

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

Steffen Gebert (@StGebert)

Wolfgang Schäfer (@wo\_wue)

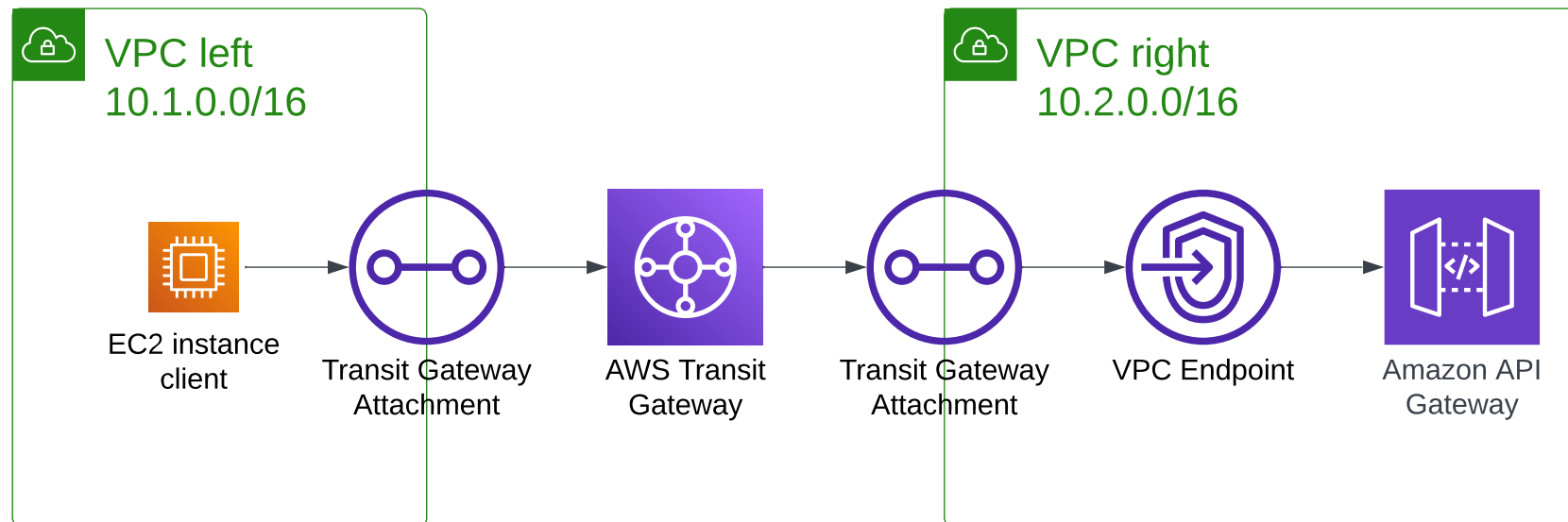
AWS Community Day DACH in Dresden

19.10.2022

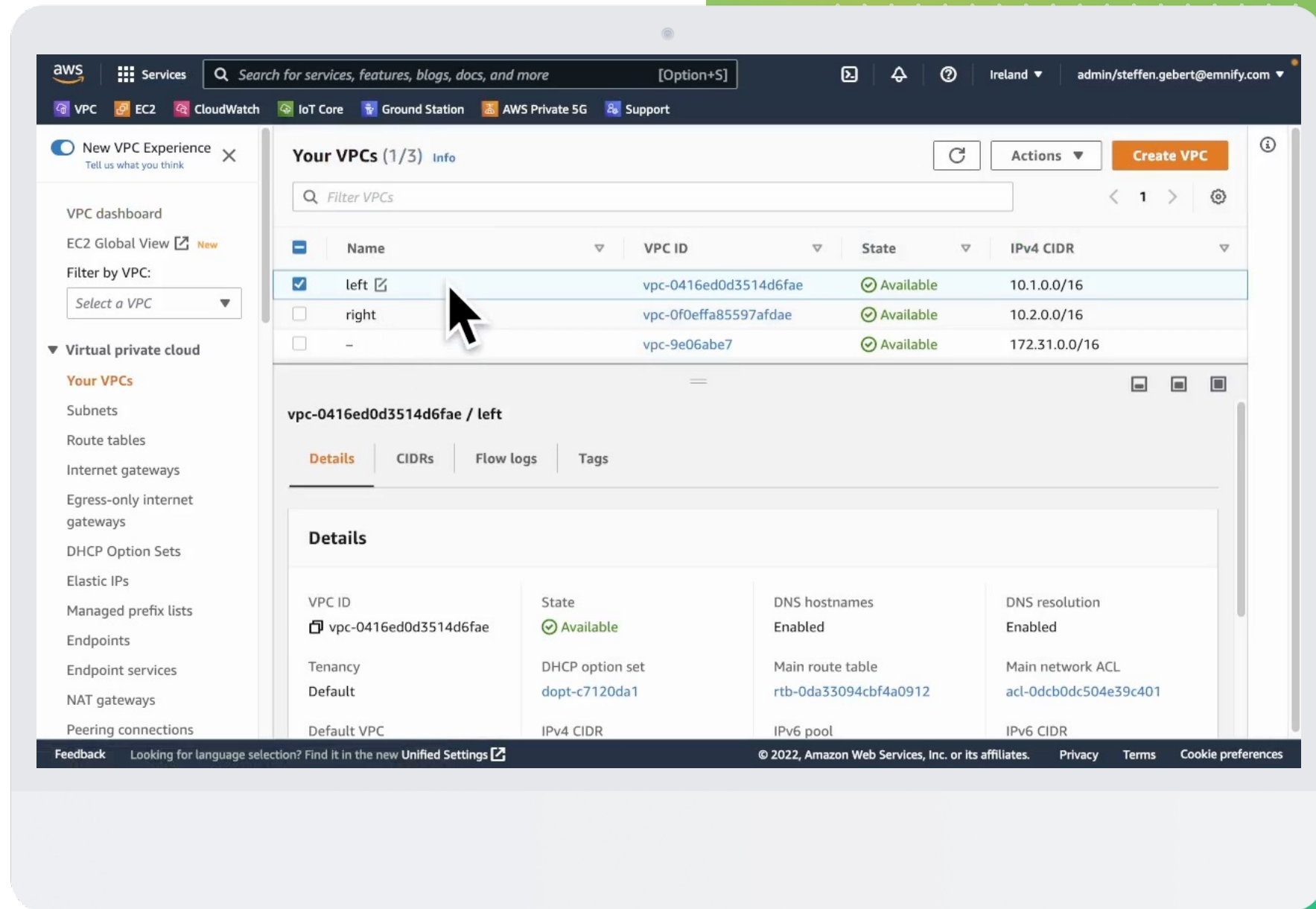
## UNSERE SPONSOREN



# | This is Our Architecture



# Problem



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and various service icons. The left sidebar contains a navigation menu with options like 'VPC dashboard', 'EC2 Global View', and 'Virtual private cloud'. The main content area displays 'Your VPCs (1/3)' with a table listing VPCs. A mouse cursor is pointing at the 'left' VPC in the table. Below the table, the details for the selected VPC (vpc-0416ed0d3514d6fae) are shown, including its state (Available), DNS settings, and route table.

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

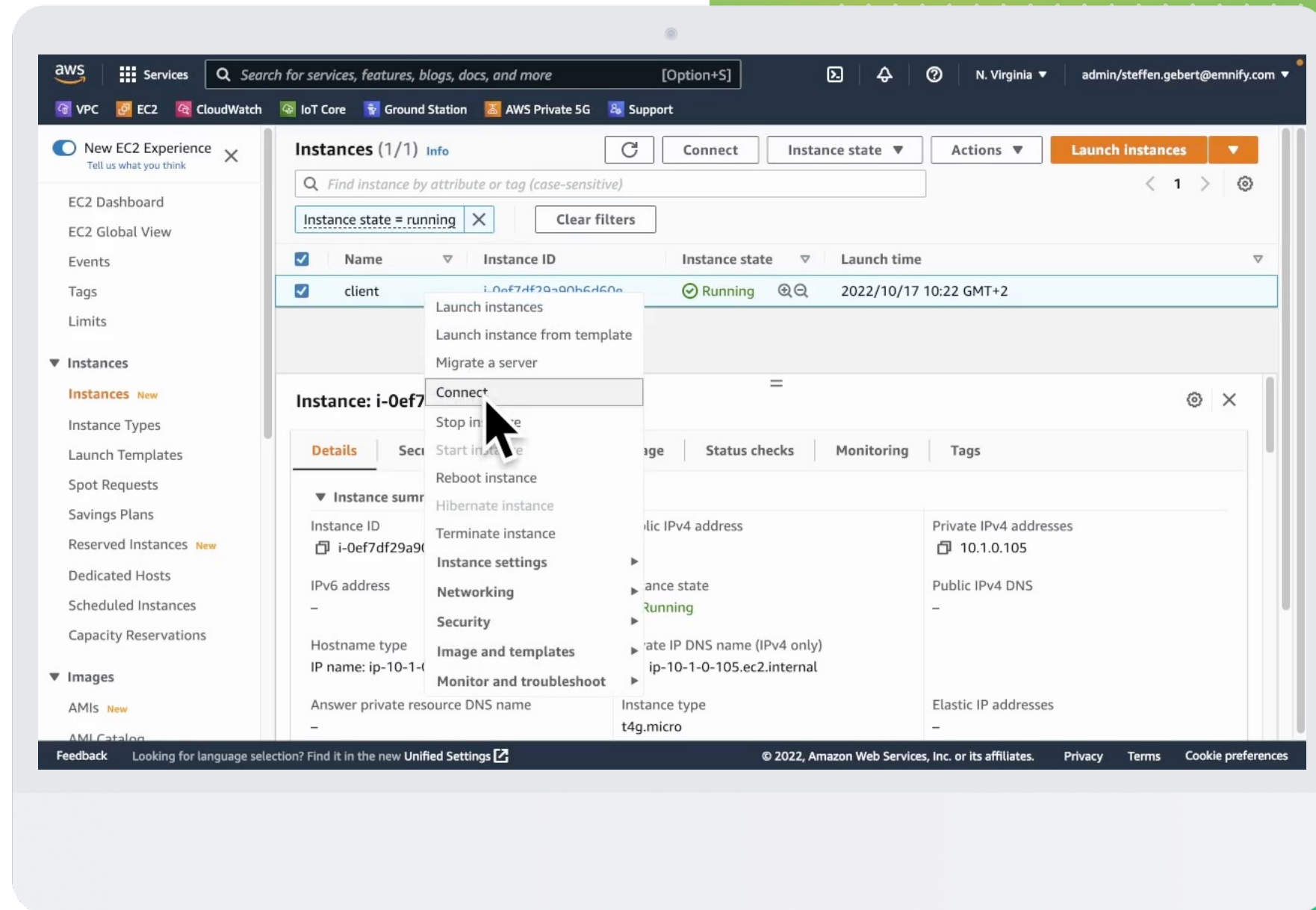
**vpc-0416ed0d3514d6fae / left**

**Details**

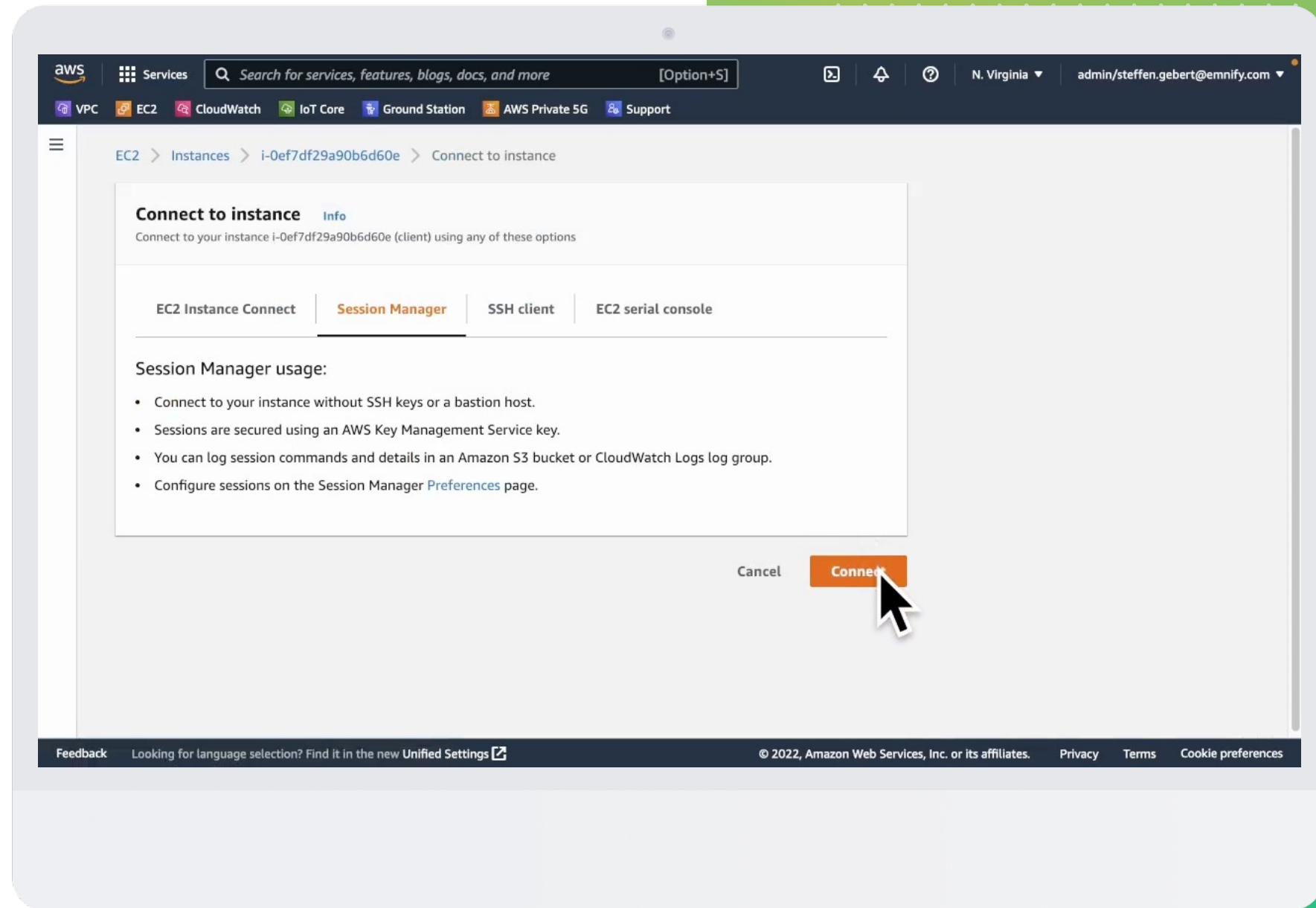
VPC ID	State	DNS hostnames	DNS resolution
vpc-0416ed0d3514d6fae	Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-c7120da1	rtb-0da33094cbf4a0912	acl-0dcb0dc504e39c401
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR



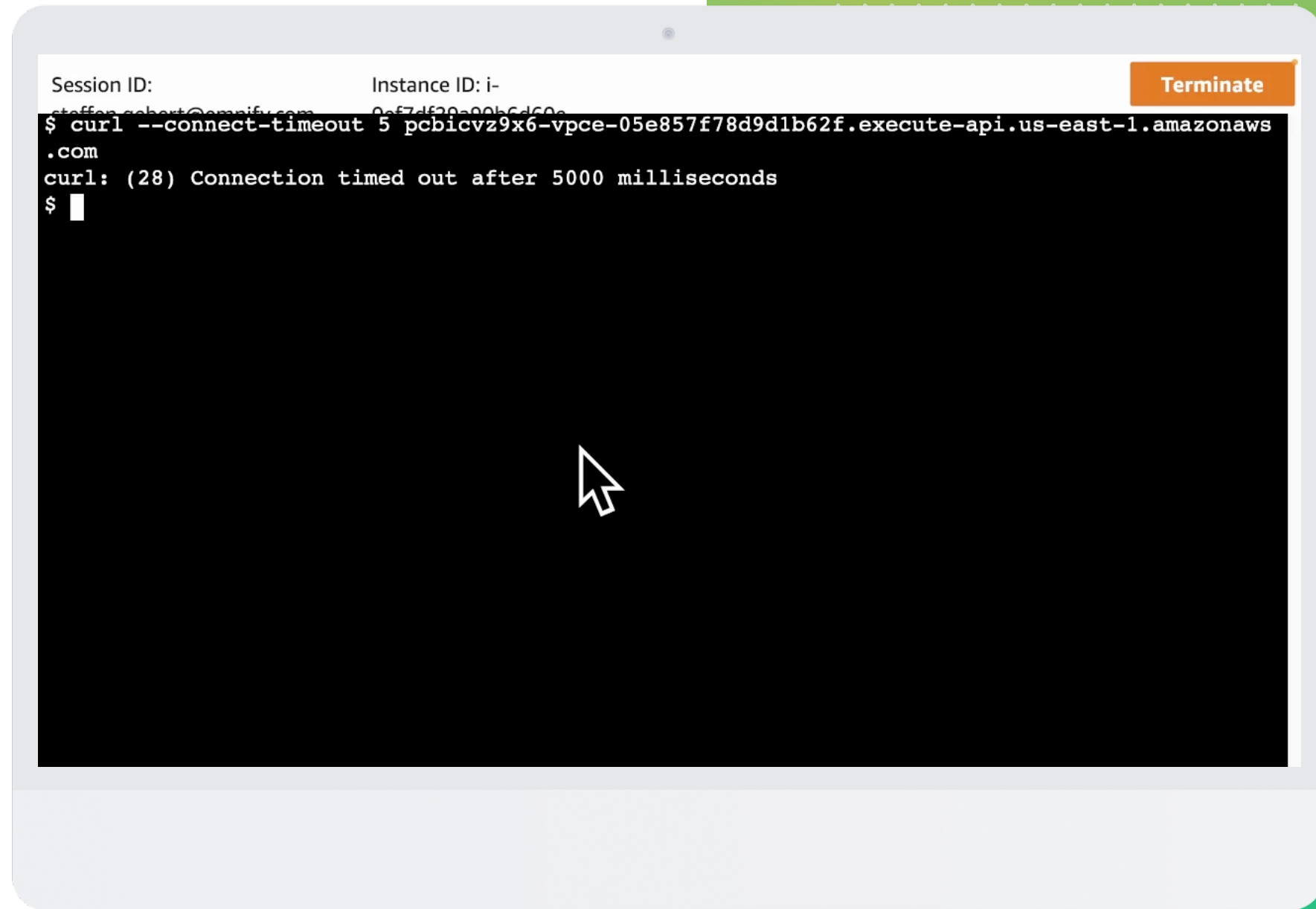
# Problem



# Problem



# I Problem



# Problem

The screenshot displays the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and user information. The left sidebar shows the 'Instances' section with a list of instance types and launch templates. The main content area shows a table of instances with the following data:

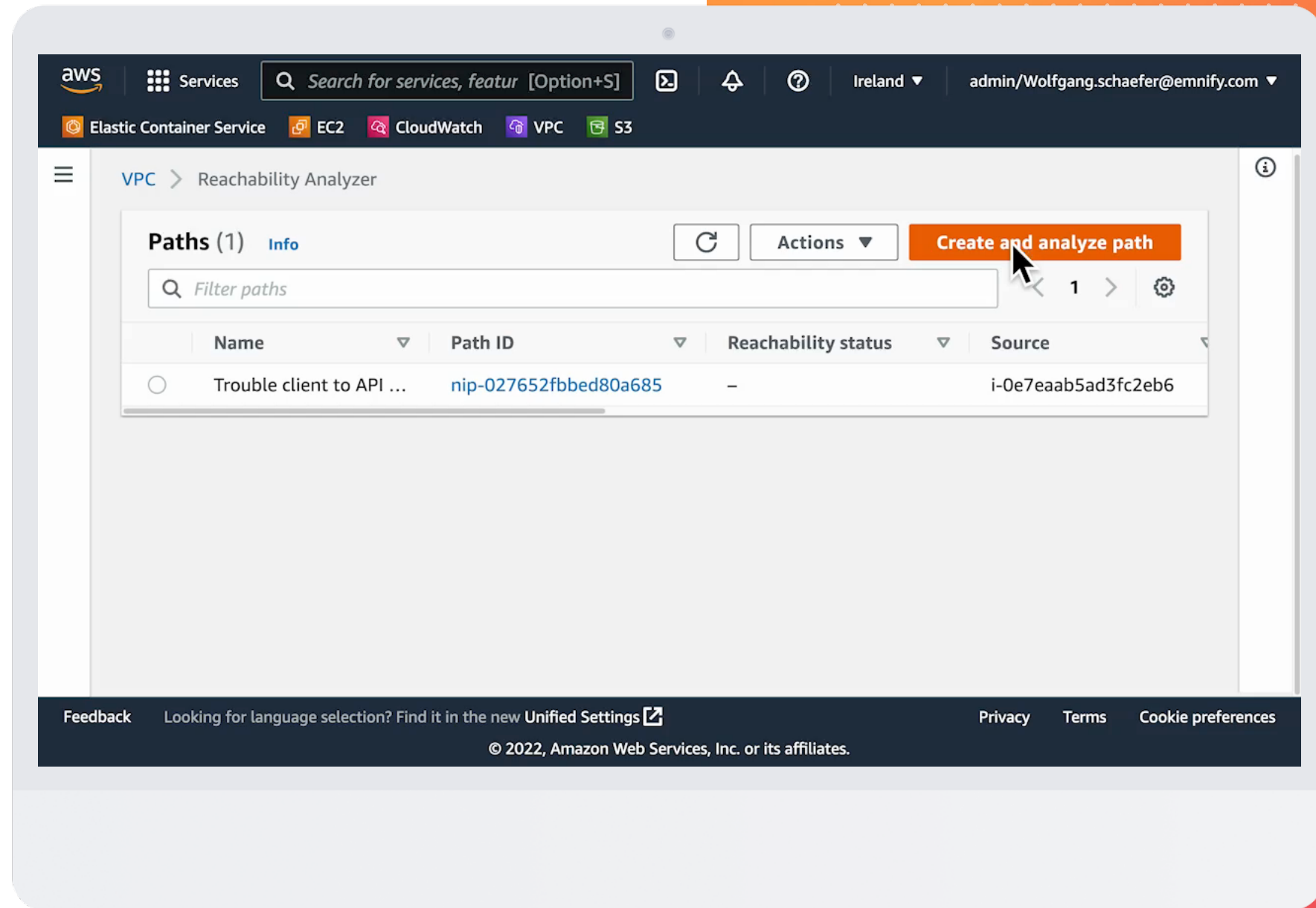
Name	Instance ID	Instance state	Launch time
client	i-0ef7df29a90b6d60e	Running	2022/10/17 10:22 GMT+2

The 'client' instance is selected, and the 'Networking' tab is active. The Networking details section shows the following information:

- Public IPv4 address: -
- Private IPv4 addresses: 10.1.0.105
- Public IPv4 DNS: -
- Private IP DNS name (IPv4 only): ip-10-1-0-105.ec2.internal
- Subnet ID: subnet-05e7ad652202c76c5 (left-...)
- IPv6 addresses: -
- VPC ID: vpc-047f9166a49868d20 (left)
- Secondary private IPv4 addresses: -

A message at the top of the Networking tab states: "You can now check network connectivity with Reachability Analyzer." with a button to "Run Reachability Analyzer".

