

Wenn selbst ‘erlaube allen Verkehr von 0.0.0.0/0’ nicht hilft - Verbindungsprobleme in AWS lösen

Steffen Gebert (@StGebert)

Wolfgang Schäfer (@wo_wue)

AWS Community Day DACH in Dresden

19.10.2022

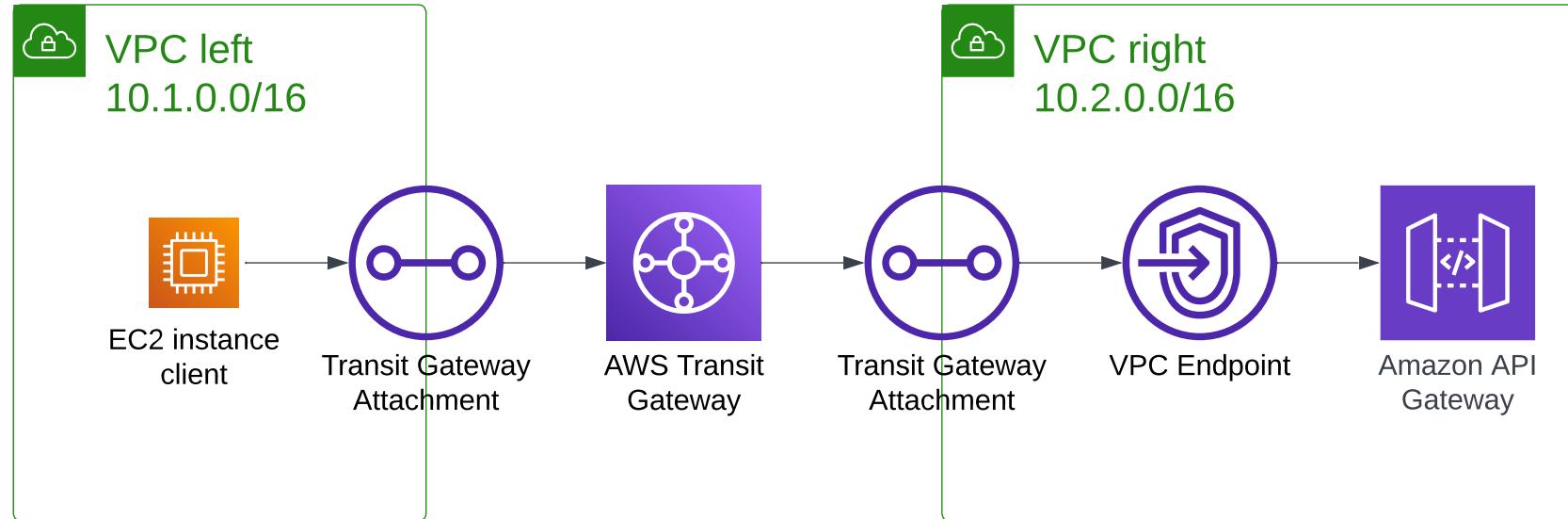
UNSERE SPONSOREN



T-Systems



This is Our Architecture



Problem

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with options like VPC dashboard, EC2 Global View, Filter by VPC, and a list of VPC components including Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP Option Sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main area is titled "Your VPCs (1/3)" and shows a table with three rows:

Name	VPC ID	State	IPv4 CIDR
left	vpc-0416ed0d3514d6fae	Available	10.1.0.0/16
right	vpc-0f0effa85597afdae	Available	10.2.0.0/16
-	vpc-9e06abe7	Available	172.31.0.0/16

Below the table, a specific VPC is selected: "vpc-0416ed0d3514d6fae / left". The "Details" tab is active, showing the following configuration details:

VPC ID	State	DNS hostnames	DNS resolution
vpc-0416ed0d3514d6fae	Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-c7120da1	rtb-0da33094cbf4a0912	acl-0dcba0dc504e39c401
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR

At the bottom, there are links for Feedback, Unified Settings, and various legal notices.

Problem

The screenshot shows the AWS EC2 Instances page with one instance listed:

Name	Instance ID	Instance state	Launch time
client	i-0ef7df29a90a00000	Running	2022/10/17 10:22 GMT+2

A context menu is open over the 'client' instance, with 'Connect' highlighted.

Details | **Security**

Instance summary

- Instance ID: i-0ef7df29a90a00000
- IPv6 address: -
- Hostname type: IP name: ip-10-1-0-105.ec2.internal
- IP name: ip-10-1-0-105.ec2.internal
- Monitor and troubleshoot
- Answer private resource DNS name: -
- Instance type: t4g.micro

Networking

- Public IPv4 address: 10.1.0.105
- Private IPv4 addresses: 10.1.0.105
- Public IPv4 DNS: -

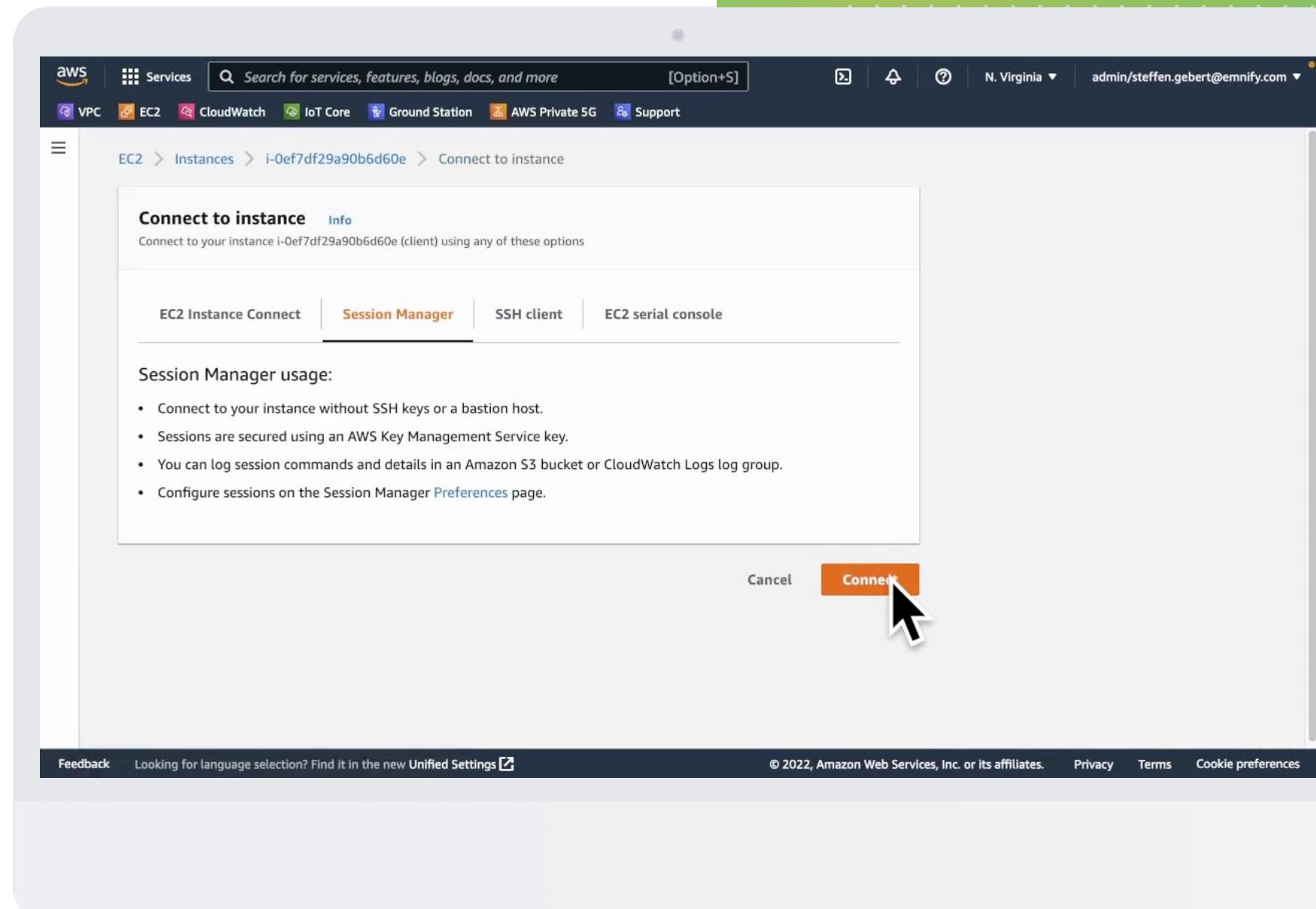
Security

- Instance settings
- State: Running
- Image and templates
- Create IP DNS name (IPv4 only): ip-10-1-0-105.ec2.internal
- Monitor and troubleshoot

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Problem



Problem

Session ID: Instance ID: i-
Terminate

```
$ curl --connect-timeout 5 pcbicvz9x6-vpce-05e857f78d9d1b62f.execute-api.us-east-1.amazonaws.com
curl: (28) Connection timed out after 5000 milliseconds
$ 
```



Problem

The screenshot shows the AWS EC2 Instances page. The left sidebar has a 'New EC2 Experience' toggle and lists categories like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with sub-options for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), and Images (AMIs). The main content area shows 'Instances (1/1)' with a single entry: 'client' (Instance ID: i-0ef7df29a90b6d60e), which is 'Running' and was launched on 2022/10/17 10:22 GMT+2. A large mouse cursor is positioned over the instance row. The 'Networking' tab is selected in the instance details panel, which displays network information including Public IPv4 address (empty), Private IPv4 addresses (10.1.0.105), Private IP DNS name (ip-10-1-0-105.ec2.internal), Subnet ID (subnet-05e7ad652202c76c5), IPV6 addresses (empty), and VPC ID (vpc-047f9166a49868d20). A message indicates that network connectivity can be checked using the Reachability Analyzer.

Instances (1/1) [Info](#)

Find instance by attribute or tag (case-sensitive)

Instance state = running

Clear filters

Name Instance ID Instance state Launch time

client i-0ef7df29a90b6d60e Running 2022/10/17 10:22 GMT+2

Instance: i-0ef7df29a90b6d60e (client)

Details Security Networking Storage Status checks Monitoring Tags

You can now check network connectivity with Reachability Analyzer. [Run Reachability Analyzer](#)

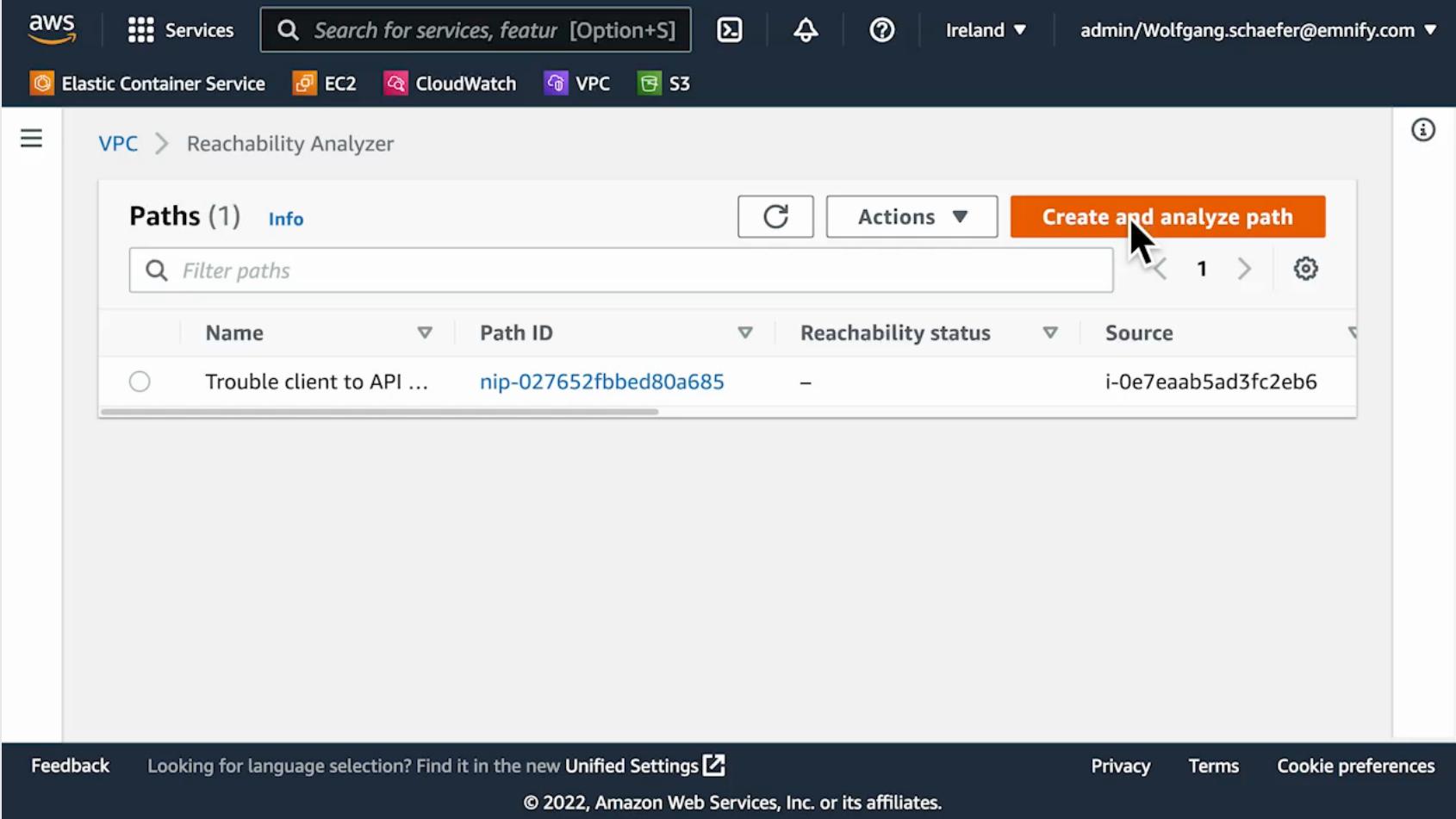
Networking details

Public IPv4 address	Private IPv4 addresses	VPC ID
-	10.1.0.105	vpc-047f9166a49868d20 (left)
Public IPv4 DNS	Private IP DNS name (IPv4 only)	
-	ip-10-1-0-105.ec2.internal	
Subnet ID	IPV6 addresses	Secondary private IPv4 addresses
subnet-05e7ad652202c76c5 (left)	-	-

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

VPC Reachability Analyzer



The screenshot shows the AWS VPC Reachability Analyzer interface. At the top, the AWS logo and services menu are visible, along with a search bar containing "Search for services, feature [Option+S]". The navigation bar includes links for Elastic Container Service, EC2, CloudWatch, VPC, and S3. The current view is under the VPC section, specifically the Reachability Analyzer. A table titled "Paths (1)" displays one entry:

Name	Path ID	Reachability status	Source
Trouble client to API ...	nip-027652fbbed80a685	-	i-0e7eaab5ad3fc2eb6

Below the table, there are buttons for "Actions" and "Create and analyze path". A "Filter paths" search bar is also present. At the bottom of the page, there are links for Feedback, Unified Settings, Privacy, Terms, and Cookie preferences, along with a copyright notice: "© 2022, Amazon Web Services, Inc. or its affiliates."

VPC Reachability Analyzer

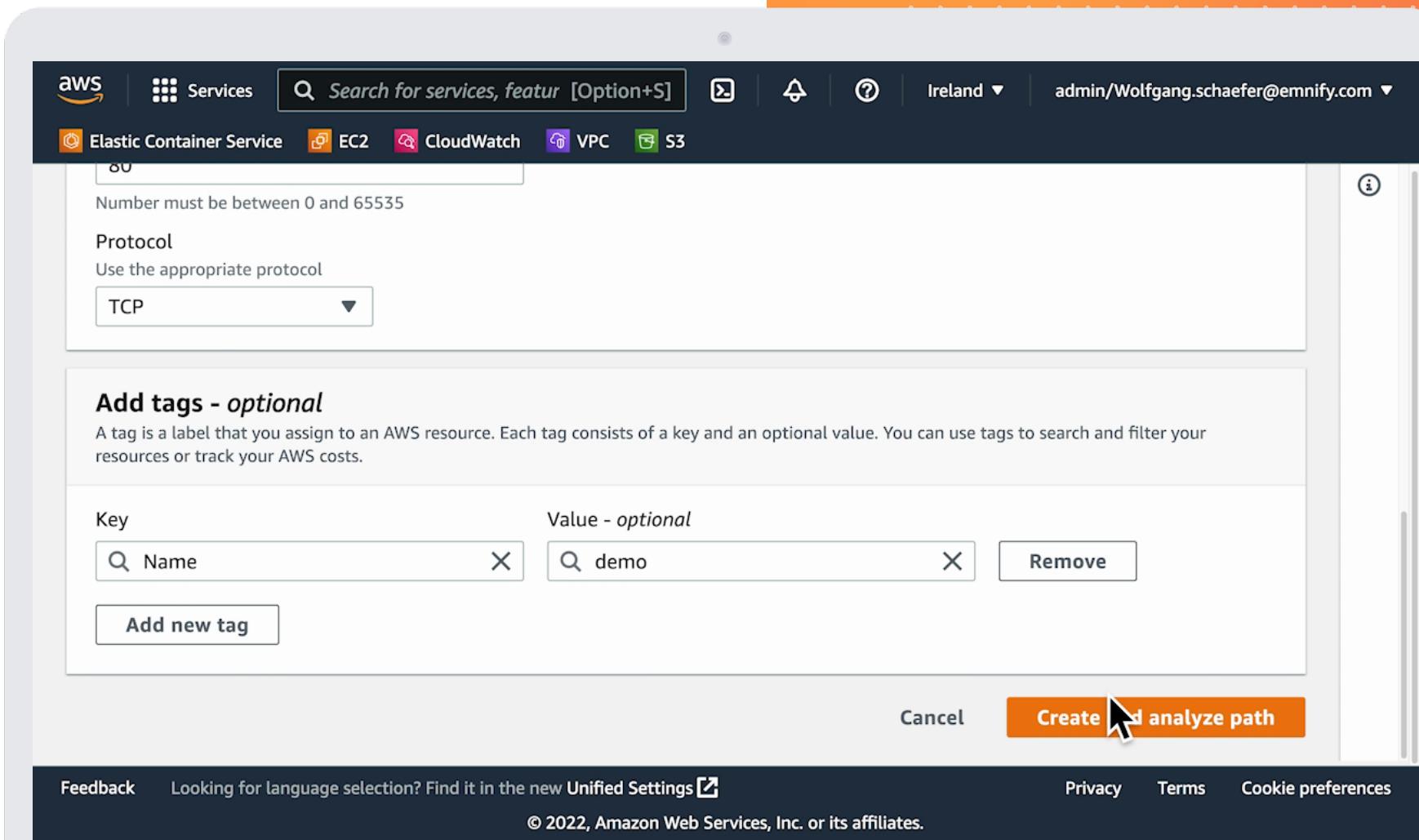
The screenshot shows the AWS VPC Reachability Analyzer interface. The top navigation bar includes the AWS logo, a services search bar, and account information for Ireland and admin/Wolfgang.schaefer@emnify.com. Below the navigation is a toolbar with icons for Elastic Container Service, EC2, CloudWatch, VPC, and S3.

