ClearPass Operational Report Detail

Derin Mellor

19/12/20

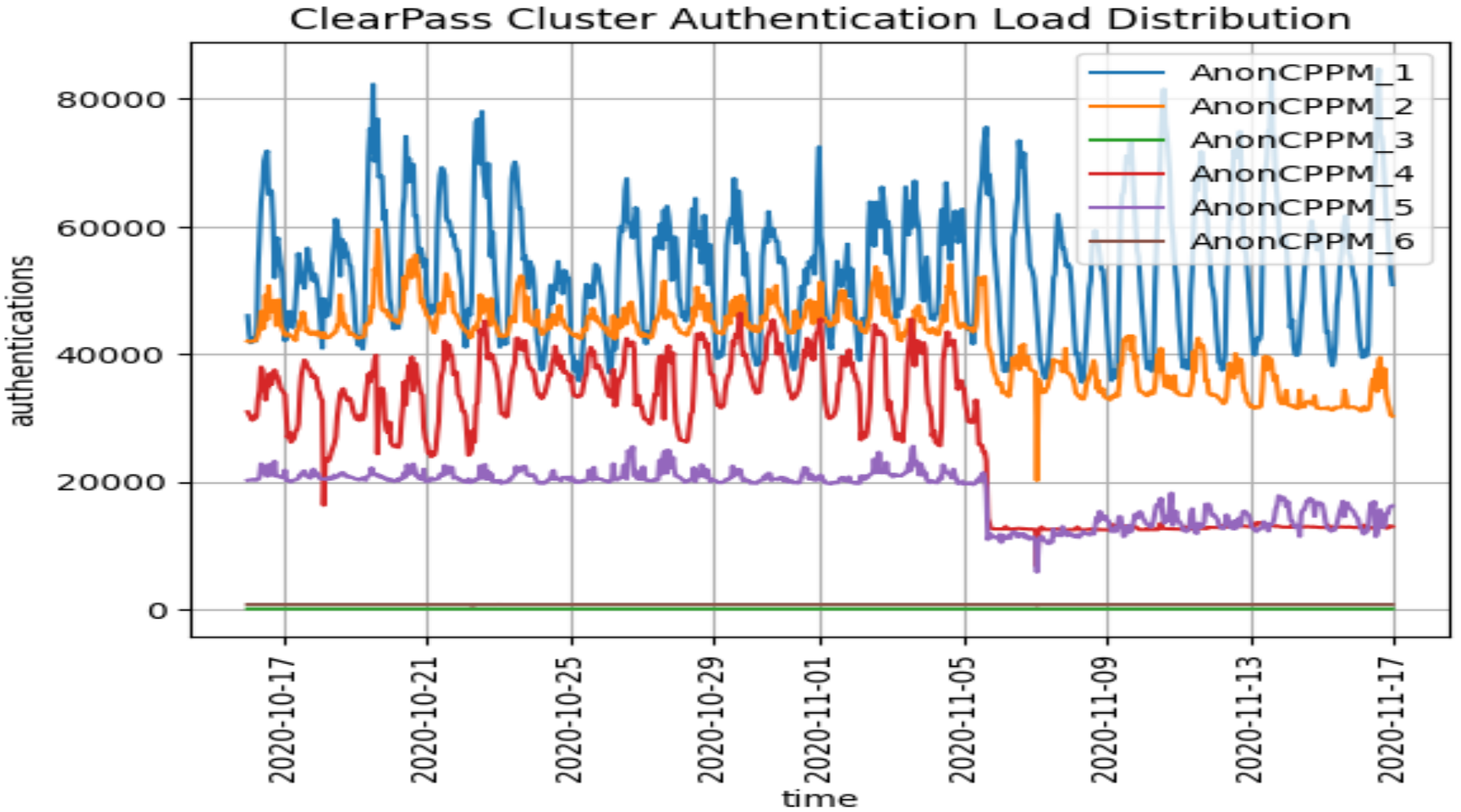
0.04 DRAFT

Timeframe 2020-10-16 to 2020-11-17

Contents

Specific Details

ClearPass Cluster Authentication Load Distribution



This graph may highlight poor distribution of authentications across the ClearPass cluster. However, this is very dependent on the cluster's architectural design.
If this is a master/hot-standby design you expect the load to be totally on the master and only transition to the hot-standby if the master has failed.
If this was a distributed design one would expect the load to be evenly shared across all the ClearPass appliances. A quick visual inspection will indicate how

well this is operating.

ClearPass Cluster Details

This reports all the ClearPass appliances that had been involved in RADIUS authentications

ClearPass	IP	Zone
AnonCPPM_1	XXXXXXXXXXXX	ZZZZZ
AnonCPPM_2	XXXXXXXXXXXX	ZZZZZ
AnonCPPM_3	XXXXXXXXXXXX	ZZZZZ
AnonCPPM_4	XXXXXXXXXXXX	ZZZZZ
AnonCPPM_5	XXXXXXXXXXXX	ZZZZZ
AnonCPPM_6	XXXXXXXXXXXX	ZZZZZ

Top 10 ClearPass Cluster Events

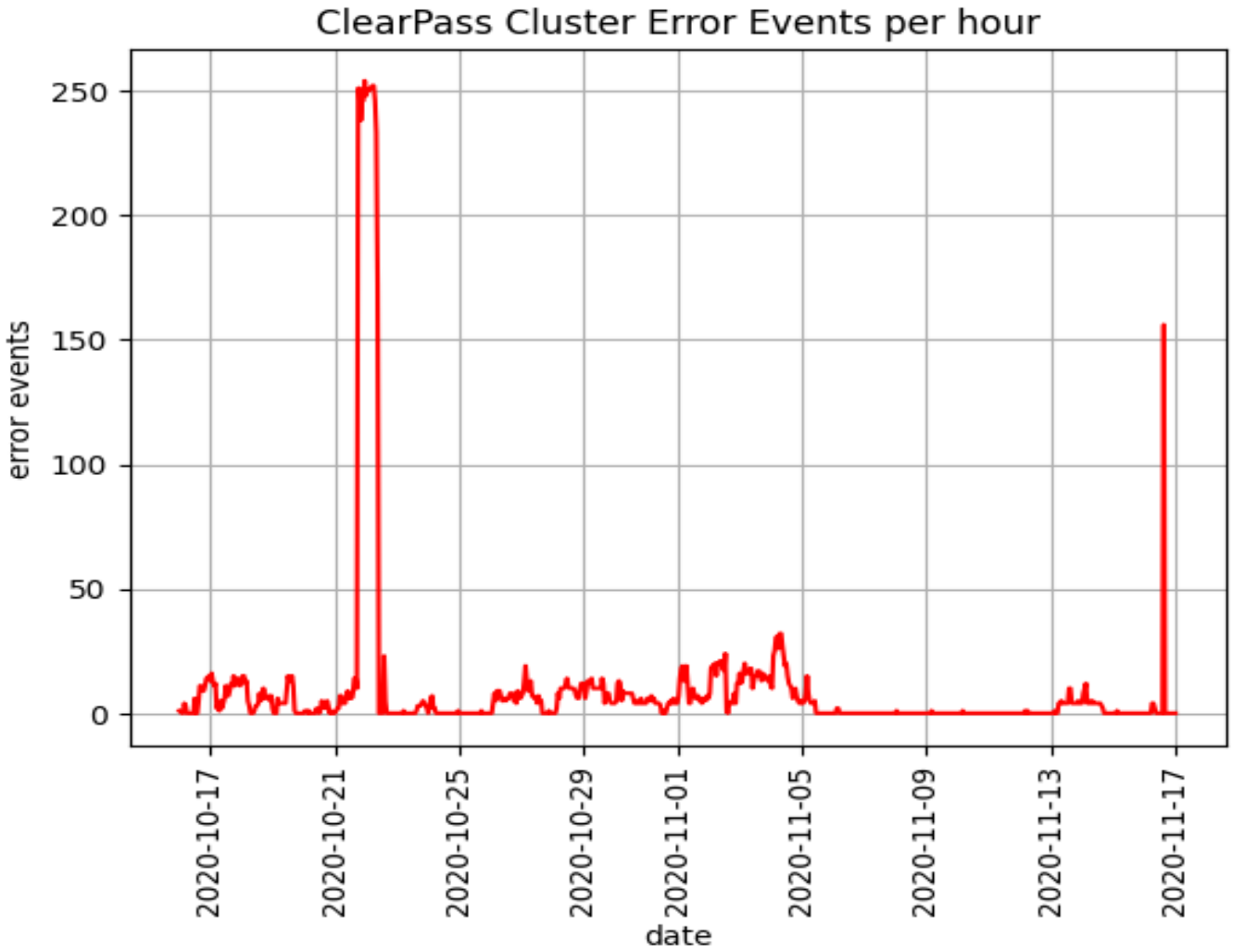
NOTE: ERROR in Red & WARNING in Amber

Count	ClearPass	Source	Level	Category	Description
3755	AnonCPPM_4	RADIUS	ERROR	Authentication	Failed to decode RADIUS packet - Received packet from XXXXX77.9 with invalid Message-Authenticator! (Shared secret may be incorrect.)
845	AnonCPPM_4	Monitor	ERROR	Fdb	DB write service(fdb) unstable backlog:1
767	AnonCPPM_1	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=XXXXX100.169
763	AnonCPPM_2	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for

					device=XXXXX100.19
762	AnonCPPM_3	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device XXXXX100.203 with error=No response received\nReading sysObjectId failed for device=XXXXX100.203\nReading switch initialization info failed for XXXXX100.203
759	AnonCPPM_5	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device XXXXX100.179 with error=Authorization error\nReading sysObjectId failed for device=XXXXX100.179\nReading switch initialization info failed for XXXXX100.179
747	AnonCPPM_3	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=XXXXX100.4
744	AnonCPPM_2	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device XXXXX100.205 with error=No response received\nReading sysObjectId failed for device=XXXXX100.205\nReading switch initialization info failed for XXXXX100.205
741	AnonCPPM_1	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device XXXXX204.170 with error=No response received\nReading sysObjectId failed for device=XXXXX204.170\nReading switch initialization info failed for XXXXX204.170
737	AnonCPPM_2	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=XXXXX100.43

This reports the number of matching events and which ClearPass they occurred on. Error events are highlighted in red. Warning events are highlighted in red. Ultimately it is desirable to minimise these.