# VPC Reachability Analyzer



# VPC Reachability Analyzer

The screenshot shows the AWS VPC Reachability Analyzer console. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar with the placeholder 'Search for services, features [Option+S]', and icons for notifications, help, and a dropdown for the region 'Ireland'. The user's email 'admin/Wolfgang.schaefer@emnify.com' is displayed on the right. Below the navigation bar, a row of service icons includes Elastic Container Service, EC2, CloudWatch, VPC, and S3. The main content area contains the following form fields:

- Source type:** A dropdown menu with 'Instances' selected.
- Source:** A dropdown menu with the ID 'i-0e7eaab5ad3fc2eb6' selected.
- Source IP address - optional:** A text input field containing '192.0.2.1'.
- Destination type:** A dropdown menu with 'VPC Endpoints' selected.
- Destination:** A dropdown menu with the ID 'vpce-032a75ff4fbb16bb9' selected.
- Destination port - optional:** A text input field containing '80'. Below this field is a note: 'Number must be between 0 and 65535'.
- Protocol:** A dropdown menu with 'TCP' selected. Above this field is the text 'Use the appropriate protocol'.

The bottom of the console features a dark footer with links for 'Feedback', 'Looking for language selection? Find it in the new Unified Settings' (with an external link icon), 'Privacy', 'Terms', and 'Cookie preferences'. A copyright notice '© 2022, Amazon Web Services, Inc. or its affiliates.' is centered at the bottom.

# VPC Reachability Analyzer

The screenshot displays the AWS VPC Reachability Analyzer console. At the top, the AWS navigation bar shows the 'Services' menu, a search bar, and the user's profile. Below the navigation bar, a horizontal list of services includes Elastic Container Service, EC2, CloudWatch, VPC, and S3. The main content area is divided into sections. The first section contains a text input field with the value '80', a message 'Number must be between 0 and 65535', a 'Protocol' dropdown menu set to 'TCP', and a note 'Use the appropriate protocol'. The second section, titled 'Add tags - optional', explains that a tag is a label for an AWS resource and provides a table to manage tags. The table has two columns: 'Key' and 'Value - optional'. It shows one tag with the key 'Name' and the value 'demo', and a 'Remove' button next to it. Below the table is an 'Add new tag' button. At the bottom right of the form, there are 'Cancel' and 'Create and analyze path' buttons. The footer of the console includes links for 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences', along with a copyright notice for Amazon Web Services, Inc. or its affiliates.

aws Services Search for services, featur [Option+S] Ireland admin/Wolfgang.schaefer@emnify.com

Elastic Container Service EC2 CloudWatch VPC S3

80

Number must be between 0 and 65535

Protocol

Use the appropriate protocol

TCP

**Add tags - optional**

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
Name	demo	Remove

Add new tag

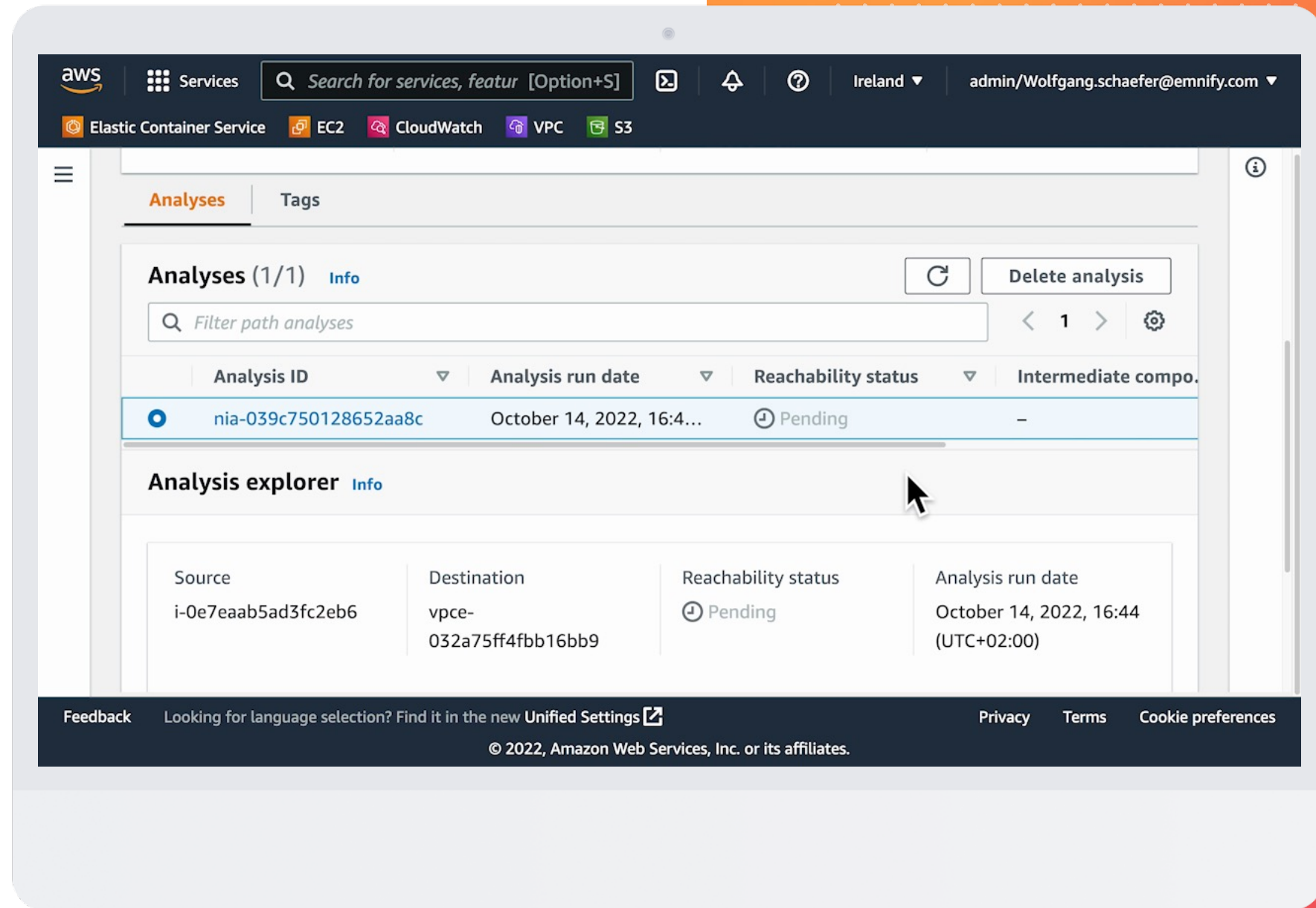
Cancel Create and analyze path

Feedback Looking for language selection? Find it in the new Unified Settings Privacy Terms Cookie preferences

© 2022, Amazon Web Services, Inc. or its affiliates.



# VPC Reachability Analyzer





# VPC Reachability Analyzer

The screenshot displays the AWS VPC Reachability Analyzer interface. At the top, the AWS navigation bar includes the logo, a 'Services' menu, a search bar, and regional/user information (Ireland, admin/Wolfgang.schaefer@emnify.com). Below this, a horizontal bar lists services: Elastic Container Service, EC2, CloudWatch, VPC, and S3. The main content area is titled 'Analyses (1/1)' and includes a search bar for 'Filter path analyses'. A table lists the analysis details:

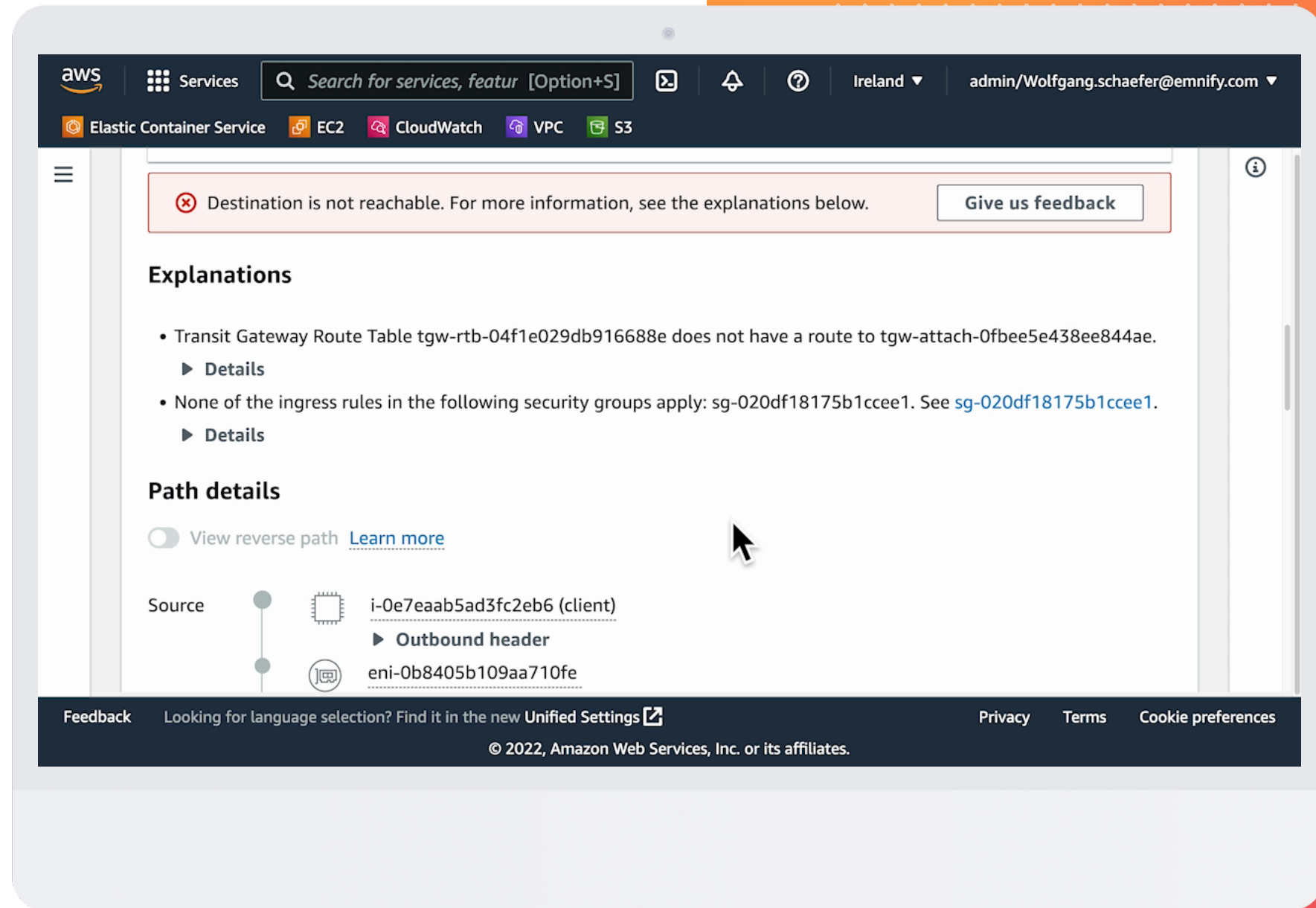
Analysis ID	Analysis run date	Reachability status	Intermediate compo.
nia-039c750128652aa8c	October 14, 2022, 16:4...	⊗ Not reachable	-

Below the table is the 'Analysis explorer' section, which provides a detailed view of the selected analysis:

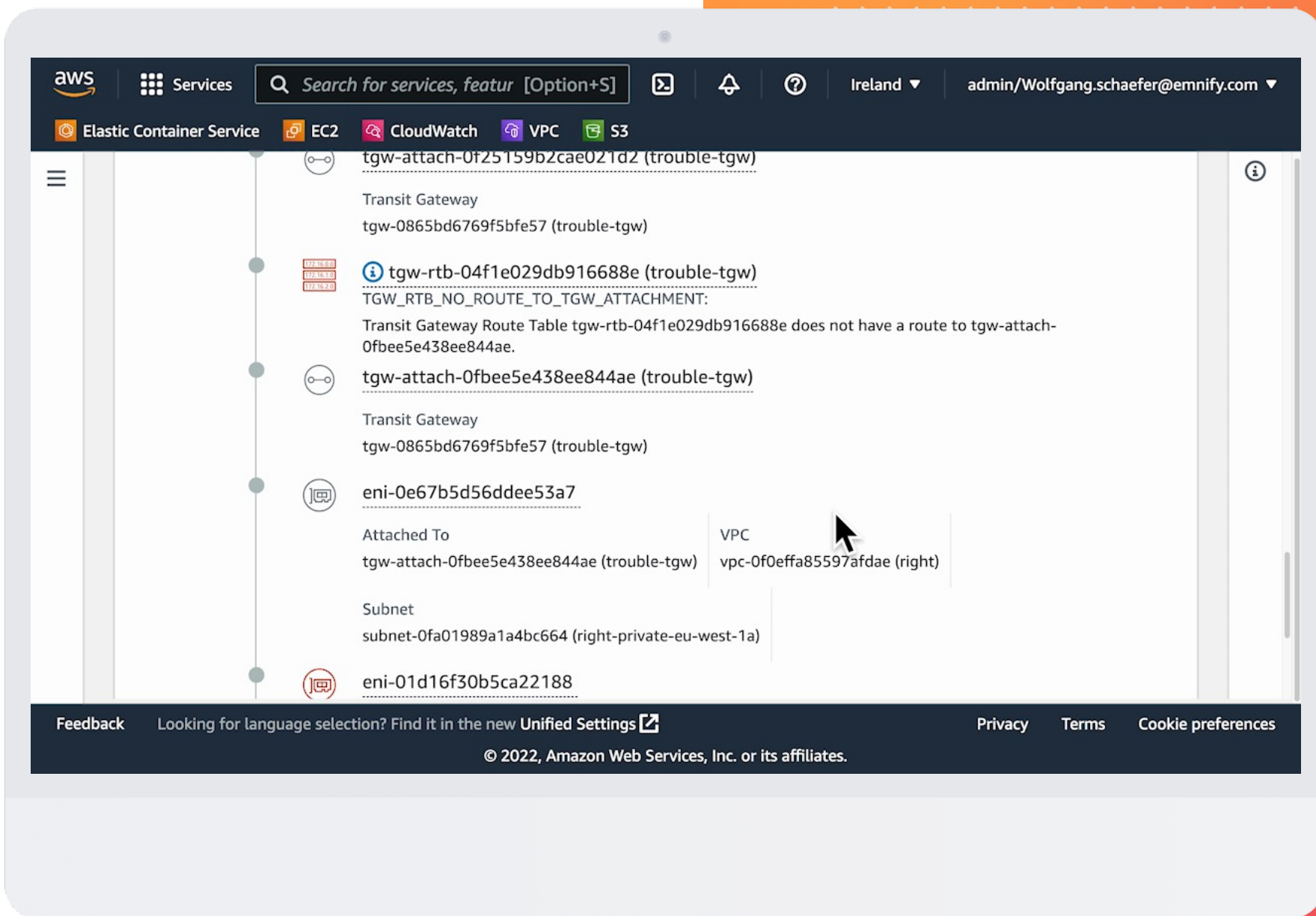
Source	Destination	Reachability status	Analysis run date
i-0e7eaab5ad3fc2eb6	vpce-032a75ff4fbb16bb9	⊗ Not reachable	October 14, 2022, 16:44 (UTC+02:00)

An 'Intermediate component filter' is also visible. The footer contains links for Feedback, Privacy, Terms, and Cookie preferences, along with a copyright notice for Amazon Web Services, Inc. or its affiliates.

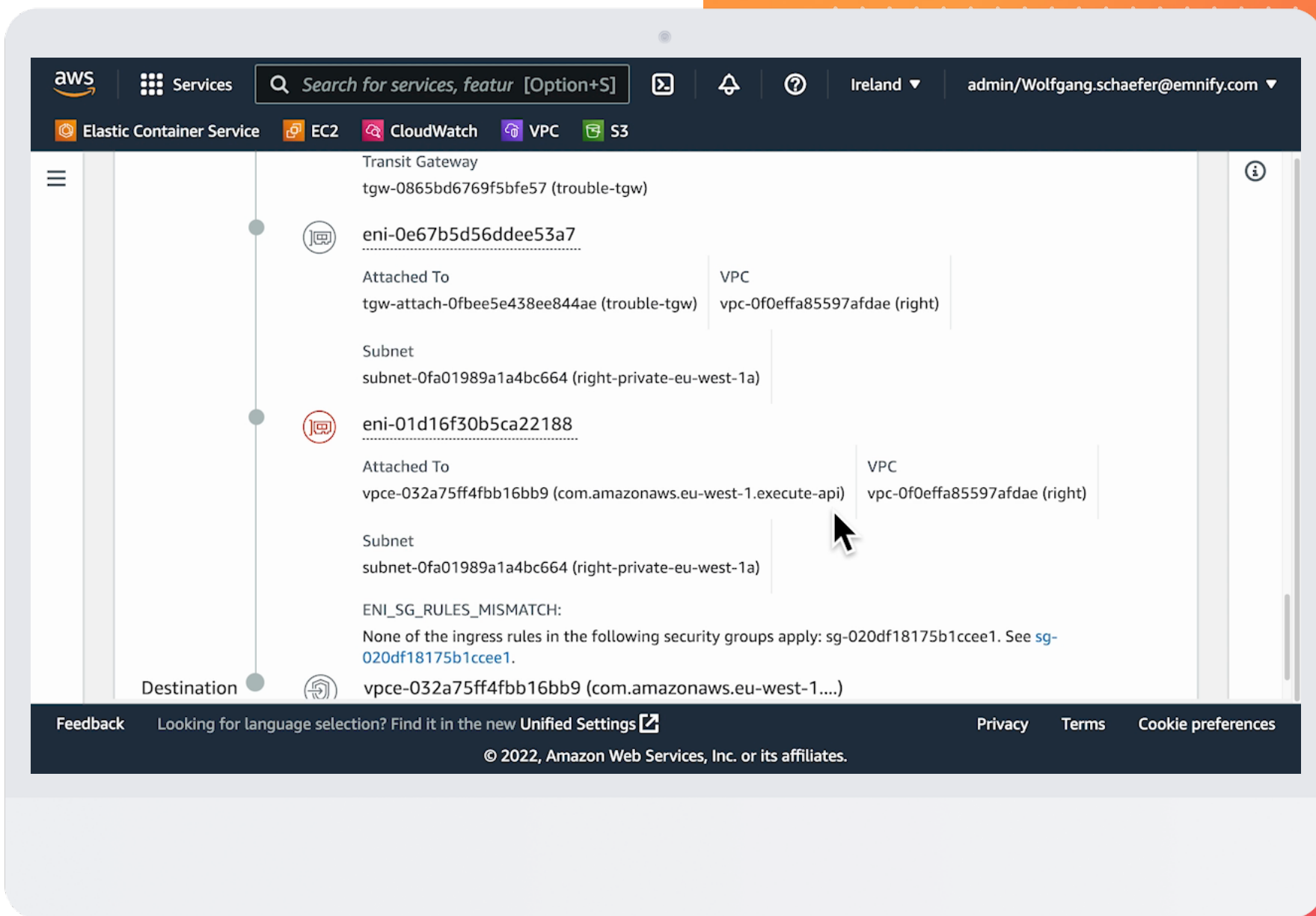
# VPC Reachability Analyzer



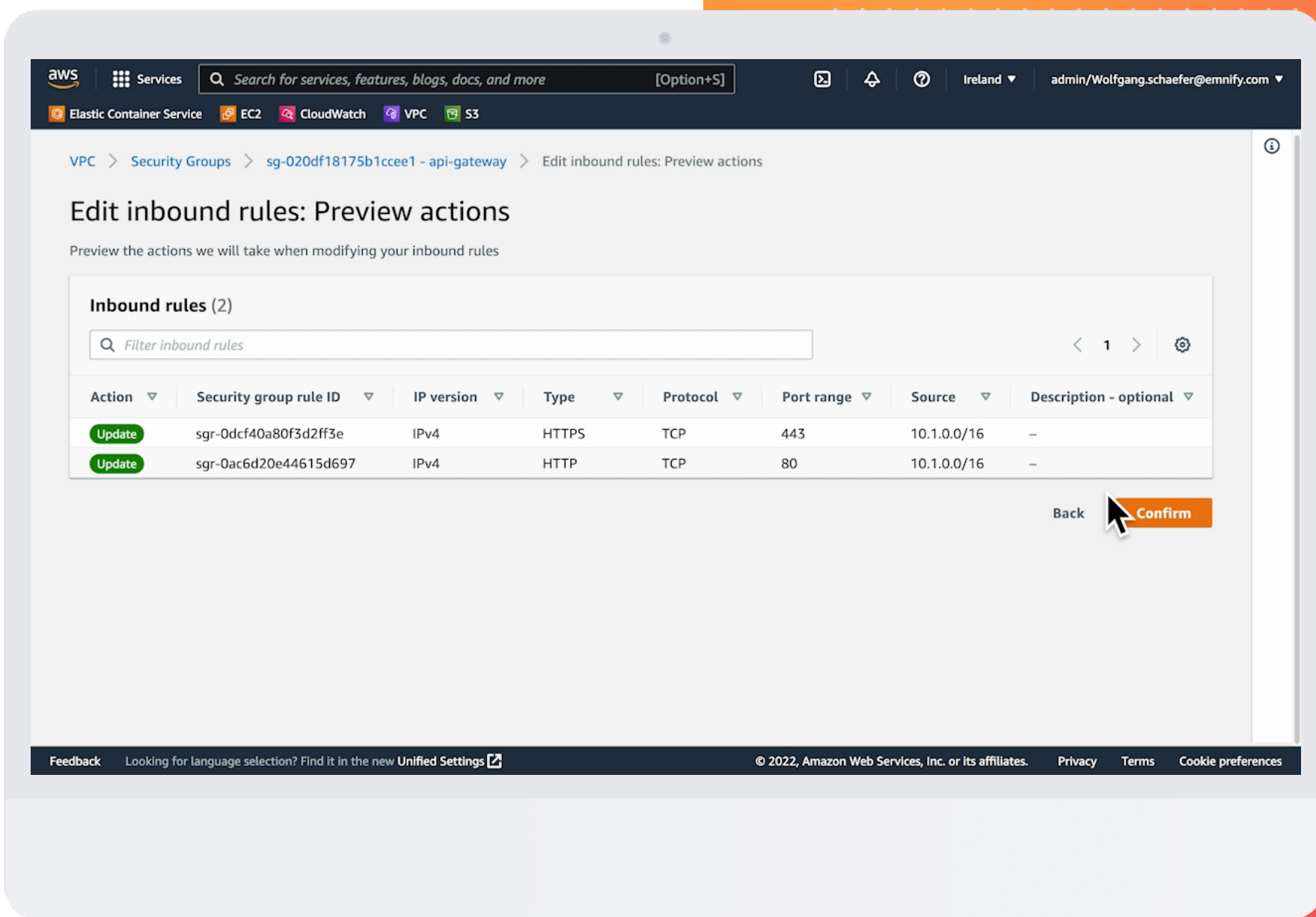
# VPC Reachability Analyzer



# VPC Reachability Analyzer



# Fixing Connectivity



# VPC Reachability Analyzer

The screenshot displays the AWS VPC Reachability Analyzer console. The left sidebar shows the navigation menu with categories like Elastic Container Service, EC2, CloudWatch, VPC, and S3. The main content area shows the details for a specific path (nip-02b2830e744593ca7). The 'Summary' tab is active, displaying a table with path details. The 'Analyses' tab is also visible, showing a list of analyses with columns for Analysis ID, Analysis run date, Reachability status, Intermediate components, and State. The 'Analyze path' button is highlighted with a mouse cursor.

