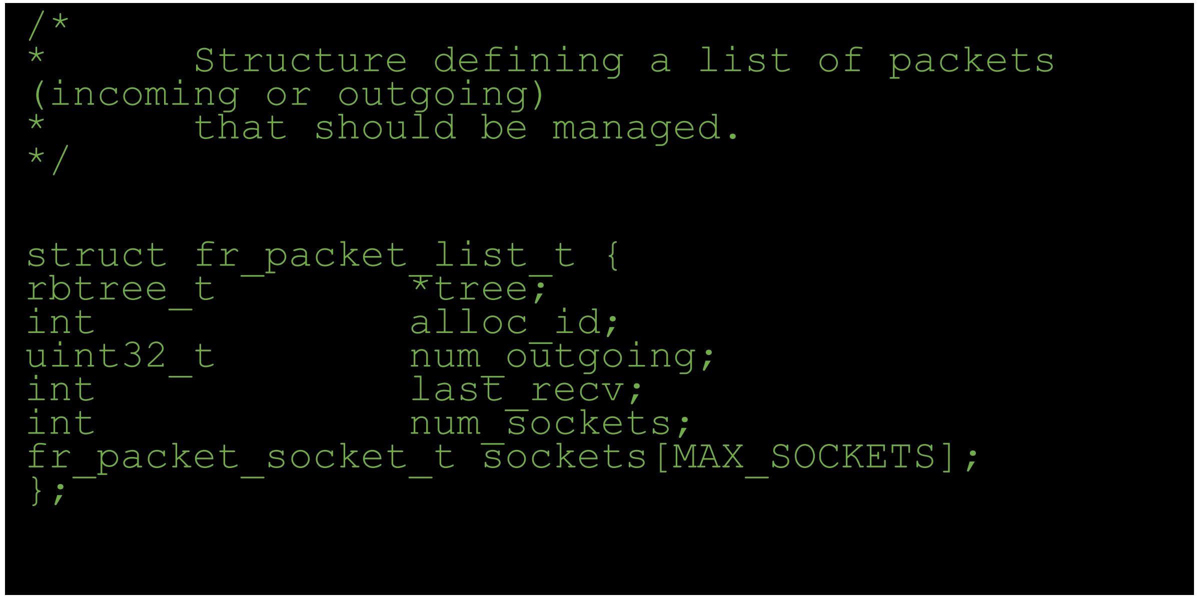
- The errors are not associated with any specific SPs or IDPs



```
2023-02-13T18:59:59.81…  Mon Feb 13 18:59:59 2023 : Proxy: (4114216) Failed to insert request into the proxy list
2023-02-13T18:59:59.78…  Mon Feb 13 18:59:59 2023 : Proxy: (4114196) Failed to insert request into the proxy list
2023-02-13T18:59:59.27…  Mon Feb 13 18:59:59 2023 : Proxy: (4113821) Failed to insert request into the proxy list
2023-02-13T18:59:59.01…  Mon Feb 13 18:59:59 2023 : Proxy: (4113629) Failed to insert request into the proxy list
2023-02-13T18:59:59.01…  Mon Feb 13 18:59:59 2023 : Proxy: (4113626) Failed to insert request into the proxy list
2023-02-13T18:59:59.01…  Mon Feb 13 18:59:59 2023 : Proxy: (4113625) Failed to insert request into the proxy list
2023-02-13T18:59:58.61…  Mon Feb 13 18:59:58 2023 : Proxy: (4113316) Failed to insert request into the proxy list
2023-02-13T18:59:58.60…  Mon Feb 13 18:59:58 2023 : Proxy: (4113302) Failed to insert request into the proxy list
2023-02-13T18:59:58.51…  Mon Feb 13 18:59:58 2023 : Proxy: (4113243) Failed to insert request into the proxy list
2023-02-13T18:59:58.08…  Mon Feb 13 18:59:58 2023 : Proxy: (4112864) Failed to insert request into the proxy list
2023-02-13T18:59:58.08…  Mon Feb 13 18:59:58 2023 : Proxy: (4112868) Failed to insert request into the proxy list
2023-02-13T18:59:57.27…  Mon Feb 13 18:59:57 2023 : Proxy: (4112216) Failed to insert request into the proxy list
2023-02-13T18:59:56.31…  Mon Feb 13 18:59:56 2023 : Proxy: (4111422) Failed to insert request into the proxy list
2023-02-13T18:59:56.30…  Mon Feb 13 18:59:56 2023 : Proxy: (4111416) Failed to insert request into the proxy list
2023-02-13T18:59:54.92…  Mon Feb 13 18:59:54 2023 : Proxy: (4110321) Failed to insert request into the proxy list
2023-02-13T18:59:54.74…  Mon Feb 13 18:59:54 2023 : Proxy: (4110175) Failed to insert request into the proxy list
2023-02-13T18:59:31.29…  Mon Feb 13 18:59:31 2023 : Proxy: (4090617) Failed to insert request into the proxy list
2023-02-13T18:59:31.29…  Mon Feb 13 18:59:31 2023 : Proxy: (4090616) Failed to insert request into the proxy list
2023-02-13T18:59:31.29…  Mon Feb 13 18:59:31 2023 : Proxy: (4090615) Failed to insert request into the proxy list
```

FreeRADIUS proxy

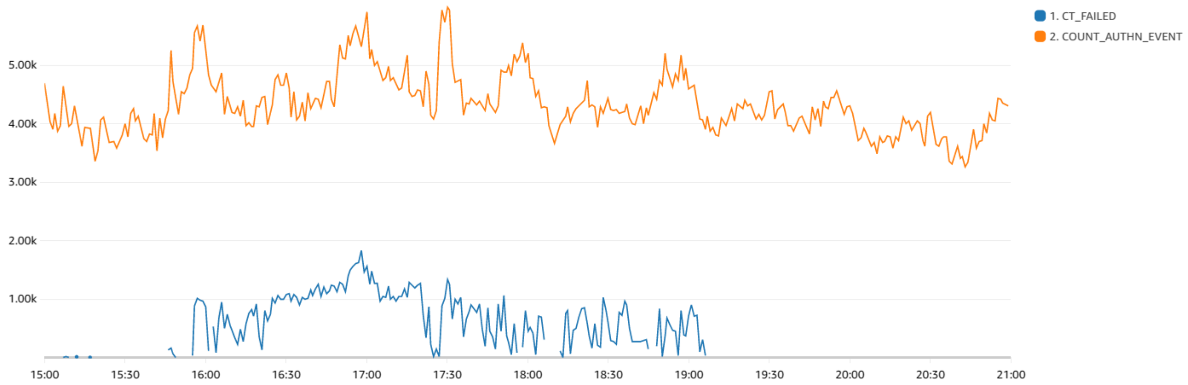
- FreeRADIUS uses a structure named `proxy_list` to track proxied packets of type `fr_packet_list_t`
- `alloc_id` is type `int`, so `proxy_list` can track 65K packets
- The error messages indicate that the proxies are exhausting this ID space