The main form is used to configure a connection:

- Source type:** Instances (selected)
- Source:** i-0e7eaab5ad3fc2eb6
- Source IP address - optional:** 192.0.2.1
- Destination type:** VPC Endpoints (selected)
- Destination:** vpce-032a75ff4fbb16bb9
- Destination port - optional:** 80
- Protocol:** TCP (selected)

At the bottom of the interface, there are links for Feedback, Unified Settings, Privacy, Terms, and Cookie preferences, along with a copyright notice for © 2022, Amazon Web Services, Inc. or its affiliates.

VPC Reachability Analyzer



VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. At the top, the AWS logo and services menu are visible, along with a search bar and navigation icons. The user is signed in as admin/Wolfgang.schaefer@emnify.com. Below the header, the VPC service is selected. The main area displays an 'Analyses' section with one entry:

Analysis ID	Analysis run date	Reachability status	Intermediate compo.
nia-039c750128652aa8c	October 14, 2022, 16:4...	Pending	-

Below the table, an 'Analysis explorer' section provides detailed information about the analysis:

Source	Destination	Reachability status	Analysis run date
i-0e7eaab5ad3fc2eb6	vpce-032a75ff4fbb16bb9	Pending	October 14, 2022, 16:44 (UTC+02:00)

At the bottom of the interface, there are links for Feedback, Unified Settings, Privacy, Terms, and Cookie preferences, along with a copyright notice for 2022, Amazon Web Services, Inc. or its affiliates.

VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. At the top, there's a navigation bar with the AWS logo, a 'Services' button, a search bar containing 'Search for services, feature [Option+S]', and various icons for different AWS services like Elastic Container Service, EC2, CloudWatch, VPC, and S3. The 'VPC' icon is highlighted. On the far right, it shows 'Ireland' and the user 'admin/Wolfgang.schaefer@emnify.com'. Below the navigation bar, the main content area has a title 'Analyses (1/1)' with a 'Info' link. There's a search bar labeled 'Filter path analyses'. A table lists one analysis entry:

Analysis ID	Analysis run date	Reachability status	Intermediate compo.
nia-039c750128652aa8c	October 14, 2022, 16:4...	✖ Not reachable	-

Below the table is a section titled 'Analysis explorer' with an 'Info' link. It displays the following details:

Source	Destination	Reachability status	Analysis run date
i-0e7eaab5ad3fc2eb6	vpce-032a75ff4fbb16bb9	✖ Not reachable	October 14, 2022, 16:44 (UTC+02:00)

At the bottom of the interface, there are links for 'Feedback', 'Unified Settings' (with a note about language selection), 'Privacy', 'Terms', and 'Cookie preferences'.

VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing 'Search for services, feature [Option+S]', and account information for 'Ireland' and 'admin/Wolfgang.schaefer@emnify.com'. Below the navigation bar, there are links for Elastic Container Service, EC2, CloudWatch, VPC, and S3.

A prominent red error message box states: 'Destination is not reachable. For more information, see the explanations below.' It includes a 'Give us feedback' button and a small info icon.

The main content area is titled 'Explanations' and lists two items:

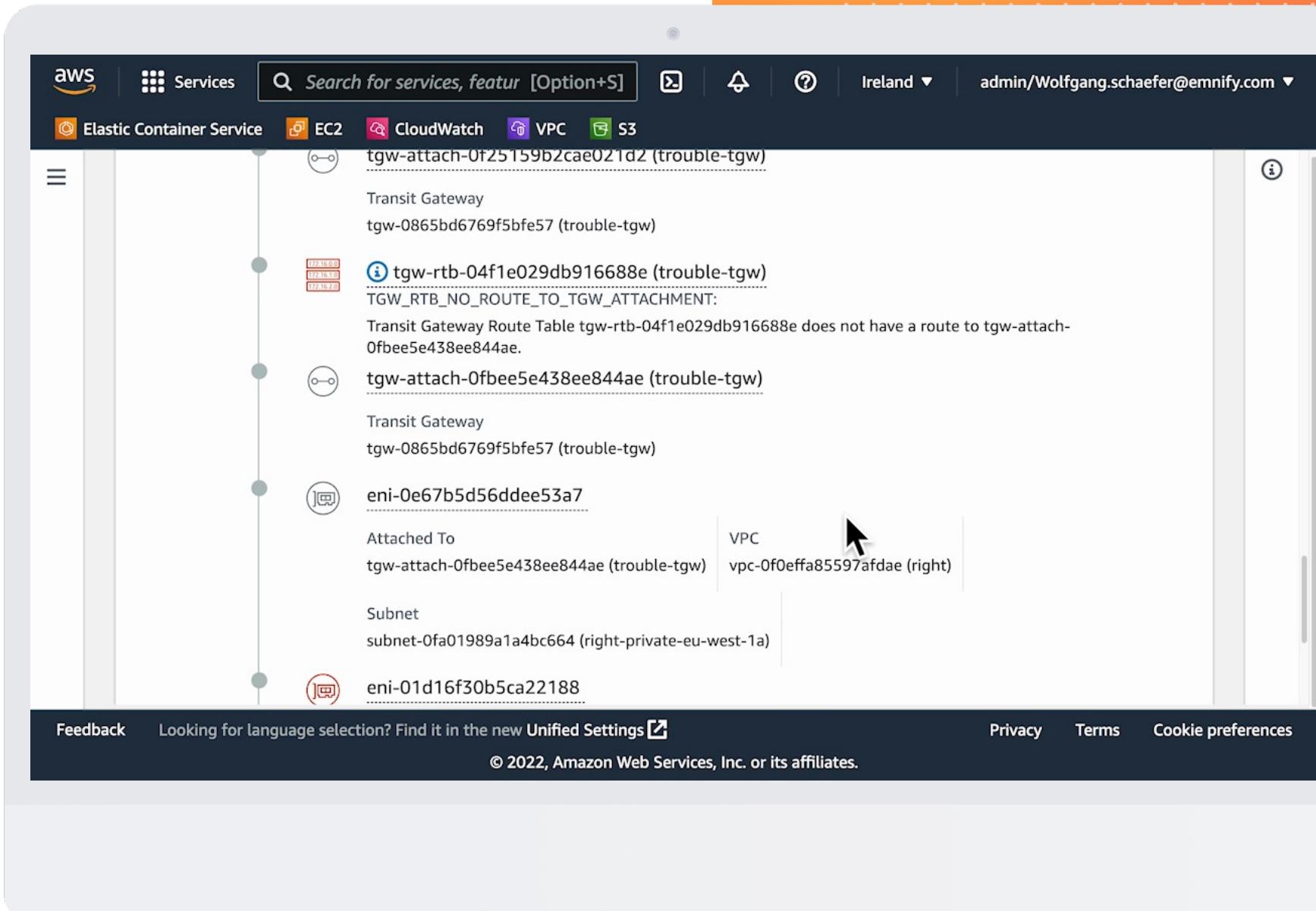
- Transit Gateway Route Table tgw-rtb-04f1e029db916688e does not have a route to tgw-attach-0fbee5e438ee844ae.
 - ▶ Details
- None of the ingress rules in the following security groups apply: sg-020df18175b1ccee1. See [sg-020df18175b1ccee1](#).
 - ▶ Details

Below the explanations is a section titled 'Path details' with a 'View reverse path' toggle switch (which is off) and a 'Learn more' link. A cursor arrow points towards the 'Learn more' link.

The path diagram shows the flow from a 'Source' (represented by a grey dot) through an 'Outbound header' (represented by a network card icon) to a 'client' (represented by a grey dot) with the identifier 'i-0e7eaab5ad3fc2eb6'. The path also connects to an 'eni-0b8405b109aa710fe' interface.

At the bottom of the interface, there are links for 'Feedback', 'Unified Settings' (with a note about language selection), 'Privacy', 'Terms', and 'Cookie preferences'.

VPC Reachability Analyzer



VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. At the top, there's a navigation bar with the AWS logo, a 'Services' button, a search bar containing 'Search for services, feature [Option+S]', and various icons for different AWS services like Elastic Container Service, EC2, CloudWatch, VPC, and S3. The 'VPC' icon is highlighted.

The main area displays a network diagram with nodes connected by lines. The nodes are represented by icons: a grey circle for 'Destination', two red circles with a white interface symbol for 'eni-0e67b5d56ddee53a7' and 'eni-01d16f30b5ca22188', and a blue square with a white interface symbol for 'tgw-0865bd6769f5bfe57'. A tooltip for 'eni-0e67b5d56ddee53a7' shows it's attached to a Transit Gateway and a specific subnet. Another tooltip for 'eni-01d16f30b5ca22188' shows it's attached to a VPCE endpoint and a specific subnet. A tooltip for the 'Destination' node indicates an 'ENI_SG_RULES_MISMATCH' error, stating that no ingress rules apply to the security group sg-020df18175b1ccee1.

At the bottom of the interface, there are links for 'Feedback', 'Looking for language selection? Find it in the new Unified Settings', 'Privacy', 'Terms', and 'Cookie preferences'.

Fixing Connectivity

The screenshot shows the AWS Management Console interface for managing security groups. The top navigation bar includes the AWS logo, a 'Services' dropdown, a search bar, and user information for 'admin/Wolfgang.schaefer@emnify.com'. Below the search bar are links for Elastic Container Service, EC2, CloudWatch, VPC, and S3.

The main content area shows the path: VPC > Security Groups > sg-020df18175b1ccee1 - api-gateway > Edit inbound rules: Preview actions. The title of the page is 'Edit inbound rules: Preview actions'.

A sub-header states: 'Preview the actions we will take when modifying your inbound rules'.

The central part of the screen displays a table titled 'Inbound rules (2)'. The table has columns: Action, Security group rule ID, IP version, Type, Protocol, Port range, Source, and Description - optional. Two rows are listed:

Action	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description - optional
<button>Update</button>	sgr-0dcf40a80f3d2ff3e	IPv4	HTTPS	TCP	443	10.1.0.0/16	-
<button>Update</button>	sgr-0ac6d20e44615d697	IPv4	HTTP	TCP	80	10.1.0.0/16	-

At the bottom right of the preview window, there are 'Back' and 'Confirm' buttons. A cursor arrow points to the 'Confirm' button.

At the very bottom of the page, there are links for Feedback, Unified Settings, Copyright notice (© 2022, Amazon Web Services, Inc. or its affiliates.), Privacy, Terms, and Cookie preferences.

VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. On the left, a sidebar lists various network components: Egress-only Internet gateways, DHCP Option Sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. Below these are sections for Security (Network ACLs, Security groups), Network Analysis (Reachability Analyzer, Network Access Analyzer), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls). The main content area displays a summary of a path analysis. The summary table includes:

Path ID	Last analysis date	Reachability status	Last analysis status
nip-02b2830e744593ca7	October 14, 2022, 16:44 (UTC+02:00)	☒ Not reachable	☑ Succeeded

Below the summary is a table for 'Analyses (1/1)'. It shows one entry:

Analysis ID	Analysis run date	Reachability status	Intermediate compo...	State
nia-039c750128652aa8c	October 14, 2022, 16:4...	☒ Not reachable	-	☑ Success

At the bottom of the main content area, there is an 'Analysis explorer' section which is currently empty.

At the very bottom of the page, there are links for Feedback, Unified Settings, Copyright notice (© 2022, Amazon Web Services, Inc. or its affiliates.), Privacy, Terms, and Cookie preferences.

VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer interface. On the left, a sidebar lists various network components: Egress-only Internet gateways, DHCP Option Sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. Below these are sections for Security (Network ACLs, Security groups), Network Analysis (Reachability Analyzer, Network Access Analyzer), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls). The main content area displays analysis results for a specific connection:

Source	Destination	Destination port	Protocol
i-0e7aab5ad3fc2eb6	vpce-032a75ff4fb16bb9	80	TCP

Below this, there are two tabs: "Analyses" (selected) and "Tags". The "Analyses" tab shows a list of 1/2 analyses:

Analysis ID	Analysis run date	Reachability status	Intermediate compo...	State
nia-014ee5113dd80d3d3	October 14, 2022, 16:5...	Reachable	-	Success
nia-039c750128652aa8c	October 14, 2022, 16:4...	Not reachable	-	Success

The "Analysis explorer" section provides detailed information for the first analysis:

Source	Destination	Reachability status	Analysis run date
i-0e7aab5ad3fc2eb6	vpce-032a75ff4fb16bb9	Reachable	October 14, 2022, 16:54 (UTC+02:00)

At the bottom, there are links for Feedback, Unified Settings, and various AWS terms like Privacy, Terms, and Cookie preferences.

Connectivity Test

Session ID: Instance ID: i-
Terminate

```
$ curl --connect-timeout 5 pcbicvz9x6-vpce-05e857f78d9d1b62f.execute-api.us-east-1.amazonaws.com
curl: (28) Connection timed out after 5000 milliseconds
$
```

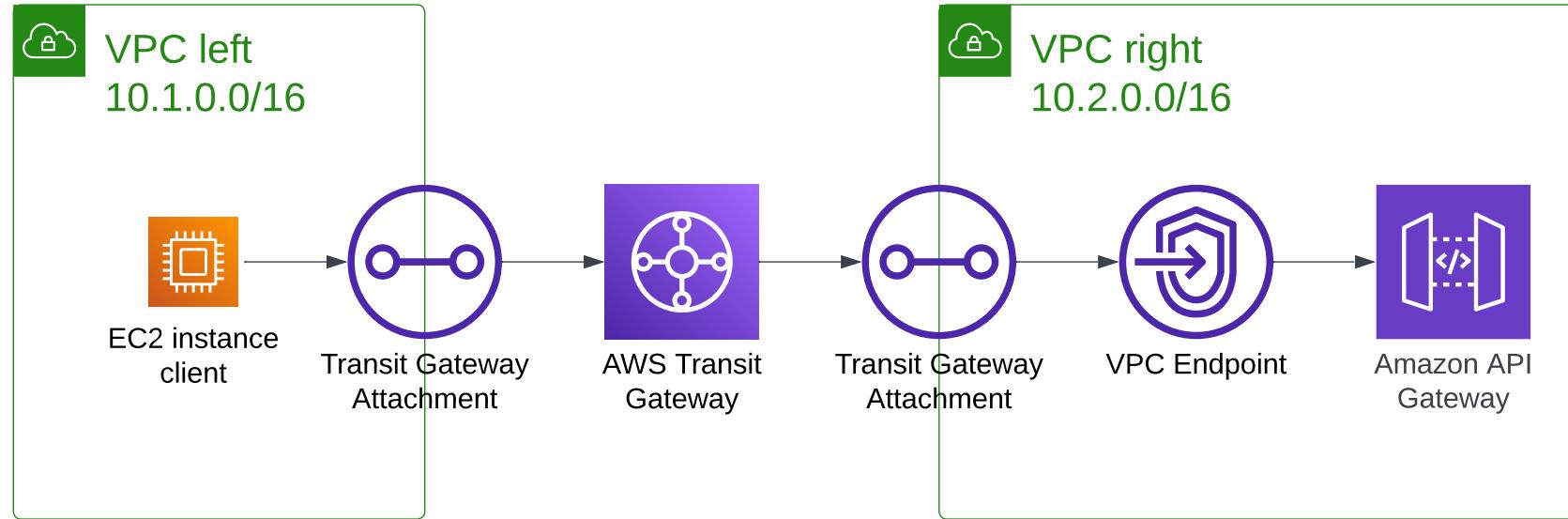


EMnify

Metrics



This is Our Architecture



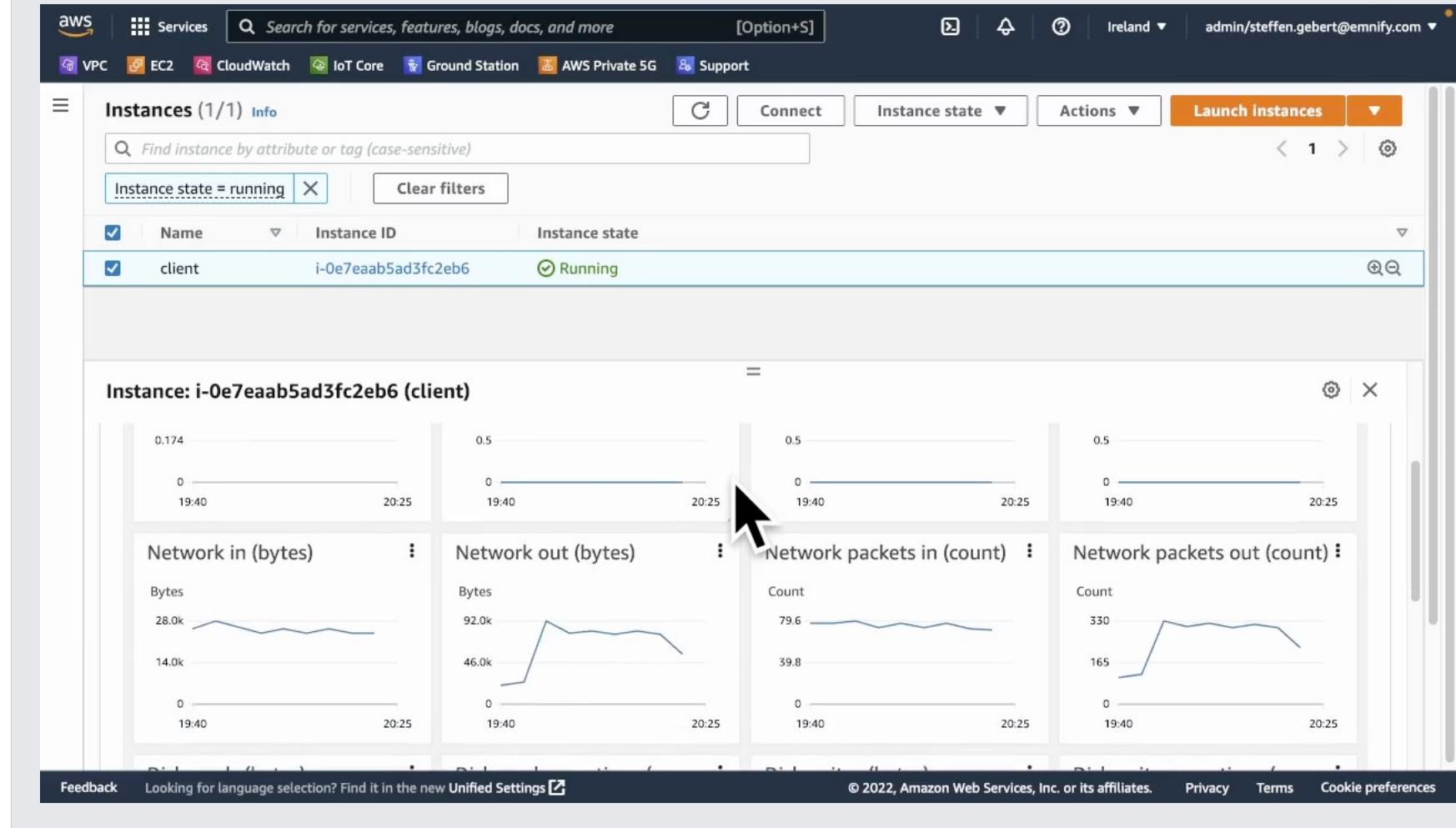
Metrics

The screenshot shows the AWS EC2 Instances page. At the top, there's a search bar and navigation links for VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support. The main table shows one instance:

Name	Instance ID	Instance state
client	i-0e7eaab5ad3fc2eb6	Running

Below the table, the instance details for **Instance: i-0e7eaab5ad3fc2eb6 (client)** are shown. The **Monitoring** tab is selected, indicated by an orange underline and a black cursor arrow pointing to it. Other tabs include Details, Security, Networking, Storage, Status checks, and Tags. The Monitoring section displays four metrics: CPU utilization (%), Status check failed (any), Status check failed (instance), and Status check failed (system). Each metric has a chart and some numerical values.