**Summary** [Info](#) Actions ▾ Analyze path

Path ID	Last analysis date	Reachability status	Last analysis status
nip-02b2830e744593ca7	October 14, 2022, 16:44 (UTC+02:00)	⊗ Not reachable	✔ Succeeded
Source	Destination	Destination port	Protocol
i-0e7eaab5ad3fc2eb6	vpce-032a75ff4fbb16bb9	80	TCP

**Analyses** [Tags](#)

**Analyses (1/1)** [Info](#) ↻ Delete analysis

Analysis ID	Analysis run date	Reachability status	Intermediate compo...	State
nia-039c750128652aa8c	October 14, 2022, 16:4...	⊗ Not reachable	–	✔ Succeeded

**Analysis explorer** [Info](#)

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 displays the AWS VPC Reachability Analyzer interface. The left sidebar shows the navigation menu with categories like Security, Network Analysis, DNS firewall, and Network Firewall. The main content area shows the 'Analyses' tab with a table of analysis results. Below this is the 'Analysis explorer' section, which provides a detailed view of a specific analysis, including source and destination information, reachability status, and intermediate component filter.

**Analyses (1/2)**

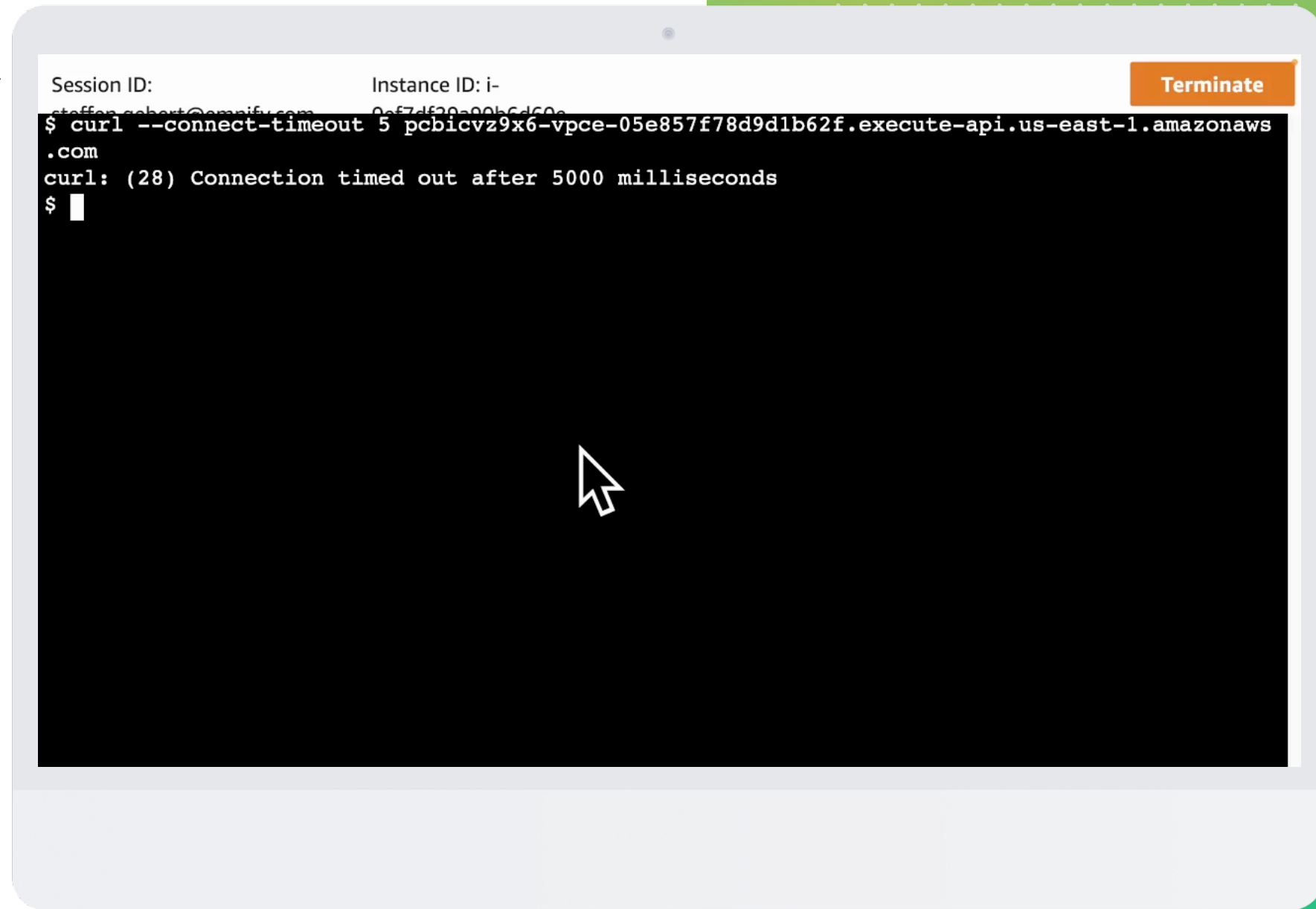
Analysis ID	Analysis run date	Reachability status	Intermediate compo...	State
nia-014ee5113dd80d3d3	October 14, 2022, 16:5...	✓ Reachable	-	✓ Success
nia-039c750128652aa8c	October 14, 2022, 16:4...	✗ Not reachable	-	✓ Success

**Analysis explorer**

Source	Destination	Reachability status	Analysis run date
i-0e7eaab5ad3fc2eb6	vpce-032a75ff4fbb16bb9	✓ Reachable	October 14, 2022, 16:54 (UTC+02:00)

Intermediate component filter: -

# Connectivity Test





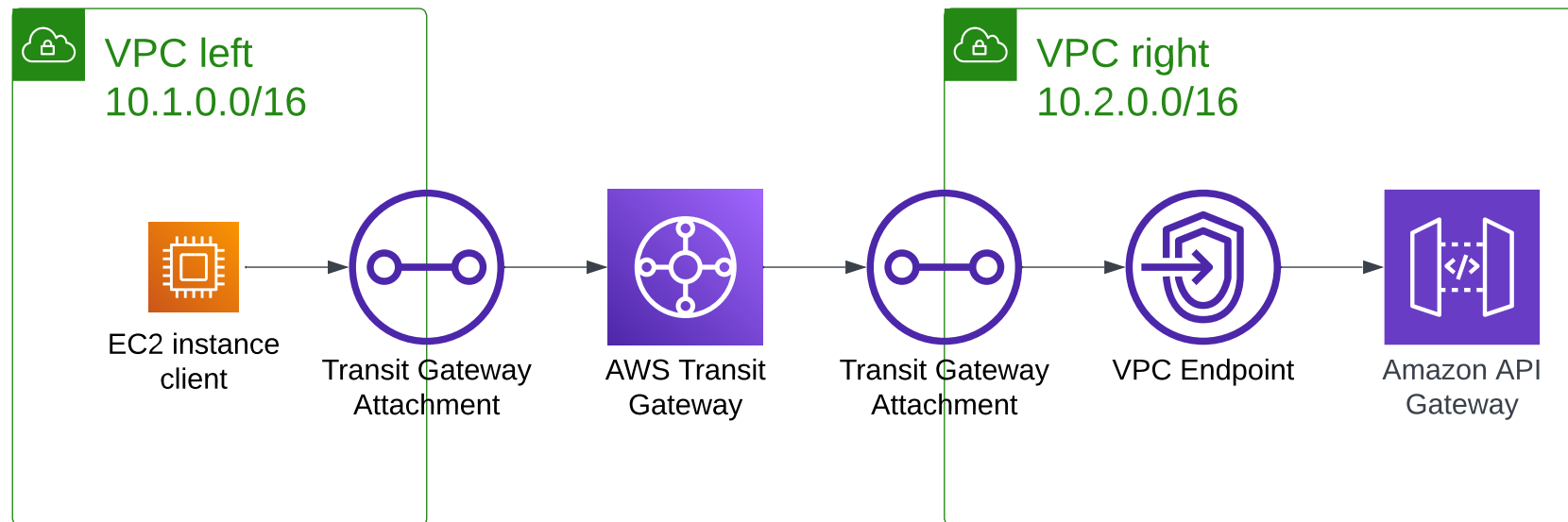


EMnify

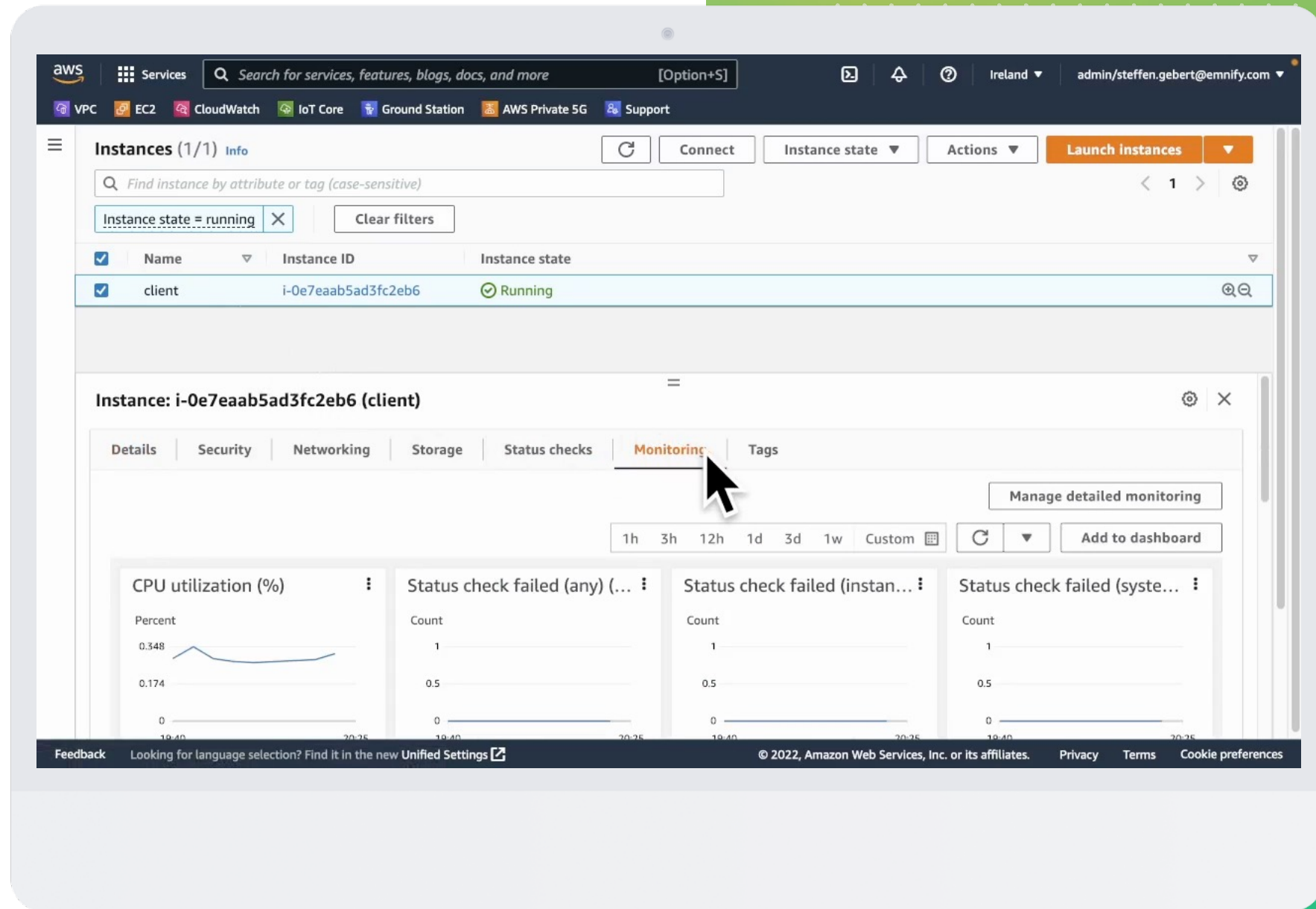
# Metrics



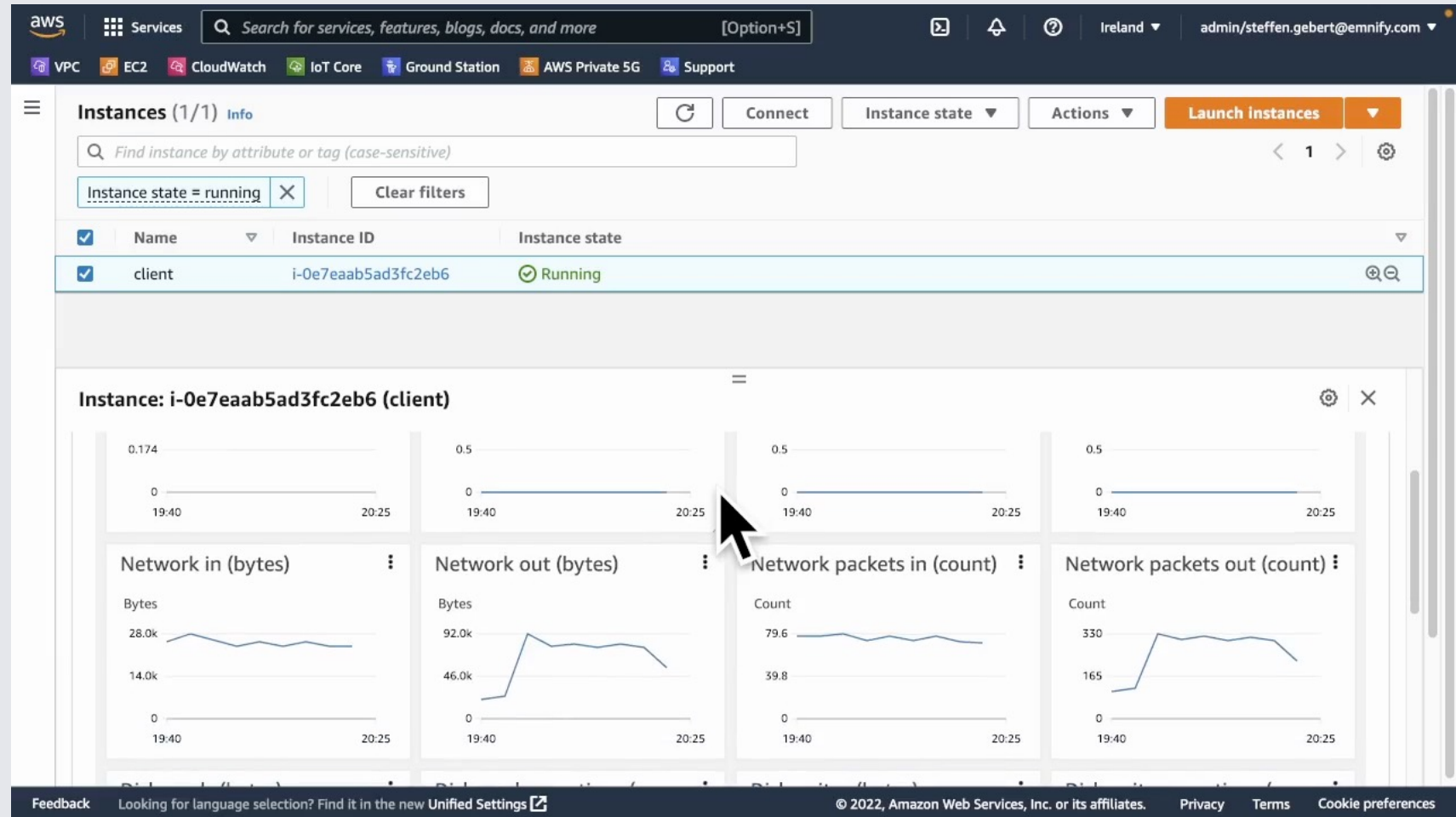
# | This is Our Architecture



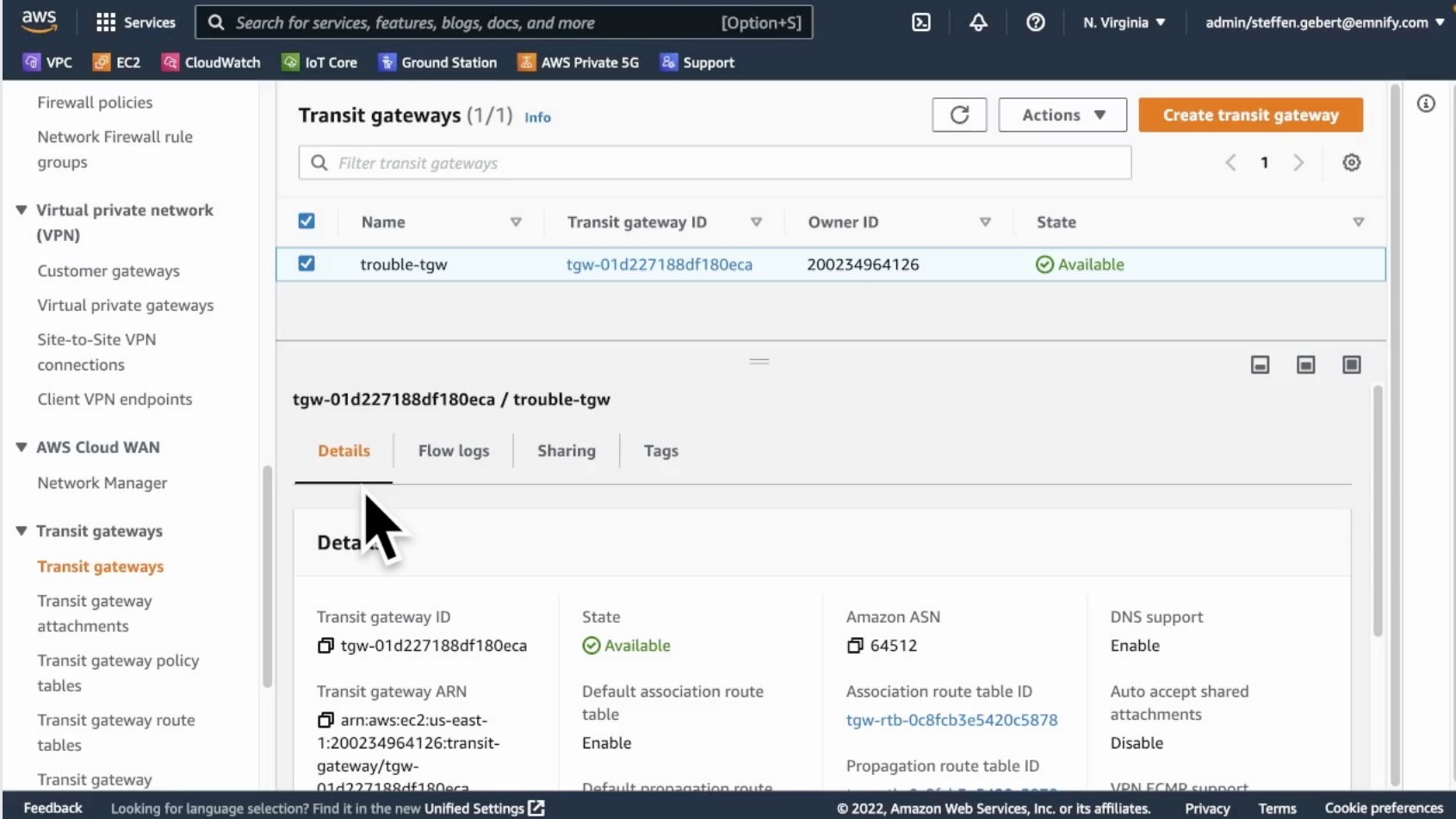
# Metrics



# Metrics



# Metrics Transit GW



The screenshot displays the AWS Management Console interface for Transit Gateways. The left-hand navigation pane includes sections for Firewall policies, Virtual private network (VPN), AWS Cloud WAN, and Transit gateways. The 'Transit gateways' section is expanded, showing options like Transit gateway attachments, policy tables, route tables, and the gateway itself. The main panel, titled 'Transit gateways (1/1)', contains a search bar and a table with one entry: 'trouble-tgw' with ID 'tgw-01d227188df180eca' and Owner ID '200234964126', in an 'Available' state. Below the table, the 'Details' tab for the selected gateway is shown, displaying a grid of key-value pairs for its configuration.