ClearPass Cluster Error Events per hour



This graph summaries the ClearPass cluster's error events. Clearly any error events are not good, but may not be directly related to authentications. If these do correlate with increased authentication failures they should be investigate.

ClearPass Cluster Error Events Burst Details

These tables highlights the break down of events in key bursts

Event burst between 2020-10-21 23:00-2020-10-22 00:00

Count	ClearPass	Category	Description
240	AnonCPPM_4	Authentication	Failed to decode RADIUS packet - Received packet from 10.4.77.9 with invalid Message-Authenticator
4	AnonCPPM_4	Fdb	DB write service(fdb) unstable backlog:1
2	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 44
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 49
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 52
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:10.74 Load5:11.47 Load15:10.13}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:7.84 Load5:10.21 Load15:10.34}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:9.41 Load5:9.49 Load15:9.74}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:9.45 Load5:9.01 Load15:8.53}
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 45
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 47

Event burst between 2020-10-22 05:00-2020-10-22 06:00

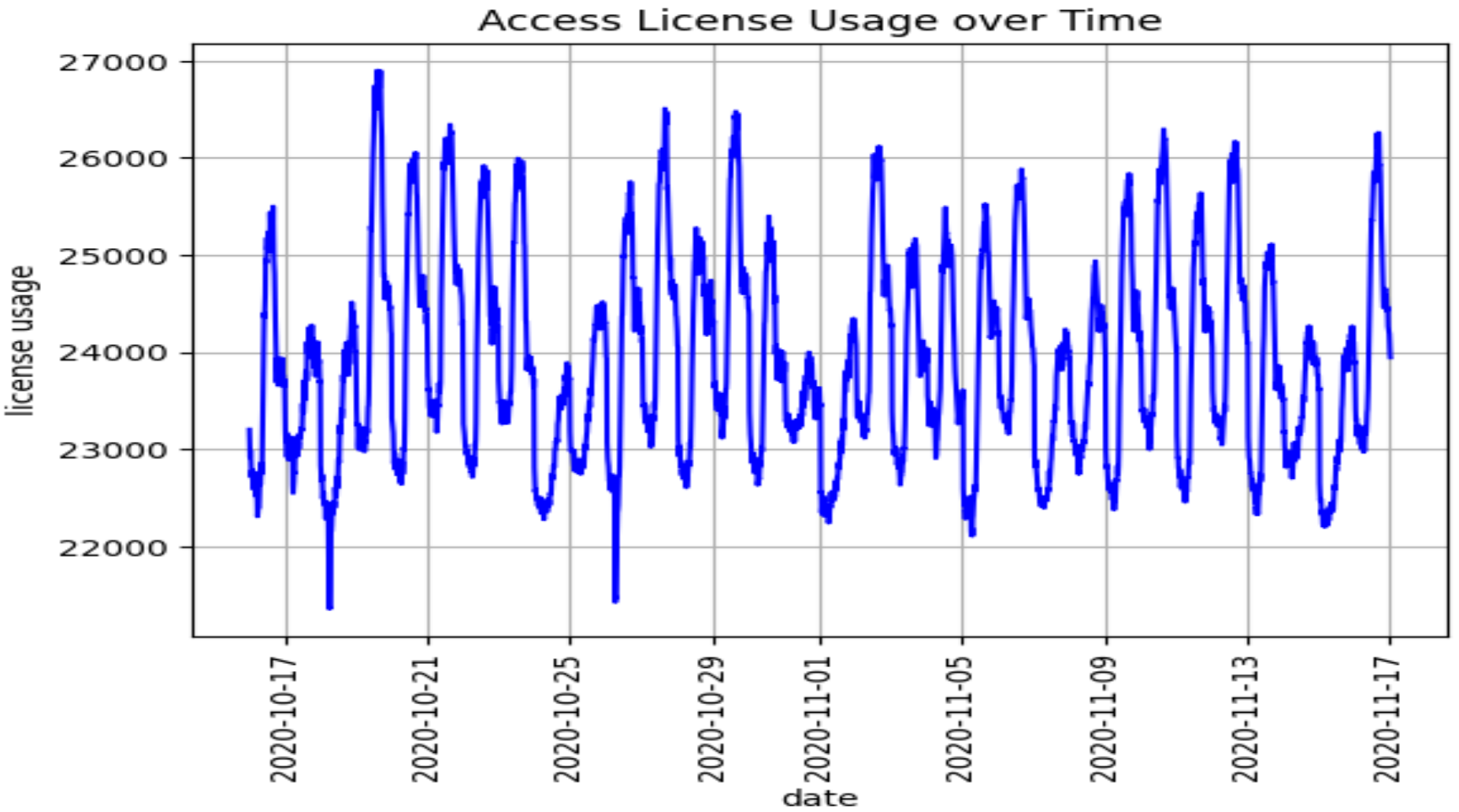
Count	ClearPass	Category	Description
240	AnonCPPM_4	Authentication	Failed to decode RADIUS packet - Received packet from 10.4.77.9 with invalid Message-Authenticator
2	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 48
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 49
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 51
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 52
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:10.38 Load5:11.08 Load15:11.7}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:10.95 Load5:10.27 Load15:10.32}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:11.48 Load5:13.18 Load15:12.29}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:11.65 Load5:10.69 Load15:10.39}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:8.97 Load5:9.44 Load15:10.5}

1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:9.68 Load5:12.19 Load15:12.48}
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 46

Event burst between 2020-10-22 06:00-2020-10-22 07:00

Count	ClearPass	Category	Description
240	AnonCPPM_4	Authentication	Failed to decode RADIUS packet - Received packet from 10.4.77.9 with invalid Message-Authenticator
3	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 47
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 46
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 50
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:10.09 Load5:10.68 Load15:11.15}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:10.47 Load5:10.78 Load15:10.43}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:8.09 Load5:9.09 Load15:9.86}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:8.71 Load5:9.4 Load15:10.26}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:8.9 Load5:10.12 Load15:10.77}
1	AnonCPPM_4	Os(Cpu)	High load average(5 min) {Load1:9.44 Load5:11.53 Load15:11.36}
1	AnonCPPM_4	System(CPU)	High I/O wait(10 min avg) - 45

Access License Usage over Time



These highlights when licenses are being used. If the report is over a long period of time it may indicate changes in network usage. Unexpected peaks may indicate malicious behaviour.

Stale Access License Recover

Nothing exceptional

These are a count of 'stale' access licenses that are recovered overnight. An access license becomes 'stale' if after 24 hours ClearPass has not seen a RADIUS Accounting Interim or a RADIUS Accounting Stop. The session may still exist but ClearPass has no visibility or control over it.

Endpoint Categorization

Category	Total
SmartDevice	22744
No Fingerprint	9916
Home Audio/Video Equipment	219
Medical Device	1
Computer	10906
Network Boot Agents	112
Projectors	2
Presentation	1
Audio/Video Devices	4
Monitoring Devices	34

This reports the top 10 endpoints of particular type.
Endpoints reported as 'No Fingerprint' are highlighted in red: These have not been fingerprinted - question is why? This could indicate lack of DHCP Request or no proactive scanning?
Endpoints reported as 'Generic' are highlighted in amber: These either have been fingerprinted purely on the OUI or the fingerprint is not recognised. If only an OUI why? If the fingerprint is not recognised best to feed this information back via Aruba TAC - they will update the fingerprint file appropriately (this is automatically loaded on the 1st or 15th of every month) Alternatively, manually create the appropriate fingerprint categorization.

Endpoint IP Address Assignment

Total	Static IP	DHCP Address
52520	10262	42258

This reports the distribution between devices with static IP address and using DHCP. ClearPass assumes all devices have a static IP address and only makes the device 'DHCP' if it receives an associated DHCP Request relayed to ClearPass (usually). Generally, it is preferred to use dynamic IP addresses. Hence, if the Static IP count is greater than the DHCP count it is reported in amber. This could be an indication that there are excessive number of devices with a static IP address. Or that DHCP Requests are not being relayed to the ClearPass.
DHCP is highly desirable that ClearPass receives DHCP Requests as it can use these to profile the device, and possibly identify spoofed devices.
Static IP addresses can be profile using SNMP, SSH, WMI, NMAP or device's HTTP user-agent (reliant on ClearPass seeing the web request). NMAP and user-agent are both very unreliable for fingerprint, but may be useful to identify specific usage or spoofing.

Endpoint MAC & IP Address Details

Total	MAC Only	MAC & IP	IP Only
52520	8162	44321	37

This reports the number of devices that ClearPass knows - this is split in to three categories:
1) Devices with MAC address only: Possibly indicates that RADIUS Account is not working or the RADIUS Accounting is not populating the Framed-IP-Address. If the NAS does not support RADIUS Accounting with Framed-IP-Address ClearPass can be configured to read the appropriate ARP table (e.g. local access router) - using the suitable SNMP credentials. NOTE the default poll is once an hour, this can be tuned down to 10 minutes. But this is likely to be too slow for effective RESTful API upper-layer injection where the IP address is required (e.g. firewall). These are always highlighted in amber. Also NASs dealing with devices that have static IP addresses are likely to require special configuration to proactively set the Framed-IP-Address - some NAS do not support this or are slow at learning a static IP addresses.
2) Devices with MAC and IP address: This is where we want everything.
3) Devices with IP address only: These are devices that typically have been learnt via a proactive scan (SNMP, SSH, WMI or NMAP) or via ClearPass observing the device's HTTP user-agent. These could be devices that are not being controlled by ClearPass? - these need checking.

Endpoints with Randomized MAC Addresses

Total	0

This is the total number of endpoints using randomized MAC addresses. Theoretically you should only see this on devices connecting to open SSID.

Number of Suspected Spoofs Detected

7432

Device spoofing is a serious concern. Though ClearPass' ability to detect them is not great. False positives are common. Likewise, many devices my be commissioned using PXE Boot - there is a setting to disable identifying these. Alternatively whitelist in this report's ini file.