Metrics



Metrics Transit GW

The screenshot shows the AWS Management Console interface for managing Transit Gateways. The left sidebar navigation includes:

- VPC
- EC2
- CloudWatch
- IoT Core
- Ground Station
- AWS Private 5G
- Support

The main content area displays the "Transit gateways (1/1)" list, showing one entry:

Name	Transit gateway ID	Owner ID	State
trouble-tgw	tgw-01d227188df180eca	200234964126	Available

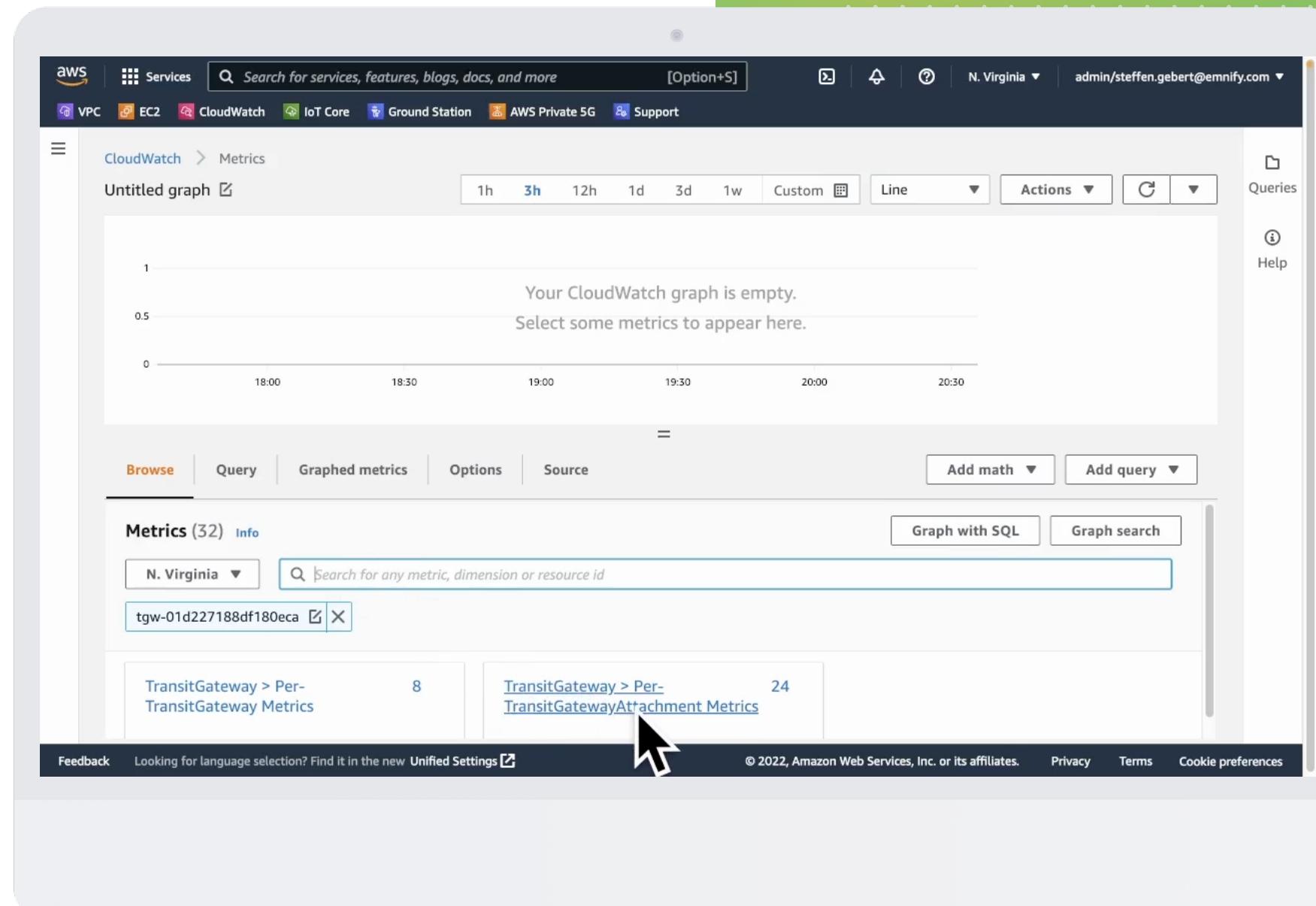
Below the list, the details for the selected Transit Gateway (tgw-01d227188df180eca / trouble-tgw) are shown. The "Details" tab is active, displaying the following configuration:

Transit gateway ID	tgw-01d227188df180eca	State	Available	Amazon ASN	64512	DNS support	Enable
Transit gateway ARN	arn:aws:ec2:us-east-1:200234964126:transit-gateway/tgw-01d227188df180eca	Default association route table	Enable	Association route table ID	tgw-rtb-0c8fc3e5420c5878	Auto accept shared attachments	Disable
		Default propagation route		Propagation route table ID		Propagation route table ID	

At the bottom of the page, there are links for Feedback, Unified Settings, and various legal notices.

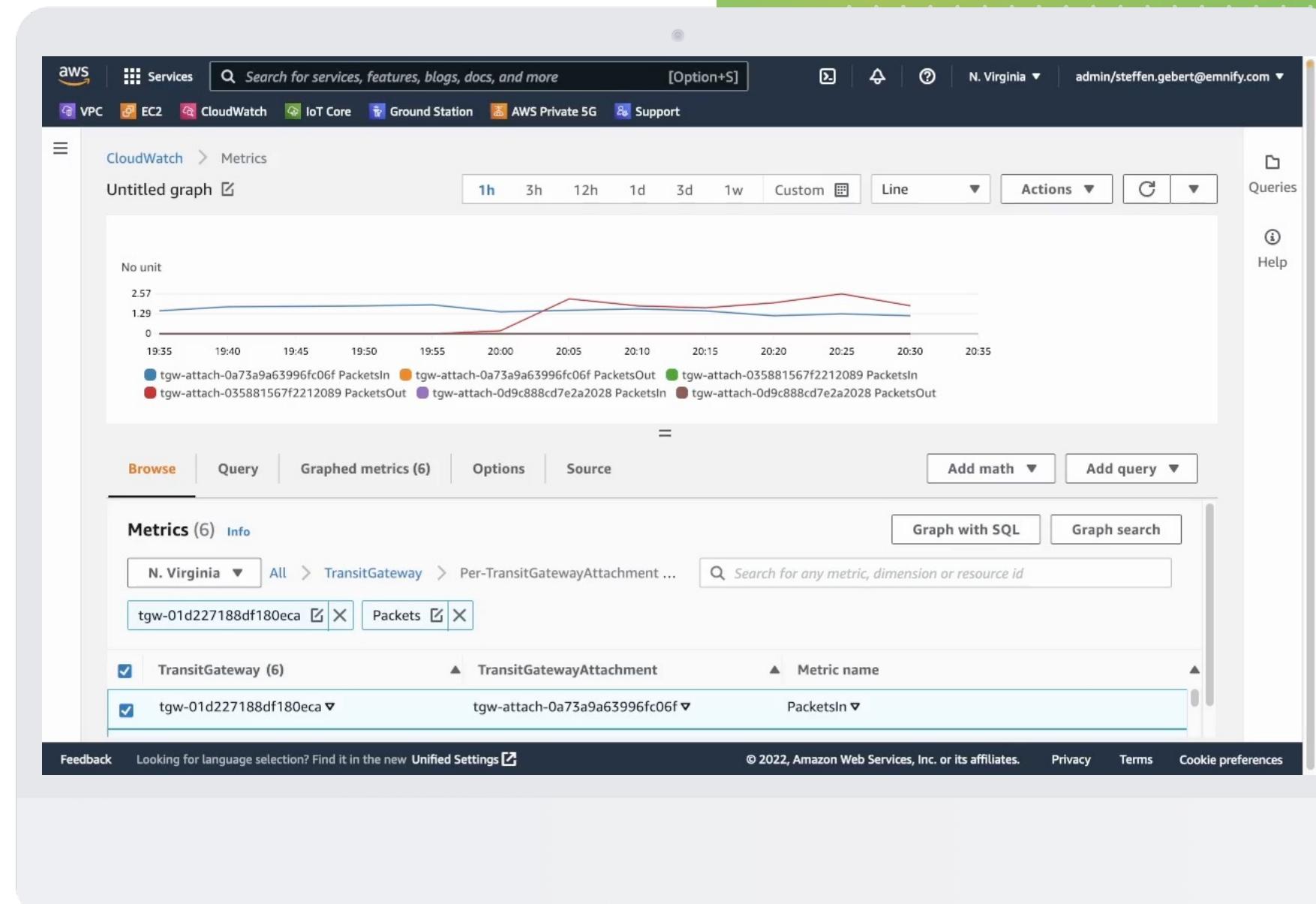
Metrics Transit GW

- Per TGW and per TGW Attachments
- In and out bytes and packets
- Blackhole and NoRoute metrics



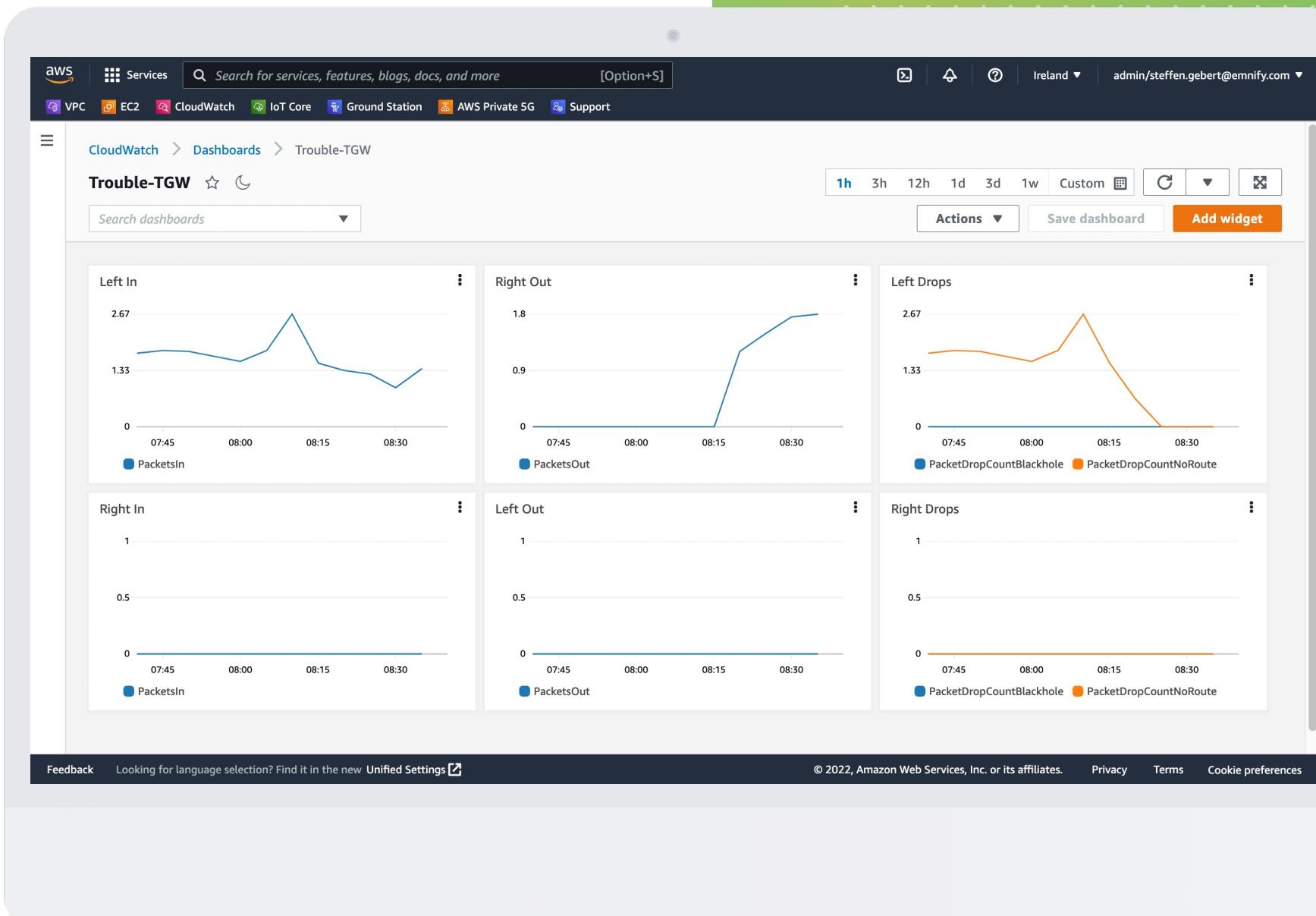
Metrics Transit GW

- Per TGW and per TGW Attachments
- In and out bytes and packets
- Blackhole and NoRoute metrics



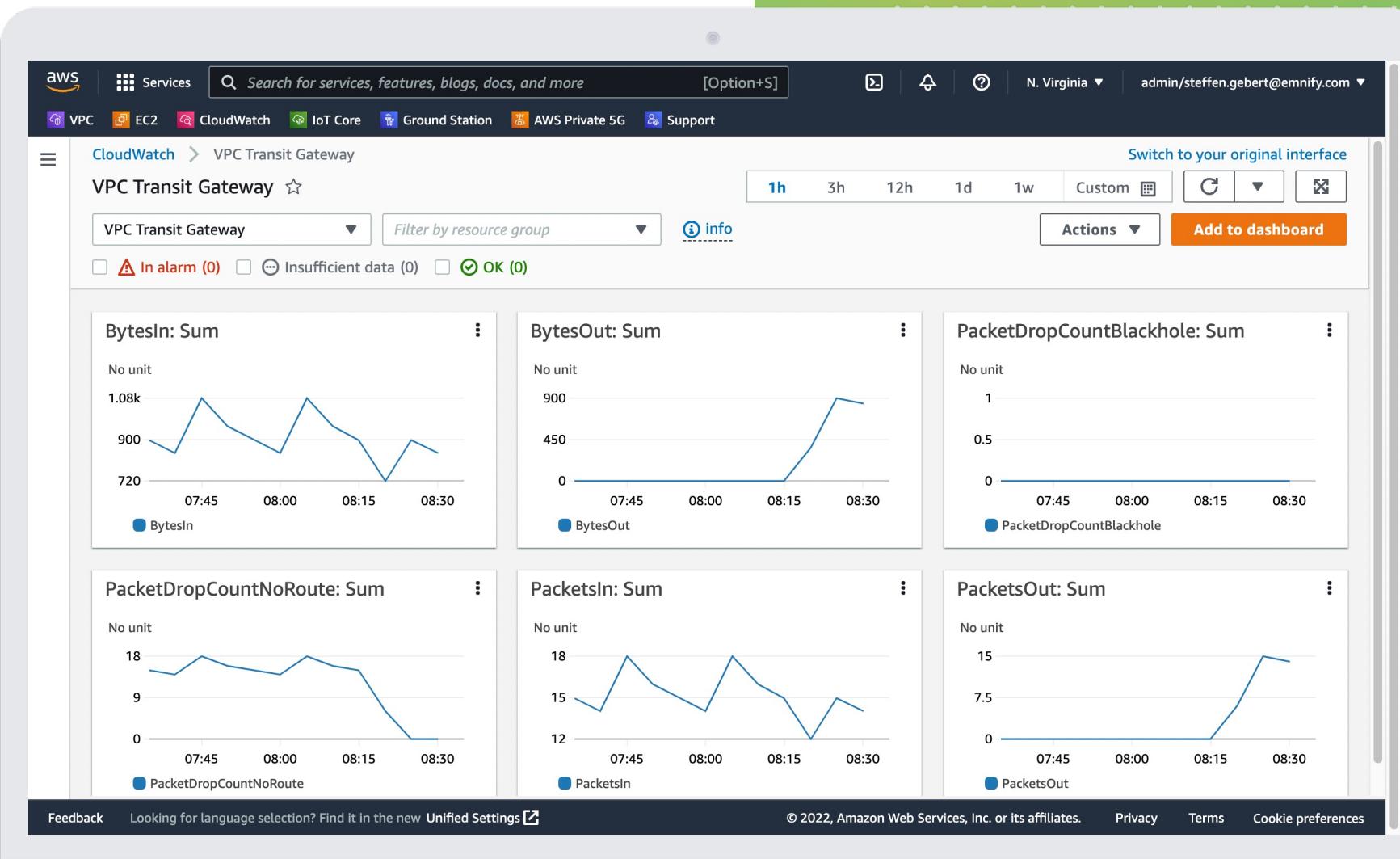
Metrics Transit GW

Custom Dashboard



Metrics Transit GW

- Automatic Dashboard
“VPC Transit Gateway”



EMnify

Flow Logs



Flow Logs

- VPC Flow Logs
- TGW Flow Logs **new**

The screenshot shows the 'Create flow log' configuration page in the AWS VPC console. At the top, the breadcrumb navigation shows 'VPC > Your VPCs > Create flow log'. The main title is 'Create flow log' with an 'Info' link. A descriptive text states: 'Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.' Below this is a table titled 'Selected resources' with columns 'Name', 'Resource ID', and 'State'. One row is listed: 'left' with 'vpc-0416ed0d3514d6fae' and 'Available'. The next section is 'Flow log settings'.