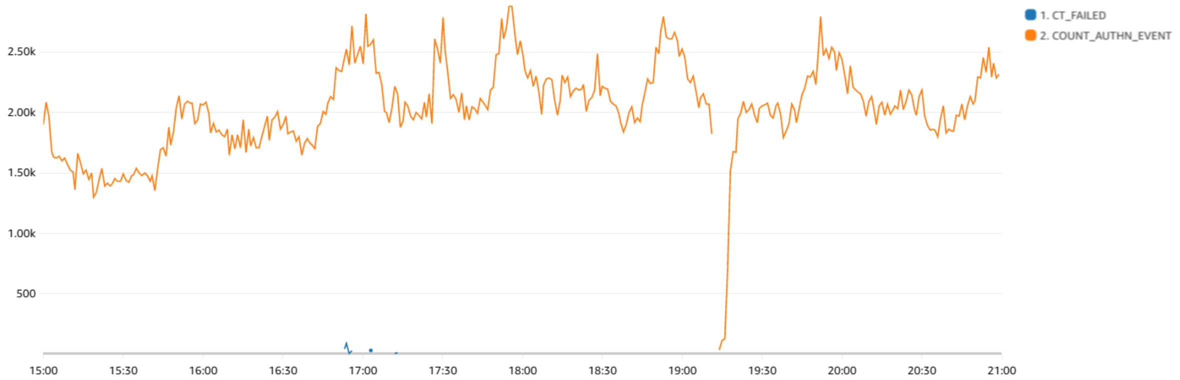


```
/*
*       Structure defining a list of packets
(incoming or outgoing)
*       that should be managed.
*/


struct fr_packet_list_t {
rbtree_t            *tree;
int                 alloc_id;
uint32_t            num_outgoing;
int                 last_recv;
int                 num_sockets;
fr_packet_socket_t sockets[MAX_SOCKETS];
};
```

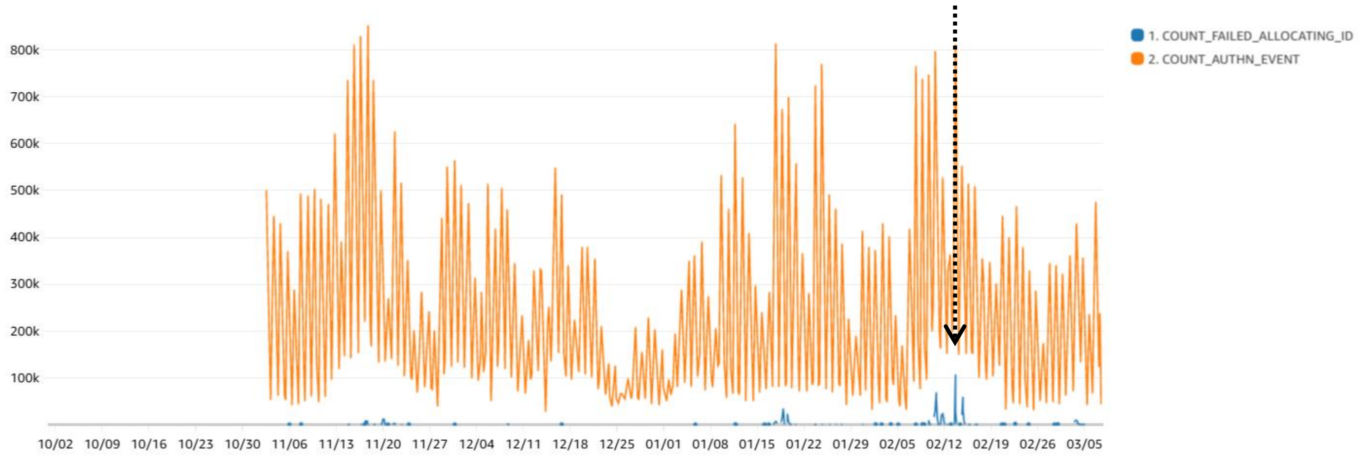
Allocation errors on primary proxy containers



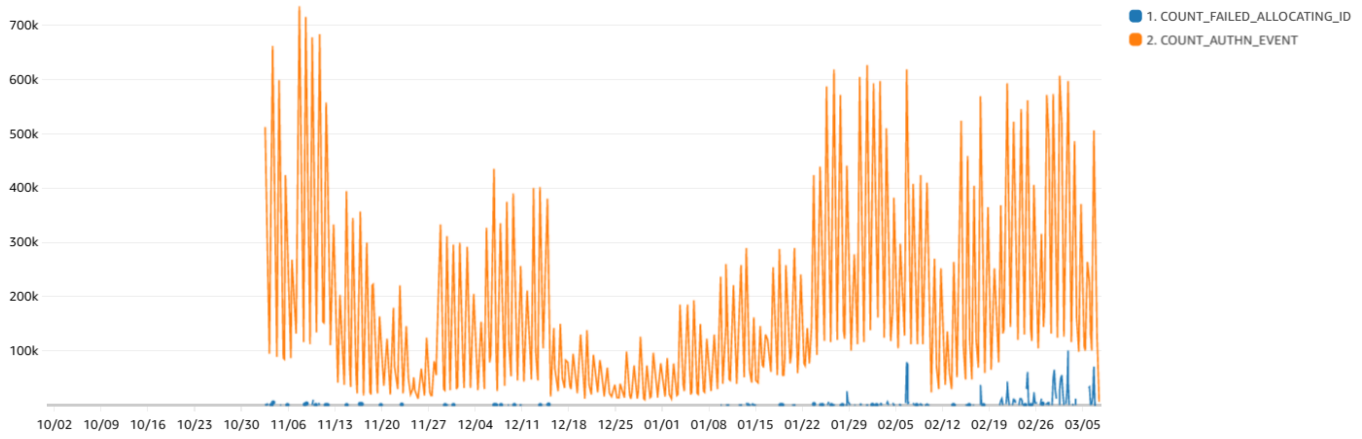


- 13th February 2023
- 1-minute sampling
- Typical pattern with proxy exhaustion between 1600Z and 2000Z
- Container 2 is barely effected – is traffic volume a factor?