10 Most Recent Spoof

MAC	Category	Family	DevType	Spoof Category	Spoof Family	Spoof DevType
AnonMAC_1	Computer	Windows	Surface	Computer	Windows	Surface
AnonMAC_2	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X
AnonMAC_3	Computer	Windows	Windows	Computer	Windows	Windows
AnonMAC_4	Computer	Windows	Windows	Building Automation	Liteon	Liteon Storage
AnonMAC_5	Game Console	Microsoft	Xbox	Computer	Windows	Windows 10
AnonMAC_6	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X
AnonMAC_7	Computer	Apple Mac	Mac OS X	SmartDevice	Apple	Apple iOS Device
AnonMAC_8	Computer	Windows	Windows	Building Automation	Liteon	Liteon Storage
AnonMAC_9	SmartDevice	Apple	Apple iPad	Computer	Apple Mac	Mac OS X

AnonMAC_10	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X

Missing Known Endpoints

26755

Last Seen	MAC Address	IP Address	Hostname	Username	NAS Name	NAS IP	Media	Port/SSID
2020/10/15	AnonMAC_11	AnonIP_1	AnonHost_1	AnonUser_1	AnonNAS_1	AnonNAS_1	Wifi	eduroam
2020/10/15	AnonMAC_12	AnonIP_2	AnonHost_2	AnonUser_2	AnonNAS_2	AnonNAS_2	Wifi	eduroam
2020/10/15	AnonMAC_13	AnonIP_3		AnonUser_3	AnonNAS_3	AnonNAS_3	Virtual	
2020/10/15	AnonMAC_14	AnonIP_4	AnonHost_3		AnonNAS_4	AnonNAS_4	Wifi	eduroam
2020/10/15	AnonMAC_15	AnonIP_5		AnonUser_4	AnonNAS_2	AnonNAS_2	Wifi	eduroam
2020/10/15	AnonMAC_16	AnonIP_6	AnonHost_4		AnonNAS_3	AnonNAS_3	Virtual	
2020/10/15	AnonMAC_17	AnonIP_7	AnonHost_5	AnonUser_5	AnonNAS_4	AnonNAS_4	Wifi	eduroam
2020/10/15	AnonMAC_18	AnonIP_8			AnonNAS_3	AnonNAS_3	Virtual	
2020/10/15	AnonMAC_19	AnonIP_9	AnonHost_6		AnonNAS_3	AnonNAS_3	Virtual	
2020/10/15	AnonMAC_20	AnonIP_10			AnonNAS_3	AnonNAS_3	Virtual	

This indicates the number of Known endpoints that have not connected in the time frame of the report. WARNING: This maybe misleading as the Insight database does not indicate whether a Known endpoint has been deleted.

Authentications per Service

Service	Total	Successes	Failures
Anonymous Service_1	47919771	47840766	79005
Anonymous Service_2	28986029	28986029	0
Anonymous Service_3	23241745	18791330	4450415
Anonymous Service_4	2991696	512439	2479257
Anonymous Service_5	2066775	2066775	0
Anonymous Service_6	807574	478930	328644
Anonymous Service_7	522262	0	522262
Anonymous Service_8	407155	407155	0
Anonymous Service_9	326125	326125	0
Anonymous Service_10	307708	307708	0
Anonymous Service_11	179236	0	179236
Anonymous Service_12	154774	145583	9191
Anonymous Service_13	138518	133	138385
Anonymous Service_14	126169	123351	2818
Anonymous Service_15	112235	112191	44
Anonymous Service_16	91431	91426	5
Anonymous Service_17	89575	89562	13
Anonymous Service_18	89382	89176	206
Anonymous Service_19	52478	52132	346
Anonymous Service_20	49495	40631	8864
Anonymous Service_21	38799	38791	8
Anonymous Service_22	30543	28863	1680
Anonymous Service_23	29861	7310	22551
Anonymous Service_24	26020	25409	611
Anonymous Service_25	17736	17733	3
Anonymous Service_26	14623	14620	3

Anonymous Service_27	10379	10162	217
Anonymous Service_28	7617	7477	140
Anonymous Service_29	6579	3891	2688
Anonymous Service_30	4451	4451	0
Anonymous Service_31	4394	4394	0
Anonymous Service_32	3176	1152	2024
Anonymous Service_33	3108	0	3108
Anonymous Service_34	2641	2641	0
Anonymous Service_35	2516	2128	388
Anonymous Service_36	1912	1912	0
Anonymous Service_37	1828	0	1828
Anonymous Service_38	1305	1299	6
Anonymous Service_39	1281	1266	15
Anonymous Service_40	1051	763	288
Anonymous Service_41	872	802	70
Anonymous Service_42	508	508	0
Anonymous Service_43	360	36	324
Anonymous Service_44	153	153	0
Anonymous Service_45	61	25	36
Anonymous Service_46	44	32	12
Anonymous Service_47	33	23	10
Anonymous Service_48	27	27	0
Anonymous Service_49	16	16	0
Anonymous Service_50	13	13	0
Anonymous Service_51	9	0	9
Anonymous Service_52	8	8	0

This orders the services based on the total number of authentications handled. It might be desirable to order the services so that the most commonly hit are near the top, though this is not likely to make much difference in performance.

Top 15 Failed Authentications per Server

NOTE: Red >= 50% & Amber >= 25%

Service	Total	Successes	Failures	% Failed
Anonymous Service_7	522262	0	522262	**100**
Anonymous Service_11	179236	0	179236	**100**
Anonymous Service_33	3108	0	3108	**100**
Anonymous Service_37	1828	0	1828	**100**
Anonymous Service_51	9	0	9	**100**
Anonymous Service_13	138518	133	138385	**99**
Anonymous Service_43	360	36	324	**90**
Anonymous Service_4	2991696	512439	2479257	**82**
Anonymous Service_23	29861	7310	22551	**75**
Anonymous Service_32	3176	1152	2024	**63**
Anonymous Service_45	61	25	36	**59**
Anonymous Service_6	807574	478930	328644	**40**
Anonymous Service_29	6579	3891	2688	**40**
Anonymous Service_47	33	23	10	**30**
Anonymous Service_40	1051	763	288	**27**

This is based on the percentage failure. Anything about 50% failure rate is highlighted in red. Above 25% is highlighted in amber. These should be investigated to understand why such high failure rates. It is highly desirable to minimize failures.

Top Endpoints not Matching a Service

NOTE: Red threshold=9600 , Amber threshold=960

#	MAC	Username	NAS	NAS IP	Media	Port/SSID
12	AnonMAC_21	AnonUser_6	AnonNAS_5	AnonNAS_5	Wired	
11	AnonMAC_22	AnonUser_6	AnonNAS_6	AnonNAS_6	Wired	
11	AnonMAC_23	AnonUser_6	AnonNAS_7	AnonNAS_7	Wired	
11	AnonMAC_24	AnonUser_6	AnonNAS_8	AnonNAS_8	Wired	
11	AnonMAC_25	AnonUser_6	AnonNAS_9	AnonNAS_9	Wired	
10	AnonMAC_26	AnonUser_6	AnonNAS_10	AnonNAS_10	Wired	
10	AnonMAC_27	AnonUser_6	AnonNAS_11	AnonNAS_11	Wired	
10	AnonMAC_28	AnonUser_6	AnonNAS_12	AnonNAS_12	Wired	
10	AnonMAC_29	AnonUser_6	AnonNAS_13	AnonNAS_13	Wired	
10	AnonMAC_30	AnonUser_6	AnonNAS_14	AnonNAS_14	Wired	
10	AnonMAC_31	AnonUser_6	AnonNAS_15	AnonNAS_15	Wired	
9	AnonMAC_32	AnonUser_6	AnonNAS_16	AnonNAS_16	Wired	
9	AnonMAC_33	AnonUser_6	AnonNAS_17	AnonNAS_17	Wired	
9	AnonMAC_34	AnonUser_6	AnonNAS_18	AnonNAS_18	Wired	
9	AnonMAC_35	AnonUser_6	AnonNAS_19	AnonNAS_19	Wired	

Authentication request that don't match a service will be rejected. But why did that request not match a service? These needs investigating...

Top Wired Endpoints Authentications

NOTE: Red threshold=8000 , Amber threshold=800

Auths	Success	Failed	MAC
236074	235653	421	AnonMAC_36
236050	235602	448	AnonMAC_37
218157	217708	449	AnonMAC_38
217941	217518	423	AnonMAC_39
217932	217529	403	AnonMAC_40
217930	217487	443	AnonMAC_41
217930	217466	464	AnonMAC_42
217930	217504	426	AnonMAC_43
217929	217521	408	AnonMAC_44
217929	217490	439	AnonMAC_45
217929	217474	455	AnonMAC_28
217928	217507	421	AnonMAC_46
217928	217515	413	AnonMAC_47
217927	217488	439	AnonMAC_48
217927	217505	422	AnonMAC_49

These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

MAC 'AnonMAC_36' Authentication Details

Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
235653	Success	AnonUser_6	Anonymous Service_1	AnonNAS_20	AnonNAS_20	