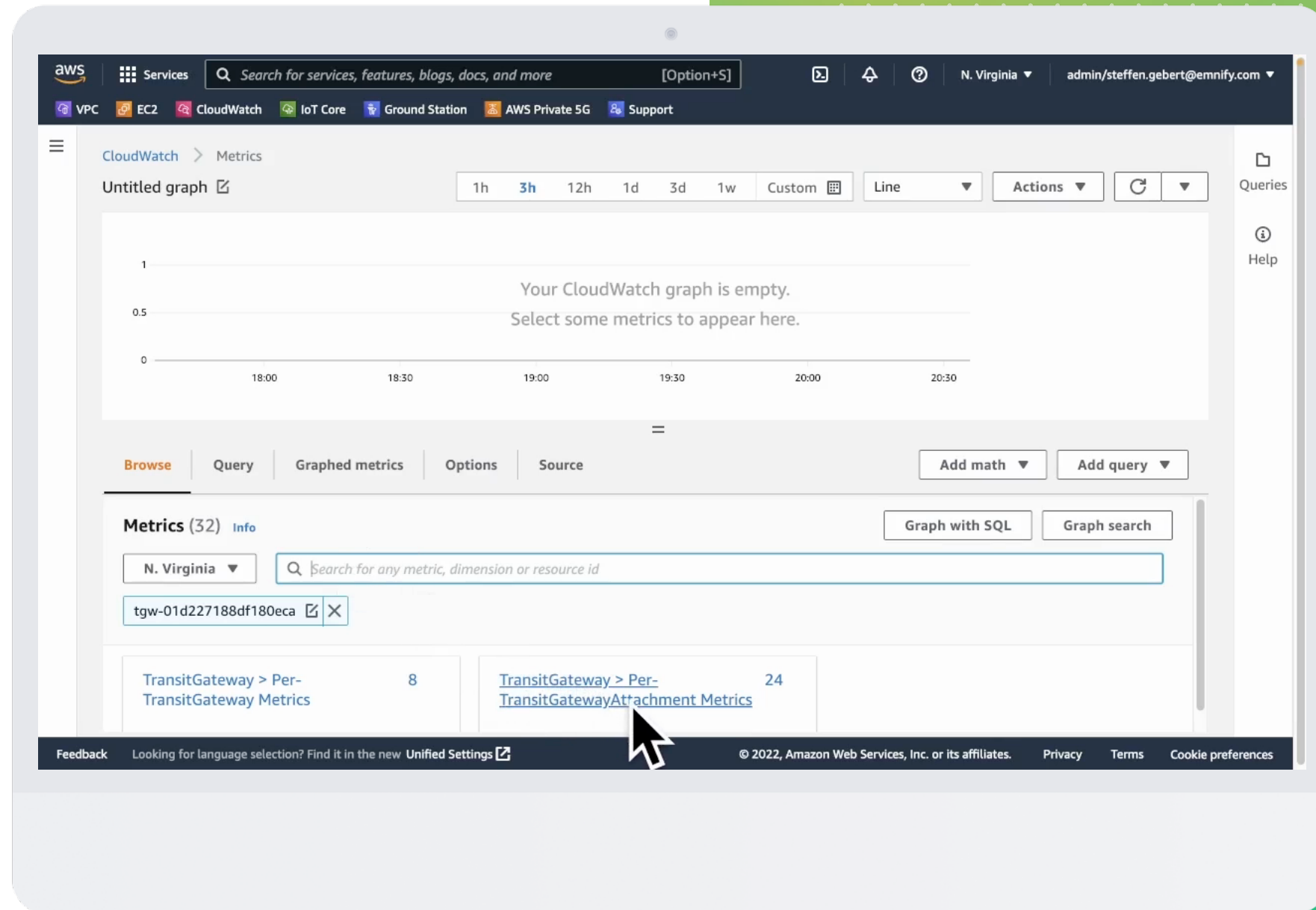
Name	Transit gateway ID	Owner ID	State
trouble-tgw	tgw-01d227188df180eca	200234964126	Available

Transit gateway ID	State	Amazon ASN	DNS support
tgw-01d227188df180eca	Available	64512	Enable
Transit gateway ARN	Default association route table	Association route table ID	Auto accept shared attachments
arn:aws:ec2:us-east-1:200234964126:transit-gateway/tgw-01d227188df180eca	Enable	tgw-rtb-0c8fcb3e5420c5878	Disable
	Default propagation route	Propagation route table ID	VPN ECMP support

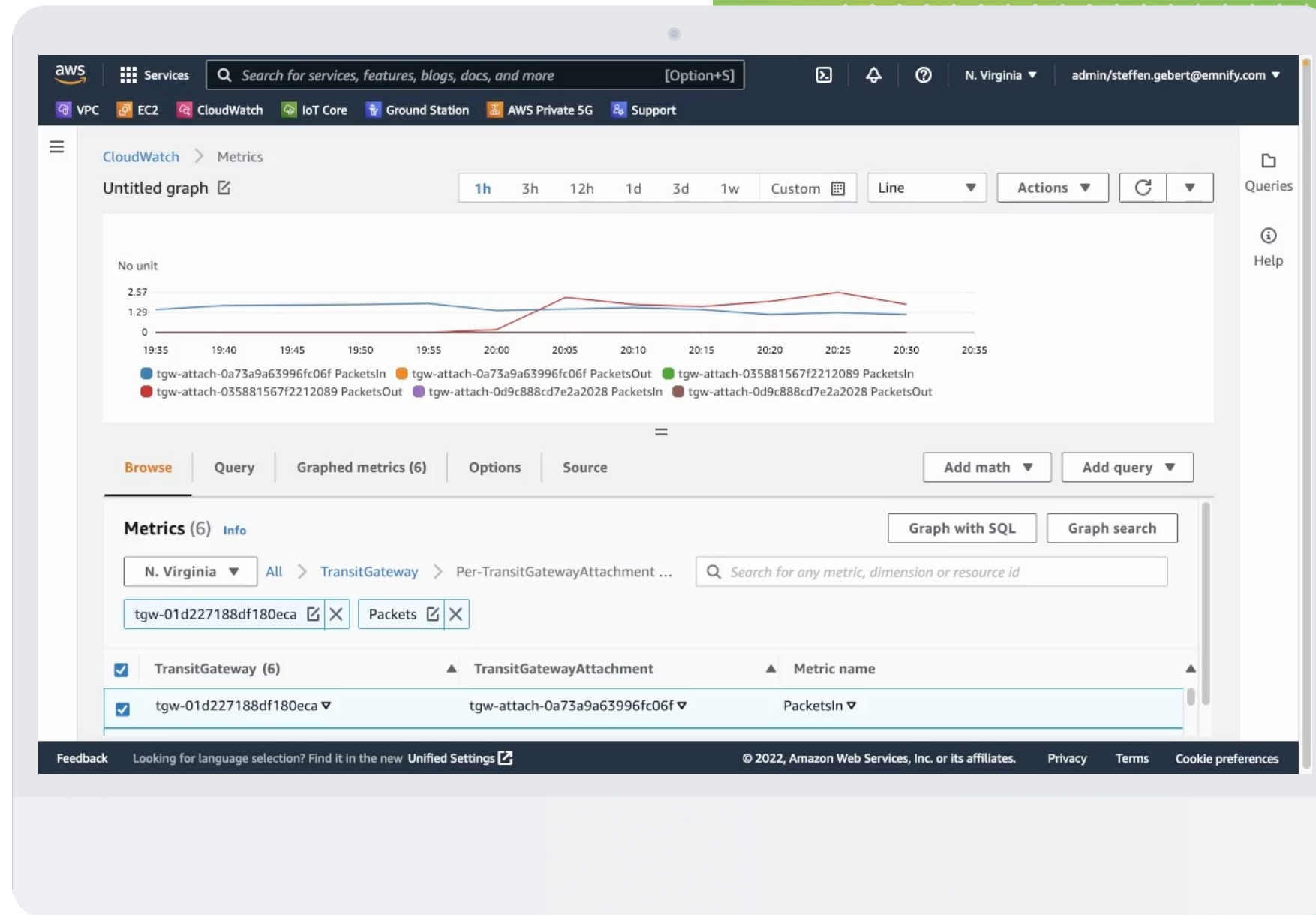
# Metrics Transit GW

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



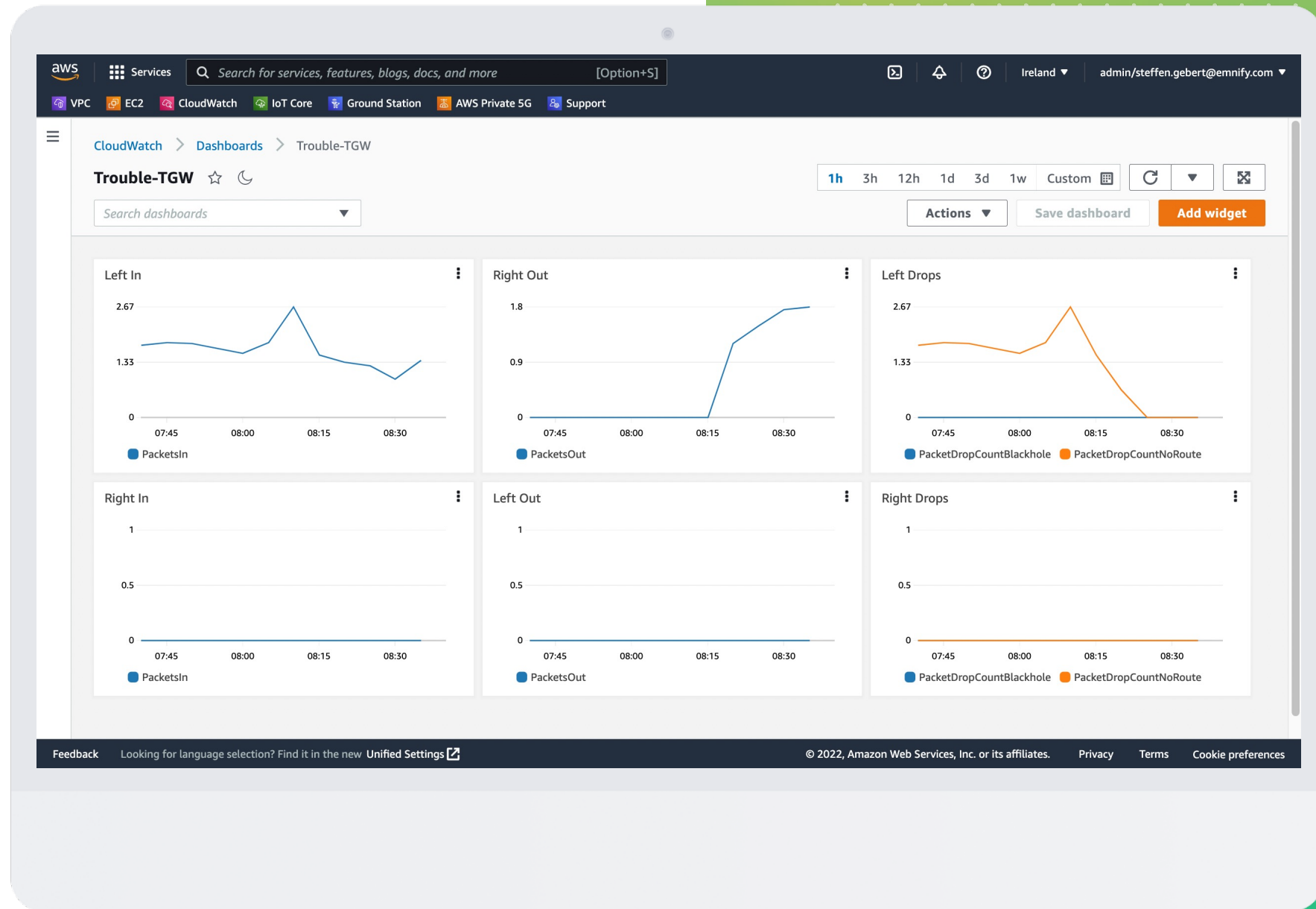
# Metrics Transit GW

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



# Metrics Transit GW

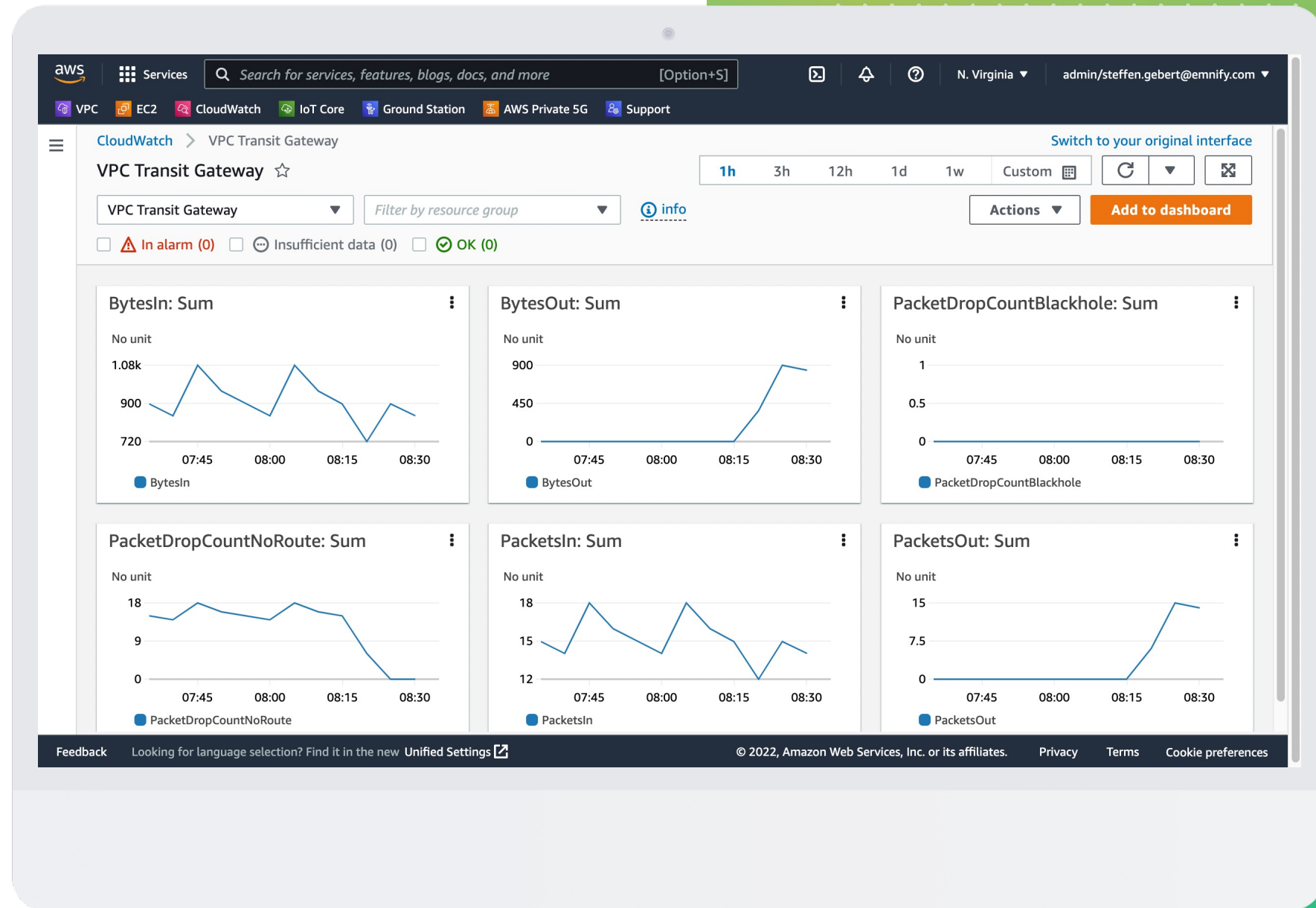
## ■ Custom Dashboard





# Metrics Transit GW

- Automatic Dashboard “VPC Transit Gateway”



EMnify

# Flow Logs



# Flow Logs

- VPC Flow Logs

- TGW Flow Logs

new

VPC / Your VPCs / Create flow log

## Create flow log [Info](#)

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.

### Selected resources [Info](#)

Name	Resource ID	State
left	vpc-0416ed0d3514d6fae	✔ Available

### Flow log settings

Name - optional

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.

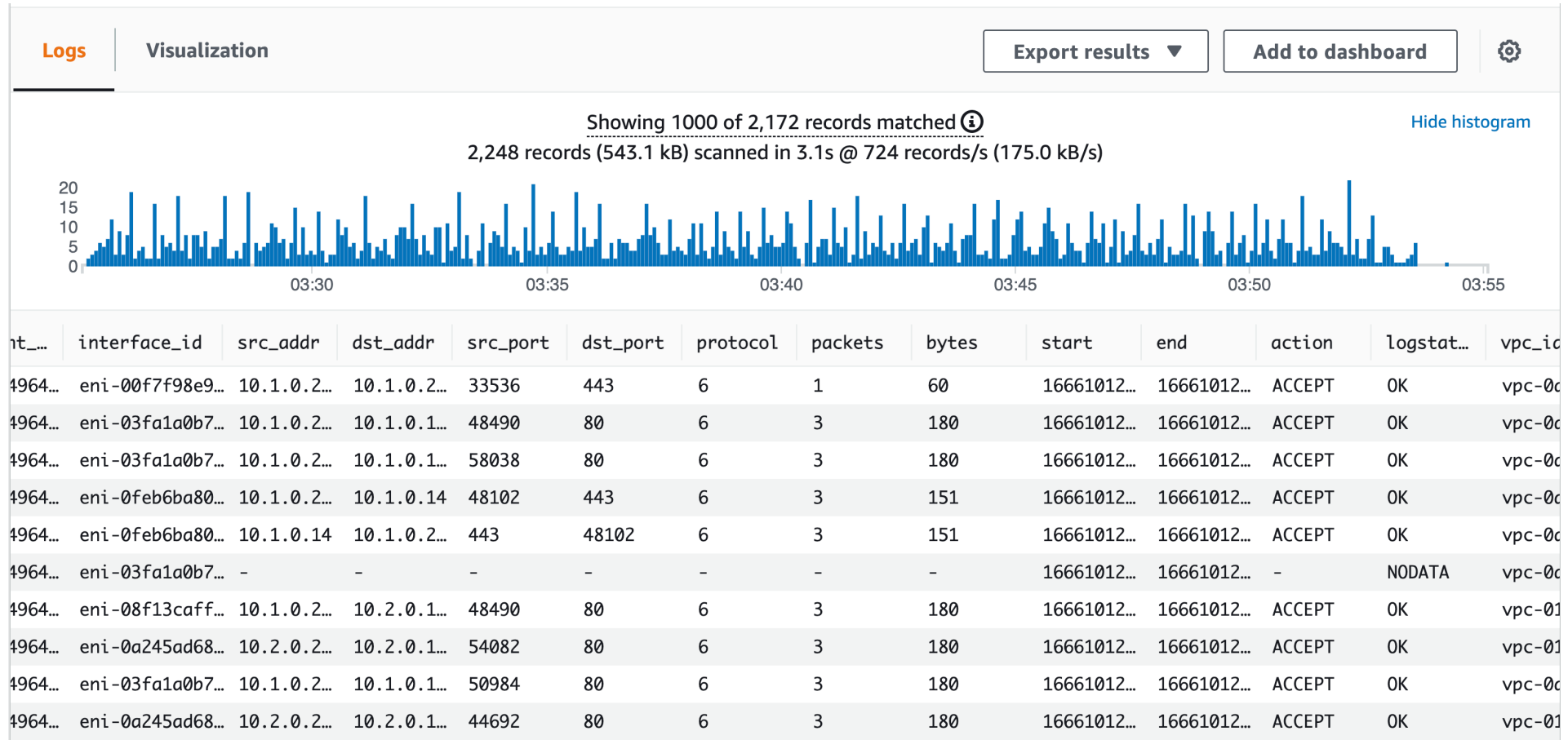
- ☒ 10 minutes
- ☐ 1 minute

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

## Logs Insights

Select log groups, and then run a query or [choose a sample query](#).

5m 30m 1h 3h 12h Custom

Select log group(s) ▼

vpc-flow-logs-trouble-eu-central-1 X

```
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
```

Run query Cancel Save Actions ▼ History

Queries are allowed to run for up to 15 minutes.