Flow log settings

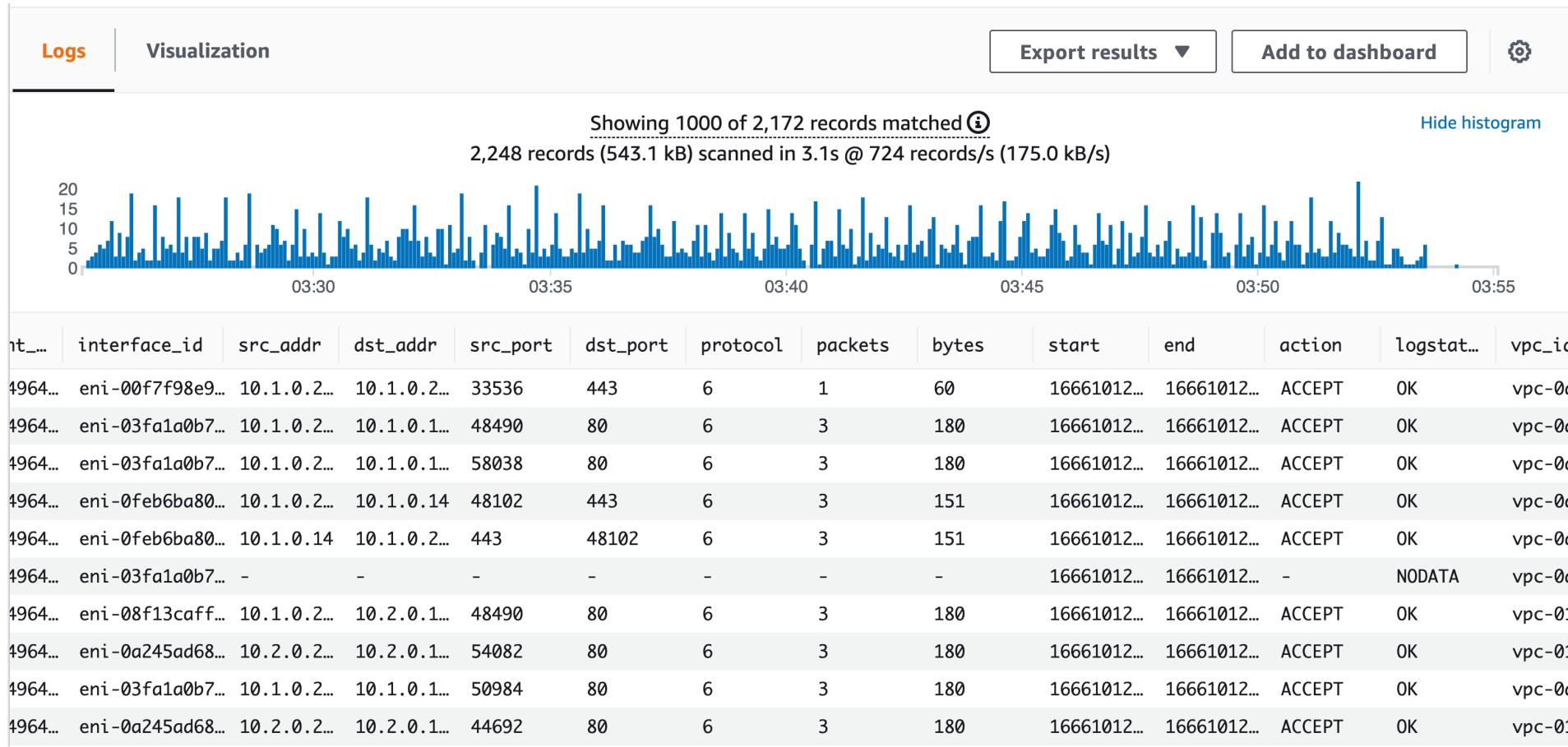
Name - optional
my-flow-log-01

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).
 Accept
 Reject
 All

Maximum aggregation interval [Info](#)
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.
 10 minutes
 1 minute

Destination
The destination to which to publish the flow log data.
 Send to CloudWatch Logs
 Send to an Amazon S3 bucket

CloudWatch Logs Insights



CloudWatch Logs Insights

The screenshot shows the CloudWatch Logs Insights interface. At the top, there's a navigation bar with a red vertical bar icon, followed by the text "Logs Insights", "Select log groups, and then run a query or [choose a sample query](#)", and a time range selector with options: 5m, 30m (selected), 1h, 3h, 12h, and Custom.

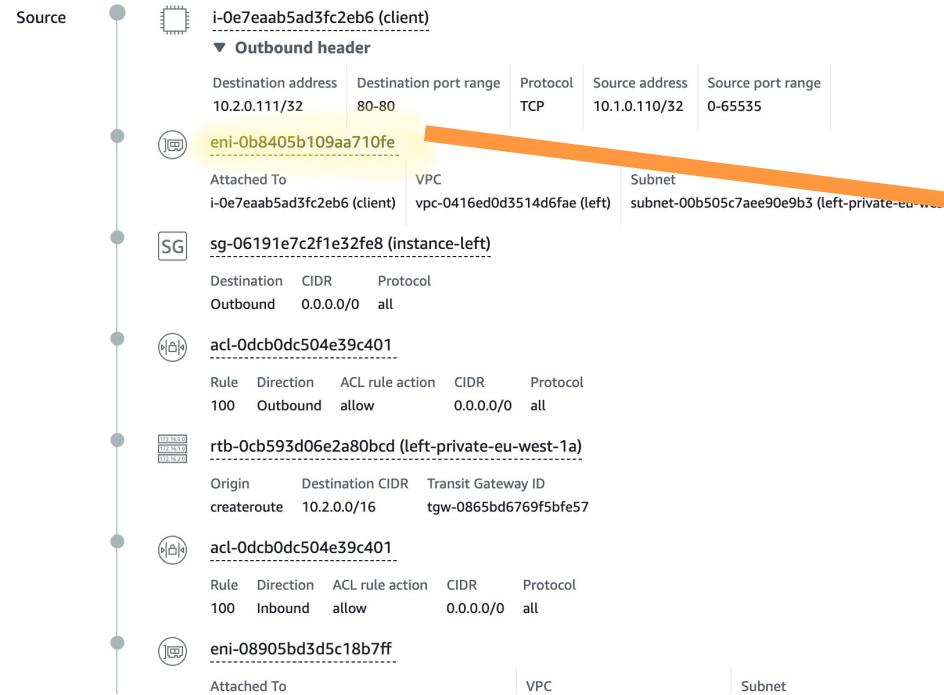
Below the navigation is a dropdown menu labeled "Select log group(s)" containing the entry "vpc-flow-logs-trouble-eu-central-1".

The main area contains a code editor with a red border, displaying the following Logstash-style query:

```
1 parse @message "* * * * * * * * * * * * * * * * * * * * * * * * * *"
2 | as version, account_id, interface_id, src_addr, dst_addr, src_port, dst_port, protocol, packets, bytes, start, end, action, logstatus,
3 | vpc_id, subnet_id, instance_id, tcp_flags, type, pkt_srcaddr, pkt_dstaddr,
4 | region, az_id, sublocation_type, sublocation_id,
5 | pkt_src_aws_service, pkt_dst_aws_service, flow_direction, traffic_path
6 | sort start desc
7
```

At the bottom of the code editor are five buttons: "Run query" (orange), "Cancel", "Save", "Actions ▾", and "History". A note below the buttons states: "Queries are allowed to run for up to 15 minutes."

Reachability Analyzer zu Flow Logs



interface_id	vpc_id	src_port	dst_port	action	flow_di...
eni-0b8405b10...	vpc-0416ed...	12345	80	ACCEPT	egress
eni-08905bd3d...	vpc-0416ed...	12345	80	ACCEPT	ingress
eni-0e67b5d56...	vpc-0f0eff...	12345	80	ACCEPT	egress
eni-01d16f30b...	vpc-0f0eff...	12345	80	ACCEPT	ingress
eni-01d16f30b...	vpc-0f0eff...	12345	80	REJECT	ingress

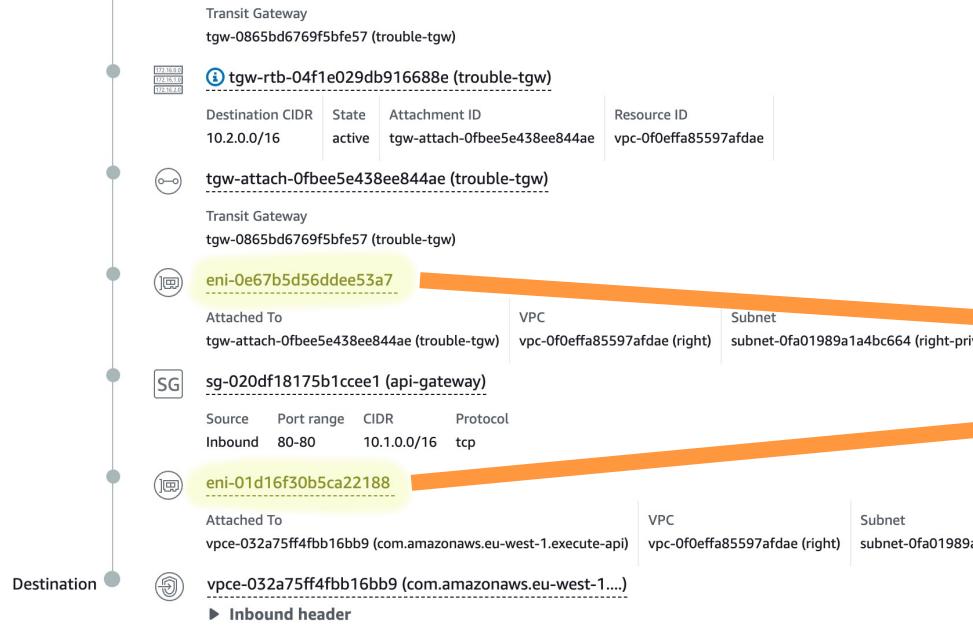
Reachability Analyzer zu Flow Logs

100	Outbound	allow	0.0.0.0/0	all
rtb-0cb593d06e2a80bcd (left-private-eu-west-1a)				
Origin	Destination CIDR	Transit Gateway ID		
createroute 10.2.0.0/16 tgw-0865bd6769f5bfe57				
acl-0dcb0dc504e39c401				
Rule	Direction	ACL rule action	CIDR	Protocol
100	Inbound	allow	0.0.0.0/0	all
eni-08905bd3d5c18b7ff				
Attached To	VPC	Subnet		
tgw-attach-0f25159b2cae021d2 (trouble-tgw)	vpc-0416ed0d3514d6fae (left)	subnet-00b505c7aee90e9b3 (left-priv)		
tgw-attach-0f25159b2cae021d2 (trouble-tgw)				
Transit Gateway				
tgw-0865bd6769f5bfe57 (trouble-tgw)				
tgw-rtb-04f1e029db916688e (trouble-tgw)				
Destination CIDR	State	Attachment ID	Resource ID	
10.2.0.0/16	active	tgw-attach-0fbe5e438ee844ae	vpc-0f0effa85597afdae	
tgw-attach-0fbe5e438ee844ae (trouble-tgw)				
Transit Gateway				
tgw-0865bd6769f5bfe57 (trouble-tgw)				
eni-0e67b5d56ddee53a7				

interface_id	vpc_id	src_port	dst_port	action	flow_di...
eni-0b8405b10...	vpc-0416ed...	12345	80	ACCEPT	egress
eni-08905bd3d...	vpc-0416ed...	12345	80	ACCEPT	ingress
eni-0e67b5d56...	vpc-0f0eff...	12345	80	ACCEPT	egress
eni-01d16f30b...	vpc-0f0eff...	12345	80	ACCEPT	ingress
eni-01d16f30b...	vpc-0f0eff...	12345	80	REJECT	ingress



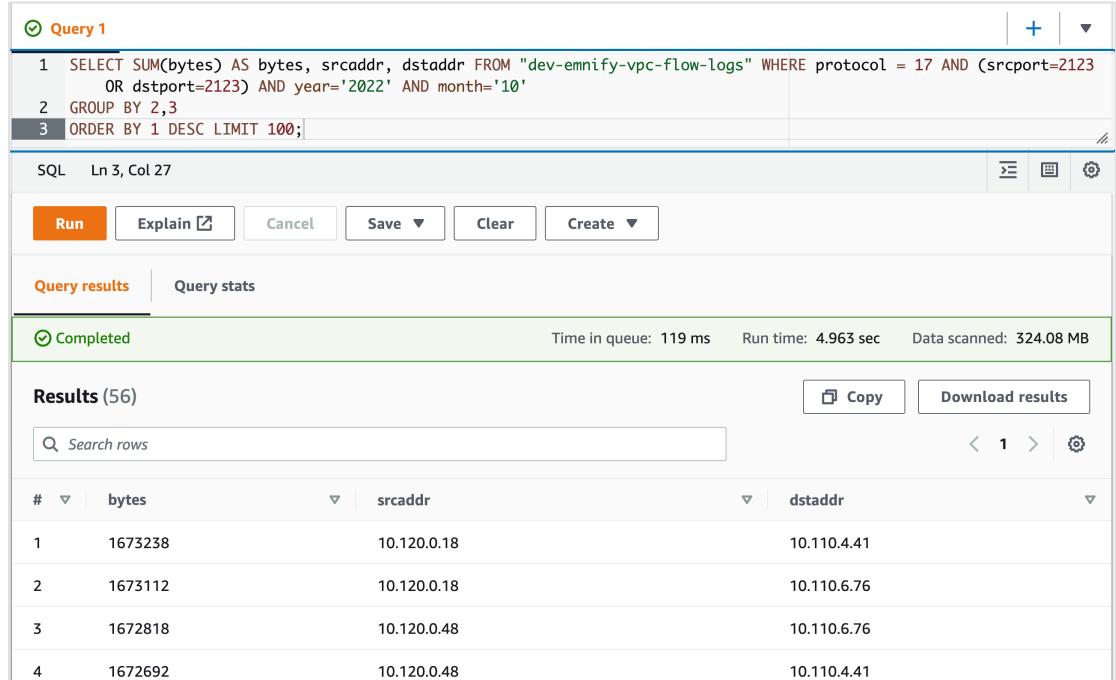
Reachability Analyzer zu Flow Logs



interface_id	vpc_id	src_port	dst_port	action	flow_di...
eni-0b8405b10...	vpc-0416ed...	12345	80	ACCEPT	egress
eni-08905bd3d...	vpc-0416ed...	12345	80	ACCEPT	ingress
eni-0e67b5d56...	vpc-0f0eff...	12345	80	ACCEPT	egress
eni-01d16f30b...	vpc-0f0eff...	12345	80	ACCEPT	ingress
eni-01d16f30b...	vpc-0f0eff...	12345	80	REJECT	ingress

Flow Logs – Additional Destinations

- S3 and Kinesis Firehose
- Use cases
 - Continuous monitoring
 - Retrospective analysis



The screenshot shows a database query interface with the following details:

Query 1

```
1 SELECT SUM(bytes) AS bytes, srcaddr, dstaddr FROM "dev-emnify-vpc-flow-logs" WHERE protocol = 17 AND (srcport=2123  
OR dstport=2123) AND year='2022' AND month='10'  
2 GROUP BY 2,3  
3 ORDER BY 1 DESC LIMIT 100;
```

SQL Ln 3, Col 27

Run Explain Cancel Save Clear Create

Query results | Query stats

Completed Time in queue: 119 ms Run time: 4.963 sec Data scanned: 324.08 MB

Results (56)

#	bytes	srcaddr	dstaddr
1	1673238	10.120.0.18	10.110.4.41
2	1673112	10.120.0.18	10.110.6.76
3	1672818	10.120.0.48	10.110.6.76
4	1672692	10.120.0.48	10.110.4.41

Copy Download results < 1 > ⌂

EMnify

Packet Capture



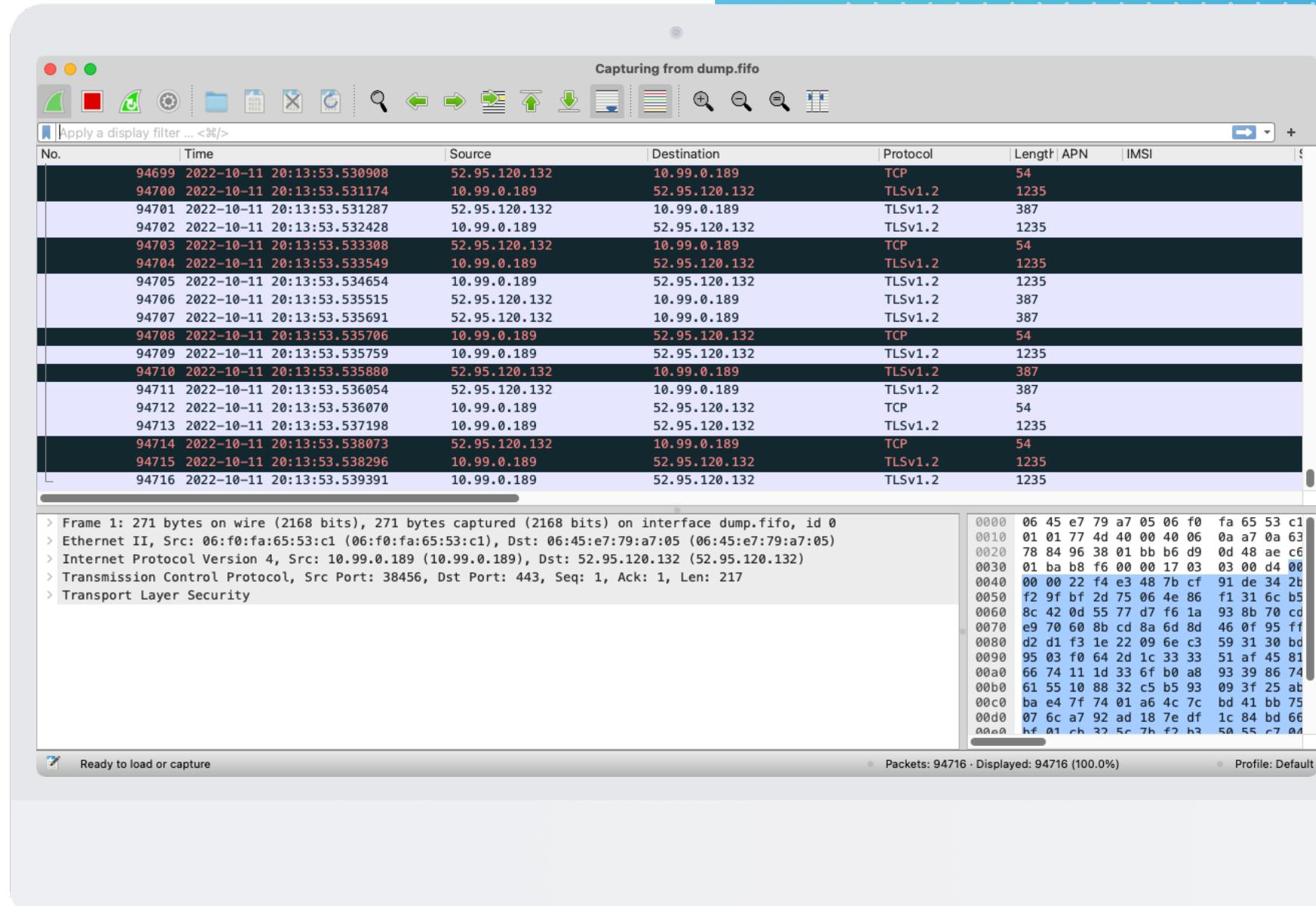
Wireshark

- tcpdump running on client instance
- Streamed through SSH or SSM connection

```
→ ~ mkfifo dump fifo
→ ~ ssh i-0c45681d7bbb8a872 'sudo tcpdump -U -i ens5 -w -' > dump fifo&
[1] 12222
→ ~ wireshark -k -i dump fifo
** (wireshark:12225) 21:10:44.258820 [GUI WARNING] -- QObject::connect: No such slot WiresharkMainWindow::on_actionCaptureOptions_triggered() in ui/qt/main.cpp:700
** (wireshark:12225) 21:10:44.258841 [GUI WARNING] -- QObject::connect: (receiver name: 'WiresharkMainWindow')
** (wireshark:12225) 21:10:44.817352 [GUI WARNING] -- Populating font family aliases took 81 ms.
Replace uses of missing font family ".AppleSystemUIFont" with one that exists to avoid this cost
.
** (wireshark:12225) 21:10:45.510525 [Capture MESSAGE] -- Capture Start ...
```

Wireshark

- tcpdump running on client instance
- Streamed through SSH or SSM connection
- Comfortably displayed on local computer