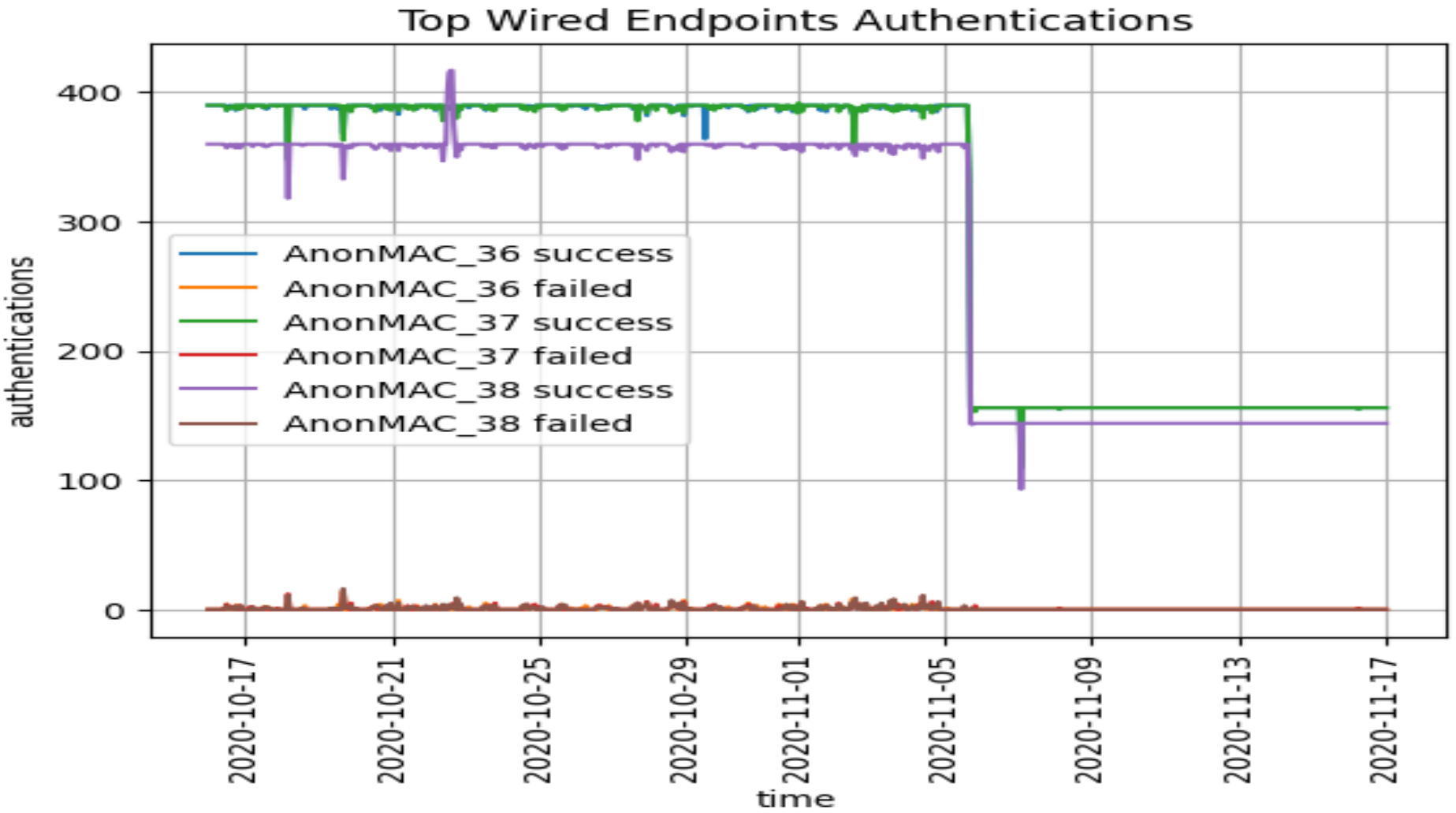
413	Request timed out	AnonUser_6	Anonymous Service_1	AnonNAS_20	AnonNAS_20	
3	User authentication failed	AnonUser_6	Anonymous Service_1	AnonNAS_20	AnonNAS_20	
3	Failed to classify request to s	AnonUser_6	Anonymous Service_53	AnonNAS_20	AnonNAS_20	
2	Internal error in RADIUS ser	AnonUser_6	Anonymous Service_53	AnonNAS_20	AnonNAS_20	

MAC 'AnonMAC_37' Authentication Details

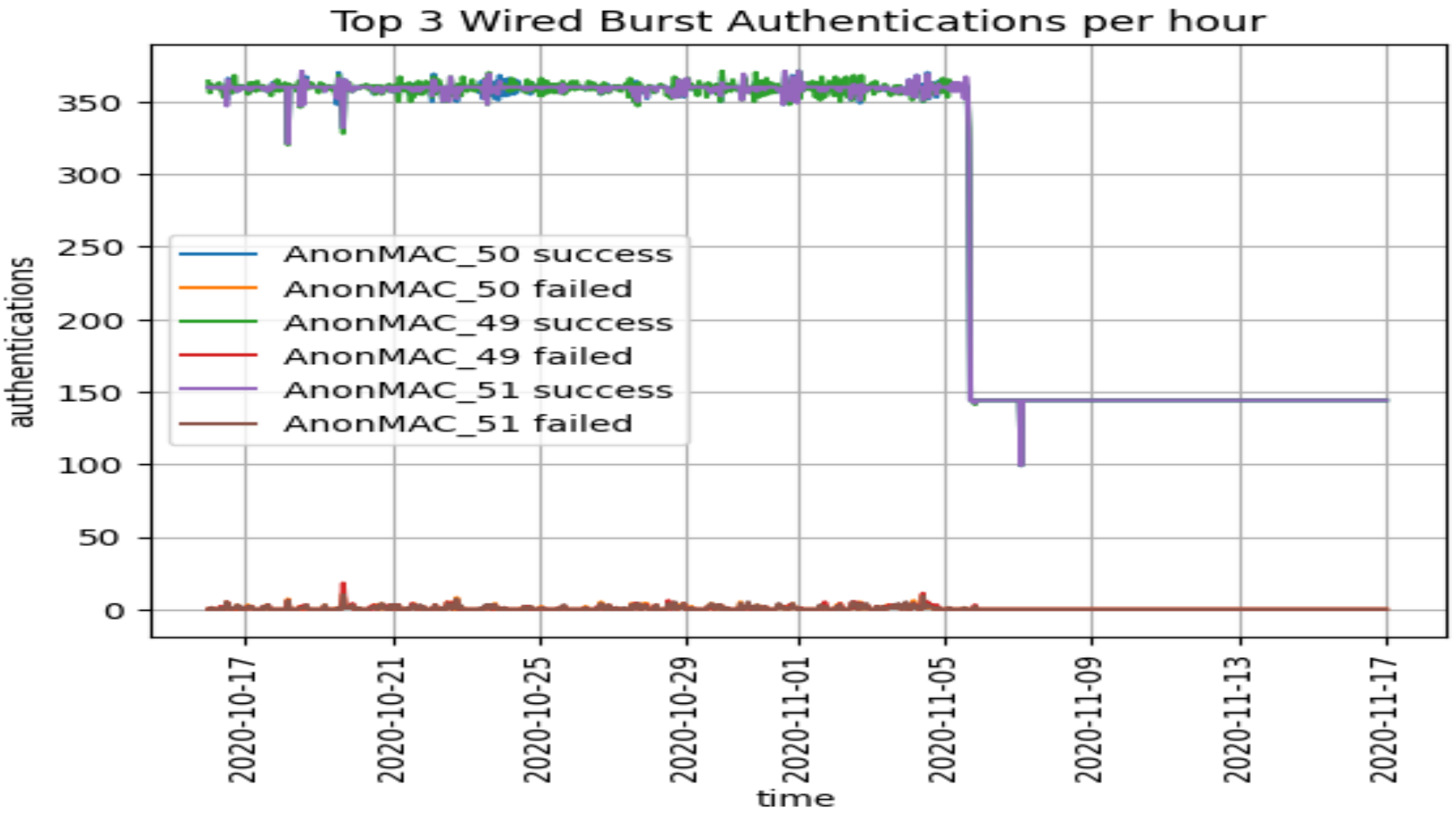
Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
235602	Success	AnonUser_6	Anonymous Service_1	AnonNAS_21	AnonNAS_21	
432	Request timed out	AnonUser_6	Anonymous Service_1	AnonNAS_21	AnonNAS_21	
9	User authentication failed	AnonUser_6	Anonymous Service_1	AnonNAS_21	AnonNAS_21	
7	Failed to classify request to s	AnonUser_6	Anonymous Service_53	AnonNAS_21	AnonNAS_21	

MAC 'AnonMAC_38' Authentication Details

Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
217473	Success	AnonUser_6	Anonymous Service_1	AnonNAS_22	AnonNAS_22	
435	Request timed out	AnonUser_6	Anonymous Service_1	AnonNAS_22	AnonNAS_22	
235	Success		Anonymous Service_2	AnonNAS_23	AnonNAS_23	slot=1;subslot=0;port=35;vlanid=3718
7	Failed to classify request to s	AnonUser_6	Anonymous Service_53	AnonNAS_22	AnonNAS_22	
5	User authentication failed	AnonUser_6	Anonymous Service_1	AnonNAS_22	AnonNAS_22	
2	Internal error in RADIUS ser	AnonUser_6	Anonymous Service_53	AnonNAS_22	AnonNAS_22	



These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top Wireless Endpoints Authentications

NOTE: Red threshold=8000 , Amber threshold=800

Auths	Success	Failed	MAC
246994	0	246994	AnonMAC_52
178960	178738	222	AnonMAC_53
61155	609	60546	AnonMAC_54
46893	540	46353	AnonMAC_55
40864	0	40864	AnonMAC_56
37761	553	37208	AnonMAC_57
33997	122	33875	AnonMAC_58
33891	0	33891	AnonMAC_59
26401	2	26399	AnonMAC_60
26248	25661	587	AnonMAC_61
25796	0	25796	AnonMAC_62
25518	0	25518	AnonMAC_63
23305	22502	803	AnonMAC_64
23258	22488	770	AnonMAC_65
23256	22523	733	AnonMAC_66