Allocation errors on primary proxy containers

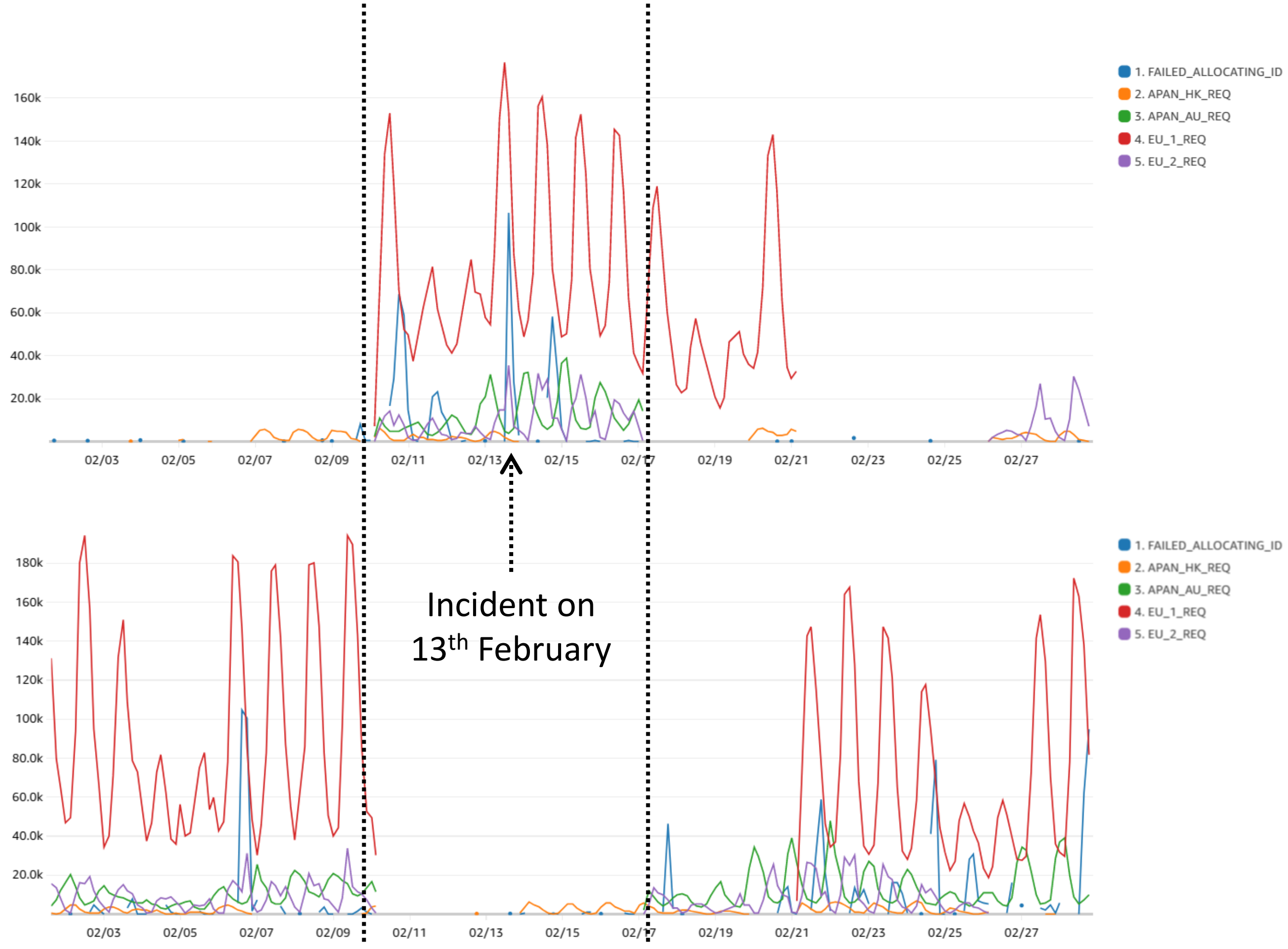


Incident on 13th February



- November 2022 through March 2023
- Overall traffic volumes have not increased
- But proxy allocation failures have increased significantly since January

Impact of international peerings


Transfer of some peerings between containers

Incident on 13th February

- The graphs show traffic data for February as the severity and frequency of events increased
- The data gives traffic volumes for the US primary's containers' international peerings
- Allocation errors (blue) follow the international peerings

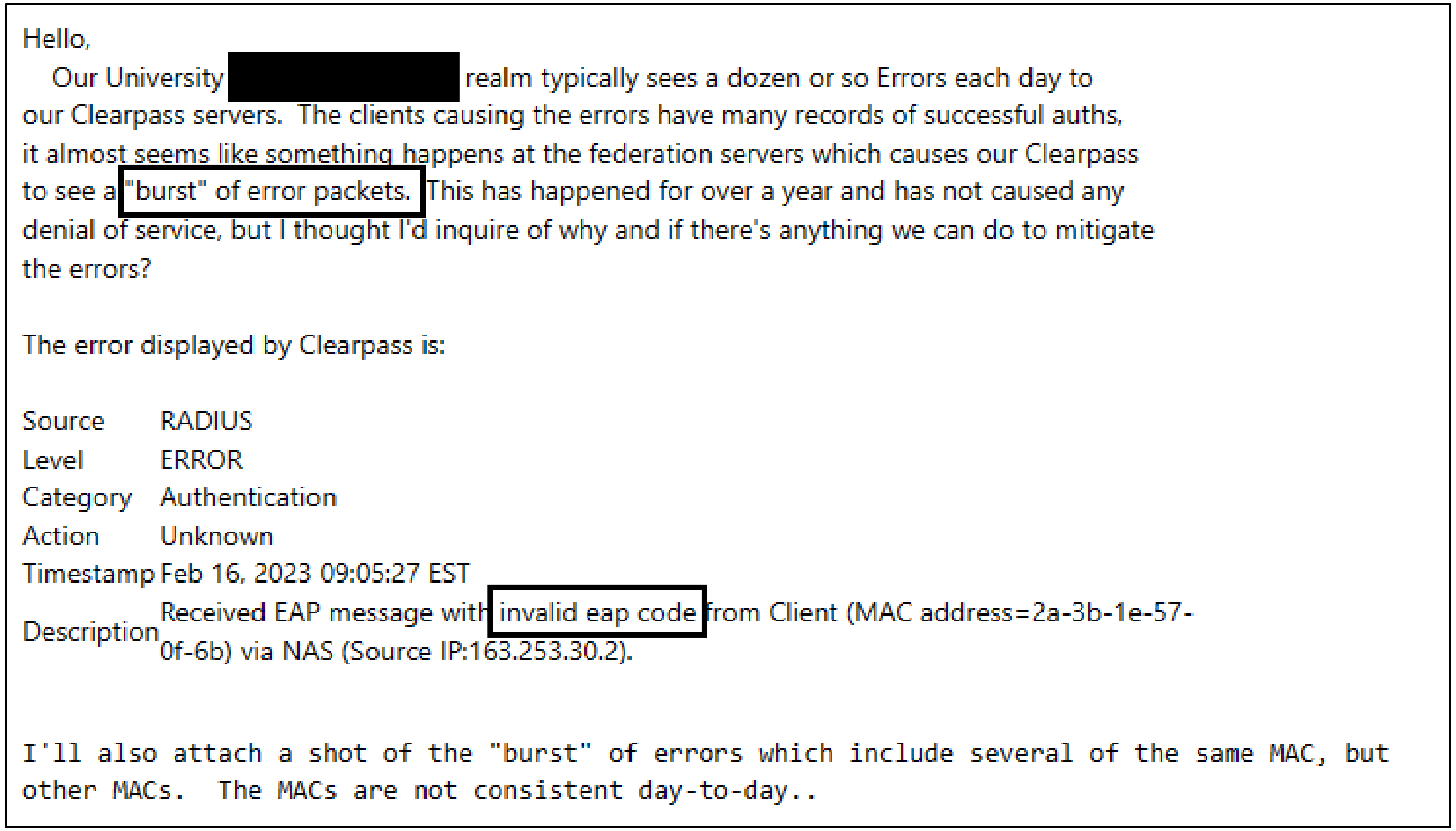
Early observations

- Loss of 20-25% of requests for 3-4 hours per day
- These episodes increase in frequency and severity from January, becoming nearly daily by mid-February
- These episodes of exhaustion coincide with peak usage, at around 1700Z
- This is no material increase in load over this period
- The episodes appear to correlate with a container's international peerings

A clue from an Identity Provider

- An Identity Provider raised a ticket concerning unexplained authentication failures on 16th February

- The issue appeared unrelated initially, but the “burstiness” chimed with the episodic nature of the first issue



Hello,

Our University [redacted] realm typically sees a dozen or so Errors each day to our Clearpass servers. The clients causing the errors have many records of successful auths, it almost seems like something happens at the federation servers which causes our Clearpass to see a "burst" of error packets. This has happened for over a year and has not caused any denial of service, but I thought I'd inquire of why and if there's anything we can do to mitigate the errors?