# Reachability Analyzer zu Flow Logs



# Reachability Analyzer zu Flow Logs

100

Outbound

allow

0.0.0.0/0

all

ROUTED

QUICKVIEW

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-private-eu-west-1a)

🔊

tgw-attach-0f25159b2cae021d2 (trouble-tgw)

Transit Gateway

tgw-0865bd6769f5bfe57 (trouble-tgw)

ROUTED

QUICKVIEW

🔊

tgw-rtb-04f1e029db916688e (trouble-tgw)

Destination CIDR

State

Attachment ID

Resource ID

10.2.0.0/16

active

tgw-attach-0fbee5e438ee844ae

vpc-0f0effa85597afdae

🔊

tgw-attach-0fbee5e438ee844ae (trouble-tgw)

Transit Gateway

tgw-0865bd6769f5bfe57 (trouble-tgw)

🔊

eni-0e67b5d56dde53a7

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

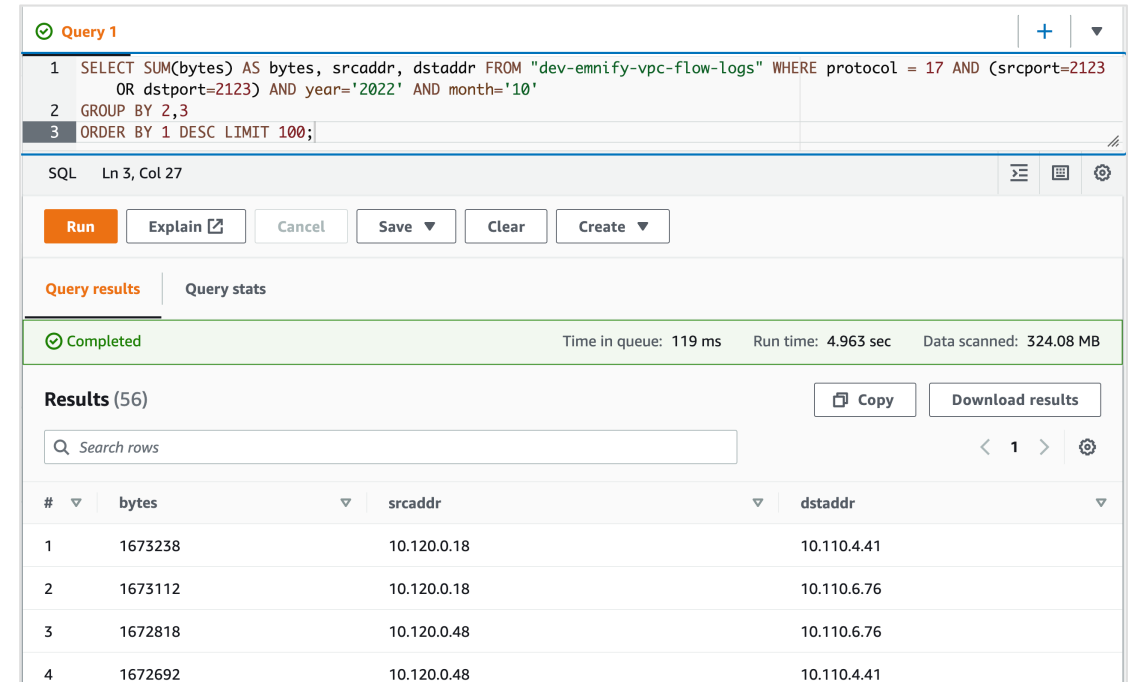
# Reachability Analyzer zu Flow Logs





# Flow Logs – Additional Destinations

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



The screenshot shows a SQL query editor with the following query:

```
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;
```

The query is executed successfully, showing the following results:

#	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

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

EMnify

# Packet Capture



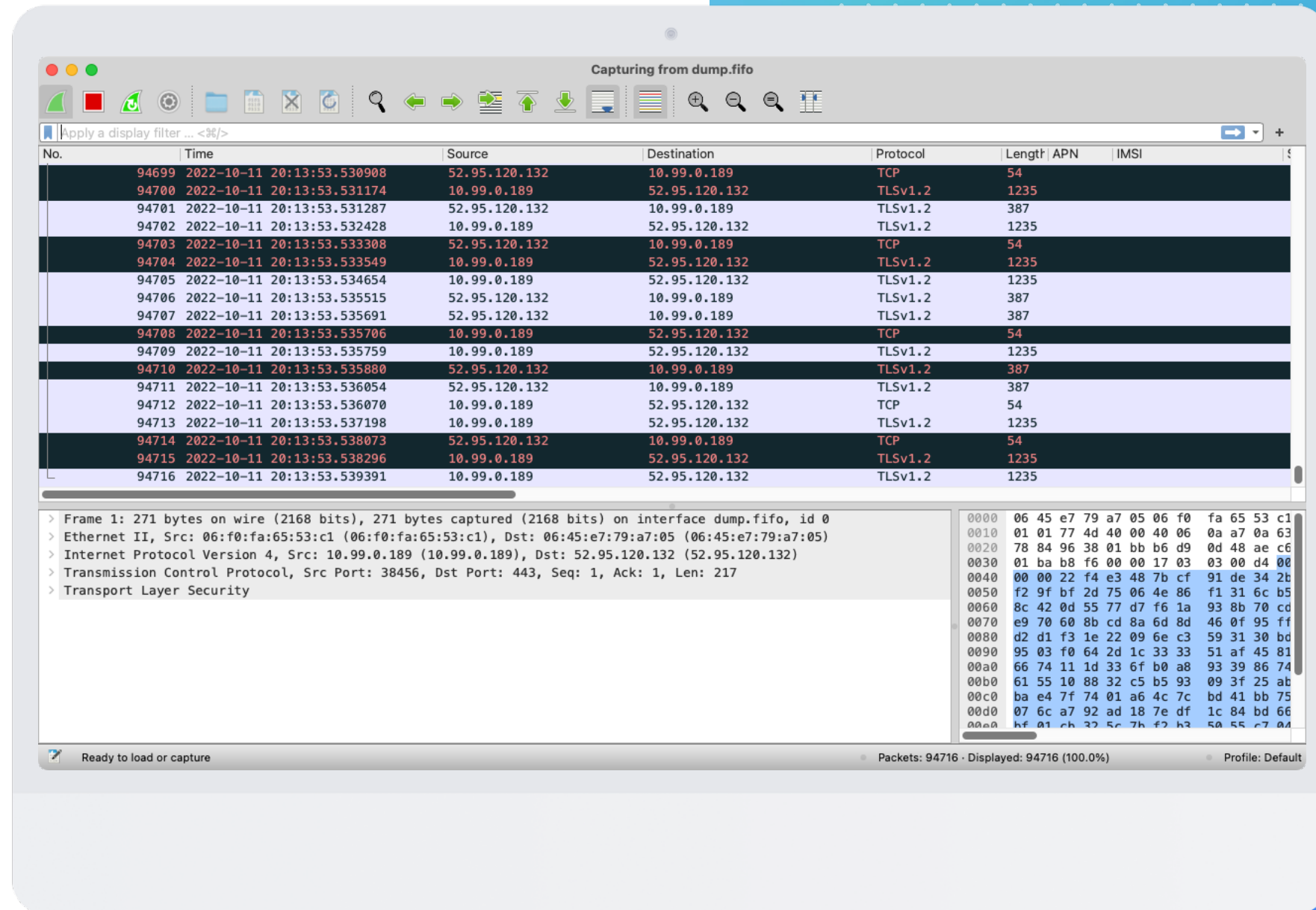
# Wireshark

- 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 WiresharkMa
inWindow::on_actionCaptureOptions_triggered() in ui/qt/main.cpp:700
** (wireshark:12225) 21:10:44.258841 [GUI WARNING] -- QObject::connect: (receiver name: 'Wiresh
arkMainWindow')
** (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 ...
```

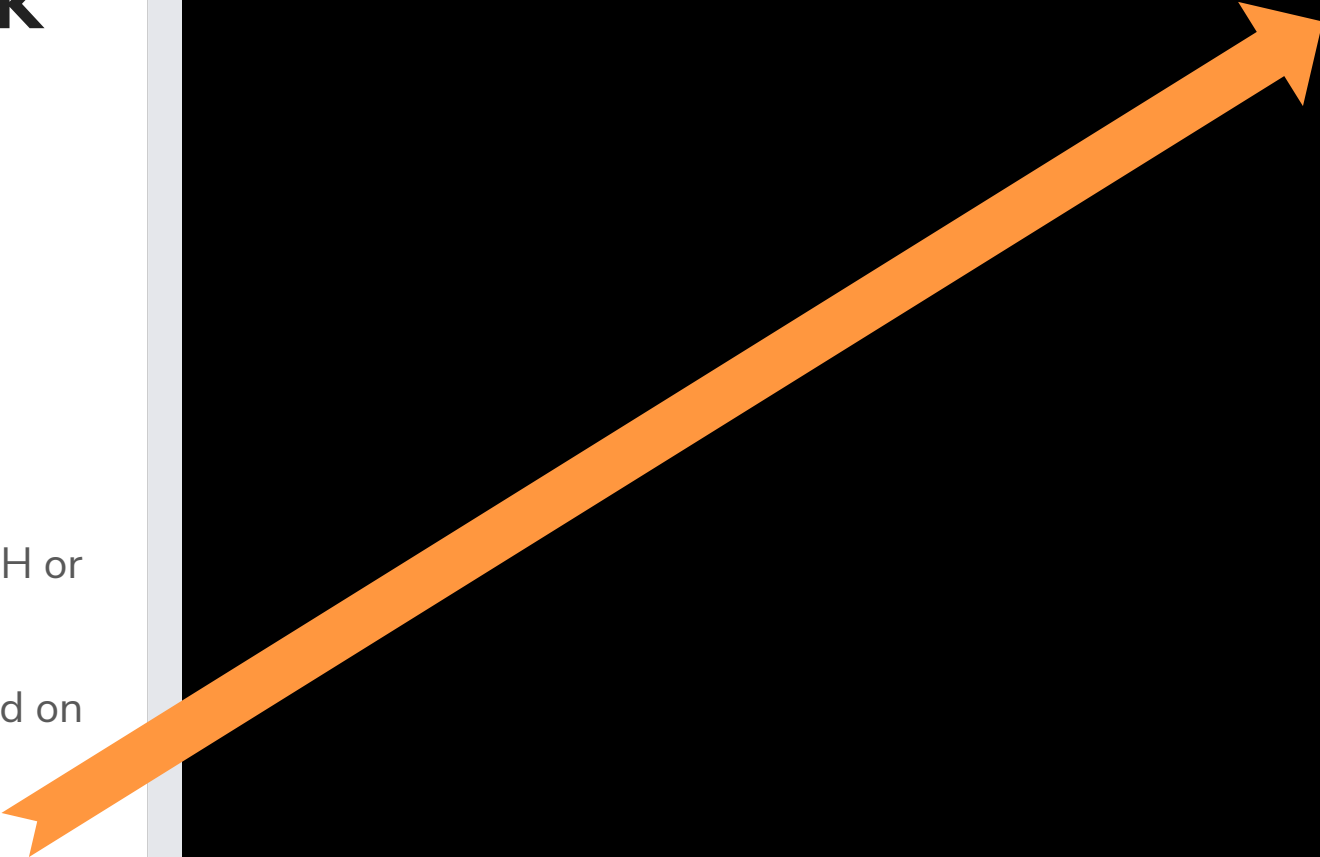
# Wireshark

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



# Wireshark

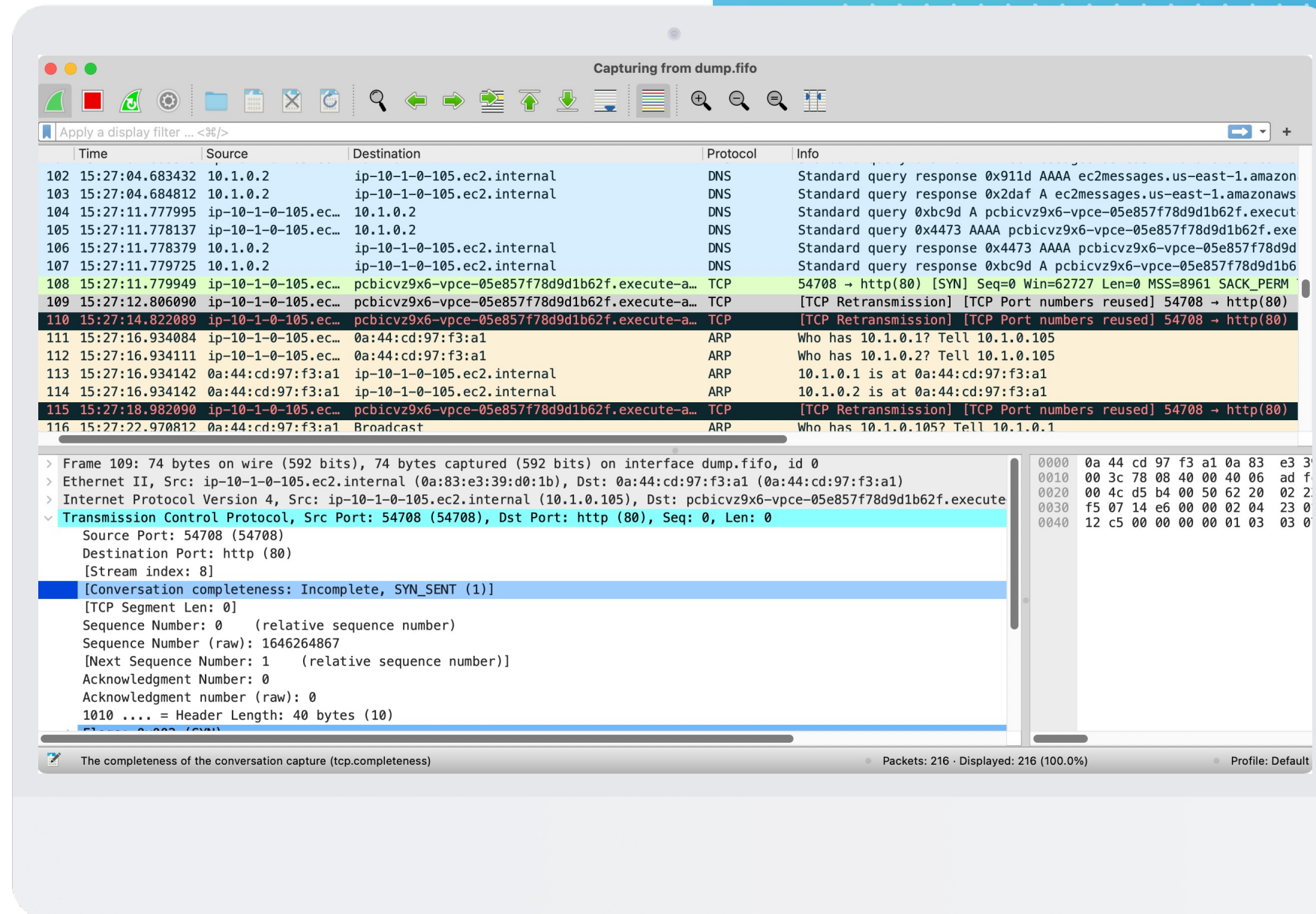
- tcpdump running on client instance
- Streamed through SSH or SSM connection
- Comfortably displayed on local computer
- Filter out own traffic!



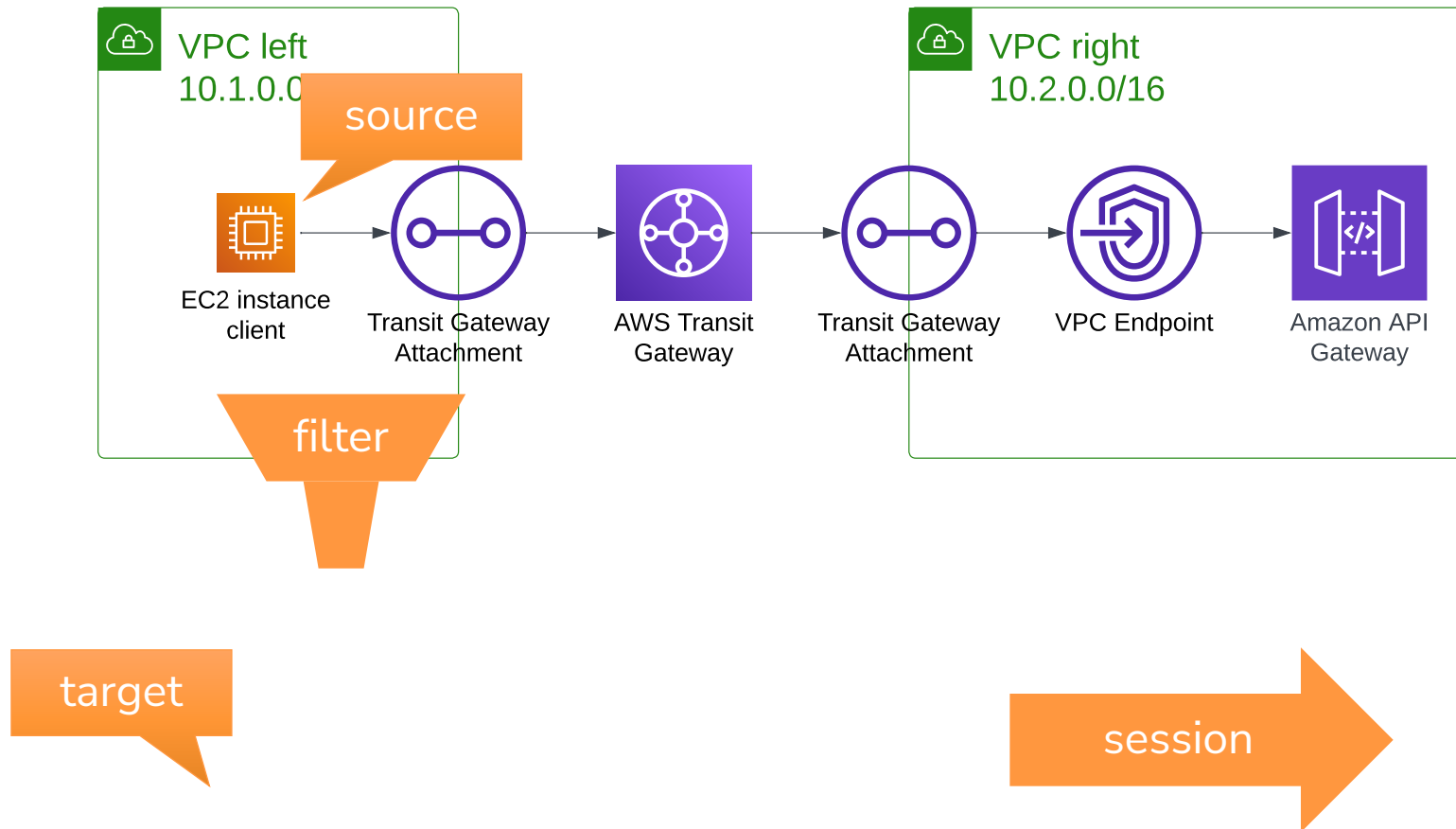
```
→ ~ ssh i-0e36abd49bb6e2d44 'sudo tcpdump -U -i ens5 -w - not port 443' > dump.fifo &
```

# Wireshark

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

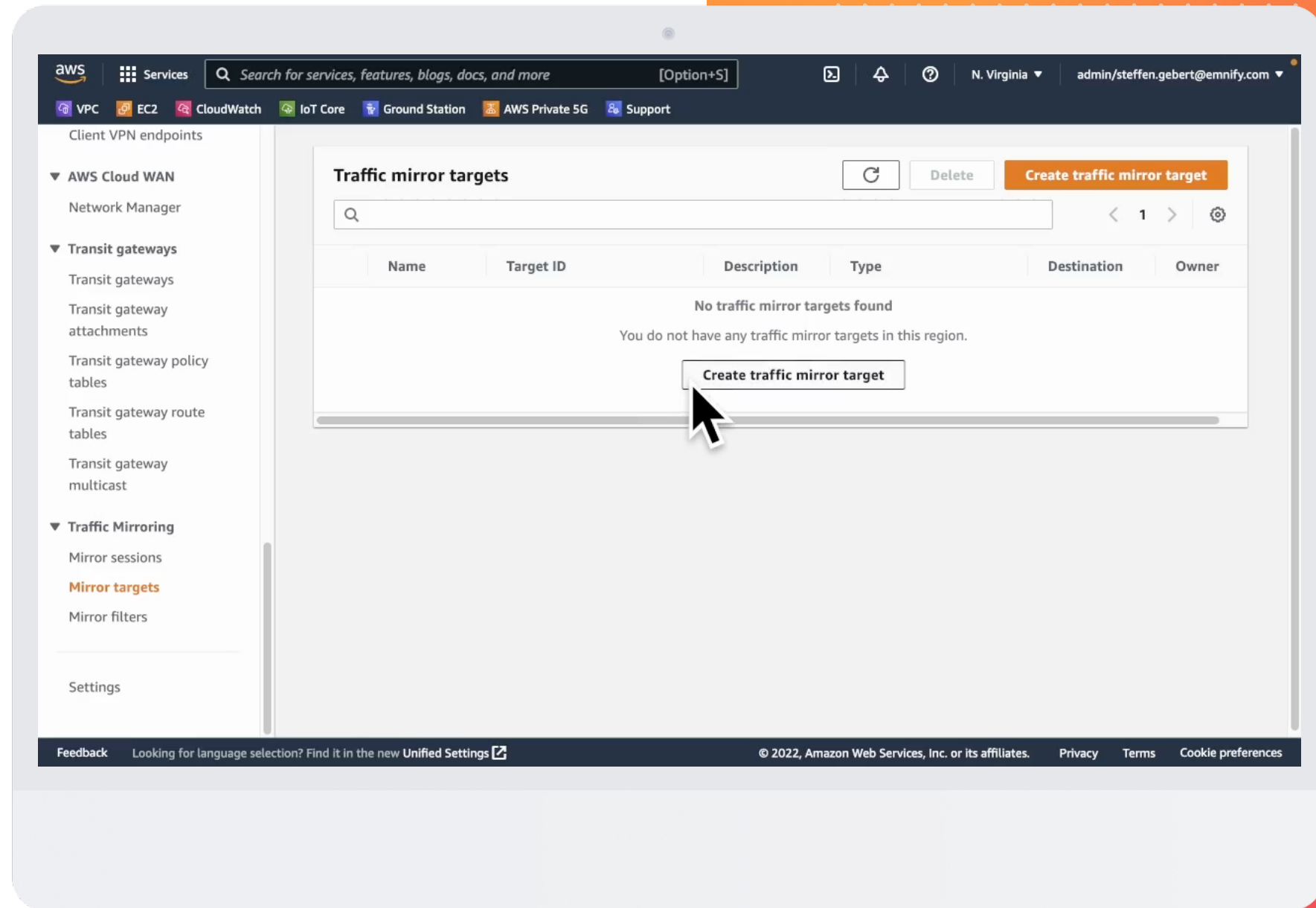


# VPC Traffic Mirroring



# 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





# 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

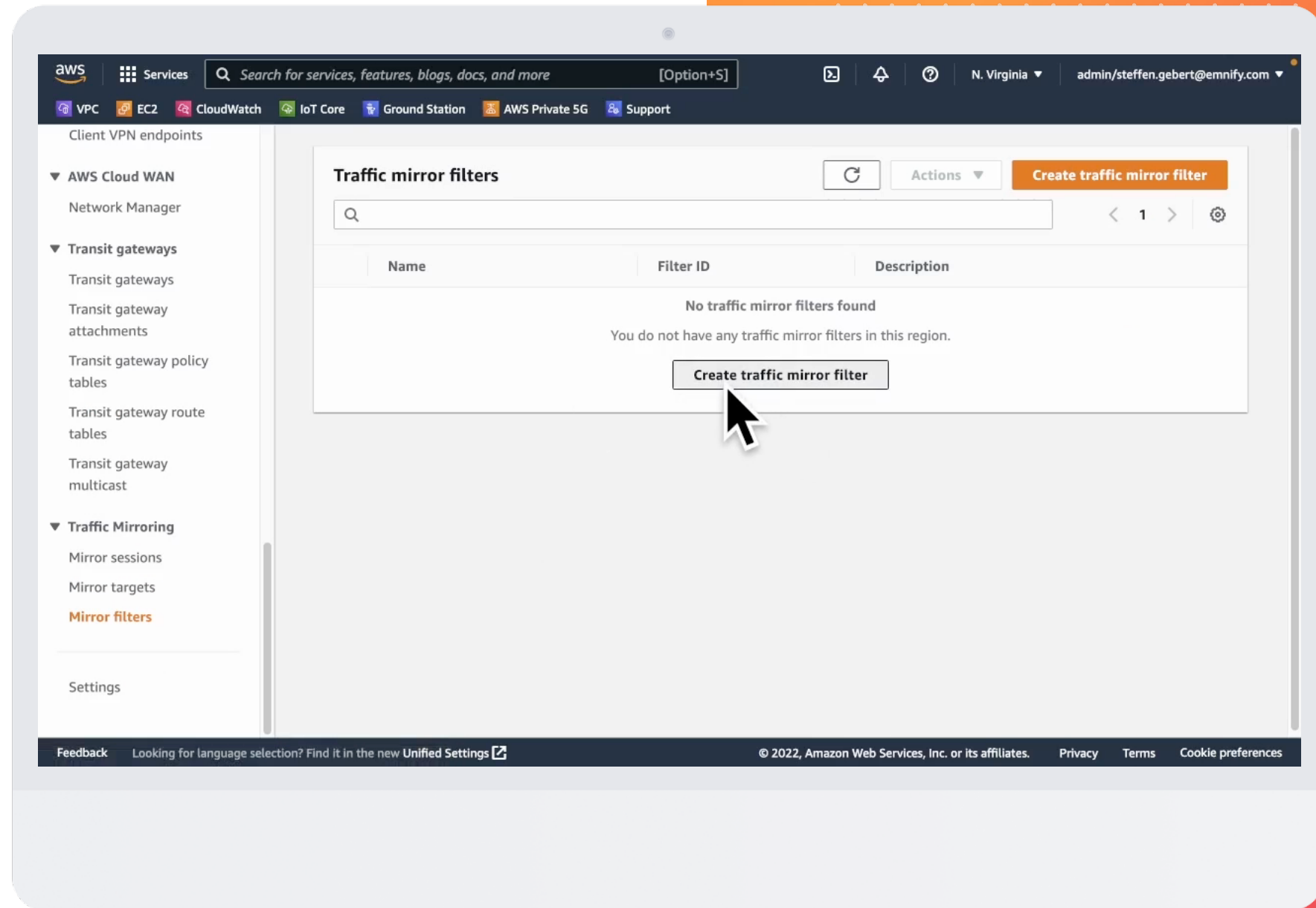
The screenshot displays the AWS Management Console interface for configuring VPC Traffic Mirroring. The top navigation bar includes the AWS logo, a search bar, and various service links like VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support. The user is logged in as 'admin/steffen.gebert@emnify.com' in the 'N. Virginia' region.

The main content area is titled 'Choose target' with a note: 'Target type cannot be modified after creation.' Below this, there is a 'Target type' dropdown menu set to 'Network Interface'. Under the 'Target' section, a search bar contains the text 'eni-011a31c4d283d8f15'. Below the target search, there is a 'Tags - optional' section with a description: 'A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.' This section includes a table with columns 'Key' and 'Value - optional'. One tag is listed with 'Name' as the key and 'Capture Receiver' as the value. There is a 'Remove' button next to the tag. Below the table is an 'Add new tag' button and a note: 'You can add 49 more tags.'

At the bottom right of the form, there are 'Cancel' and 'Create' buttons. A mouse cursor is pointing at the 'Create' button. The footer of the console includes links for 'Feedback', 'Looking for language selection? Find it in the new Unified Settings', copyright information '© 2022, Amazon Web Services, Inc. or its affiliates.', and links for 'Privacy', 'Terms', and 'Cookie preferences'.

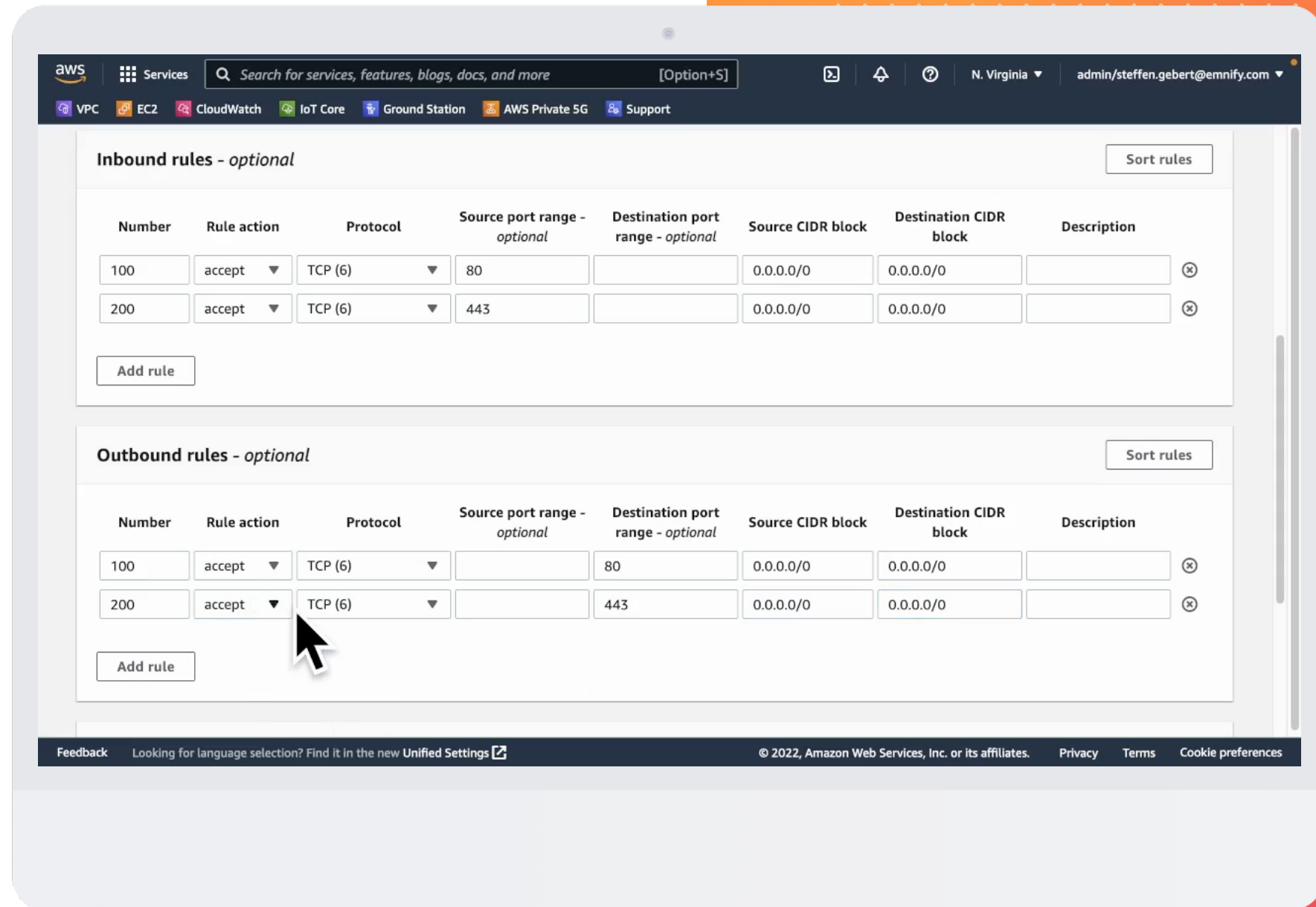
# VPC Traffic Mirroring

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



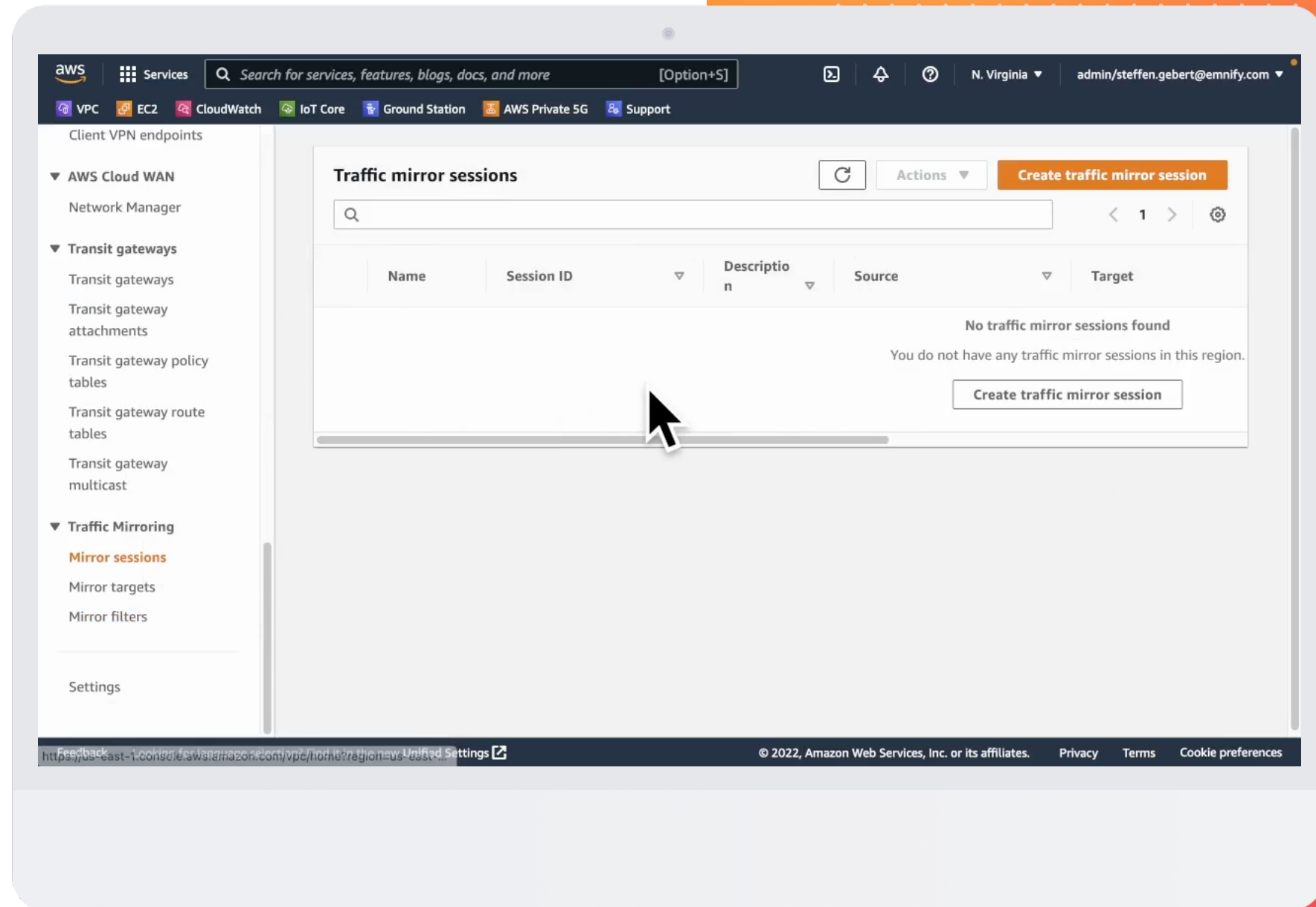
# VPC Traffic Mirroring

- 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 displays the AWS Management Console interface for creating a traffic mirror session. The breadcrumb navigation shows 'VPC > Traffic mirror sessions > Create traffic mirror session'. The main heading is 'Create traffic mirror session'. Below this, the 'Session settings' section is visible, with the instruction 'Set description, source, and target.'.

The 'Session settings' section includes the following fields:

- Name tag - optional:** A text input field containing 'Capture Trouble'.