These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

MAC 'AnonMAC_52' Authentication Details

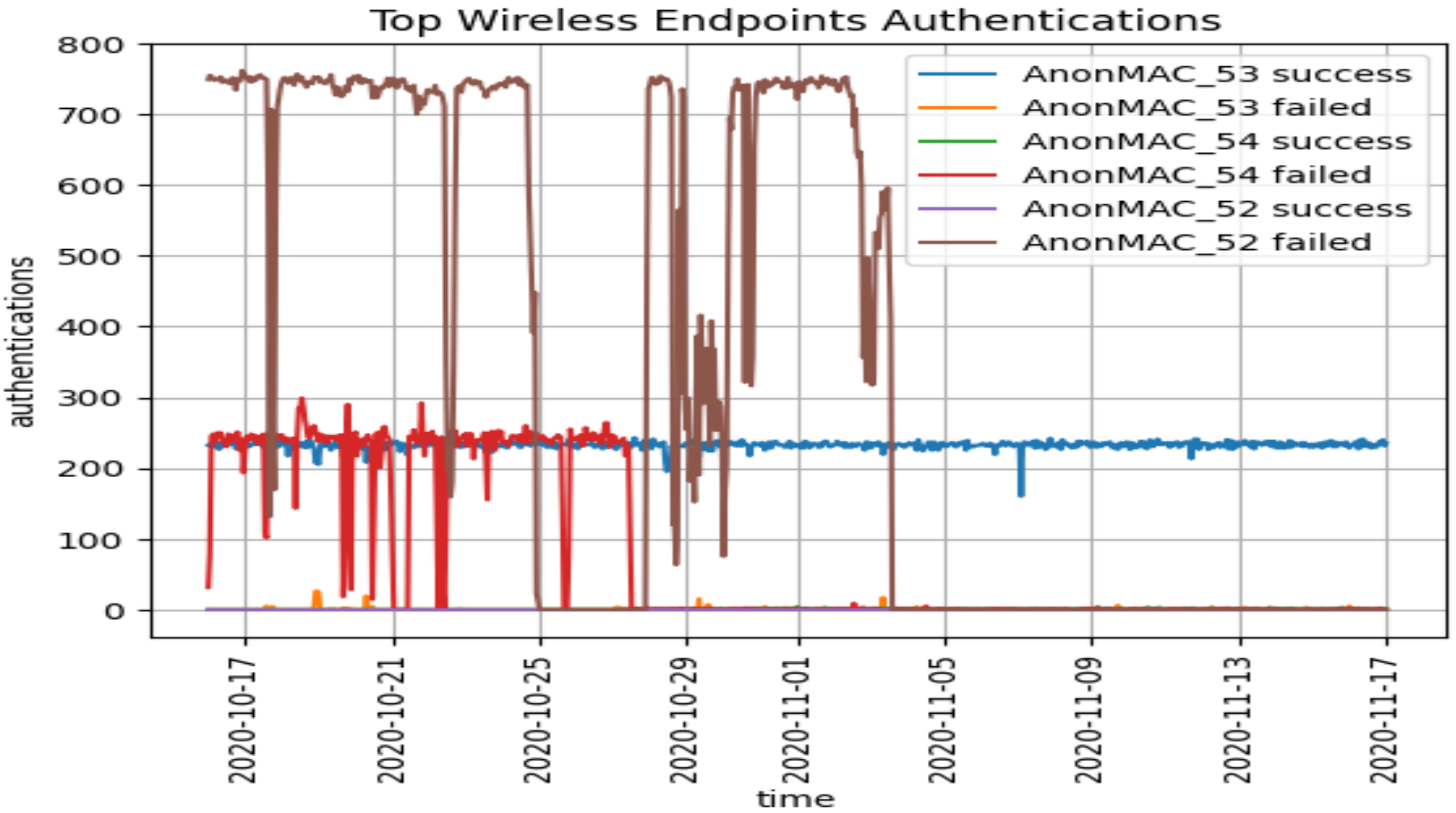
Auths	Error	Username	Service	NAS Name	NAS IP	SSID
246994	User authentication failed		Anonymous Service_4	AnonNAS_24	AnonNAS_24	mydevices

MAC 'AnonMAC_53' Authentication Details

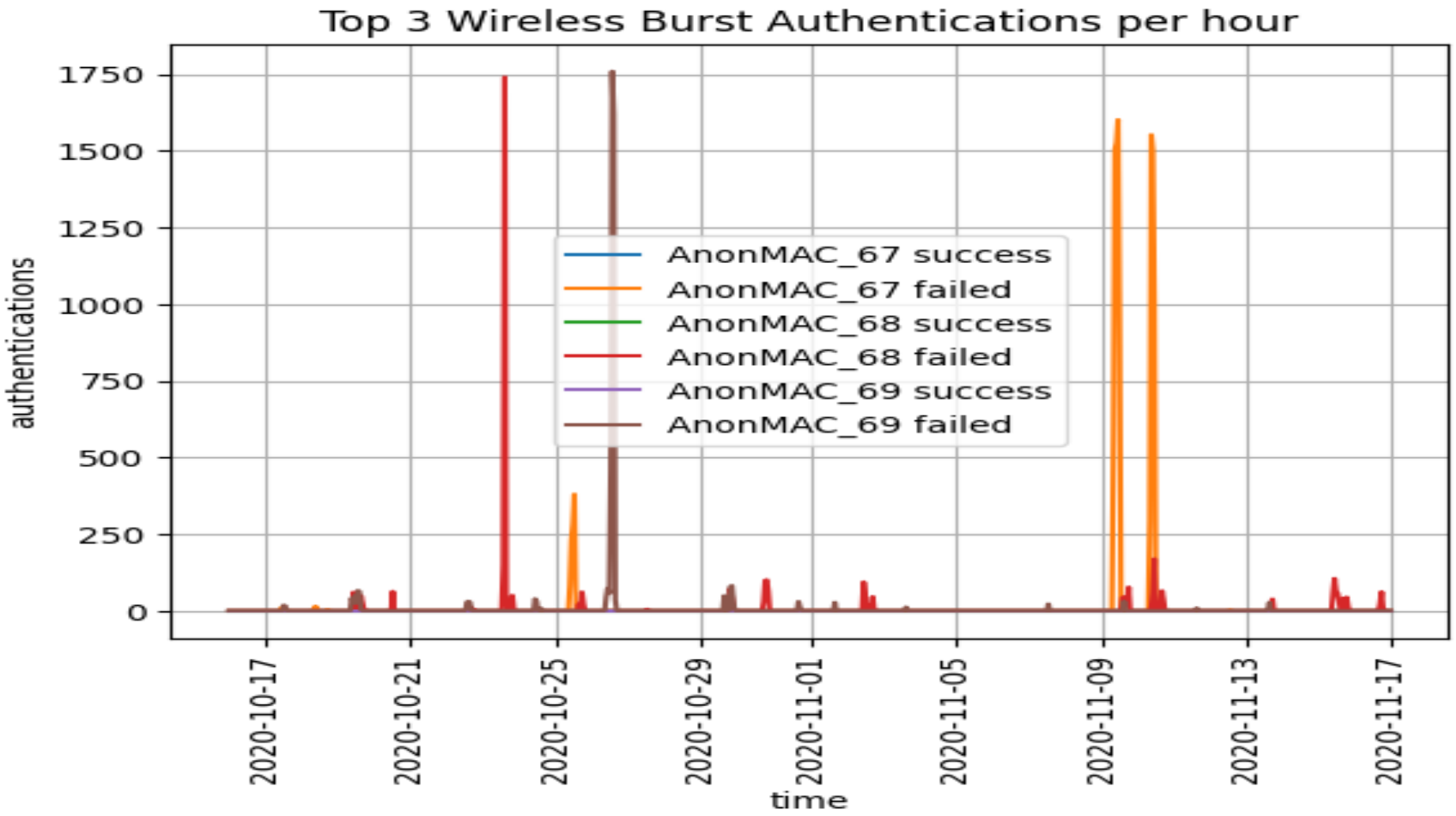
Auths	Error	Username	Service	NAS Name	NAS IP	SSID
89562	Success	AnonUser_7	Anonymous Service_17	AnonNAS_25	AnonNAS_25	
89176	Success	AnonUser_8	Anonymous Service_18	AnonNAS_26	AnonNAS_26	
180	User authentication failed	AnonUser_8	Anonymous Service_18	AnonNAS_26	AnonNAS_26	
20	No response from home s	AnonUser_8	Anonymous Service_18	AnonNAS_26	AnonNAS_26	
13	Request timed out	AnonUser_7	Anonymous Service_17	AnonNAS_25	AnonNAS_25	
6	Request timed out	AnonUser_8	Anonymous Service_18	AnonNAS_26	AnonNAS_26	
2	Internal error in RADIUS s	AnonUser_9	Anonymous Service_53	AnonNAS_25	AnonNAS_25	
1	Failed to classify request	AnonUser_9	Anonymous Service_53	AnonNAS_25	AnonNAS_25	

MAC 'AnonMAC_54' Authentication Details

Auths	Error	Username	Service	NAS Name	NAS IP	SSID
55830	User authentication failed	AnonUser_10	Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
3830	Request timed out		Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
656	Request timed out	AnonUser_10	Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
564	Success	AnonUser_10	Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
227	User not found		Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
45	Success	AnonUser_10	Anonymous Service_3	AnonNAS_3	AnonNAS_3	eduroam
5	Success		Anonymous Service_10	AnonNAS_3	AnonNAS_3	
2	TLS session error		Anonymous Service_3	AnonNAS_4	AnonNAS_4	eduroam
1	Internal error in RADIUS s	AnonUser_11	Anonymous Service_53	AnonNAS_4	AnonNAS_4	eduroam



These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top Virtual User Authentications

NOTE: Red threshold=8000 , Amber threshold=800

Auths	Success	Failed	Media	Username	Service	NAS Name	NAS IP
91538	0	91538	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_1	AnonNAS_1
91441	0	91441	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_24	AnonNAS_24
91402	0	91402	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_2	AnonNAS_2
91275	91275	0	VPN	AnonUser_13	Anonymous Service_16	AnonNAS_4	AnonNAS_4
43839	0	43839	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_27	AnonNAS_27
42918	0	42918	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_28	AnonNAS_28
19206	0	19206	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_29	AnonNAS_29
1855	0	1855	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_30	AnonNAS_30
1477	0	1477	VPN	AnonUser_12	Anonymous Service_7	AnonNAS_31	AnonNAS_31
1421	1421	0	VPN	AnonUser_14	Anonymous Service_10	AnonNAS_3	AnonNAS_3
1222	0	1222	VPN	AnonUser_15	Anonymous Service_7	AnonNAS_30	AnonNAS_30
960	0	960	VPN	AnonUser_15	Anonymous Service_7	AnonNAS_31	AnonNAS_31
903	0	903	VPN	AnonUser_12	Anonymous Service_33	AnonNAS_3	AnonNAS_3
749	749	0	VPN	AnonUser_16	Anonymous Service_10	AnonNAS_3	AnonNAS_3
696	696	0	VPN	AnonUser_17	Anonymous Service_10	AnonNAS_3	AnonNAS_3