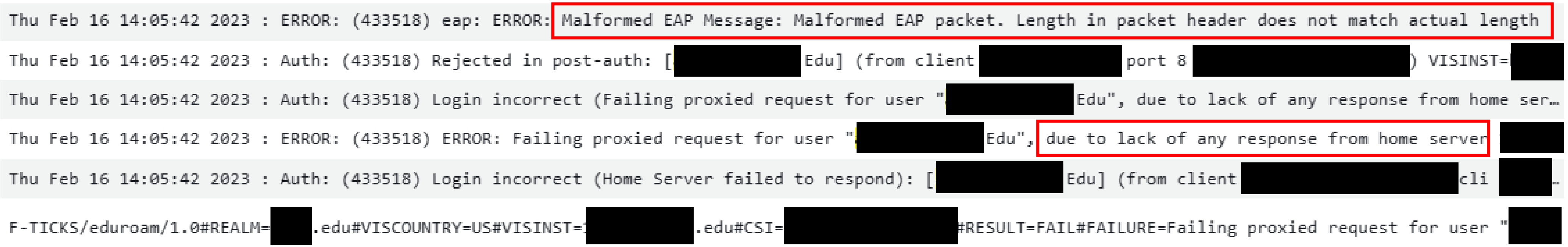
The error displayed by Clearpass is:

Source	RADIUS
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	Feb 16, 2023 09:05:27 EST
Description	Received EAP message with invalid eap code from Client (MAC address=2a-3b-1e-57-0f-6b) via NAS (Source IP:163.253.30.2).

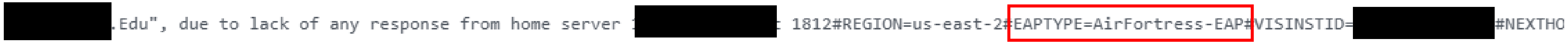
```
I'll also attach a shot of the "burst" of errors which include several of the same MAC, but
other MACs.  The MACs are not consistent day-to-day..
```

Malformed EAP messages in the proxy logs

- Looking at our RADIUS proxy logs, we see that
  - The EAP packet length claimed in the packet’s header does not match the packet’s actual length
  - The RADIUS server never responds to the proxied request
  - The EAP type (“AirFortress-EAP”) has never been implemented
  - This user has always authenticated previously using EAP-TLS



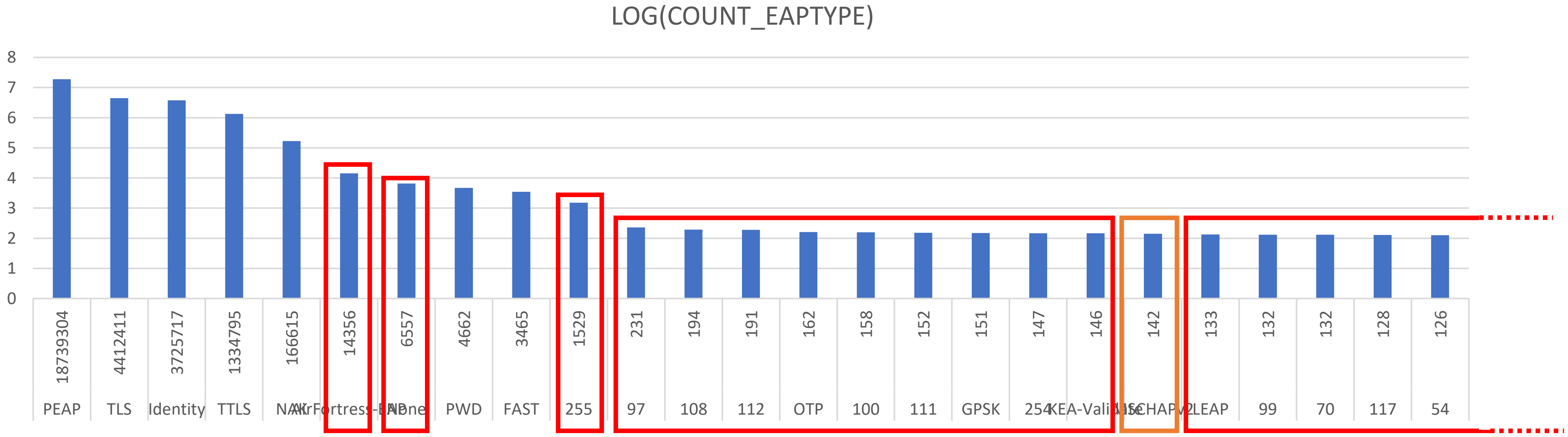
```
Thu Feb 16 14:05:42 2023 : ERROR: (433518) eap: ERROR: Malformed EAP Message: Malformed EAP packet. Length in packet header does not match actual length
Thu Feb 16 14:05:42 2023 : Auth: (433518) Rejected in post-auth: [[redacted]Edu] (from client [redacted]port 8[redacted]) VISINST=[redacted]
Thu Feb 16 14:05:42 2023 : Auth: (433518) Login incorrect (Failing proxied request for user "[redacted]Edu", due to lack of any response from home ser…
Thu Feb 16 14:05:42 2023 : ERROR: (433518) ERROR: Failing proxied request for user "[redacted]Edu", due to lack of any response from home server [redacted]
Thu Feb 16 14:05:42 2023 : Auth: (433518) Login incorrect (Home Server failed to respond): [[redacted]Edu] (from client [redacted]cli [redacted]…
F-TICKS/eduroam/1.0#REALM=[redacted].edu#VISCOUNTRY=US#VISINST=[redacted].edu#CSI=[redacted]#RESULT=FAIL#FAILURE=Failing proxied request for user "[redacted]
```