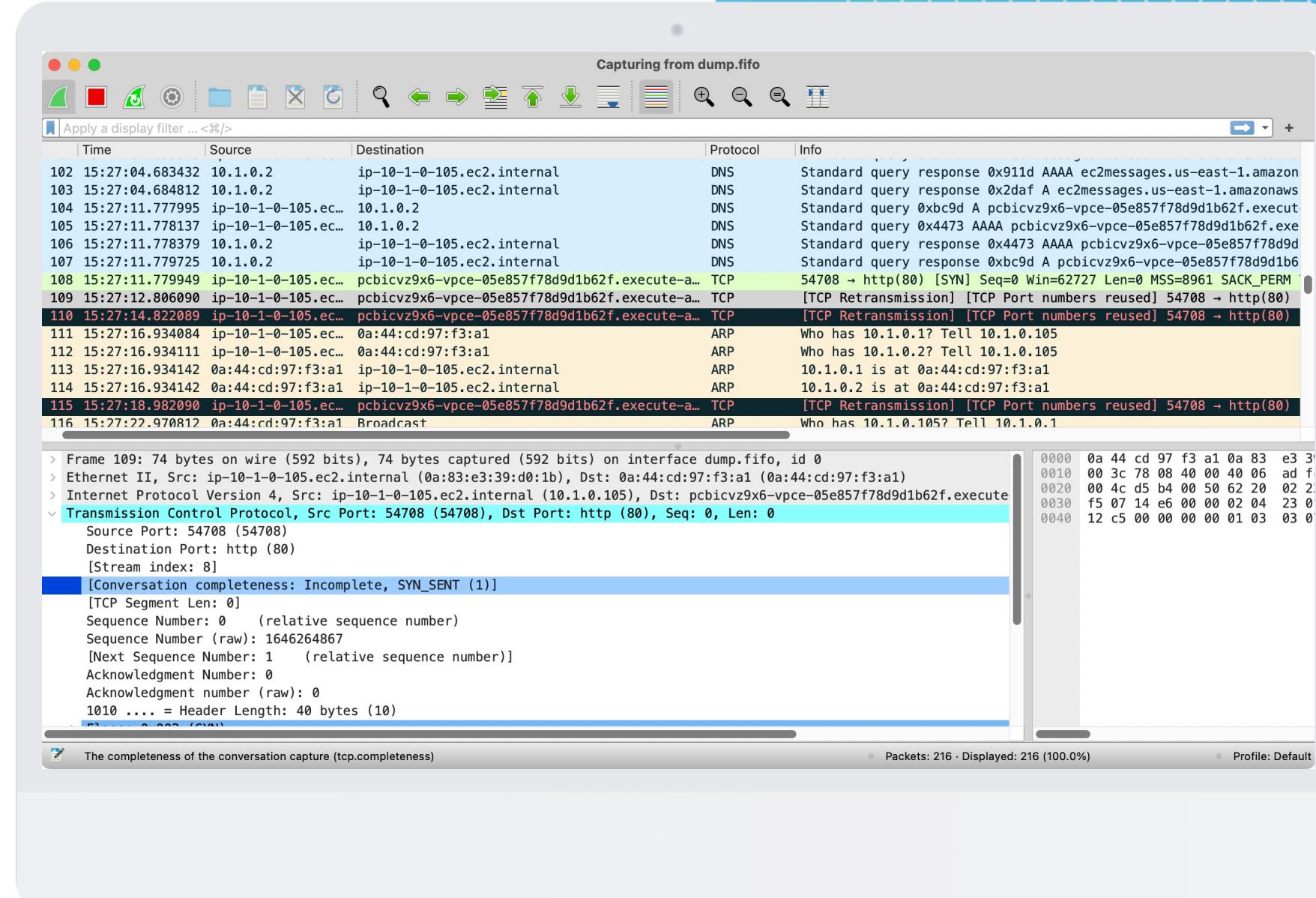
Wireshark

- tcpdump running on client instance
- Streamed through SSH or SSM connection
- Comfortably displayed on local computer
- Filter out own traffic!

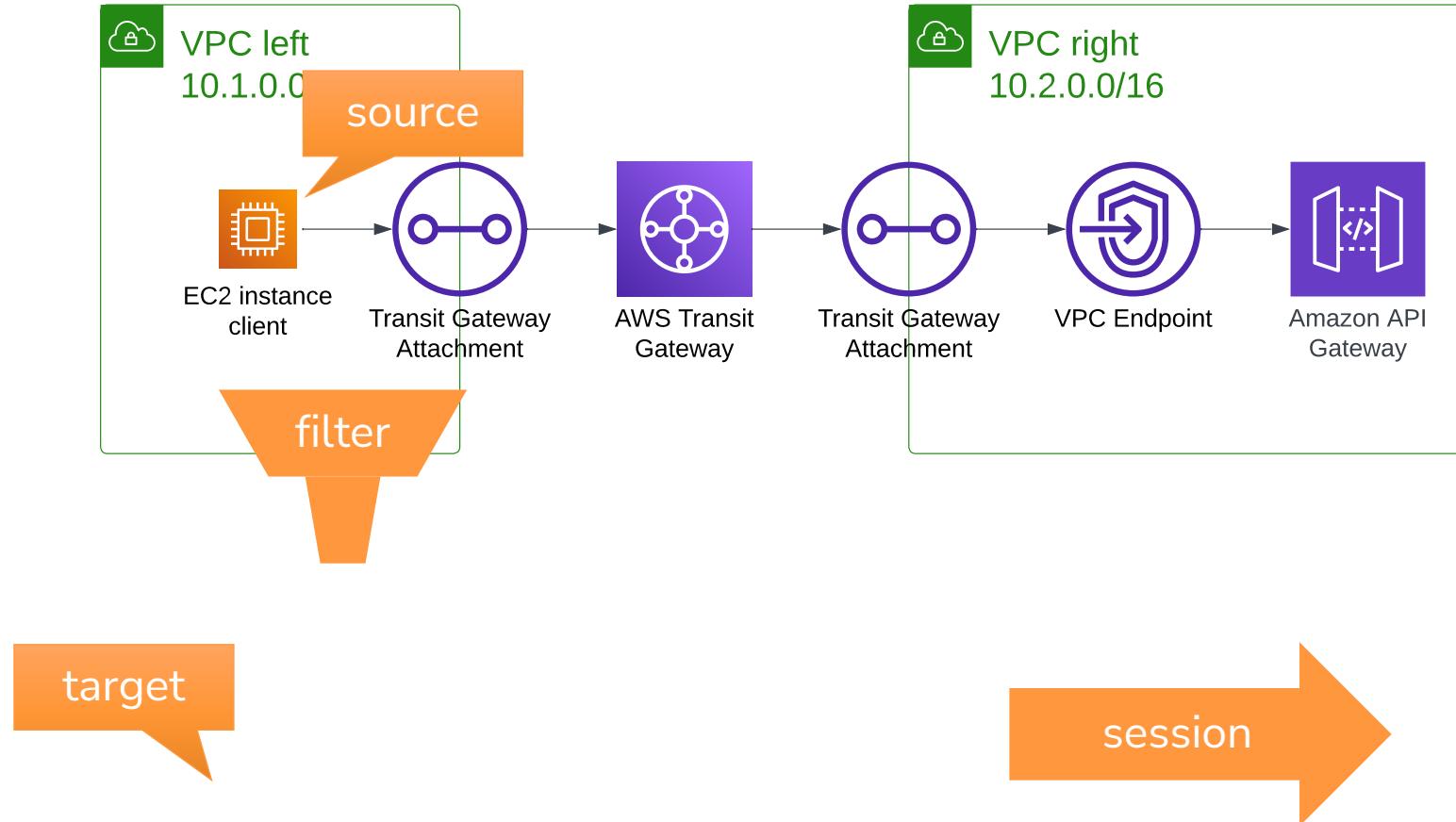
```
~ ssh i-0e36abd49bb6e2d44 'sudo tcpdump -U -i ens5 -w - not port 443' > dump fifo &
```

Wireshark

- tcpdump running on client instance
- Streamed through SSH connection
- Comfortably displayed on local computer
- Filter out own traffic!



VPC Traffic Mirroring



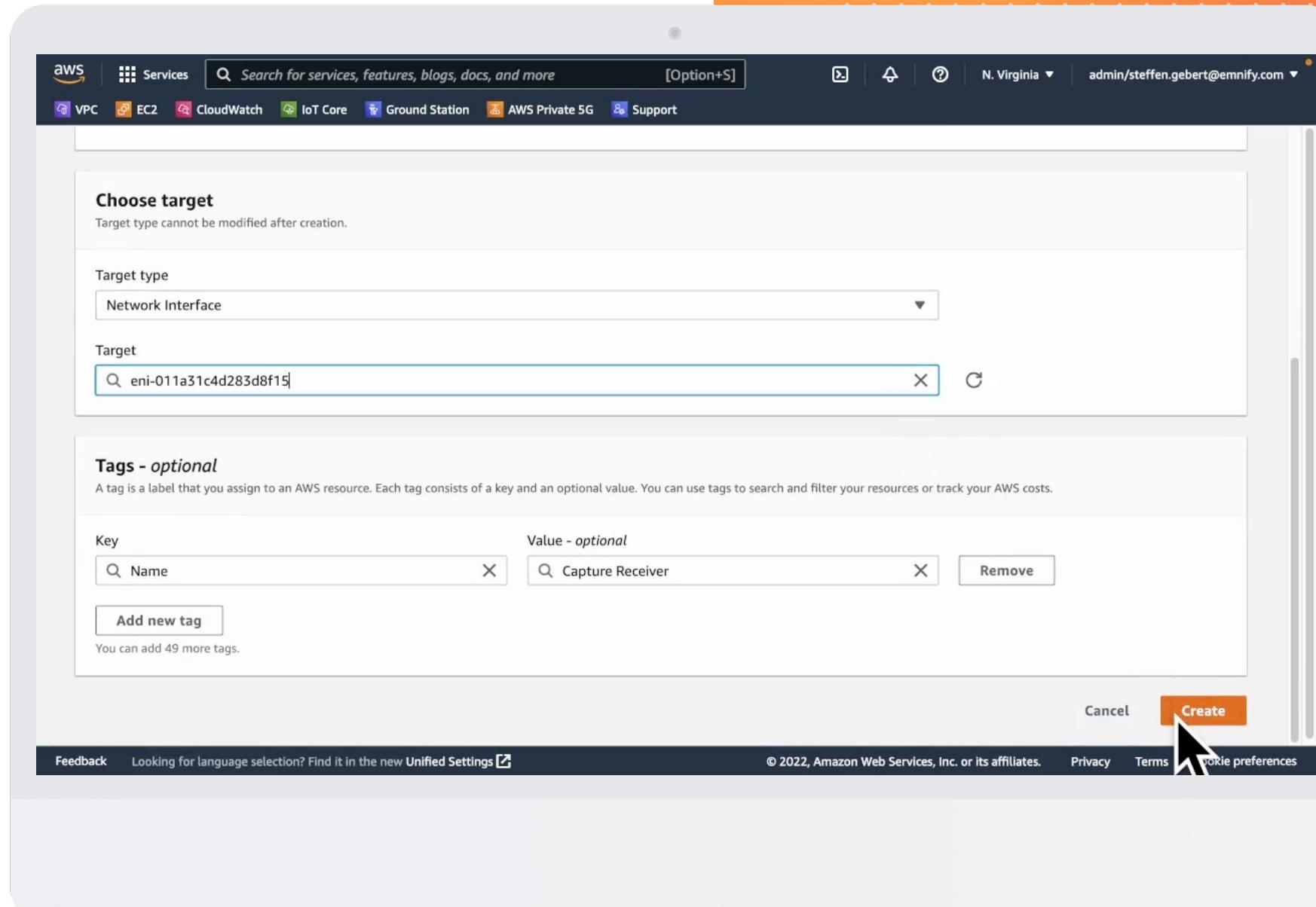
VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances

The screenshot shows the AWS Management Console interface for VPC Traffic Mirroring. The left sidebar navigation includes 'VPC', 'EC2', 'CloudWatch', 'IoT Core', 'Ground Station', 'AWS Private 5G', and 'Support'. Under 'Traffic Mirroring', the 'Mirror targets' option is selected. The main content area is titled 'Traffic mirror targets' and displays a message: 'No traffic mirror targets found' and 'You do not have any traffic mirror targets in this region.' A prominent orange button labeled 'Create traffic mirror target' is visible, with a cursor arrow pointing directly at it.

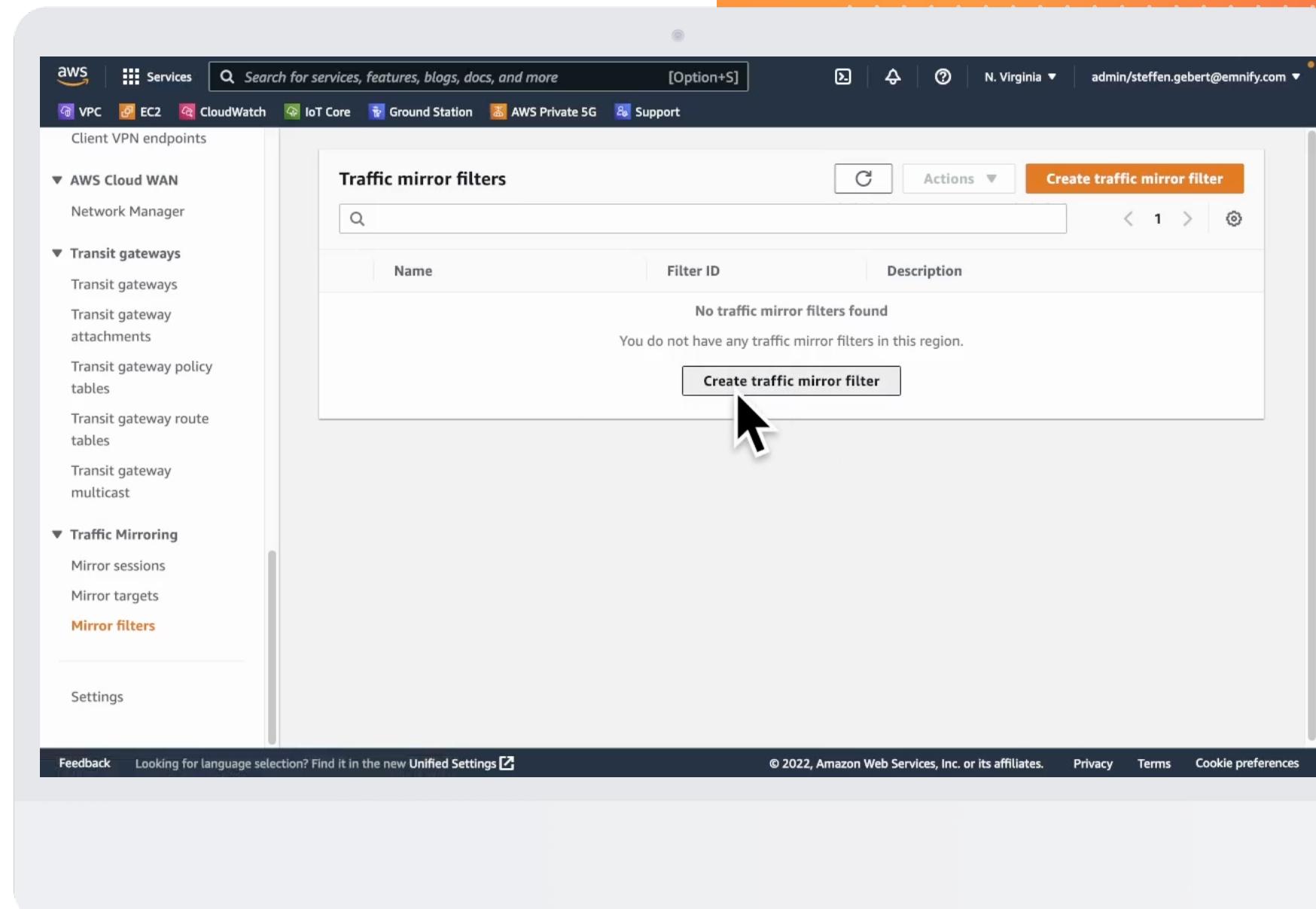
VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances



VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances



VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances

The screenshot shows the AWS VPC Traffic Mirroring configuration interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (N. Virginia, admin/steffen.gebert@emnify.com). Below the navigation bar are tabs for VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support.

The main area is divided into two sections: "Inbound rules - optional" and "Outbound rules - optional". Both sections have a header with columns: Number, Rule action, Protocol, Source port range - optional, Destination port range - optional, Source CIDR block, Destination CIDR block, and Description. Each section contains two rows of rules:

Number	Rule action	Protocol	Source port range - optional	Destination port range - optional	Source CIDR block	Destination CIDR block	Description
100	accept ▾	TCP (6) ▾	80		0.0.0.0/0	0.0.0.0/0	(X)
200	accept ▾	TCP (6) ▾	443		0.0.0.0/0	0.0.0.0/0	(X)

Below each table is a "Sort rules" button. At the bottom of each section is an "Add rule" button. A cursor arrow points to the "Add rule" button in the Outbound rules section.

At the very bottom of the page, there are links for Feedback, Unified Settings, Copyright (© 2022, Amazon Web Services, Inc. or its affiliates.), Privacy, Terms, and Cookie preferences.

VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances

The screenshot shows the AWS VPC Traffic Mirroring console. The left sidebar has a tree view with 'VPC' selected, followed by 'EC2', 'CloudWatch', 'IoT Core', 'Ground Station', 'AWS Private 5G', and 'Support'. Under 'VPC', 'Transit gateways' is expanded, showing 'Transit gateways', 'Transit gateway attachments', 'Transit gateway policy tables', 'Transit gateway route tables', and 'Transit gateway multicast'. Under 'Traffic Mirroring', 'Mirror sessions' is selected, followed by 'Mirror targets' and 'Mirror filters'. At the bottom of the sidebar is a 'Settings' section. The main content area is titled 'Traffic mirror sessions' and includes a search bar, a 'Create traffic mirror session' button, and a message stating 'No traffic mirror sessions found'. Below this message is another message: 'You do not have any traffic mirror sessions in this region.' A large black arrow points to the 'Create traffic mirror session' button.

VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances

The screenshot shows the AWS Management Console interface for creating a traffic mirror session. The top navigation bar includes the AWS logo, a search bar, and links for Services, VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support. The user is signed in as admin/steffen.gebert@emnify.com. The main page title is "Create traffic mirror session".

Session settings
Set description, source, and target.