These are users that are typically using VPN or login to a system. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

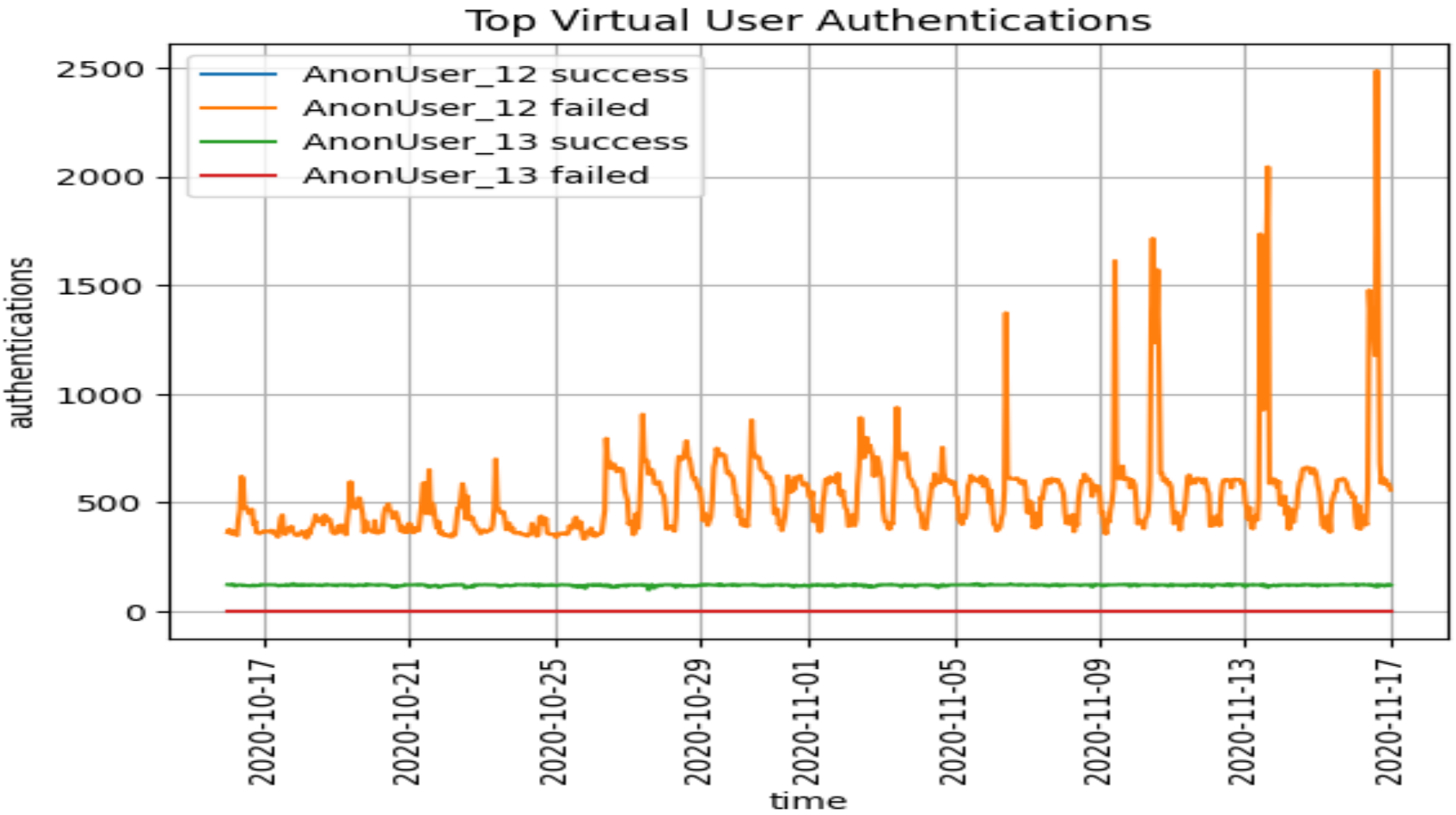
Username 'AnonUser_12' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
91538	User not found	Anonymous Service_7	AnonNAS_1	AnonNAS_1

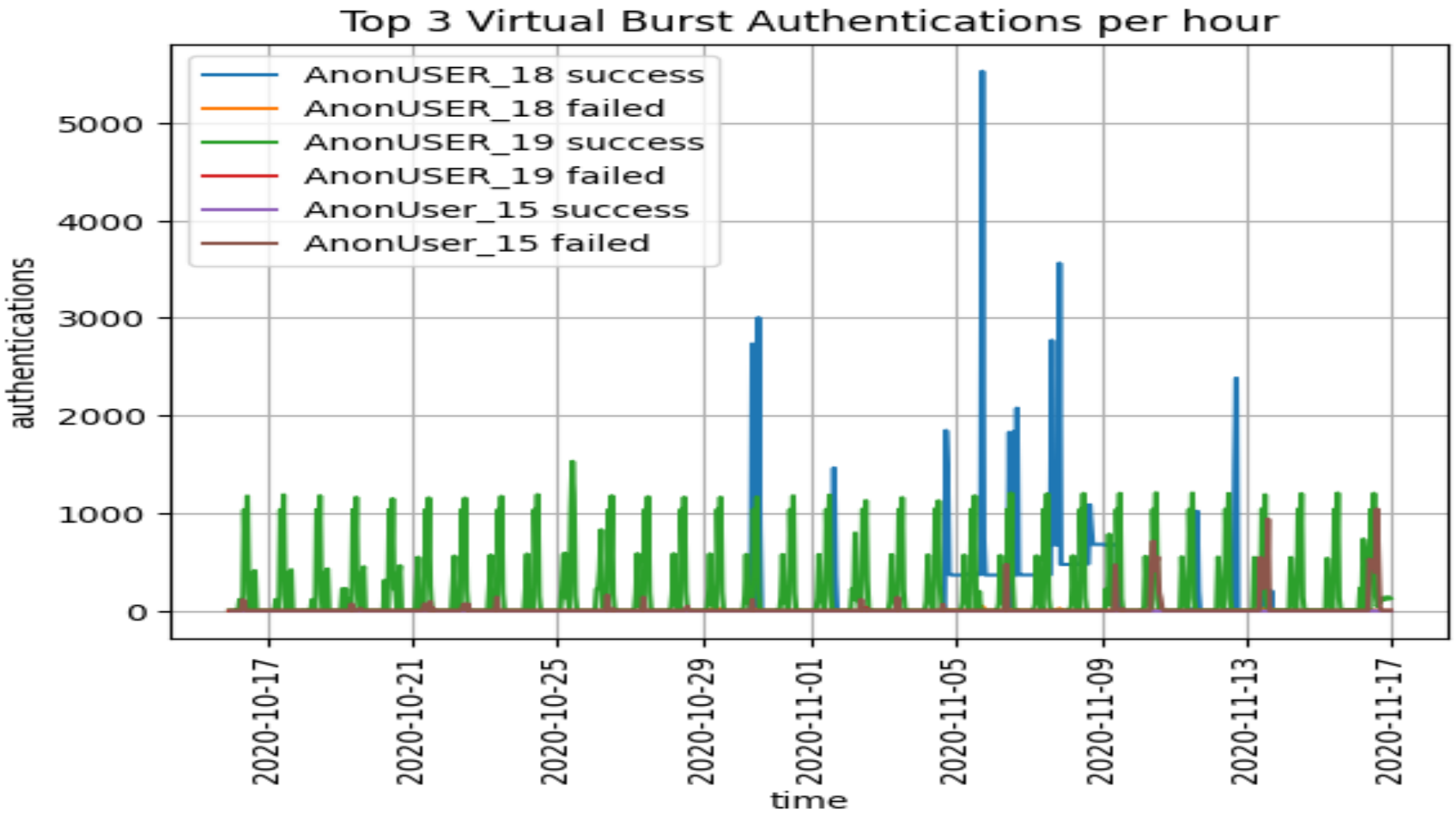
91441	User not found	Anonymous Service_7	AnonNAS_24	AnonNAS_24
91402	User not found	Anonymous Service_7	AnonNAS_2	AnonNAS_2
43839	User not found	Anonymous Service_7	AnonNAS_27	AnonNAS_27
42918	User not found	Anonymous Service_7	AnonNAS_28	AnonNAS_28
19206	User not found	Anonymous Service_7	AnonNAS_29	AnonNAS_29
1855	User not found	Anonymous Service_7	AnonNAS_30	AnonNAS_30
1477	User not found	Anonymous Service_7	AnonNAS_31	AnonNAS_31
1295	User not found	Anonymous Service_7	AnonNAS_32	AnonNAS_32
1015	User not found	Anonymous Service_7	AnonNAS_33	AnonNAS_33
903	No password in request	Anonymous Service_33	AnonNAS_3	AnonNAS_3
820	User not found	Anonymous Service_7	AnonNAS_34	AnonNAS_34
752	User not found	Anonymous Service_7	AnonNAS_35	AnonNAS_35
700	User not found	Anonymous Service_7	AnonNAS_36	AnonNAS_36
665	User not found	Anonymous Service_7	AnonNAS_37	AnonNAS_37

Username 'AnonUser_13' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
91275	Success	Anonymous Service_16	AnonNAS_4	AnonNAS_4



These are users that are typically using VPN or login to a system. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top 15 802.1X Users Authentications

NOTE: Red threshold=9600 , Amber threshold=960

Auths	Success	Failed	User
40355453	40292657	62796	AnonUser_6
92392	90504	1888	AnonUser_20
89564	89562	2	AnonUser_7
60253	3341	56912	AnonUser_10
45853	0	45853	AnonUser_21
45331	0	45331	AnonUser_22
43140	37879	5261	AnonUser_23
34640	33936	704	AnonUser_24
31482	9190	22292	AnonUser_25
31325	0	31325	AnonUser_26
27279	27050	229	AnonUser_27
26557	24264	2293	AnonUser_28
25755	4377	21378	AnonUser_29
24505	0	24505	AnonUser_30
23126	560	22566	AnonUser_31

This highlight specific 802.1X user authentications. Connection Threshold can be set, this will highlight users in red - these should be investigated. Amber are one tenth the red.