- Description - optional:** A text input field with the placeholder text 'Describe your traffic mirror session'. A mouse cursor is pointing at this field.
- Mirror source:** A section with the instruction 'The resource that you want to monitor.' and a text input field containing 'eni-097743e2ec33cd884'. Below the input field, it states 'Only network interfaces of type "interface" are allowed.'
- Mirror target:** A section with the instruction 'A network interface, or a network load balancer, or a gateway load balancer endpoint that is the destination for mirrored traffic.' and a text input field containing 'tmt-03aabf40711b41d63'. To the right of the input field is a 'Create target' button.

The bottom of the console shows a footer with 'Feedback', a link to 'Looking for language selection? Find it in the new Unified Settings', and copyright information: '© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

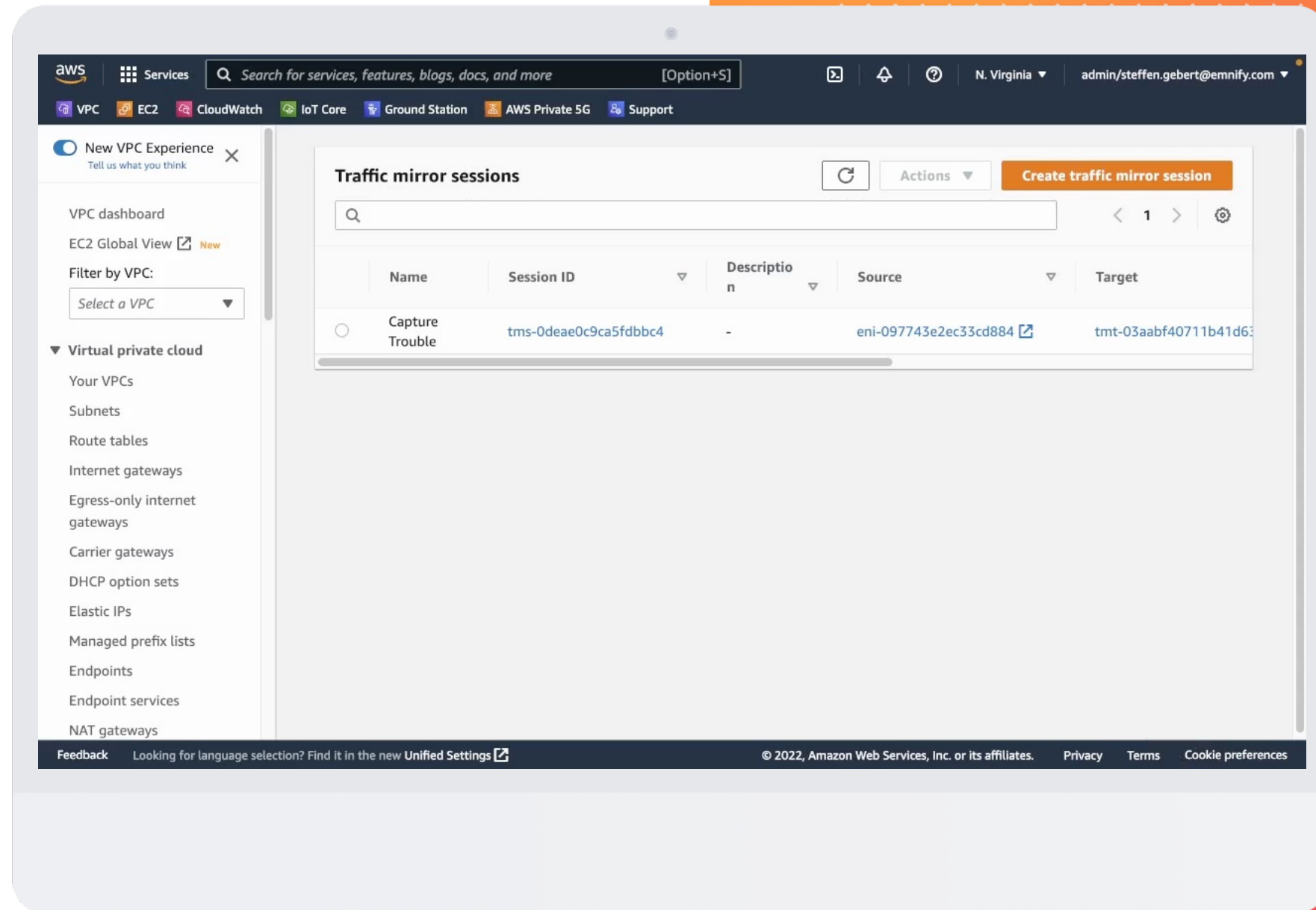
# VPC Traffic Mirroring

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

The screenshot displays the AWS VPC Traffic Mirroring configuration page. The interface includes a top navigation bar with the AWS logo, 'Services' menu, a search bar, and user information for 'N. Virginia' and 'admin/steffen.gebert@emnify.com'. Below the navigation bar, there are tabs for VPC, EC2, CloudWatch, IoT Core, Ground Station, AWS Private 5G, and Support. The main configuration area contains several sections: a 'Number between 1 and 32766' input field with the value '1'; a 'VNI - optional' section with a description and a text box containing 'A random unique VNI will be chosen unless specified.'; a 'Packet length - optional' section with a description and a text box containing 'eg 255 bytes - the entire packet is default'; a 'Filter' section with a description and a dropdown menu showing 'HTTP and HTTPS'; and a 'Tags - optional' section with a description and a list of tags with keys 'Name' and 'Capture Trouble', each with a 'Remove' button. A 'Create filter' button is located to the right of the filter dropdown. The bottom of the page features a footer with 'Feedback', 'Looking for language selection? Find it in the new Unified Settings', copyright information, and links for '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





# VPC Traffic Mirroring

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

The screenshot displays a network traffic capture interface. The top section shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The bottom section provides a detailed view of the selected packet (No. 2621), showing its structure from Ethernet II to the TCP segment.

No.	Time	Source	Destination	Protocol	Info
2621	16:12:56.424862	10.1.0.105	10.2.0.76	TCP	33648 → http(80) [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_P
2626	16:12:57.438492	10.1.0.105	10.2.0.76	TCP	[TCP Retransmission] [TCP Port numbers reused] 33648 → http(
2627	16:12:57.438526	ip-10-99-0-113.e...	10.1.0.105	ICMP	Destination unreachable (Port unreachable)
2631	16:12:59.454527	10.1.0.105	10.2.0.76	TCP	[TCP Retransmission] [TCP Port numbers reused] 33648 → http(
2632	16:12:59.454566	ip-10-99-0-113.e...	10.1.0.105	ICMP	Destination unreachable (Port unreachable)
2698	16:13:03.440831	10.1.0.105	10.2.0.76	TCP	37042 → http(80) [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_P
2699	16:13:04.446503	10.1.0.105	10.2.0.76	TCP	[TCP Retransmission] [TCP Port numbers reused] 37042 → http(