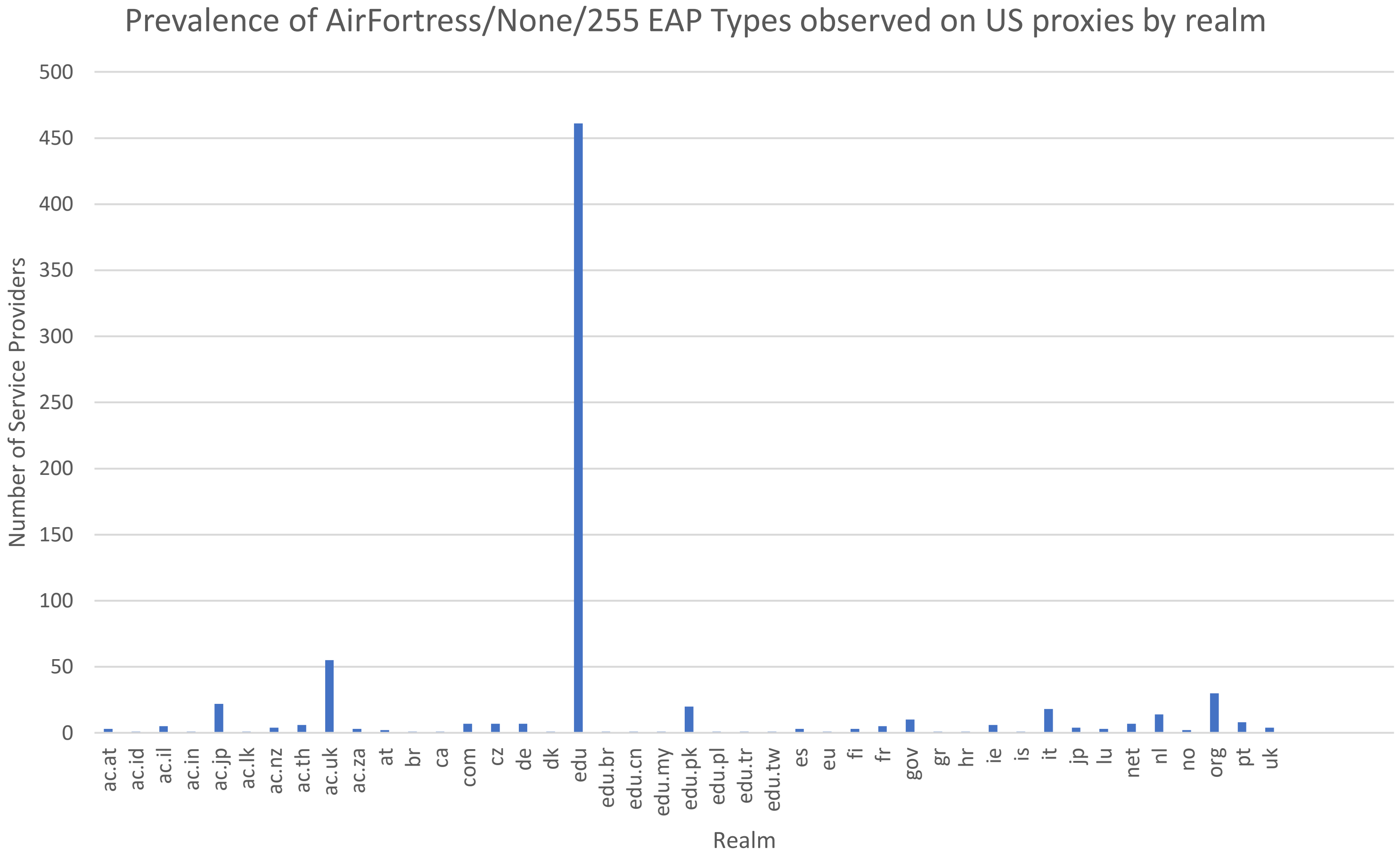
```
[redacted].Edu", due to lack of any response from home server [redacted] 1812#REGION=us-east-2#EAPTYPE=AirFortress-EAP#VISINSTID=[redacted]#NEXTHO
```

Analysis of EAP types observed by the proxies

- AirFortress is the fourth most widely requested authentication Type – **but has never been implemented**
- Types of None and 255 (none and all bits set, respectively) are fifth and eighth – **they are both invalid values**
- **All Type values** (0-255) can be observed within 3 weeks
- These unusual values are observed from **755 service providers globally** returning Operator-Name



Malformed EAP packets are emitted globally



This data is indicative because it relies on

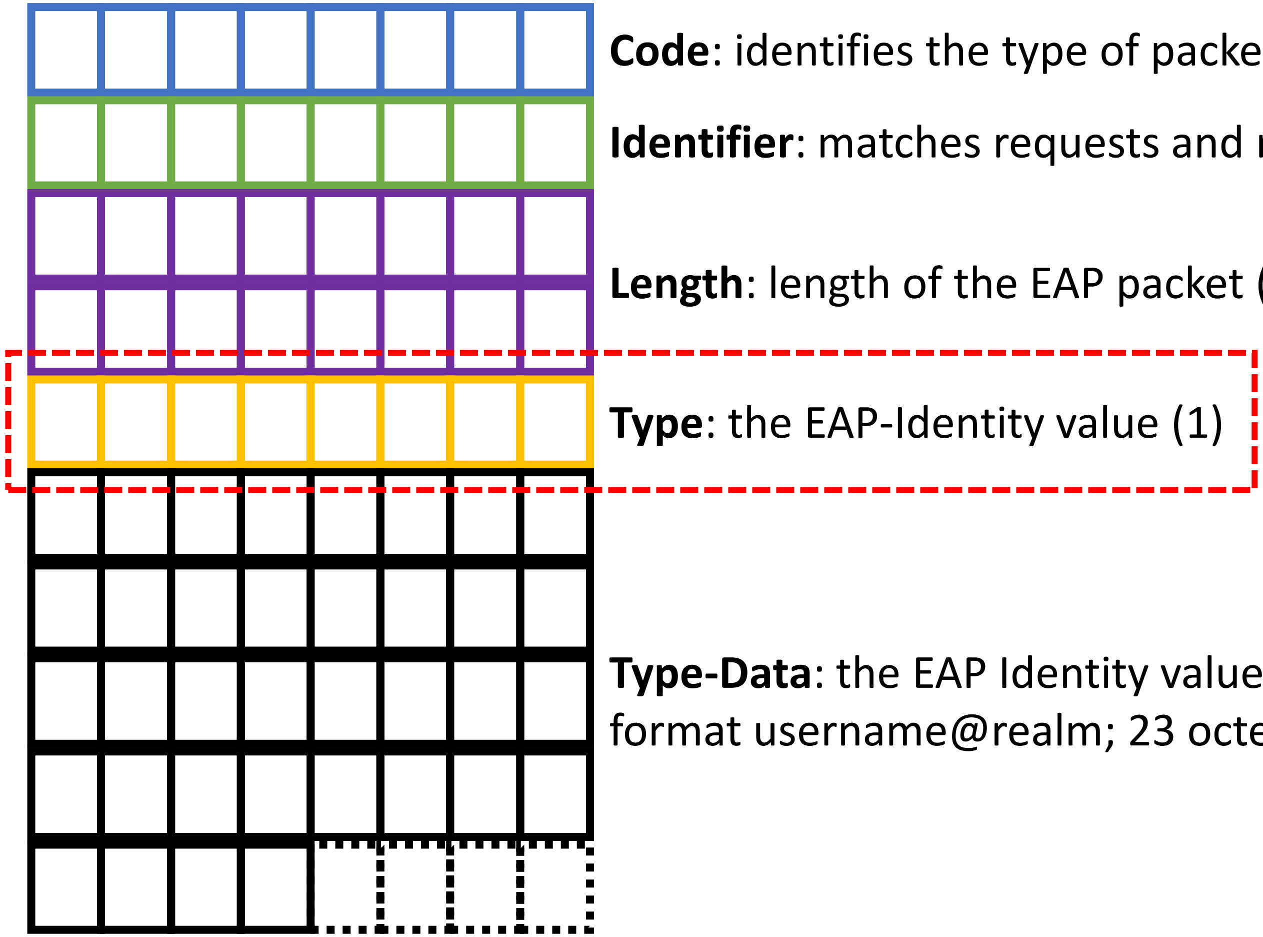
- the presence of the Operator-Name attribute
- a user from the US visiting an institution
- the malformed packet having a Type of AirFortress, None, or 255

However, it demonstrates the global distribution of malformed EAP emissions

The data is heavily weighted to .edu because our proxies know their Operator-Names

EAP Frame (Response/Identity)

The typical EAP-Request/Identity length is around 28 octets or 224 bits



Code: identifies the type of packet (request, response, success, failure) (2)

Identifier: matches requests and responses (variable)

Length: length of the EAP packet (variable)

Type: the EAP-Identity value (1)

The reported F-TICKS value is an 8-bit window into the EAP packet (or < 4% of the packet)

Type-Data: the EAP Identity value (variable, takes the format username@realm; 23 octets is the average)