Username 'AnonUser_6' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
829977	Success	Anonymous Service_1	AnonNAS_38	AnonNAS_38

829883	Success	Anonymous Service_1	AnonNAS_39	AnonNAS_39
276735	Success	Anonymous Service_1	AnonNAS_40	AnonNAS_40
235680	Success	Anonymous Service_1	AnonNAS_20	AnonNAS_20
235617	Success	Anonymous Service_1	AnonNAS_21	AnonNAS_21
217571	Success	Anonymous Service_1	AnonNAS_41	AnonNAS_41
217556	Success	Anonymous Service_1	AnonNAS_42	AnonNAS_42
217547	Success	Anonymous Service_1	AnonNAS_43	AnonNAS_43
217544	Success	Anonymous Service_1	AnonNAS_44	AnonNAS_44
217543	Success	Anonymous Service_1	AnonNAS_45	AnonNAS_45
217541	Success	Anonymous Service_1	AnonNAS_46	AnonNAS_46
217537	Success	Anonymous Service_1	AnonNAS_47	AnonNAS_47
217536	Success	Anonymous Service_1	AnonNAS_48	AnonNAS_48
217536	Success	Anonymous Service_1	AnonNAS_49	AnonNAS_49
217534	Success	Anonymous Service_1	AnonNAS_50	AnonNAS_50

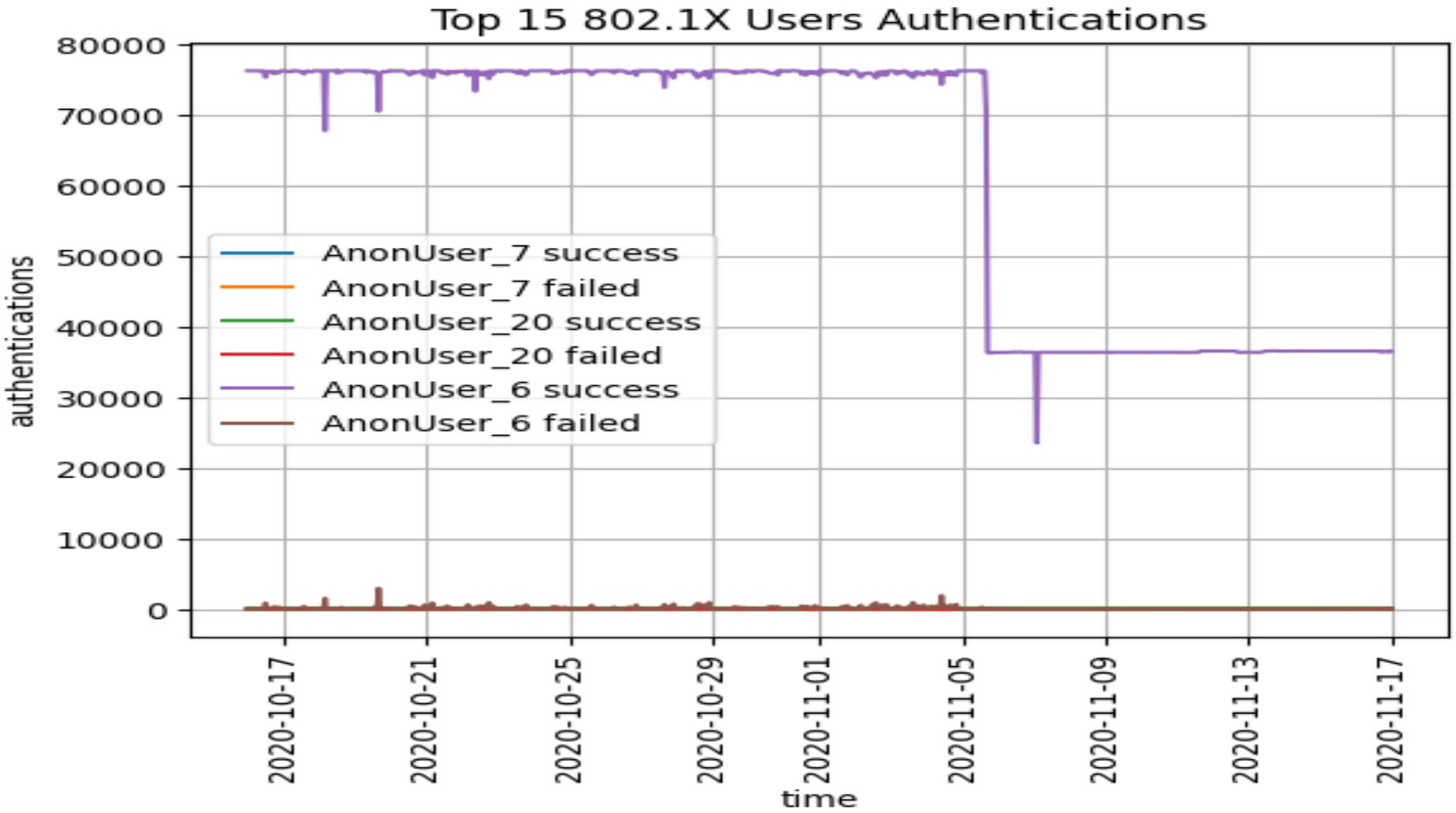
Username 'AnonUser_20' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
67514	Success	Anonymous Service_3	AnonNAS_4	AnonNAS_4
22990	Success	Anonymous Service_3	AnonNAS_2	AnonNAS_2
2305	Request timed out	Anonymous Service_3	AnonNAS_4	AnonNAS_4
124	Request timed out	Anonymous Service_3	AnonNAS_2	AnonNAS_2
1	TLS session error	Anonymous Service_3	AnonNAS_4	AnonNAS_4

Username 'AnonUser_7' Authentication Details

Auths	Error	Service	NAS Name	NAS IP

89562	Success	Anonymous Service_17	AnonNAS_25	AnonNAS_25
13	Request timed out	Anonymous Service_17	AnonNAS_25	AnonNAS_25



This highlight specific 802.1X user authentications. Connection Threshold can be set, this will highlight users in red - these should be investigated. Amber are one tenth the red.

Top 15 NAS with Most Authentications

NOTE: Red threshold=32000 , Amber threshold=3200

Media	Auths	Success	Failed	NAS Name	NAS IP
Wired	1620361	1620339	22	AnonNAS_51	AnonNAS_51
Wired	993895	993887	8	AnonNAS_52	AnonNAS_52
Wired	875566	875553	13	AnonNAS_53	AnonNAS_53
Wired	760789	760788	1	AnonNAS_10	AnonNAS_10
Wired	731014	730996	18	AnonNAS_54	AnonNAS_54
Wired	693416	693411	5	AnonNAS_55	AnonNAS_55
Wired	689561	689559	2	AnonNAS_45	AnonNAS_45
Wired	685208	685195	13	AnonNAS_56	AnonNAS_56
Wired	574273	574271	2	AnonNAS_13	AnonNAS_13
Wired	573629	573621	8	AnonNAS_18	AnonNAS_18
Wired	537938	537937	1	AnonNAS_57	AnonNAS_57
Wired	507478	507476	2	AnonNAS_58	AnonNAS_58
Wired	505841	505837	4	AnonNAS_59	AnonNAS_59
Wired	467869	467869	0	AnonNAS_60	AnonNAS_60
Wired	429276	429276	0	AnonNAS_61	AnonNAS_61

These highlights the NAS that are the source of most authentications. Typically, you would expect the wireless concentrators to be at the top. To appreciate these will likely require longer monitoring of the environment, though a NAS with excessive authentications will stand out - these should be investigated.

Top 10 NAS with Least Authentications

Media	Auths	Success	Failed	NAS Name	NAS IP

Wired	7	7	0	AnonNAS_62	AnonNAS_62
Wired	16	16	0	AnonNAS_63	AnonNAS_63
Wired	16	16	0	AnonNAS_64	AnonNAS_64
Wired	16	16	0	AnonNAS_65	AnonNAS_65
Wired	16	16	0	AnonNAS_66	AnonNAS_66
Wired	32	32	0	AnonNAS_67	AnonNAS_67
Wired	32	32	0	AnonNAS_68	AnonNAS_68
Wired	32	32	0	AnonNAS_69	AnonNAS_69
Wired	32	32	0	AnonNAS_70	AnonNAS_70
Wired	32	32	0	AnonNAS_71	AnonNAS_71

This might be useful to see if there is any equipment that can be decommissioned. WARNING: This does not report the NAS that have had no authentications! This can be got by interrogating the tipsdb directly.

Top 15 Failed Authorization

NOTE: Red threshold=1600 , Amber threshold=160

Authz	Username	MAC	Service	Method	NAS	NAS IP	Media	Port/SSID
1956	AnonUser_32	AnonMAC_70	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_4	AnonNAS_4	Wifi	eduroam
1764	AnonUser_33	AnonMAC_71	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_4	AnonNAS_4	Wifi	eduroam
1685	AnonUser_34	AnonMAC_72	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam
1354	AnonUser_35	AnonMAC_73	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_4	AnonNAS_4	Wifi	eduroam
1261	AnonUser_36	AnonMAC_74	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_4	AnonNAS_4	Wifi	eduroam
1206	AnonUser_37	AnonMAC_75	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam
1040	AnonUser_38	AnonMAC_76	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_4	AnonNAS_4	Wifi	eduroam
984	AnonUser_33	AnonMAC_77	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_1	AnonNAS_1	Wifi	eduroam
932	AnonUser_39	AnonMAC_78	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam
803	AnonUser_40	AnonMAC_79	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam
586	AnonUser_41	AnonMAC_80	Anonymous Service_3	EAP	AnonNAS_2	AnonNAS_2	Wifi	eduroam
558	AnonUser_42	AnonMAC_81	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_1	AnonNAS_1	Wifi	eduroam
537	AnonUser_43	AnonMAC_82	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_24	AnonNAS_24	Wifi	eduroam
475	AnonUser_44	AnonMAC_83	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam
473	AnonUser_45	AnonMAC_84	Anonymous Service_1	EAP-PEAP(EAP·	AnonNAS_2	AnonNAS_2	Wifi	eduroam

These are authentication requests that were successful but the authorization failed the request. Excessive failures should be investigated to understand what is wrong.