Name tag - optional
Capture Trouble

Description - optional
Describe your traffic mirror session

Mirror source
The resource that you want to monitor.
eni-097743e2ec33cd884

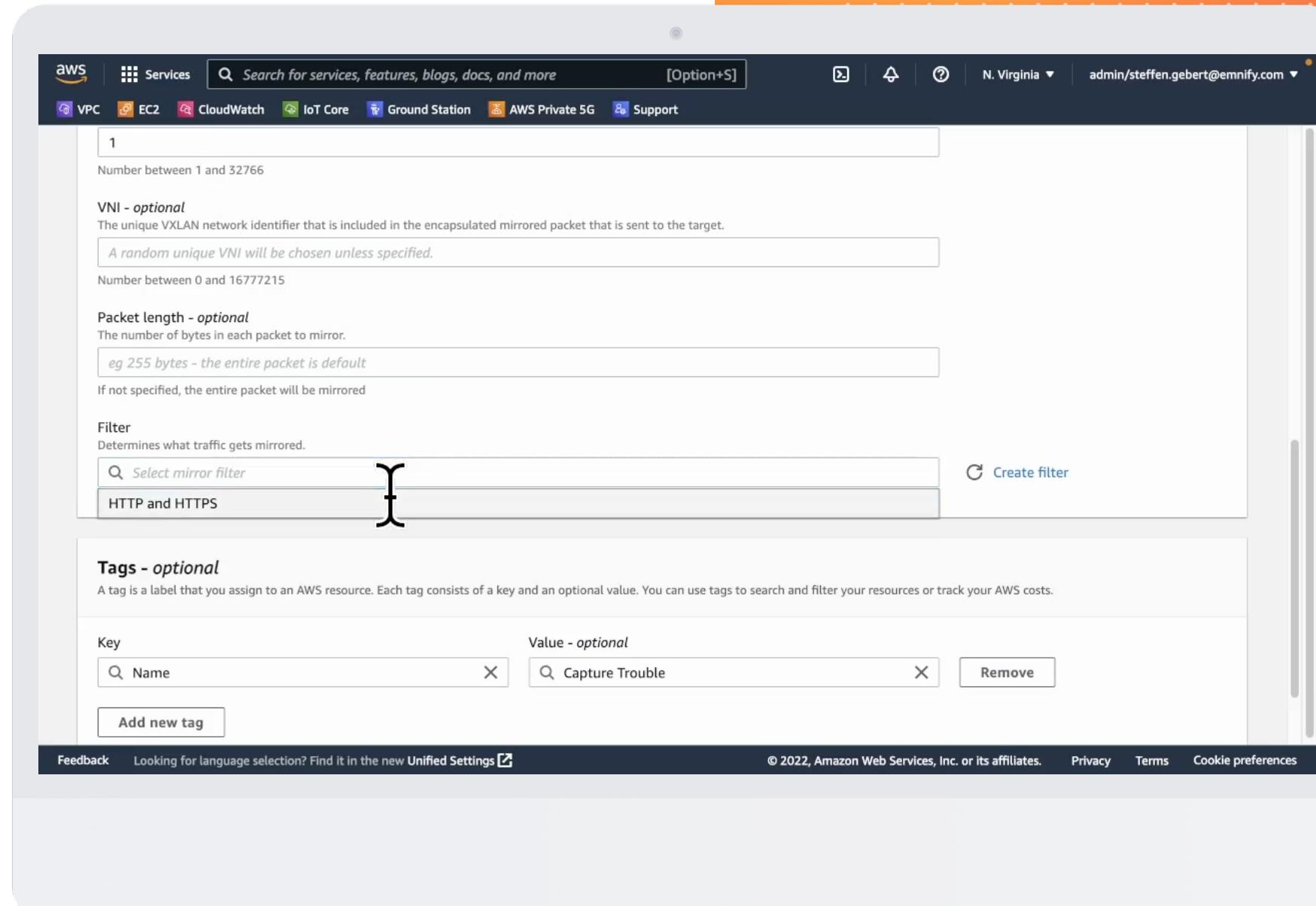
Mirror target
A network interface, or a network load balancer, or a gateway load balancer endpoint that is the destination for mirrored traffic.
tmt-03aabf40711b41d63

Additional settings

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

VPC Traffic Mirroring

- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances



VPC Traffic Mirroring

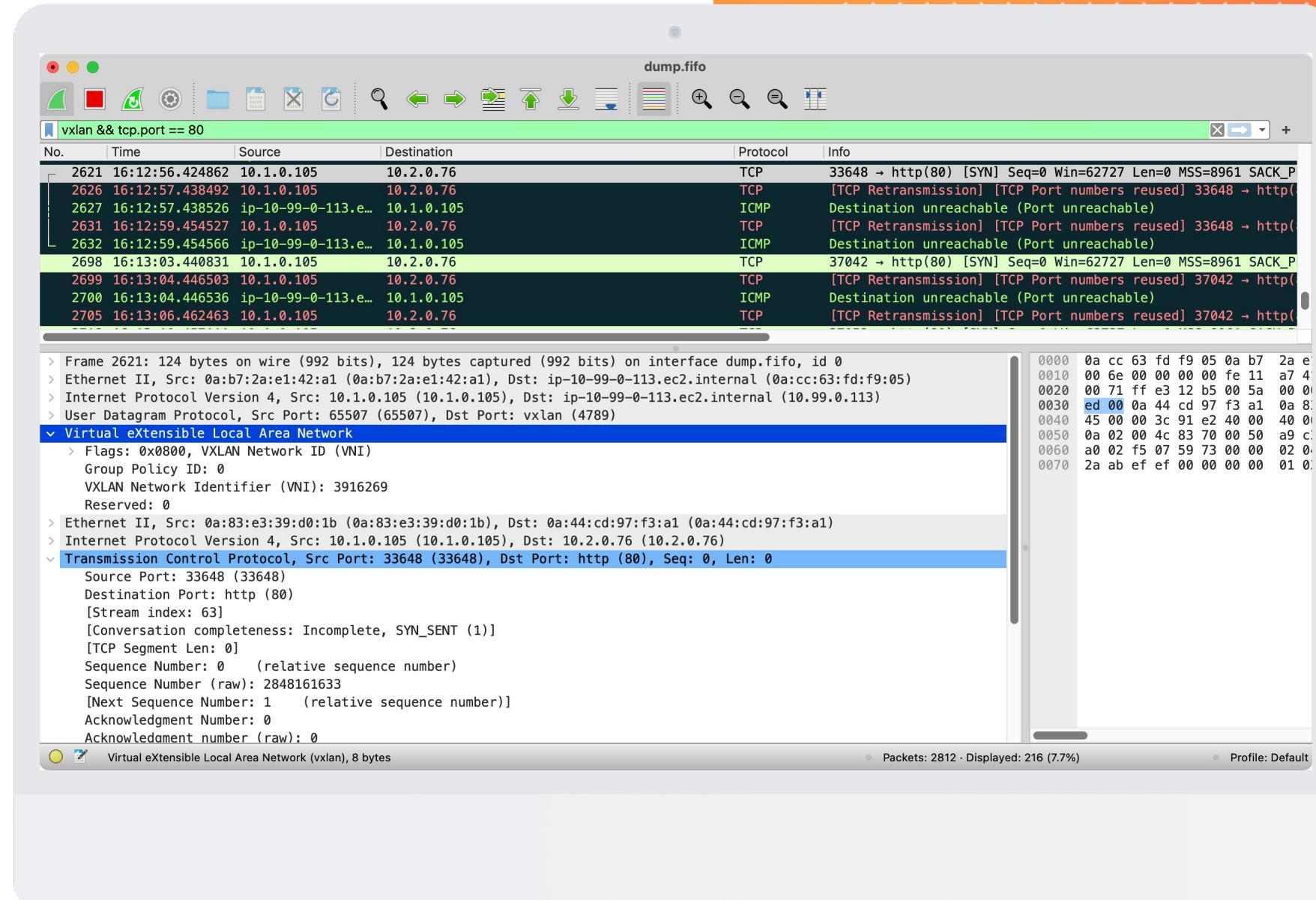
- Packets duplicated by Nitro
- Accounts to packet/sec limits of EC2 instance
- Requires connectivity from source to target
- Only for EC2 instances

The screenshot shows the AWS VPC Traffic mirror sessions page. At the top, there's a navigation bar with the AWS logo, a search bar, and links for Services, VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support. A notification for 'New VPC Experience' is visible. The main content area is titled 'Traffic mirror sessions' and contains a table with one row. The table columns are Name, Session ID, Description, Source, and Target. The single row shows a session named 'Capture Trouble' with Session ID 'tms-0deae0c9ca5fdbbc4'. The Source is listed as 'eni-097743e2ec33cd884' and the Target as 'tmt-03aabf40711b41d63'. There are buttons for 'Actions' and 'Create traffic mirror session'.

Name	Session ID	Description	Source	Target
Capture Trouble	tms-0deae0c9ca5fdbbc4	-	eni-097743e2ec33cd884	tmt-03aabf40711b41d63

VPC Traffic Mirroring

- Capturing now on target instance
- Packets received in VXLAN encapsulation



“

That's fun!

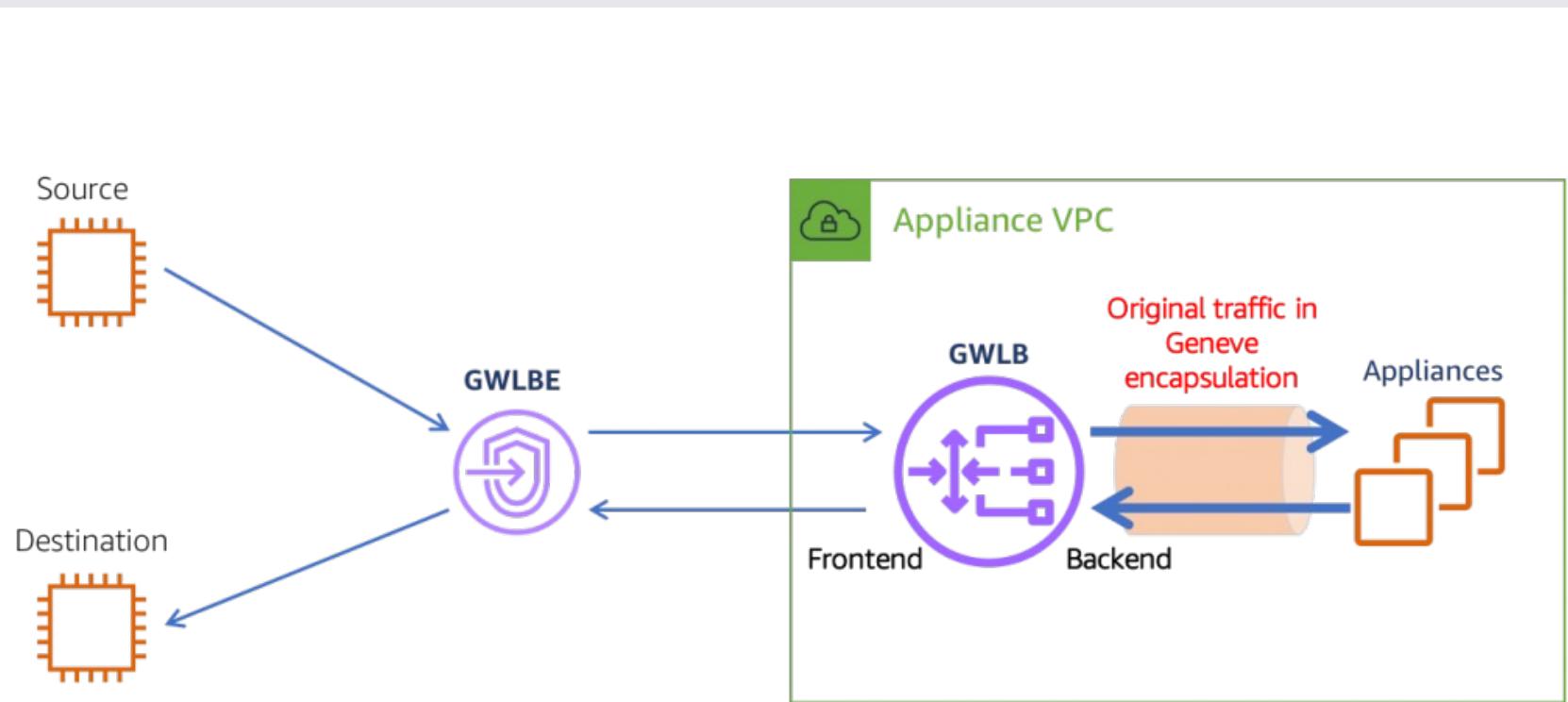
NOBODY EVER DOING THIS

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)



Aidan W Steele
 @_steele Follows you



<https://github.com/aidansteele/flowdog>

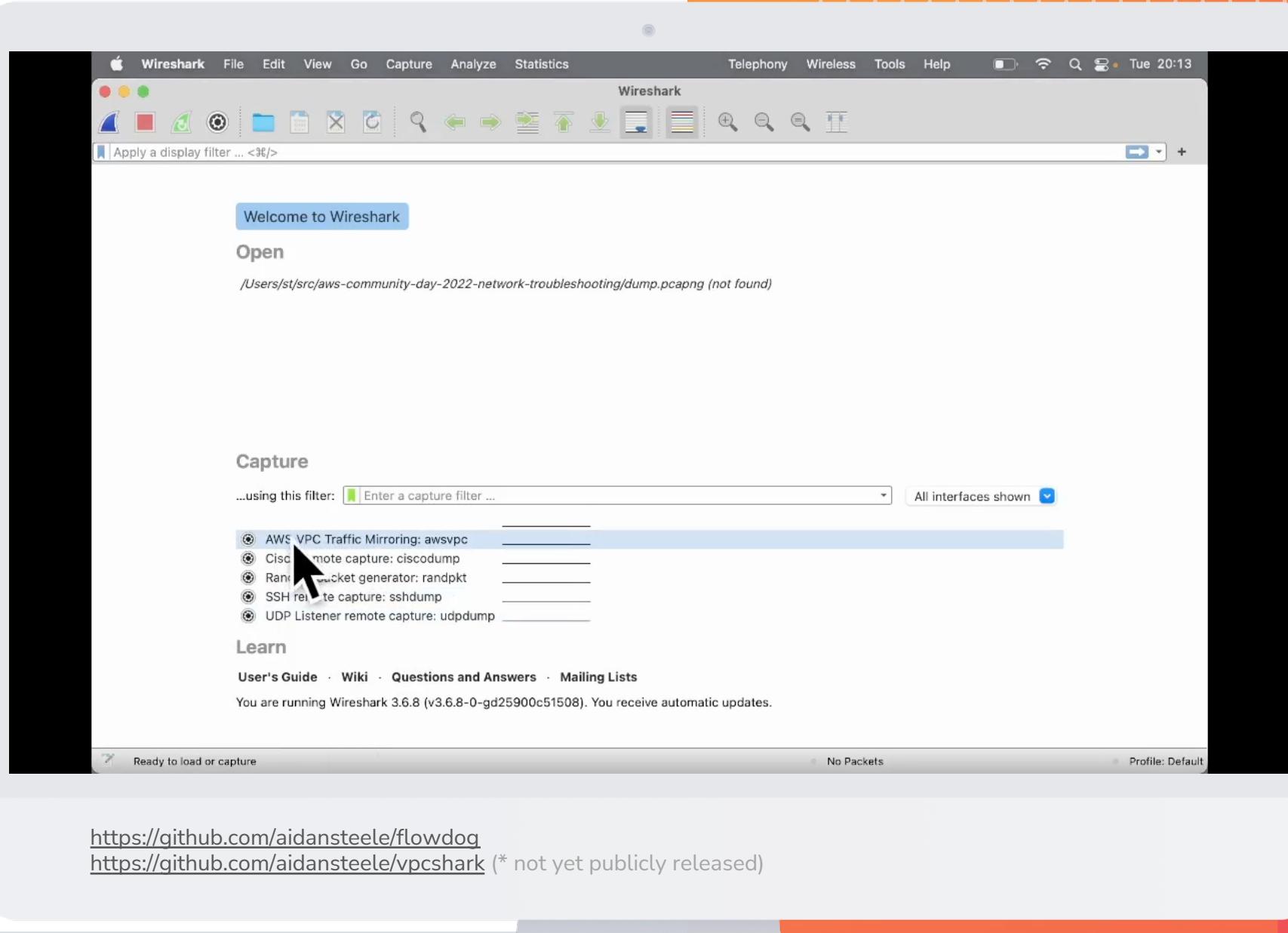
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



The screenshot shows the Wireshark interface. In the 'Capture' section, a dropdown menu is open, listing several remote capture options. The option 'AWS VPC Traffic Mirroring: awsvpc' is highlighted with a mouse cursor. Below the dropdown, the Wireshark status bar indicates 'Ready to load or capture' and 'No Packets'. The bottom of the window displays the message 'You are running Wireshark 3.6.8 (v3.6.8-0-gd25900c51508). You receive automatic updates.' At the very bottom, there are two GitHub links: <https://github.com/aidansteele/flowdog> and <https://github.com/aidansteele/vpcshark> (* not yet publicly released).

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you

The screenshot shows the Wireshark interface with a modal dialog titled "Wireshark - Interface Options: AWS VPC Traffic Mirroring: awsvpc". The dialog has tabs for "AWS", "Traffic source", and "Mirror target". Under the "AWS Profile" tab, "playground" is selected. Under "AWS Region", a dropdown menu lists various AWS regions: af-south-1, ap-east-1, ap-northeast-1, ap-northeast-2, ap-northeast-3, ap-south-1, ap-southeast-1, ap-southeast-2, ap-southeast-3, ca-central-1, eu-central-1, eu-north-1, eu-south-1, eu-west-1, eu-west-2, eu-west-3, me-south-1, sa-east-1, us-east-1, us-east-2, us-west-1, and us-west-2. The "eu-west-3" option is highlighted with a blue selection bar and a cursor arrow pointing at it. The main Wireshark window background shows the "Welcome to Wireshark" message and the "Capture" pane.

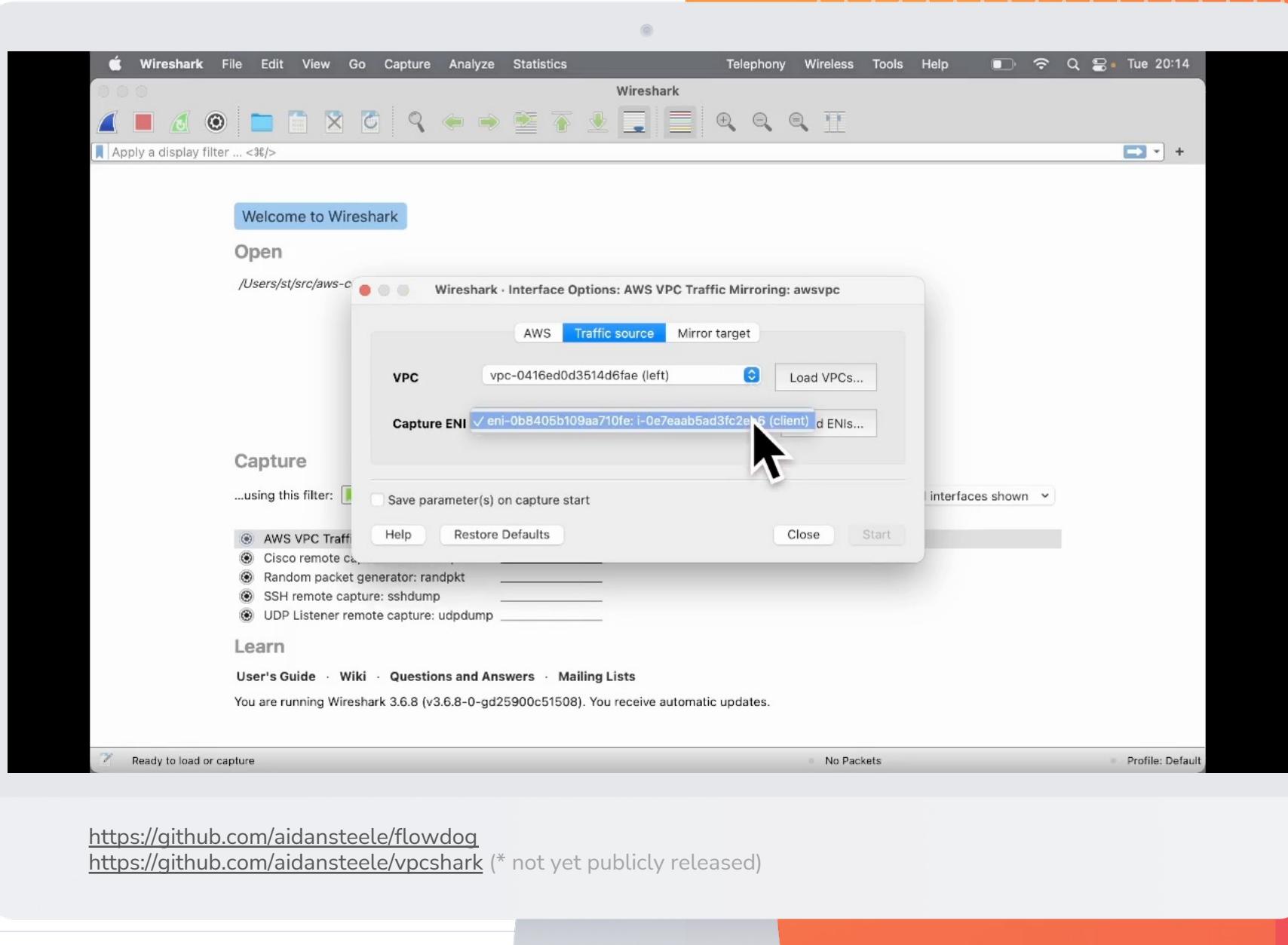
<https://github.com/aidansteele/flowdog>
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - `vpcshark` *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



The screenshot shows the Wireshark application window. A modal dialog box titled "Wireshark - Interface Options: AWS VPC Traffic Mirroring: awsvpc" is open. The "Traffic source" tab is selected. Inside, a "VPC" dropdown is set to "vpc-0416ed0d3514d6fae (left)". Below it, a "Capture ENI" dropdown has "eni-0b8405b109aa710fe: i-0e7eaab5ad3fc2e6 (client)" selected, with a cursor arrow pointing at this option. The "Capture" section contains a "using this filter:" dropdown set to "AWS VPC Traffic". Other options include "Cisco remote capture", "Random packet generator: randpkt", "SSH remote capture: sshdump", and "UDP Listener remote capture: udpdump". At the bottom of the dialog, there are "Help", "Restore Defaults", "Close", and "Start" buttons. The main Wireshark window background shows the "Welcome to Wireshark" message and the "Capture" and "Learn" sections.