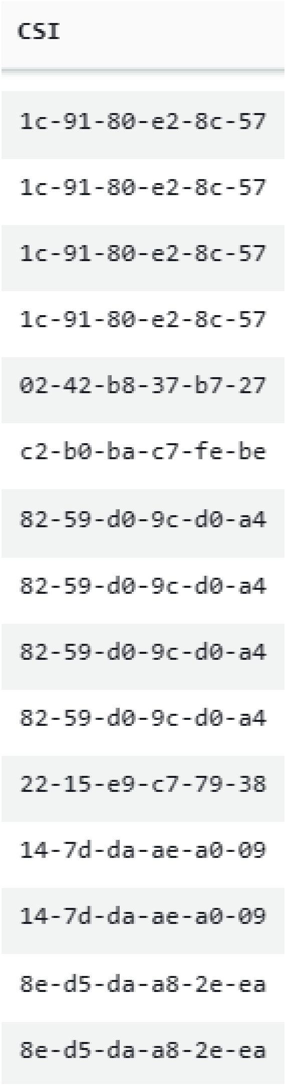
Three hypotheses

- Something is going wrong between the supplicant and the RADIUS client

1. It is a buggy supplicant
    - This seems the most likely hypothesis: supplicants have been a source of problems in the past
    - However, widespread use of MAC anonymisation (~87%) makes it impossible to correlate malformed EAP packets with supplicant platforms
2. It is wireless corruption
    - Wireless corruption is common, but CRC error detection should prevent leakage “onto the wire”
    - This is no easy way of testing this hypothesis
3. It is a buggy RADIUS client
    - This seems unlikely because
        - vendor products tend to be reliable
        - it is a bizarre failure for a “pass-through” authenticator that is meant to be transparent at the EAP layer
        - a significant proportion of SPs are emitting malformed EAP packets and it seems improbable that they (and their vendor) are all running buggy products without realising
    - There was no obvious way of fingerprinting products from the data available in our logs

Three lucky breaks

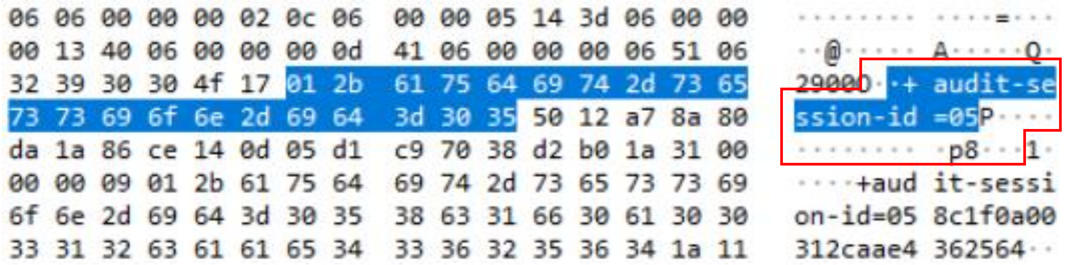
- CSI value format strongly suggests the RADIUS client is at fault
  - I noticed that about 95% of CSI values associated with malformed EAP packets use the same EUI-48 format (lower case and hyphen delimited)
  - The general prevalence of this format is only 59%
  - This suggests that the malformed EAP packets are associated with the RADIUS client, because that is the entity that creates the CSI value
- Capture of a malformed EAP packet
  - Margaret Cullen and Alan DeKok manage to identify a rare instance of a malformed packet manually using tcpdump
  - The contents of the packet are weird but intelligible (a DNS message), ruling out wireless corruption
- Discovery of the tshark tool
  - Provides much more powerful filtering than tcpdump
  - sudo tshark -w - udp and dst port 1812 and dst host 163.253.31.2 | tshark -V -n -r - "eap.code > 6"



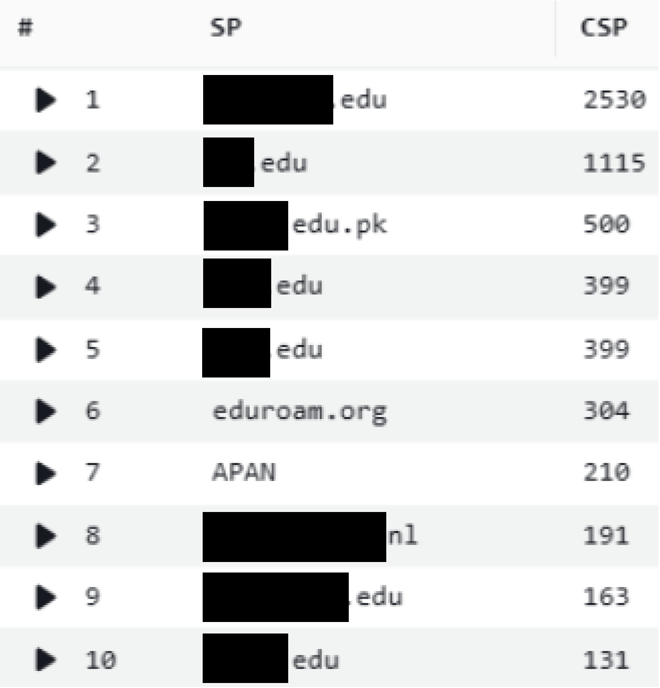
CSI
1c-91-80-e2-8c-57
1c-91-80-e2-8c-57
1c-91-80-e2-8c-57
1c-91-80-e2-8c-57
02-42-b8-37-b7-27
c2-b0-ba-c7-fe-be
82-59-d0-9c-d0-a4
82-59-d0-9c-d0-a4
82-59-d0-9c-d0-a4
82-59-d0-9c-d0-a4
22-15-e9-c7-79-38
14-7d-da-ae-a0-09
14-7d-da-ae-a0-09
8e-d5-da-a8-2e-ea
8e-d5-da-a8-2e-ea

Identifying the RADIUS client vendor

- We used tshark to obtain hundreds of malformed EAP packets for the top emitters
- The RADIUS Access-Requests for these packets all included VSAs for the same vendor
- The payloads in the packets were usually unintelligible, but often recognisable, and sometimes very unusual
    - The malformed EAP contents are probably parts of random memory in the access point and/or controller
    - The example below shows the EAP message attribute (highlighted) partially taking the value of another RADIUS attribute