Top 10 802.1X Users with Multiple Devices

NOTE: Red threshold=480 , Amber threshold=48

Devices	Username
1924	AnonUser_46
191	AnonUser_6
87	AnonUser_47
59	AnonUser_48
48	AnonUser_49
36	AnonUser_50
31	AnonUser_51
28	AnonUser_52
27	AnonUser_53
22	AnonUser_54

These highlights users that are authenticating from multiple devices. It then identifies the top 3 users and their associated devices.

Top 10 802.1X Devices with Multiple Users

NOTE: Red threshold=480 , Amber threshold=48

Users	MAC
12	AnonMAC_85
8	AnonMAC_86
8	AnonMAC_87
7	AnonMAC_88
7	AnonMAC_89
7	AnonMAC_90
6	AnonMAC_91
6	AnonMAC_92
6	AnonMAC_93
6	AnonMAC_94

These highlights shared devices.

Top 10 Wired Devices that have Moved

NOTE: Red threshold=128 , Amber threshold=12

Moves	MAC
15	AnonMAC_95
11	AnonMAC_96
11	AnonMAC_97
11	AnonMAC_98
10	AnonMAC_99
10	AnonMAC_100
10	AnonMAC_101
9	AnonMAC_102
9	AnonMAC_103
9	AnonMAC_104

These highlights wired devices that have physically been moved to different wired ports. It then identifies the top 3 devices and where they moved.

Top 10 Wireless Devices with Multiple SSID

NOTE: Red threshold=128 , Amber threshold=12

SSID moves	MAC
2	AnonMAC_105
2	AnonMAC_106
2	AnonMAC_107
2	AnonMAC_108
2	AnonMAC_109
2	AnonMAC_110
2	AnonMAC_111
2	AnonMAC_112
2	AnonMAC_113
2	AnonMAC_114

These highlights devices that are moving between different SSIDs.

Top 15 TACACS Authentications

NOTE: Red threshold=3200 , Amber threshold=320

Username	Source	Destination	Auths	Success	Failed
AnonUser_12	XXXXX	YYYYY	215	0	215
AnonUser_55	XXXXX	YYYYY	48	0	48
AnonUser_56	XXXXX	YYYYY	39	0	39
AnonUser_57	XXXXX	YYYYY	38	36	2
AnonUser_58	XXXXX	YYYYY	34	34	0
AnonUser_15	XXXXX	YYYYY	32	0	32
AnonUser_59	XXXXX	YYYYY	32	32	0
AnonUser_60	XXXXX	YYYYY	30	0	30
AnonUser_61	XXXXX	YYYYY	24	0	24
AnonUser_62	XXXXX	YYYYY	24	0	24
AnonUser_63	XXXXX	YYYYY	24	0	24
AnonUSER_18	XXXXX	YYYYY	21	18	3
AnonUser_64	XXXXX	YYYYY	20	20	0
AnonUser_65	XXXXX	YYYYY	19	7	12
AnonUser_66	XXXXX	YYYYY	18	0	18

These highlights users generating excessive TACACS authentications. These might be legitimate. WHITELIST? Connection Threshold can be set, this will highlight user in red - these should be investigated. Of these the ones in red will be drilled into more detail.

Top 15 Device Session Duration

NOTE: Red duration=100 days, Amber duration=10 days

MAC	Username	Days	In_GBytes	Out_GBytes	Total_GBytes	Device Type
AnonMAC_115		**5734**	0.000	0.000	0.000	*Not Known*
AnonMAC_116		**5730**	0.000	0.000	0.000	*Not Known*
AnonMAC_117		**2892**	0.000	0.000	0.000	*Not Known*
AnonMAC_118		**2889**	0.000	0.000	0.000	Access Points
AnonMAC_119		**2877**	0.000	0.000	0.000	VoIP Phone
AnonMAC_120		**2877**	0.000	0.000	0.000	Generic
AnonMAC_121		**2876**	0.000	0.000	0.000	VoIP Phone
AnonMAC_122		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_123		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_124		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_125		**2875**	0.000	0.000	0.000	Home Audio/Video Equipment
AnonMAC_126		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_127		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_128		**2875**	0.000	0.000	0.000	VoIP Phone
AnonMAC_129		**2875**	0.000	0.000	0.000	VoIP Phone

This reports the sessions with the longest duration. This information is supplied by the NAS within the RADIUS Accounting - sometime this my report preposterous information - this is an error of the NAS. Questions is are these top session durations reasonable?

Top 15 Device Session Total Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	Username	Days	In_GBytes	Out_GBytes	Total_GBytes	Device Category
AnonMAC_130		0	8678	121	**8799**	*Not Known*
AnonMAC_131		0	7711	196	**7906**	*Not Known*
AnonMAC_132		0	7378	182	**7561**	*Not Known*
AnonMAC_133		0	6445	163	**6608**	*Not Known*
AnonMAC_134		0	360	6230	**6590**	Computer
AnonMAC_135		0	6317	160	**6477**	*Not Known*
AnonMAC_136		0	6198	159	**6357**	*Not Known*
AnonMAC_137		0	5579	146	**5725**	*Not Known*
AnonMAC_138		0	5567	146	**5714**	*Not Known*
AnonMAC_139		0	5476	144	**5620**	*Not Known*
AnonMAC_140		0	5328	23	**5350**	*Not Known*
AnonMAC_141		0	4584	134	**4718**	*Not Known*
AnonMAC_142		0	3896	111	**4008**	*Not Known*
AnonMAC_143		0	3165	78	**3243**	*Not Known*
AnonMAC_144		0	150	2519	**2669**	*Not Known*

This reports the combination the device's ingress and egress traffic averaged over a per day basis.

Top 15 Device Session Transmit Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	Username	Days	In_GBytes	Out_GBytes	Total_GBytes	Device Category
AnonMAC_134	AnonUser_67	0	360	**6230**	6590	Computer
AnonMAC_144	AnonUser_67	0	150	**2519**	2669	*Not Known*
AnonMAC_145		0	63	**2270**	2334	Computer
AnonMAC_146		0	93	**799**	893	Home Audio/Video Equipment
AnonMAC_147		0	265	**754**	1019	Computer
AnonMAC_148		0	33	**749**	782	Computer
AnonMAC_149		0	98	**724**	822	Access Points
AnonMAC_150		2	215	**707**	922	Access Points
AnonMAC_151		1	98	**607**	705	Access Points
AnonMAC_152		1	70	**578**	648	Access Points
AnonMAC_153		0	63	**559**	622	Access Points
AnonMAC_154		1	34	**557**	591	Access Points
AnonMAC_155		0	13	**446**	459	Access Points
AnonMAC_156		2	51	**434**	485	Access Points
AnonMAC_157		0	1	**381**	382	Network Boot Agents

This reports the combination the device's egress traffic averaged over a per day basis.

Top 15 Device Session Receive Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	Username	Days	In_GBytes	Out_GBytes	Total_GBytes	Device Category
AnonMAC_130		0	**8678**	121	8799	*Not Known*
AnonMAC_131		0	**7711**	196	7906	*Not Known*
AnonMAC_132		0	**7378**	182	7561	*Not Known*
AnonMAC_133		0	**6445**	163	6608	*Not Known*
AnonMAC_135		0	**6317**	160	6477	*Not Known*
AnonMAC_136		0	**6198**	159	6357	*Not Known*
AnonMAC_137		0	**5579**	146	5725	*Not Known*
AnonMAC_138		0	**5567**	146	5714	*Not Known*
AnonMAC_139		0	**5476**	144	5620	*Not Known*
AnonMAC_140		0	**5328**	23	5350	*Not Known*
AnonMAC_141		0	**4584**	134	4718	*Not Known*
AnonMAC_142		0	**3896**	111	4008	*Not Known*
AnonMAC_143		0	**3165**	78	3243	*Not Known*
AnonMAC_158		0	**2226**	89	2315	Computer
AnonMAC_159		0	**2052**	85	2137	*Not Known*

This reports the combination the device's ingress traffic averaged over a per day basis.

ClearPass Audit

This reports the last 15 changes.

Time	User	Category	Action	Change
2020-10-16 07:49:57+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY Wireless Groupcycle MacAuth - 130916
2020-10-16 07:50:46+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY Wireless Groupcycle MacAuth - 161020
2020-10-16 07:51:39+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY IoT MacAuth - 191119
2020-10-16 07:52:18+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY IoT MacAuth - 161020
2020-10-16 07:55:13+01:00	AnonUser_64	Enforcement Policy	MODIFY	UoY Generic MacAuth Enforcement 161020
2020-10-16 07:56:23+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY Aruba AP Bridge Port MacAuth - 161020
2020-10-16 07:57:59+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY ArubaAP Wired Port Macauth - 161020
2020-10-16 07:59:45+01:00	AnonUser_64	Enforcement Policy	MODIFY	UoY IoT device enforcement 161020
2020-10-16 07:59:52+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY IoT MacAuth - 161020
2020-10-16 08:02:56+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY wireless machine auth - 030719
2020-10-16 08:03:33+01:00	AnonUser_64	Radius Enforcement Service	MODIFY	UoY wireless machine auth - 161020
2020-10-16 08:05:22+01:00	AnonUser_64	Role Mapping Policy	MODIFY	UoY VOIP Phones - 161020
2020-10-16 08:05:41+01:00	AnonUser_64	Authentication Source	REMOVE	UoY Endpoints Repository
2020-10-16 12:09:11+01:00	AnonUser_68	Guest User	ADD	AnonMAC_160
2020-10-16 12:28:32+01:00	AnonUser_69	Guest User	ADD	AnonMAC_161

OnGuard Summary

Total	Unknown	Infected	Healthy	Checkup	Quarantine	Transition	No Status
10906	4632	0	0	0	0	0	0

Reports the current state of all the OnGuard clients.

10 Most Recent OnGuard Posture Failures

Date	MAC	IP	Hostname	Username	OS

This reports the PCs that have most recently failed their posture compliance. The highlighted section shows what the failed component has - not what it failed against!