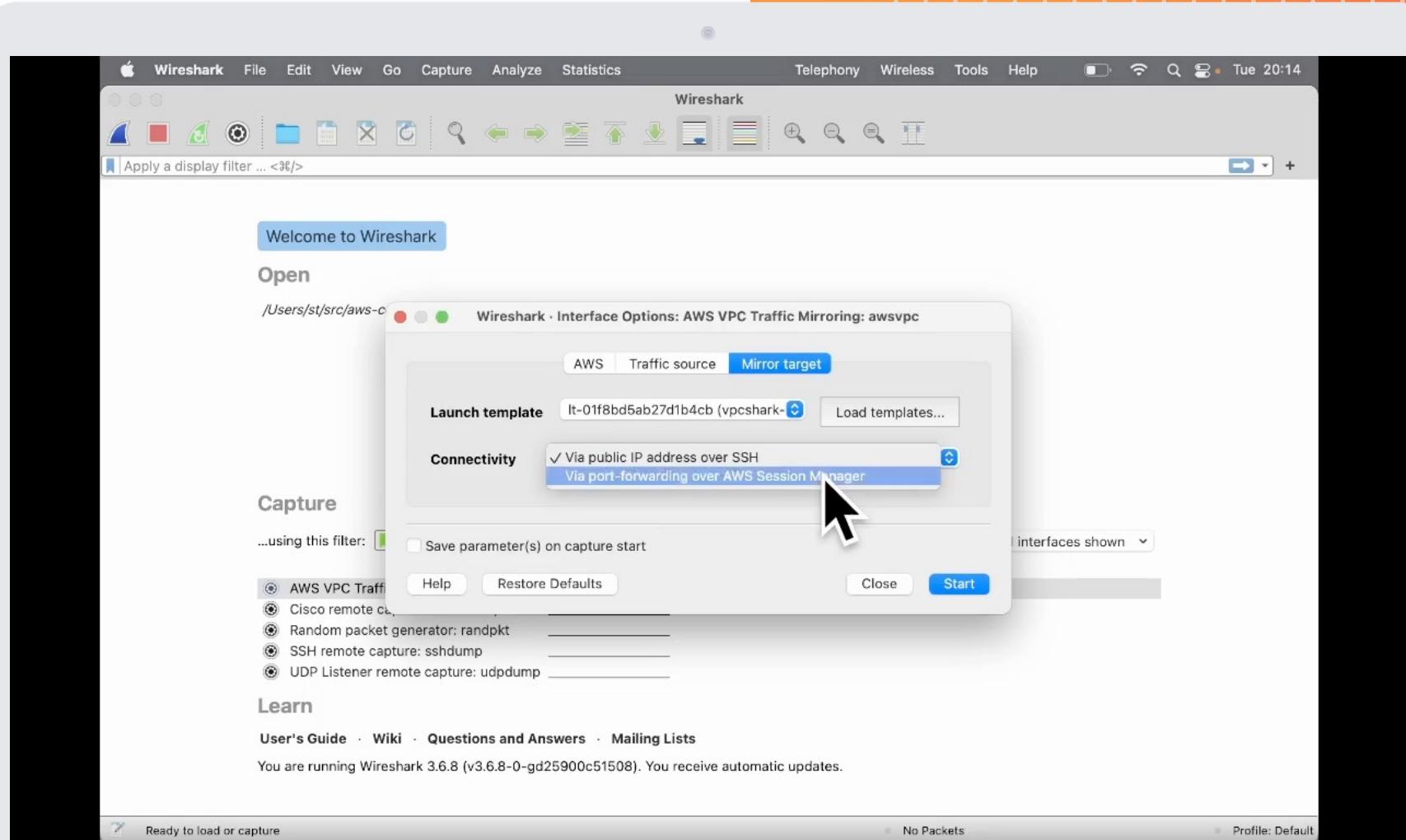
<https://github.com/aidansteele/flowdog>
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



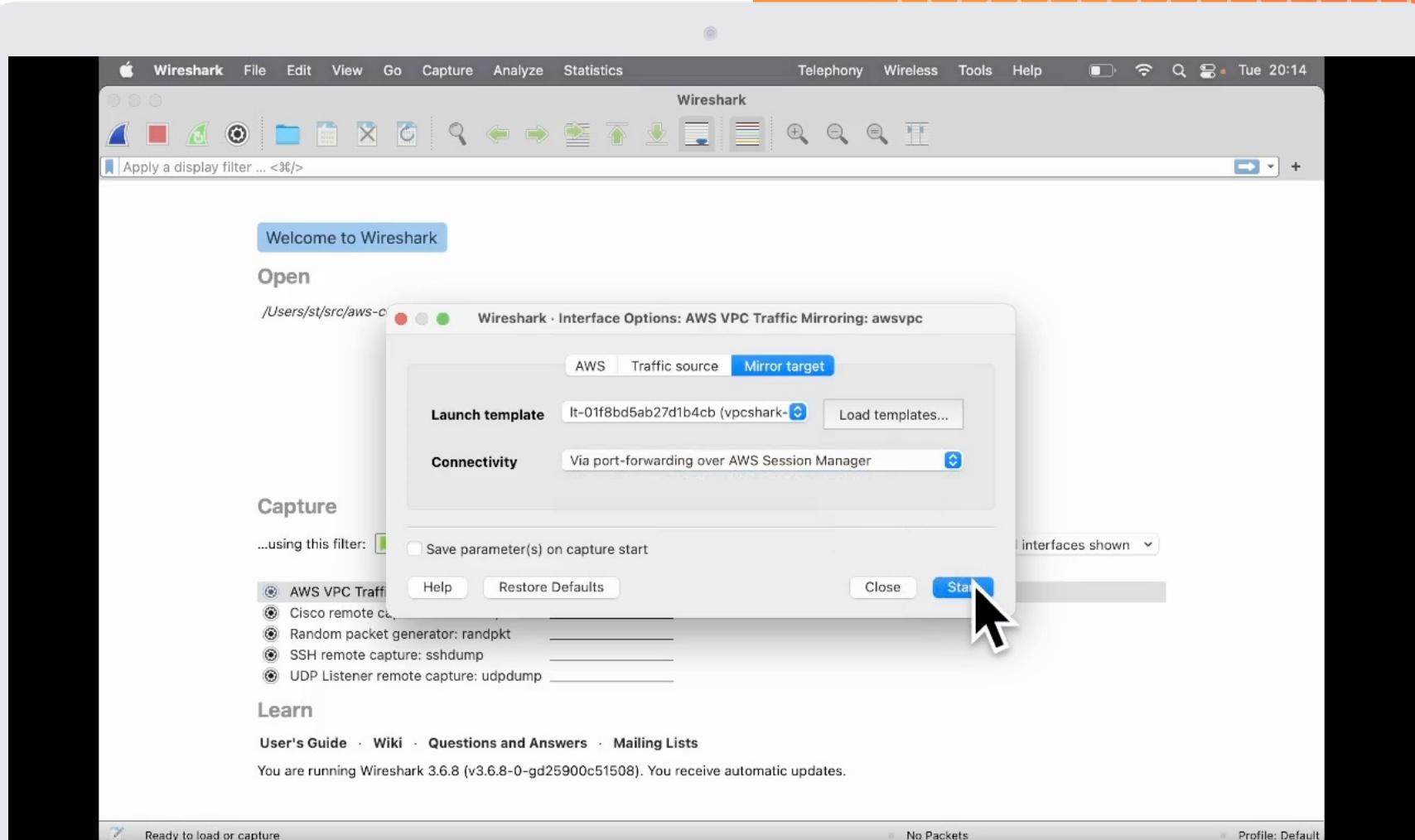
https://github.com/aidansteele/flowdog
https://github.com/aidansteele/vpcshark (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



Welcome to Wireshark

Open /Users/st/src/aws-c Wireshark - Interface Options: AWS VPC Traffic Mirroring: awsvpc

Capture ...using this filter: Save parameter(s) on capture start

AWS VPC Traffic Cisco remote capture Random packet generator: randpkt SSH remote capture: sshdump UDP Listener remote capture: udpgdump

Learn User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.8 (v3.6.8-0-gd25900c51508). You receive automatic updates.

Ready to load or capture No Packets Profile: Default

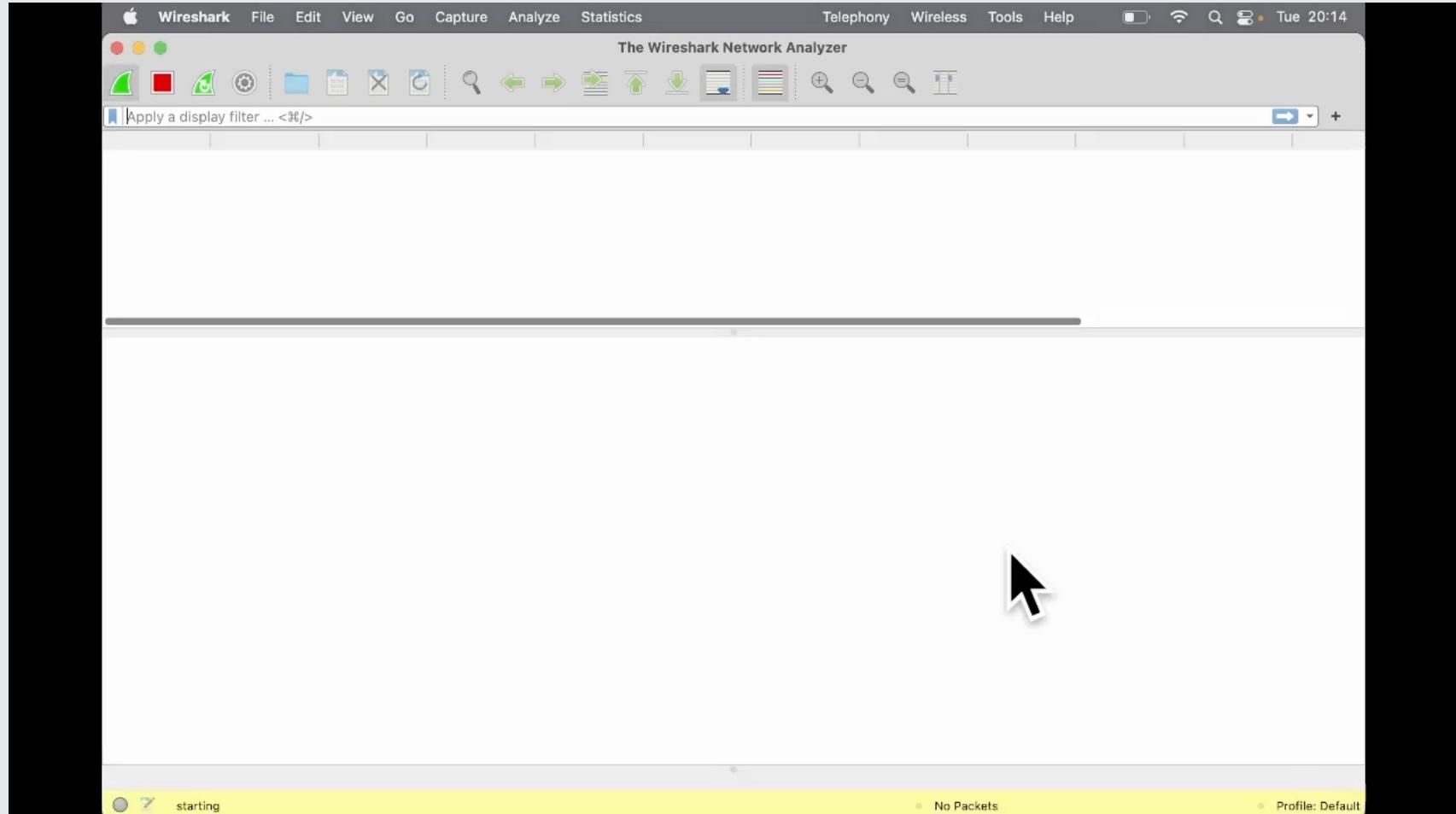
<https://github.com/aidansteele/flowdog>
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



<https://github.com/aidansteele/flowdog>

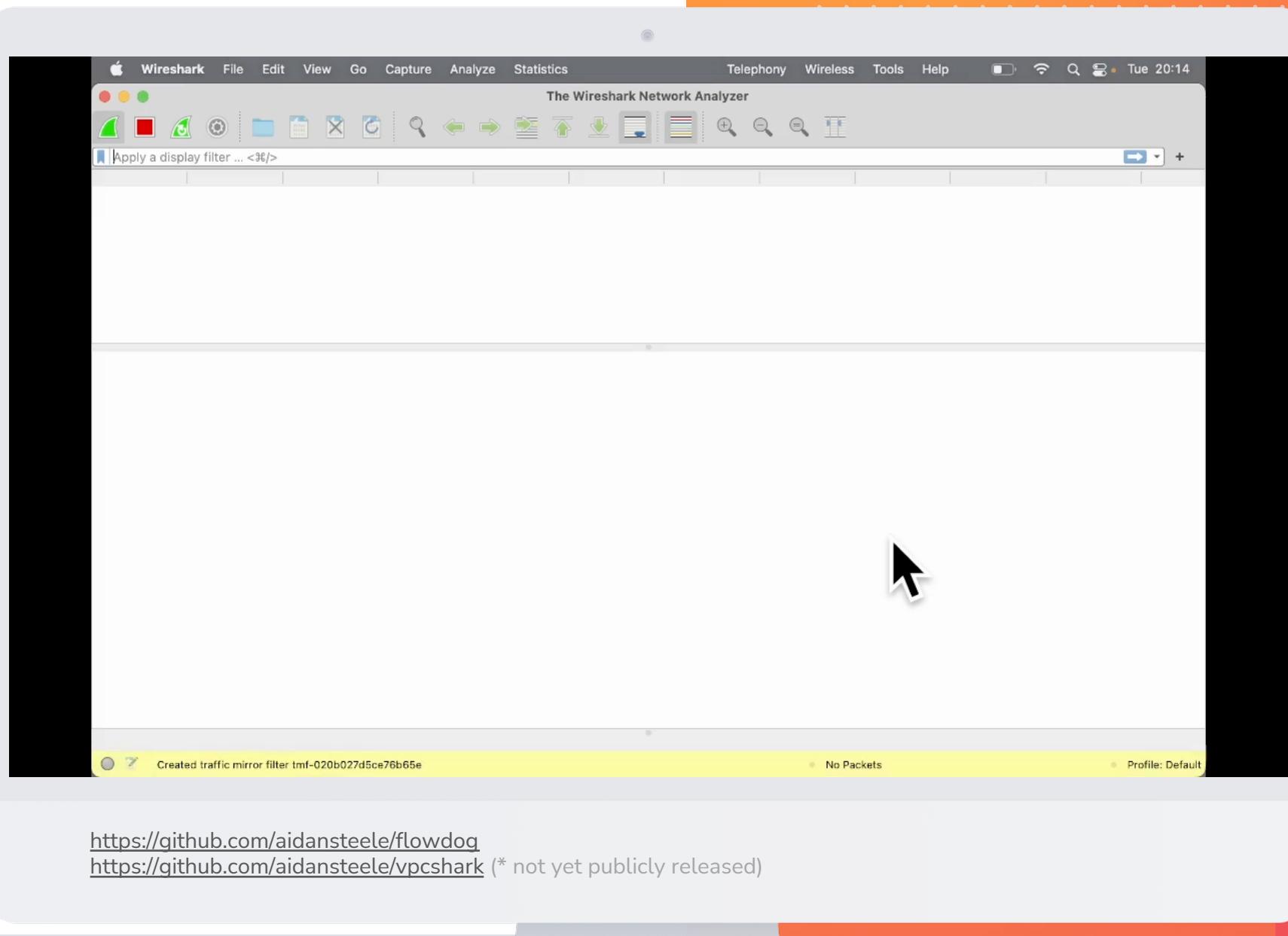
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



The screenshot shows the Wireshark Network Analyzer interface. The title bar reads "Wireshark" and "The Wireshark Network Analyzer". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a date/time stamp "Tue 20:14". The toolbar contains various icons for file operations like Open, Save, and Print. A search bar at the top says "Apply a display filter ... <36/>". The main pane is completely blank, showing no network traffic. A mouse cursor is visible in the bottom right corner of the main window area. The status bar at the bottom displays the message "Created traffic mirror filter tmf-020b027d5ce76b65e" on the left, "No Packets" in the center, and "Profile: Default" on the right.