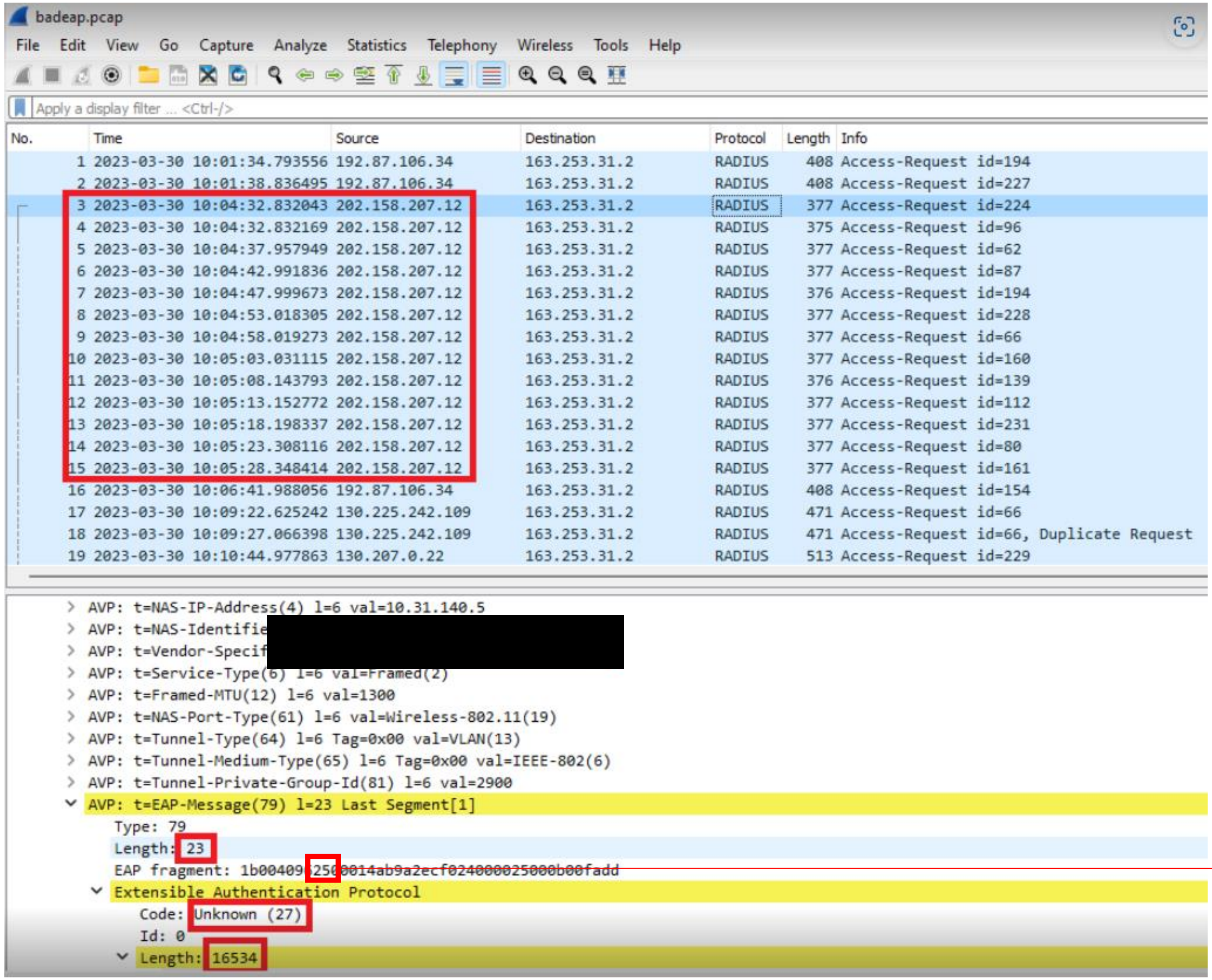


```
06 06 00 00 00 02 0c 06  00 00 05 14 3d 06 00 00   ········ ····=···
00 13 40 06 00 00 00 0d  41 06 00 00 00 06 51 06   ··@····· A·····Q·
32 39 30 30 4f 17 01 2b  61 75 64 69 74 2d 73 65   2900O··+ audit-se
73 73 69 6f 6e 2d 69 64  3d 30 35 50 12 a7 8a 80   ssion-id =05P····
da 1a 86 ce 14 0d 05 d1  c9 70 38 d2 b0 1a 31 00   ········ ·p8···1·
00 00 09 01 2b 61 75 64  69 74 2d 73 65 73 73 69   ····+aud it-sessi
6f 6e 2d 69 64 3d 30 35  38 63 31 66 30 61 30 30   on-id=05 8c1f0a00
33 31 32 63 61 61 65 34  33 36 32 35 36 34 1a 11   312caae4 362564··
```



#	SP	CSP
▶ 1	[redacted].edu	2530
▶ 2	[redacted]edu	1115
▶ 3	[redacted]edu.pk	500
▶ 4	[redacted]edu	399
▶ 5	[redacted]edu	399
▶ 6	eduroam.org	304
▶ 7	APAN	210
▶ 8	[redacted]nl	191
▶ 9	[redacted].edu	163
▶ 10	[redacted]edu	131