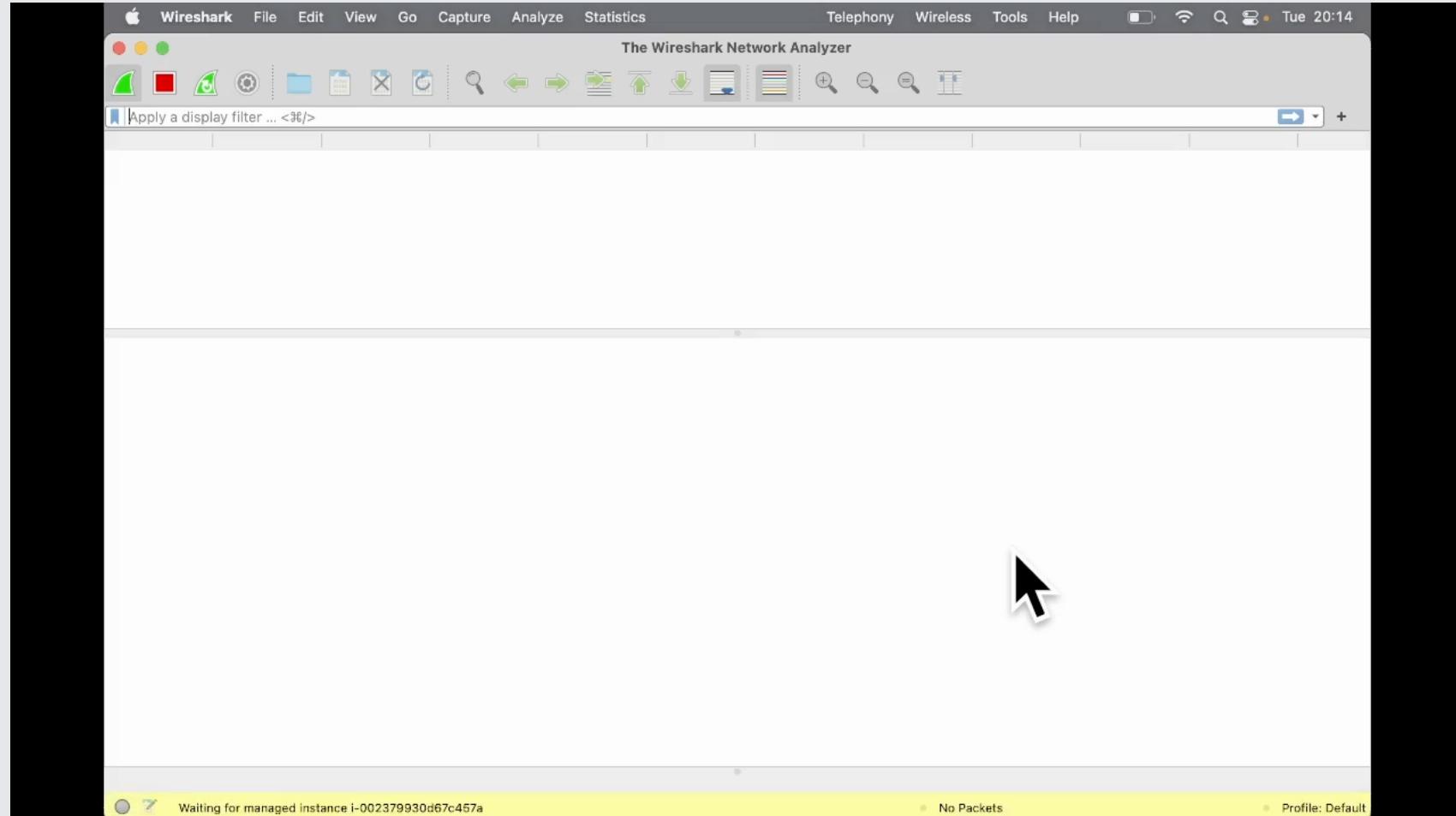
<https://github.com/aidansteele/flowdog>
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



<https://github.com/aidansteele/flowdog>

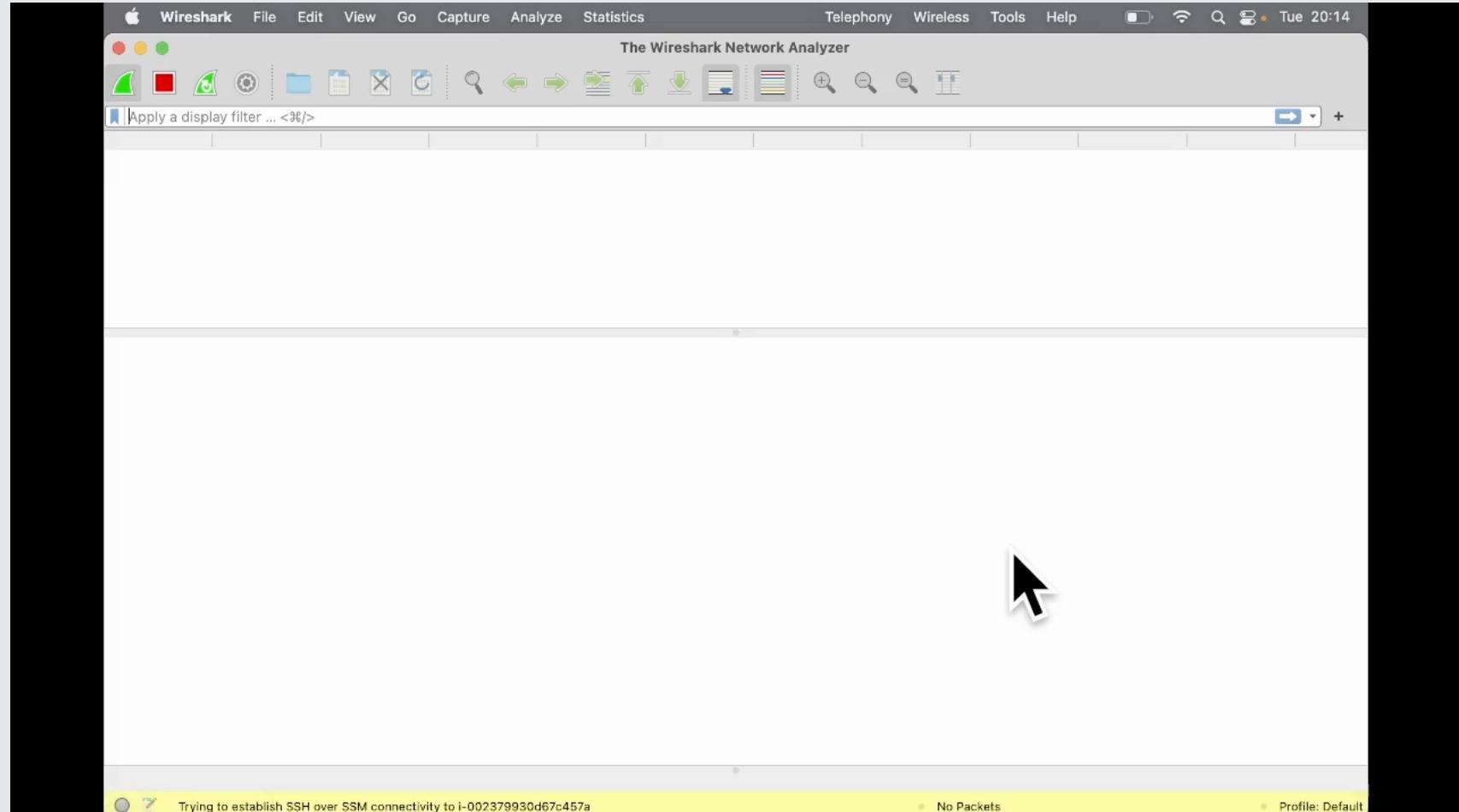
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



<https://github.com/aidansteele/flowdog>

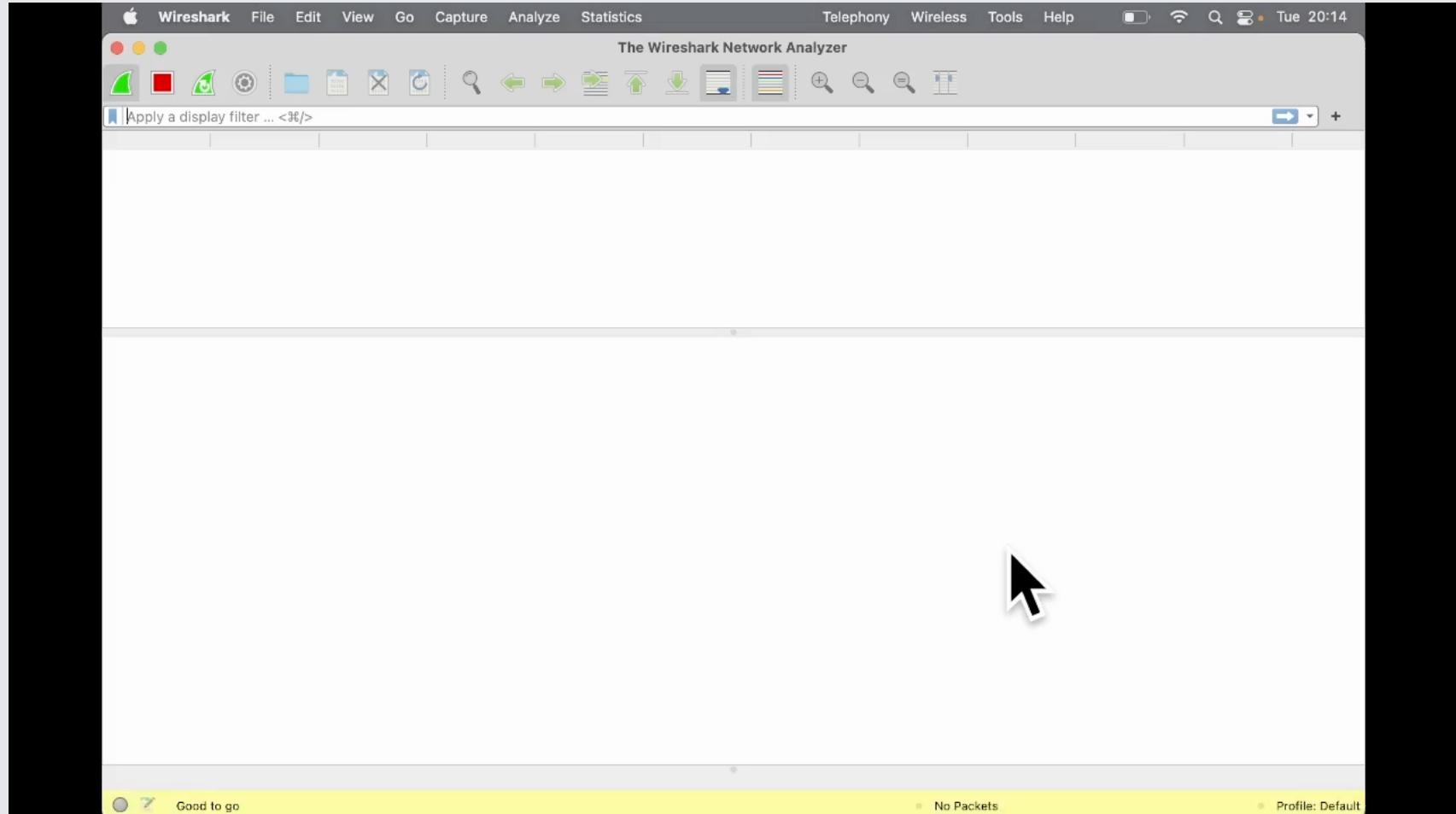
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



<https://github.com/aidansteele/flowdog>

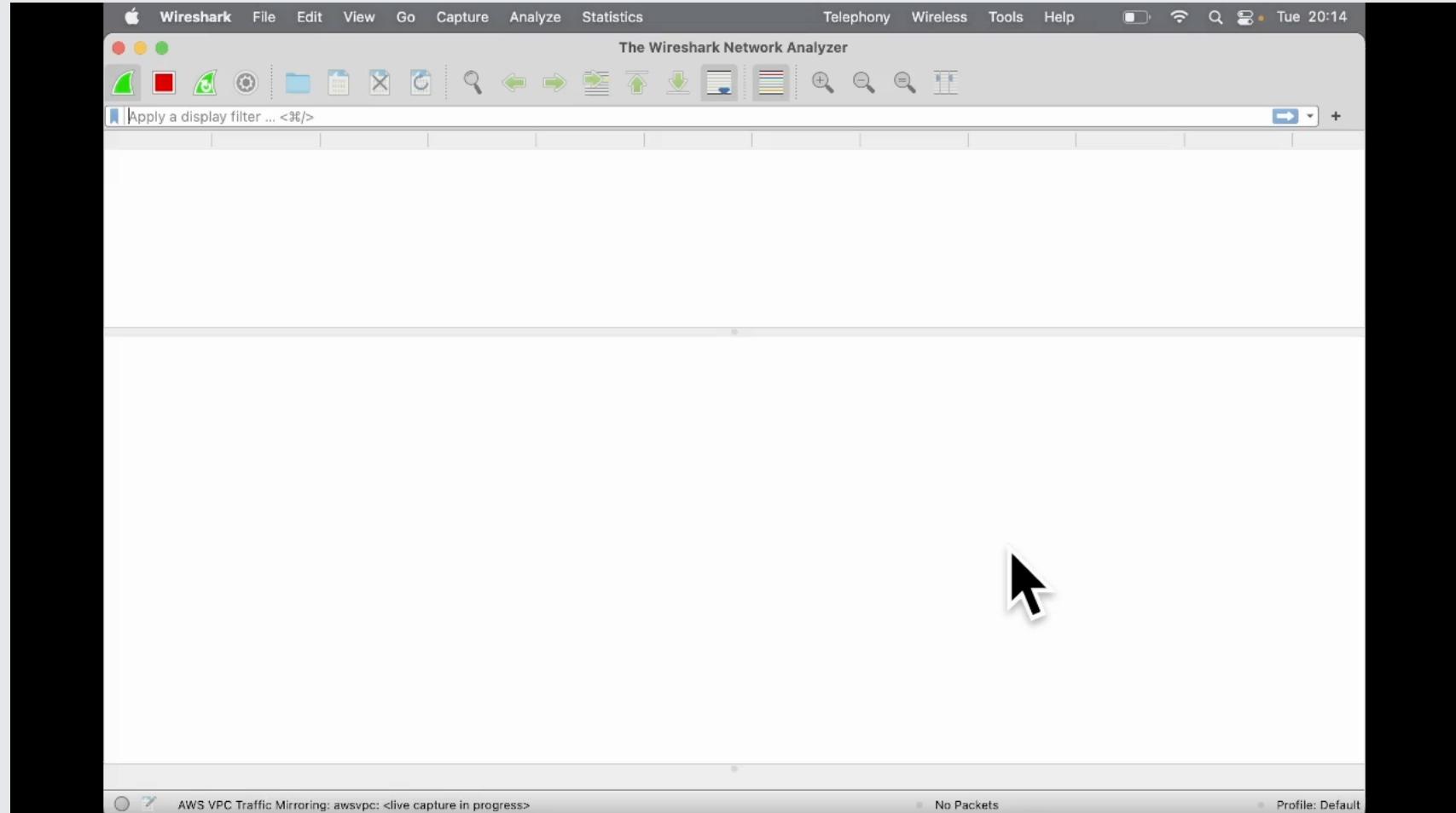
<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

Can it be easier?

- Aidan Steele's projects
 - flowdogshark (GWLB)
 - vpcshark *
- More concept studies than for production



Aidan W Steele
 @_steele Follows you



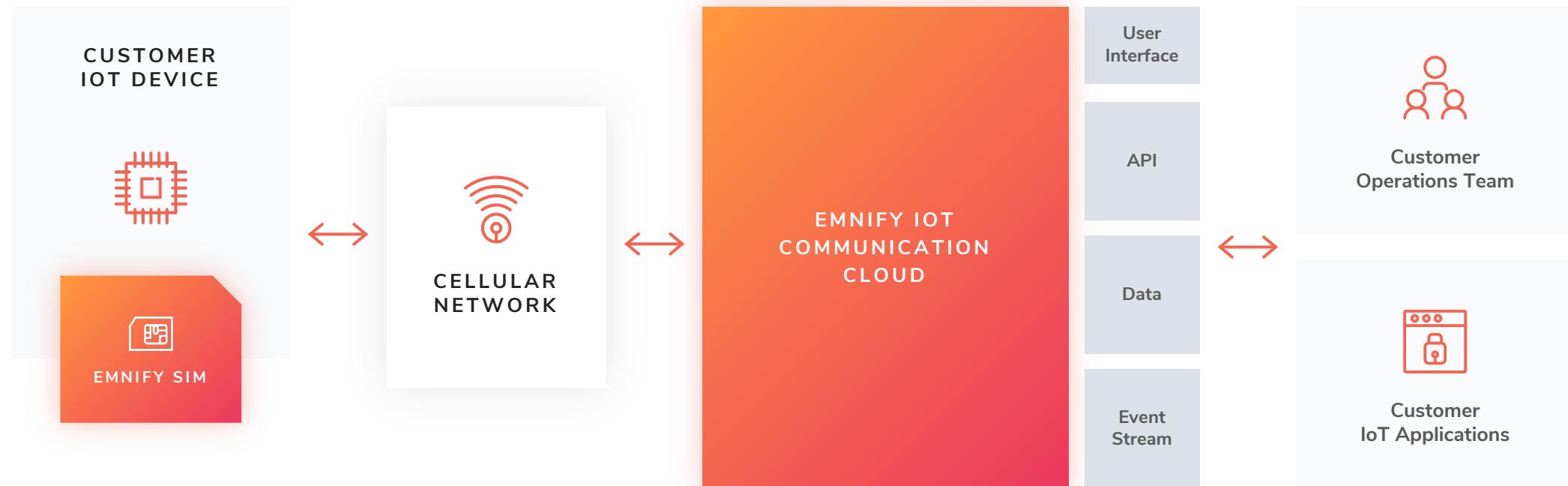
<https://github.com/aidansteele/flowdog>

<https://github.com/aidansteele/vpcshark> (* not yet publicly released)

When nothing helps...
Ask your AWS Account Team

THANKS Karl!

EMnify IoT Communication Cloud



| Your Trouble Shooters

Dr. Steffen Gebert

- Director Technology, Infrastructure
- @StGebert



Wolfgang Schäfer

- Senior Core Network Engineer
- @wo_wue



Learn from our mistakes!

- IaC definition of the setup used in this talk
 - Terraform
 - incl. Reachability Analyzer and Traffic Mirroring
- github.com/EMnify/



The screenshot shows a GitHub repository page for 'EMnify / aws-community-day-2022-network-troubleshooting'. The repository is public and contains 28 commits. The commits are listed below, showing changes made over the past few days, including enabling private DNS, setting up traffic mirroring, and adding a VPC reachability analyzer. The repository has 0 stars and 8 forks. It includes sections for About, Releases, Packages, and Contributors.

Commit	Description	Time Ago
wbwork enable private dns on vpc endpoint	enable private dns on vpc endpoint	20 hours ago
modules	enable private dns on vpc endpoint	20 hours ago
.gitignore	Initial commit	21 days ago
.pre-commit-co...	Initial version - find the mistake!	21 days ago
.terraform-version	tfenv support	yesterday
.terraform.lock.hcl	update .terraform.lock.hcl	yesterday
LICENSE	Initial commit	21 days ago
README.md	more on packet mirroring	yesterday
main.tf	add flow logs	2 days ago
metrics.tf	metrics for TGW	yesterday
outputs.tf	nicer outputs	yesterday
packet-mirrror...	more on packet mirroring	yesterday
provider.tf	Cleanup	21 days ago
vpc-reachability...	add VPC reachability analyzer	2 days ago

One More Try

Oh.. Layer 8 issues 😊

Session ID: 0cf74f20200b6d600 Instance ID: i-0cf74f20200b6d600
Terminate

```
$ curl --connect-timeout 5 pcbicvz9x6-vpce-05e857f78d9d1b62f.execute-api.us-east-1.amazonaws.com
curl: (28) Connection timed out after 5000 milliseconds
$ curl --connect-timeout 5 https://pcbicvz9x6-vpce-05e857f78d9d1b62f.execute-api.us-east-1.amazonaws.com
{"message": "Forbidden"}$
```



Agenda

- 1. Problem Scenario**
- 2. VPC Reachability Analyzer**
- 3. Metrics**
- 4. Flow Logs**
- 5. Packet capture**
- 6. About us**
- 7. Your questions, please!**