The AirFortress-EAP mystery solved


badeap.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                       Source          Destination   Protocol Length Info
   1 2023-03-30 10:01:34.793556 192.87.106.34   163.253.31.2  RADIUS   408 Access-Request id=194
   2 2023-03-30 10:01:38.836495 192.87.106.34   163.253.31.2  RADIUS   408 Access-Request id=227
   3 2023-03-30 10:04:32.832043 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=224
   4 2023-03-30 10:04:32.832169 202.158.207.12  163.253.31.2  RADIUS   375 Access-Request id=96
   5 2023-03-30 10:04:37.957949 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=62
   6 2023-03-30 10:04:42.991836 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=87
   7 2023-03-30 10:04:47.999673 202.158.207.12  163.253.31.2  RADIUS   376 Access-Request id=194
   8 2023-03-30 10:04:53.018305 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=228
   9 2023-03-30 10:04:58.019273 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=66
  10 2023-03-30 10:05:03.031115 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=160
  11 2023-03-30 10:05:08.143793 202.158.207.12  163.253.31.2  RADIUS   376 Access-Request id=139
  12 2023-03-30 10:05:13.152772 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=112
  13 2023-03-30 10:05:18.198337 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=231
  14 2023-03-30 10:05:23.308116 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=80
  15 2023-03-30 10:05:28.348414 202.158.207.12  163.253.31.2  RADIUS   377 Access-Request id=161
  16 2023-03-30 10:06:41.988056 192.87.106.34   163.253.31.2  RADIUS   408 Access-Request id=154
  17 2023-03-30 10:09:22.625242 130.225.242.109 163.253.31.2  RADIUS   471 Access-Request id=66
  18 2023-03-30 10:09:27.066398 130.225.242.109 163.253.31.2  RADIUS   471 Access-Request id=66, Duplicate Request
  19 2023-03-30 10:10:44.977863 130.207.0.22    163.253.31.2  RADIUS   513 Access-Request id=229
```

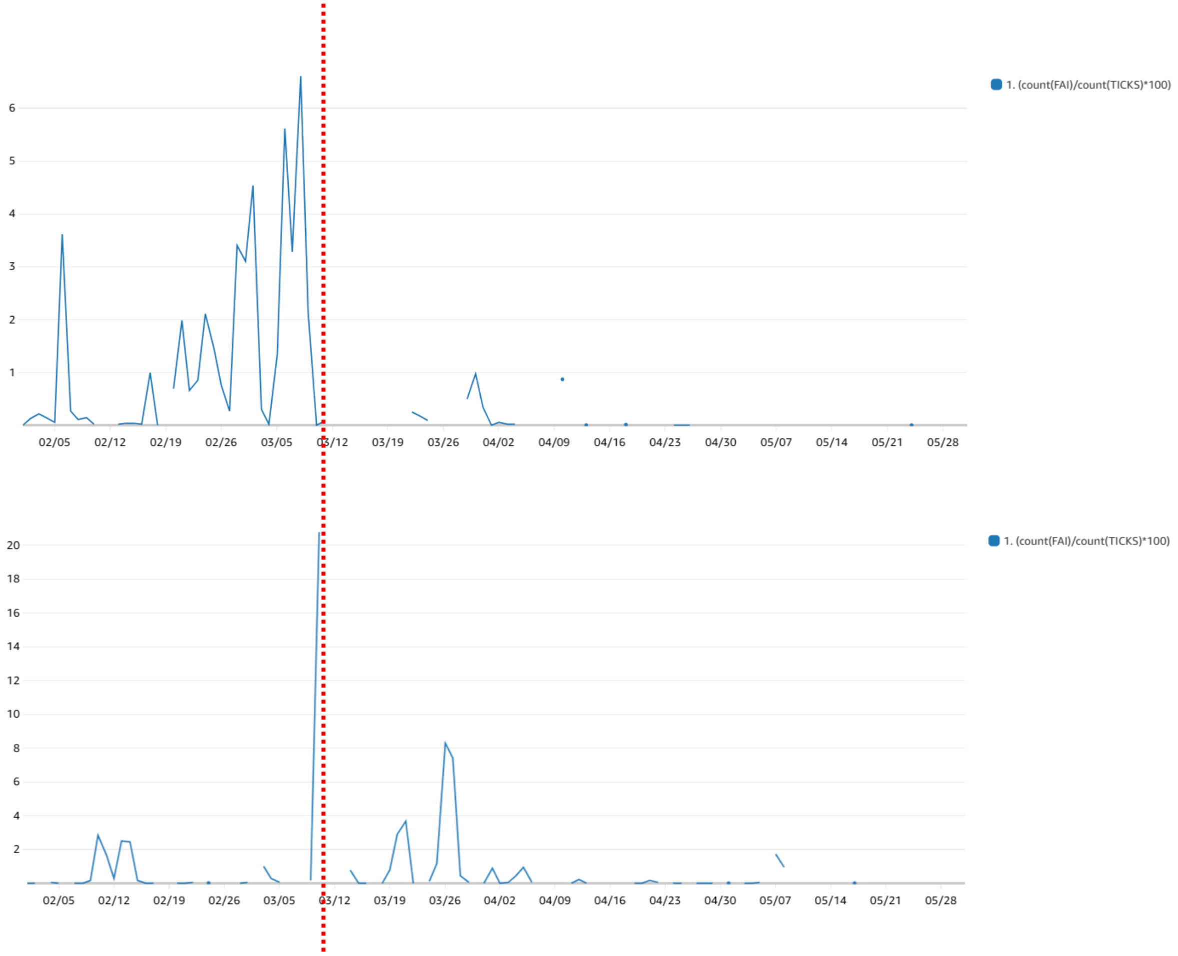
```
> AVP: t=NAS-IP-Address(4) l=6 val=10.31.140.5
> AVP: t=NAS-Identifie[redacted]
> AVP: t=Vendor-Specif
> AVP: t=Service-Type(6) l=6 val=Framed(2)
> AVP: t=Framed-MTU(12) l=6 val=1300
> AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
> AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)
> AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)
> AVP: t=Tunnel-Private-Group-Id(81) l=6 val=2900
v AVP: t=EAP-Message(79) l=23 Last Segment[1]
    Type: 79
    Length: 23
    EAP fragment: 1b0040962500014ab9a2ecf024000025000b00fadd
  v Extensible Authentication Protocol
      Code: Unknown (27)
      Id: 0
    v Length: 16534
```

The fifth byte gives the EAP Type as 25 (hex), which in decimal is 37: the value for AirFortress-EAP

Managing the issue

- The frequency and severity of the disruption continued to increase through February and March
- We increased proxy capacity as a workaround (and so increase the ID space) by adding additional RADIUS proxy containers
- The Internet2 eduroam Ops team discussed the issue with Alan DeKok at IETF 116 in late March, who provided a software solution
  - Packets with an invalid EAP code (>6) get an Access-Reject and are not proxied
  - Packets with incorrect EAP length get an Access-Reject and are not proxied
- There is an ongoing discussion on the IETF RADEXT mailing list concerning the best approach

Allocation errors and proxy capacity

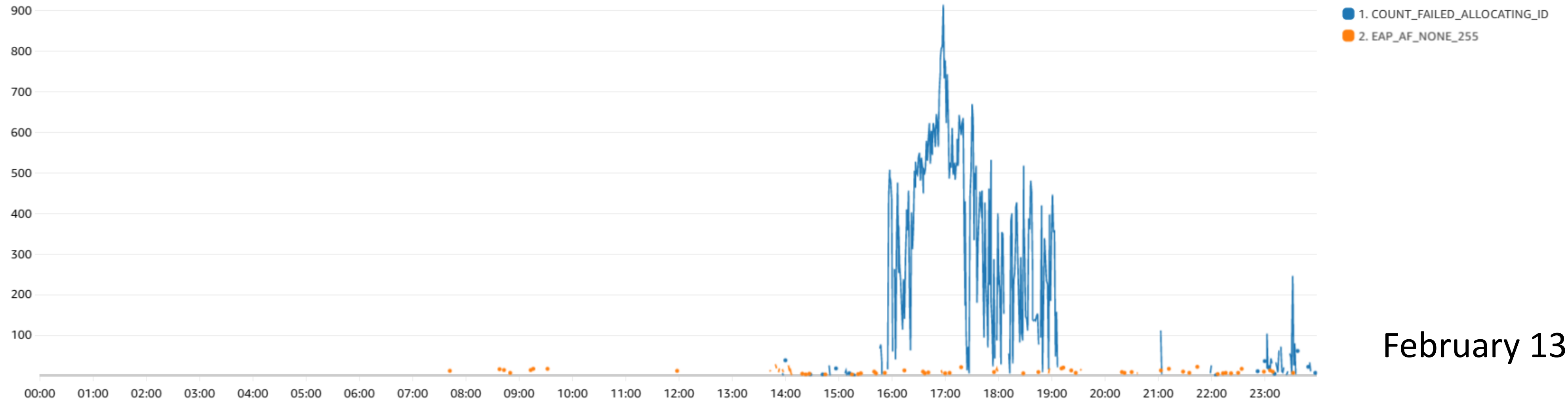


New containers created

- The graphs show allocation errors as a percentage of all requests from the start of February until end of May
- The additional proxy capacity immediately reduced the frequency of allocation errors
- This temporarily increased the cost of AWS ECS by 24%
- Alan’s patches are going into production very soon
- We expect to remove the additional containers at some point

“Dark EAP packets” on eduroam?

- The EAP Type reported in the proxy logs provides a very limited view (just 8-bits) of the EAP packets that we proxy and so we can only detect a subset of malformed packets
- There may be a larger volume of “dark EAP packets” being proxied that we cannot detect with our existing instrumentation
- We can count the RADIUS packets transporting dark EAP packets, but do we understand their impact on the infrastructure?



February 13th, 2023

Some questions remain

- Why did the severity of the problem increase after January 2023 when volumes of malformed EAP packets appear to remain static?
- Why do malformed EAP packets from our international peers appear to have a greater impact than US-sourced packets?
- CSI format analysis suggests there is at least one other vendor emitting malformed EAP packets – who are they, and do we care?

- We have completed the analysis needed to identify the root cause and find a solution and so the impetus to investigate these open questions has receded – but that doesn’t mean they’re not important

Recommendation and discussion points

- NROs should consider the implications of this issue
    - Many SPs globally are emitting malformed EAP packets
    - Correctly behaving, non-responding IDPs are degrading RADIUS proxy performance
    - Consider what steps might be appropriate to manage this issue nationally

- We are trusting of our RADIUS clients and supplicants
    - Our access points form a massive, accessible surface for EAP-Requests, benign and malicious
    - The RADIUS client vendor does not appear to be prioritising the problem
    - The vendor’s products have had this issue since at least 2018 – does our infrastructure need more intelligence and resilience to identify and manage future problems?

- We pay much less attention to EAP than RADIUS
    - But the RADIUS infrastructure exists for the sole purpose of transporting EAP
    - Should our proxies be applying policy on EAP packets?
    - See recent discussion on the IETF radext mailing list – some interesting architectural points