2700	16:13:04.446536	ip-10-99-0-113.e...	10.1.0.105	ICMP	Destination unreachable (Port unreachable)
2705	16:13:06.462463	10.1.0.105	10.2.0.76	TCP	[TCP Retransmission] [TCP Port numbers reused] 37042 → http(

**Packet Details (Frame 2621):**

- > Frame 2621: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface dump.fifo, id 0
- > Ethernet II, Src: 0a:b7:2a:e1:42:a1 (0a:b7:2a:e1:42:a1), Dst: ip-10-99-0-113.ec2.internal (0a:cc:63:fd:f9:05)
- > Internet Protocol Version 4, Src: 10.1.0.105 (10.1.0.105), Dst: ip-10-99-0-113.ec2.internal (10.99.0.113)
- > User Datagram Protocol, Src Port: 65507 (65507), Dst Port: vxlan (4789)
- ▼ Virtual eXtensible Local Area Network
  - > Flags: 0x0800, VXLAN Network ID (VNI)
    - Group Policy ID: 0
    - VXLAN Network Identifier (VNI): 3916269
    - Reserved: 0
  - > Ethernet II, Src: 0a:83:e3:39:d0:1b (0a:83:e3:39:d0:1b), Dst: 0a:44:cd:97:f3:a1 (0a:44:cd:97:f3:a1)
  - > Internet Protocol Version 4, Src: 10.1.0.105 (10.1.0.105), Dst: 10.2.0.76 (10.2.0.76)
  - ▼ Transmission Control Protocol, Src Port: 33648 (33648), Dst Port: http (80), Seq: 0, Len: 0
    - Source Port: 33648 (33648)
    - Destination Port: http (80)
    - [Stream index: 63]
    - [Conversation completeness: Incomplete, SYN\_SENT (1)]
    - [TCP Segment Len: 0]
    - Sequence Number: 0 (relative sequence number)
    - Sequence Number (raw): 2848161633
    - [Next Sequence Number: 1 (relative sequence number)]
    - Acknowledgment Number: 0
    - Acknowledgment number (raw): 0



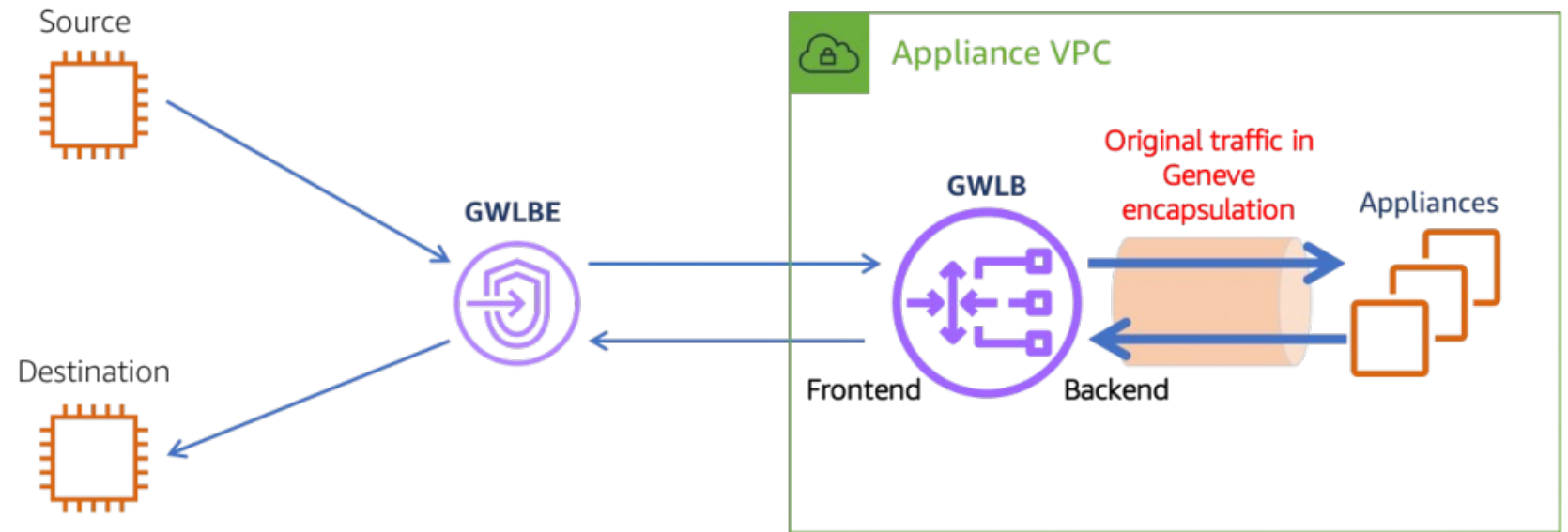


# That's fun!

NOBODY EVER DOING THIS

# Can it be easier?

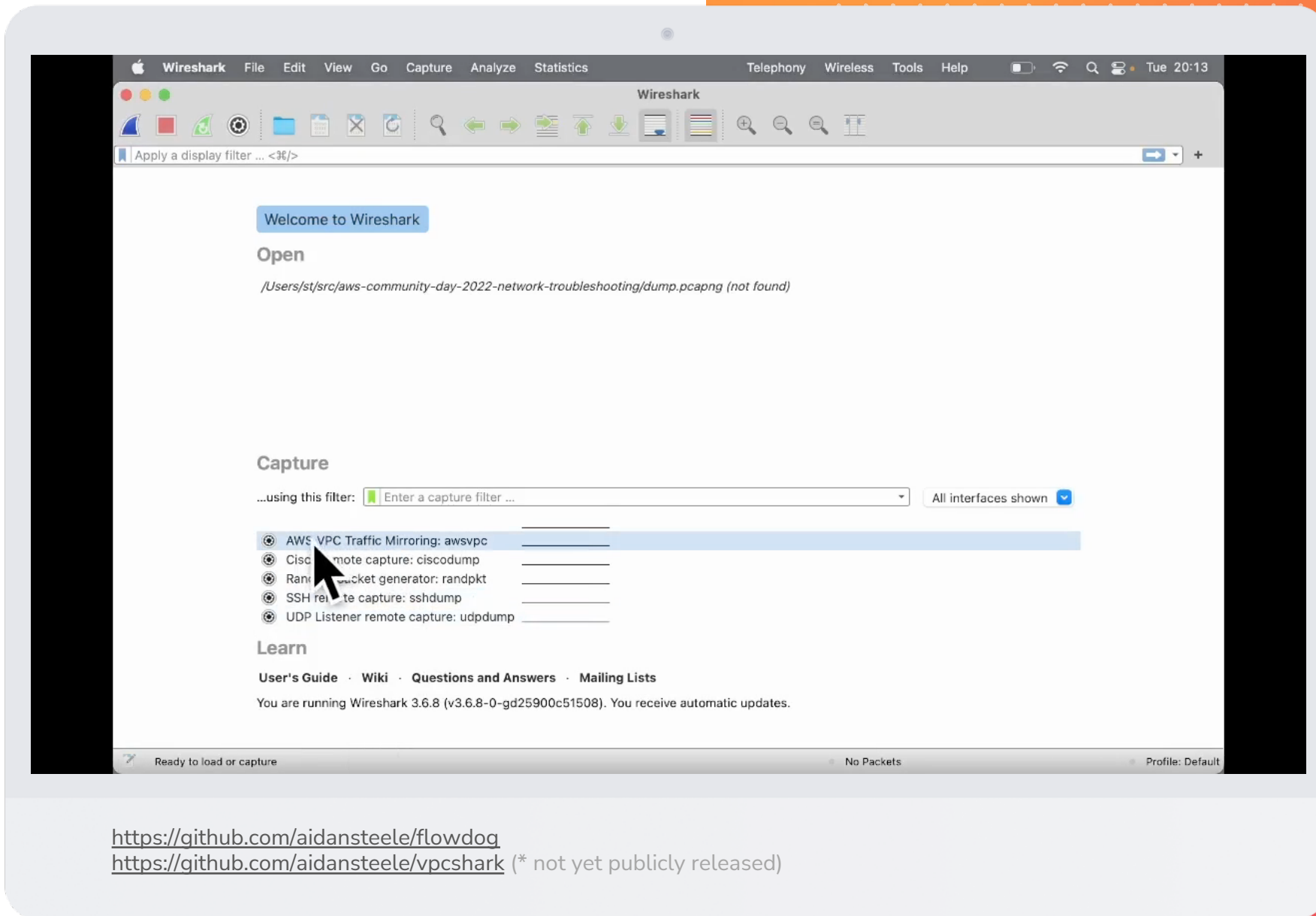
- Aidan Steele's projects
  - flowdogshark (GWLBE)



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

# Can it be easier?

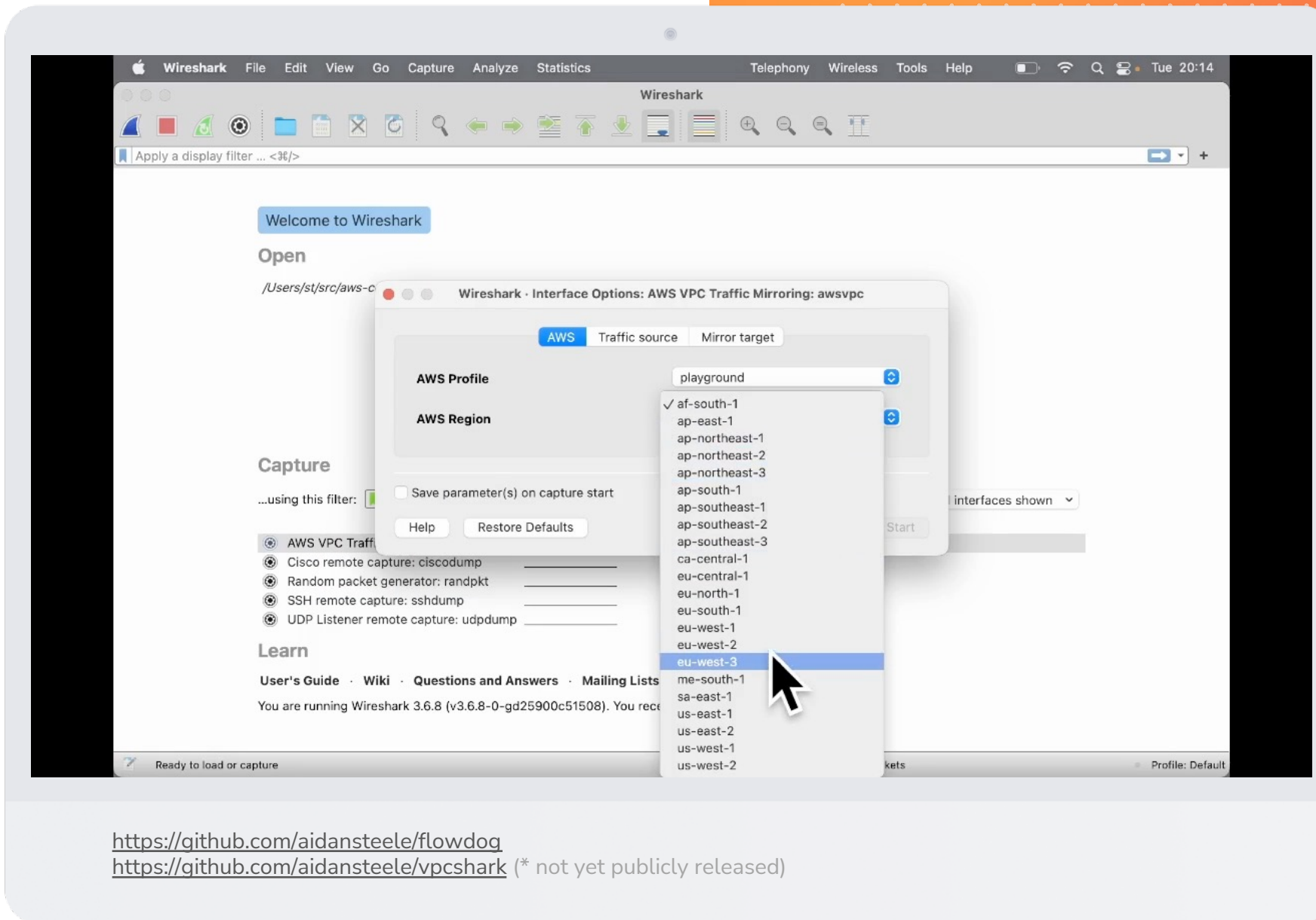
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



<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

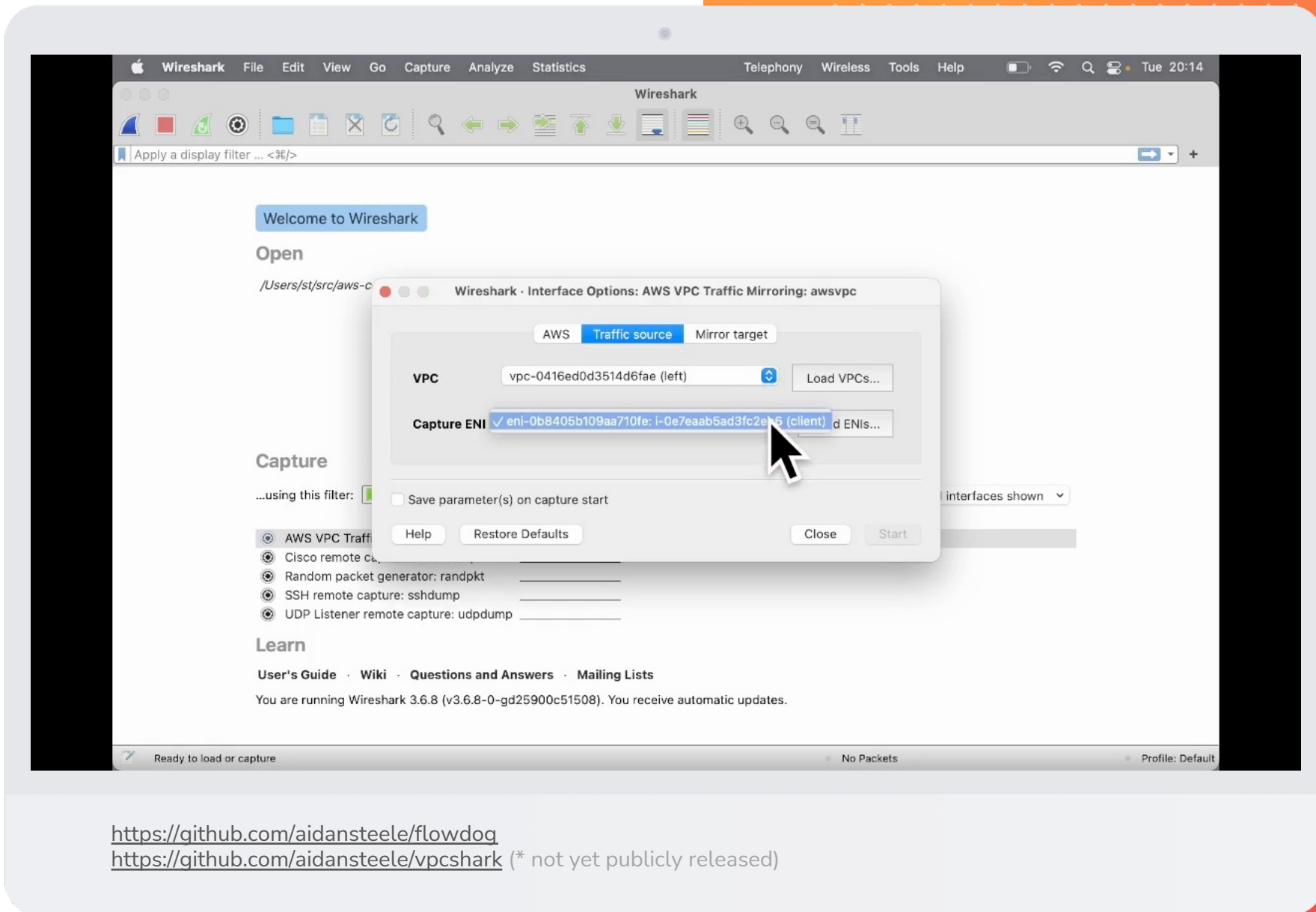


<https://github.com/aidansteele/flowdog>

<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

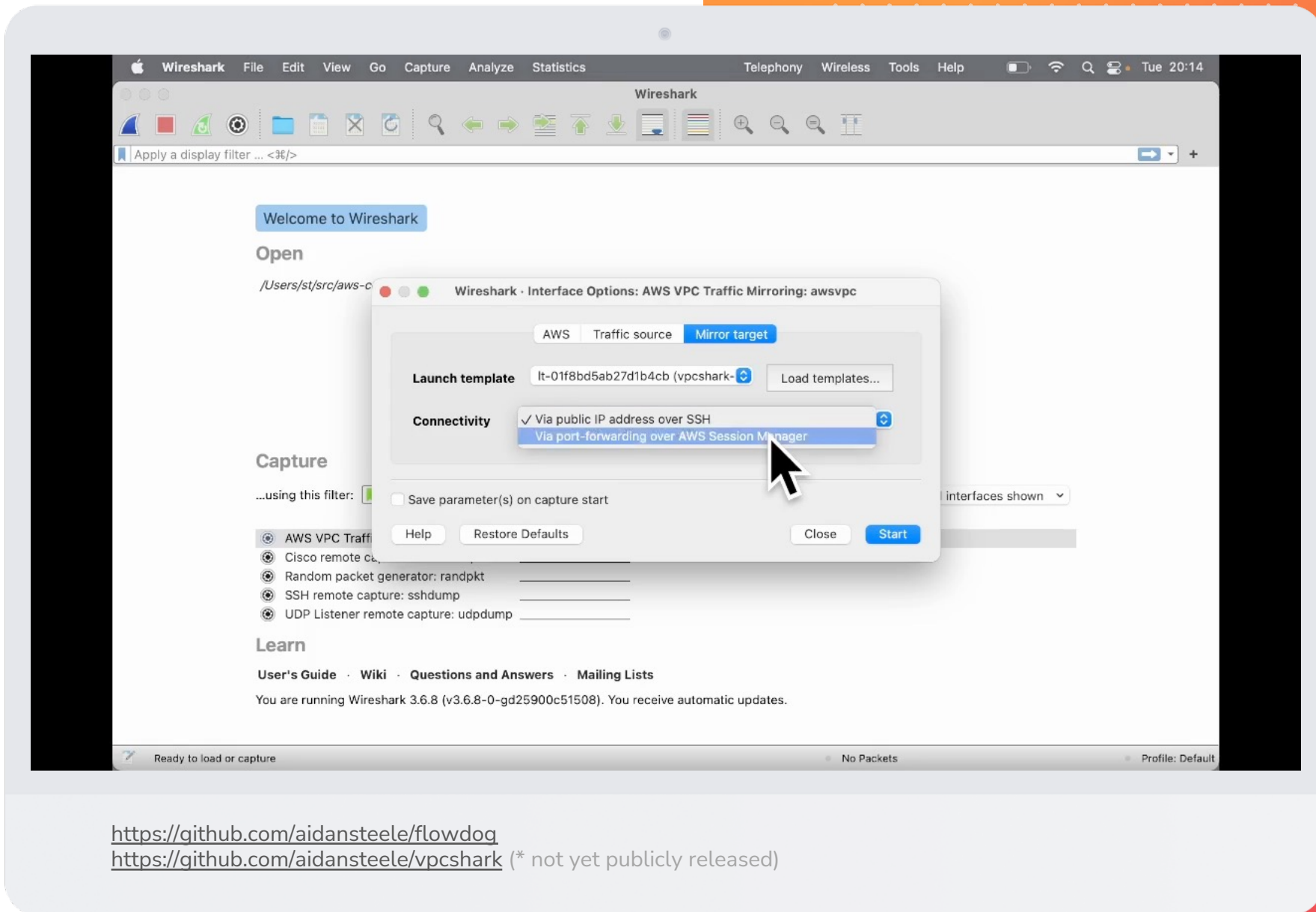


<https://github.com/aidansteele/flowdog>

<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

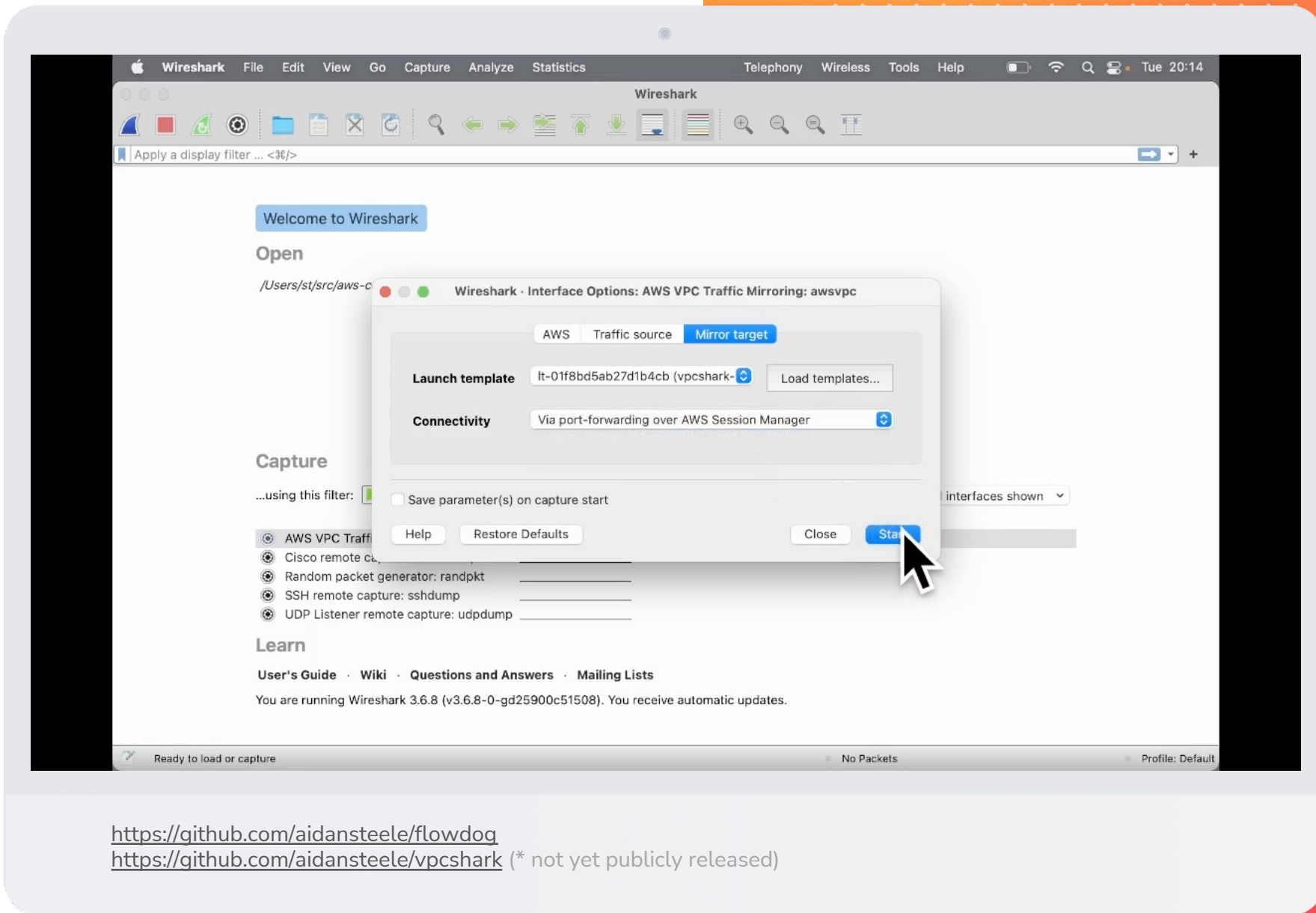


<https://github.com/aidansteele/flowdog>

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

# Can it be easier?

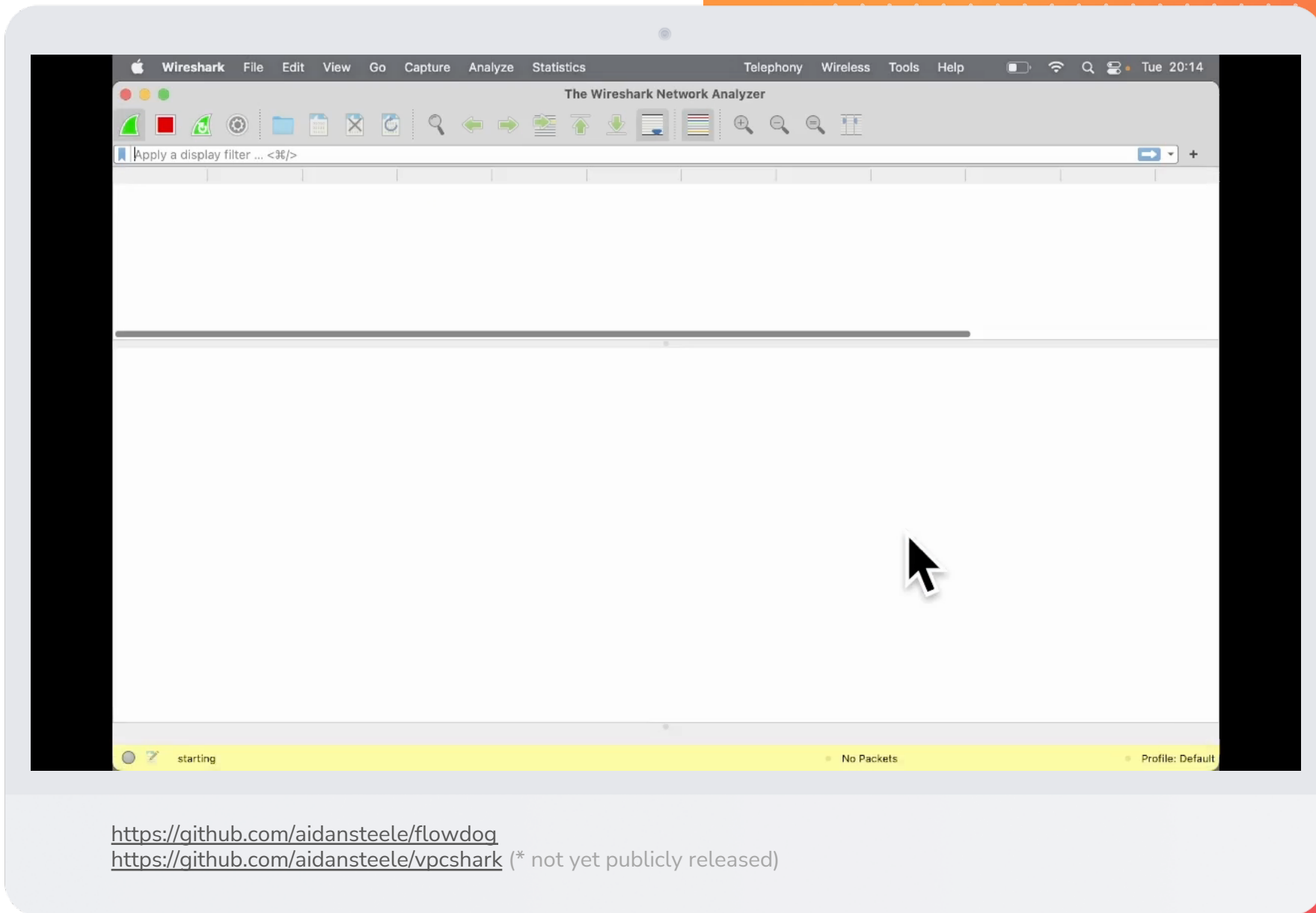
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



<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

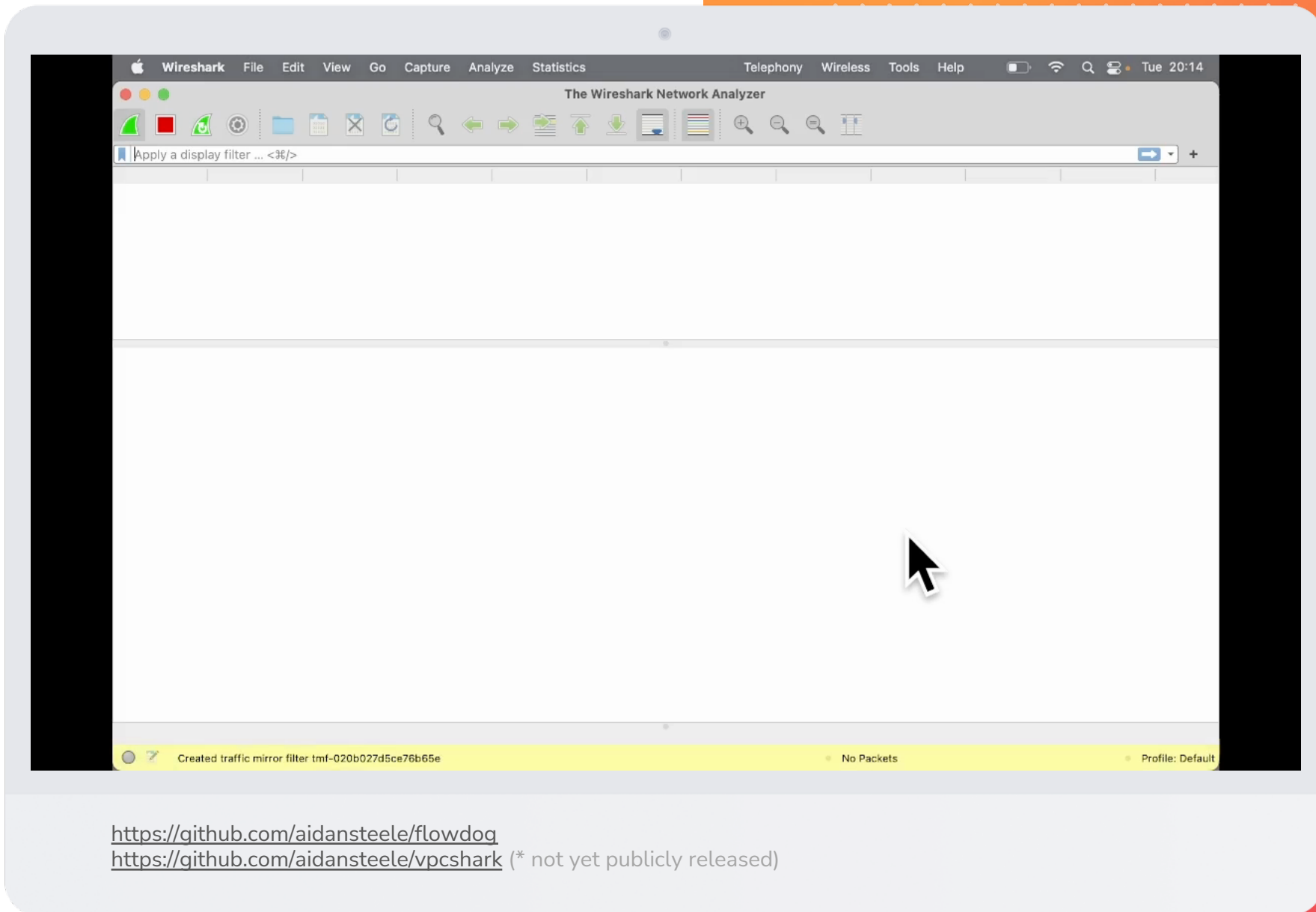


<https://github.com/aidansteele/flowdog>  
<https://github.com/aidansteele/vpcshark> (\* not yet publicly released)



# Can it be easier?

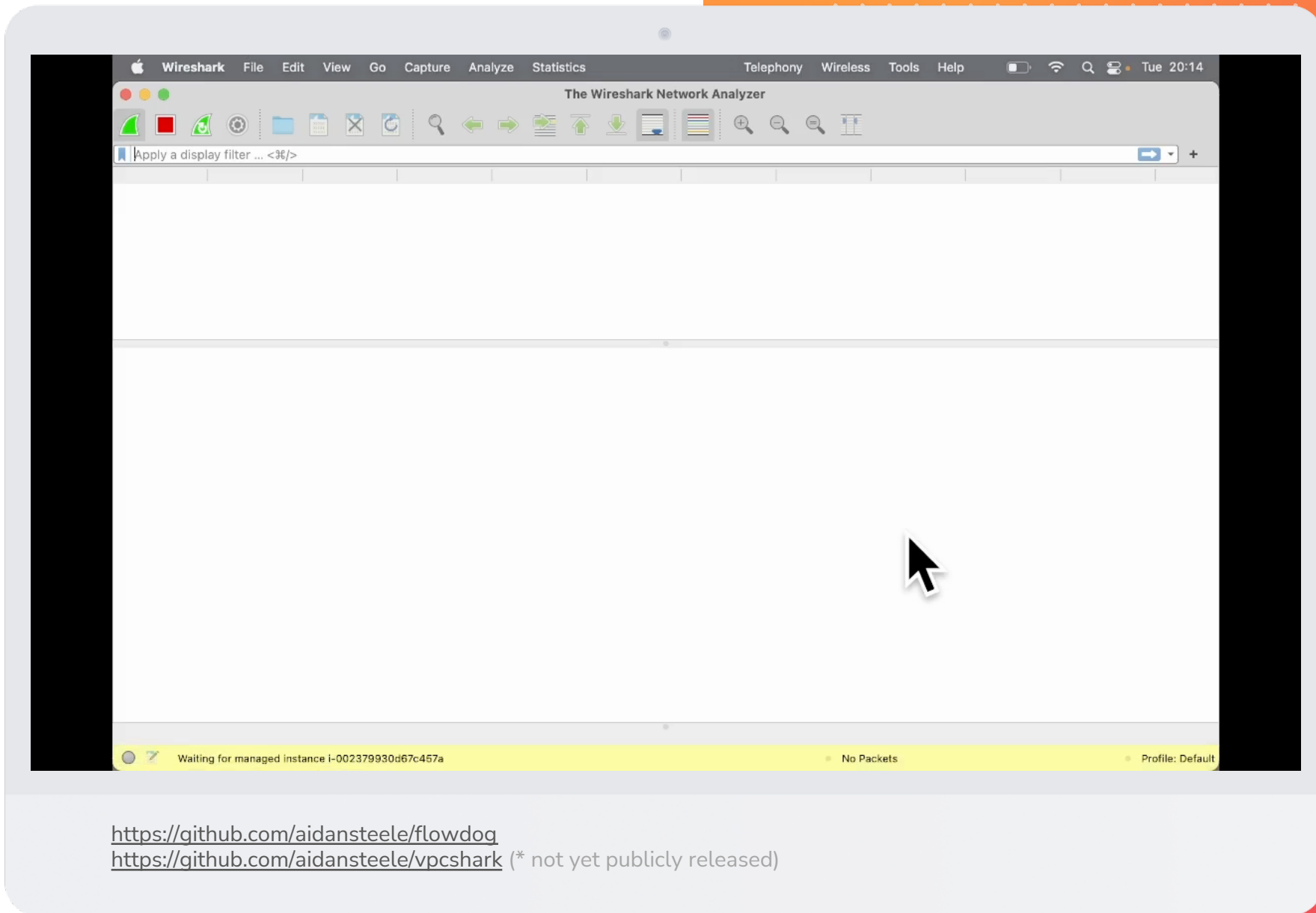
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



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

# Can it be easier?

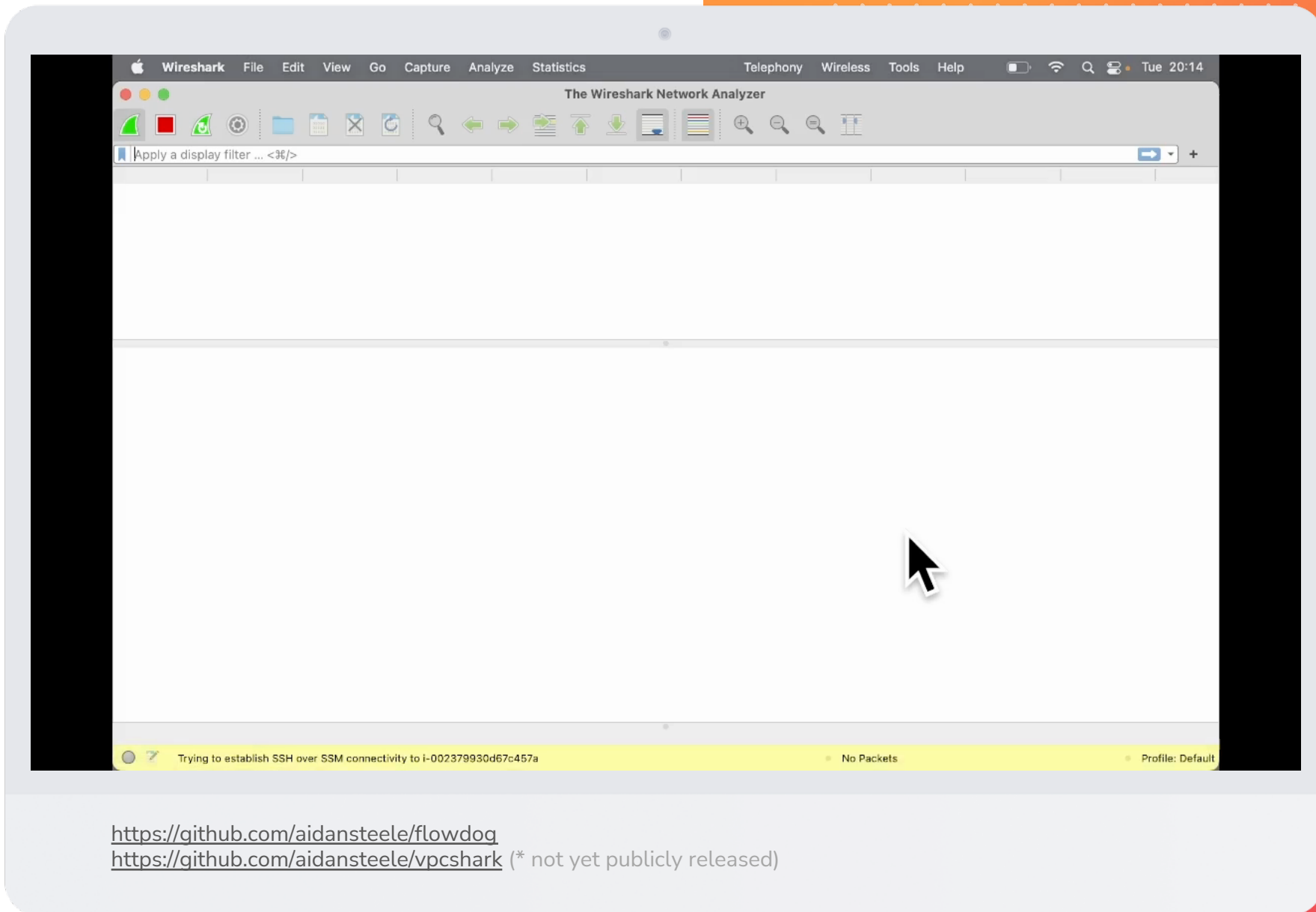
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



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

# Can it be easier?

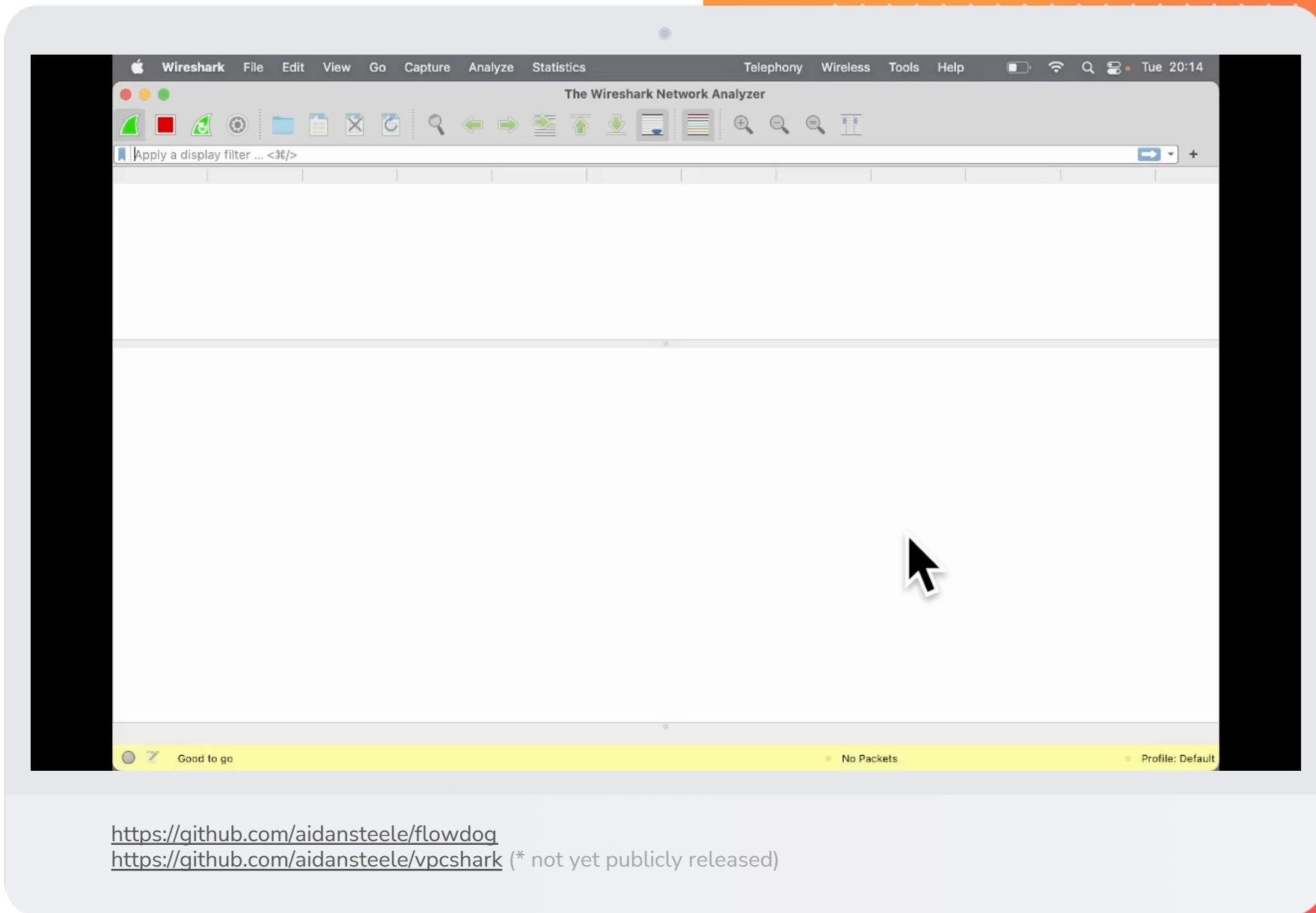
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



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

# Can it be easier?

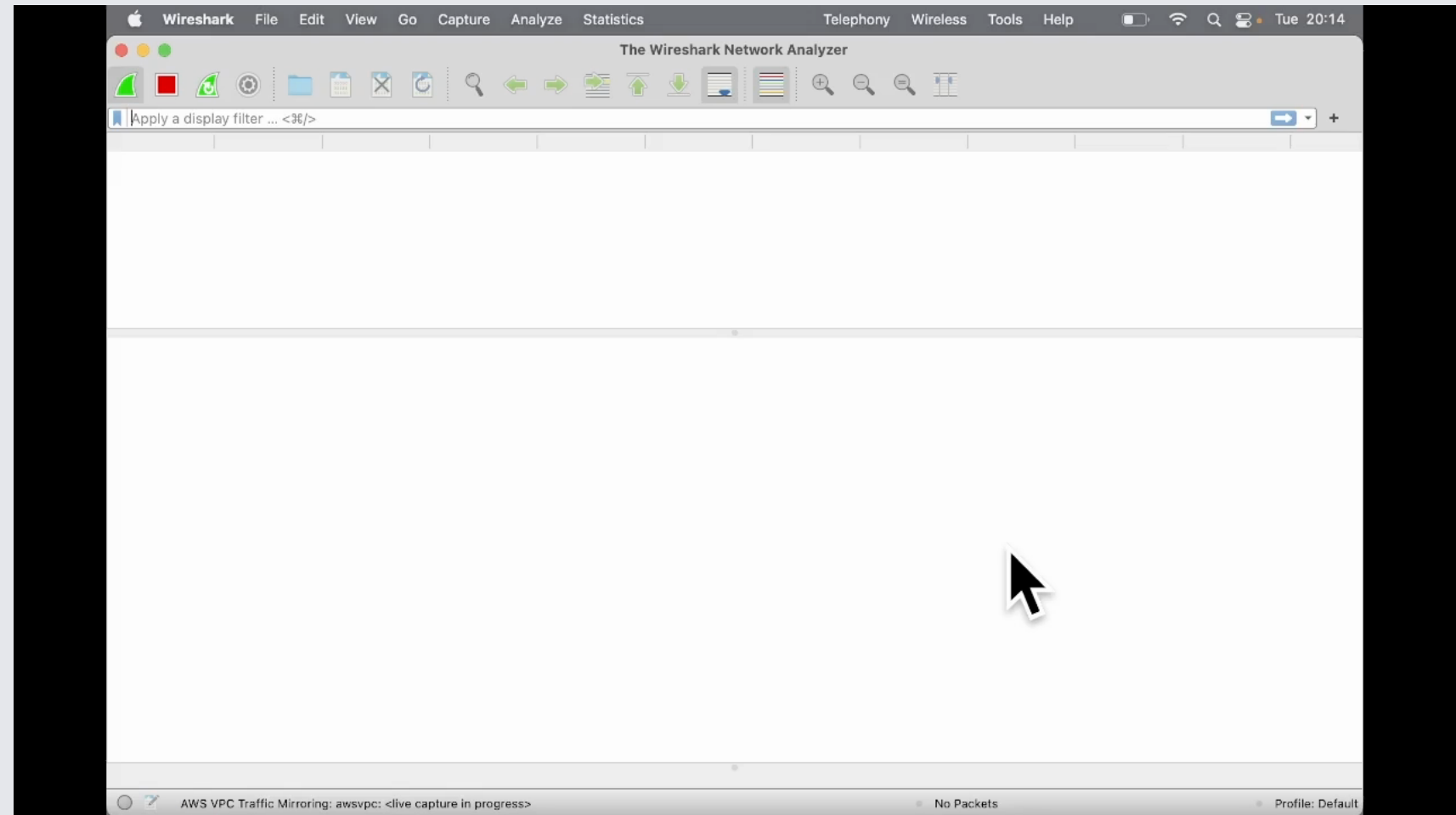
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark \*
- More concept studies than for production



<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



<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

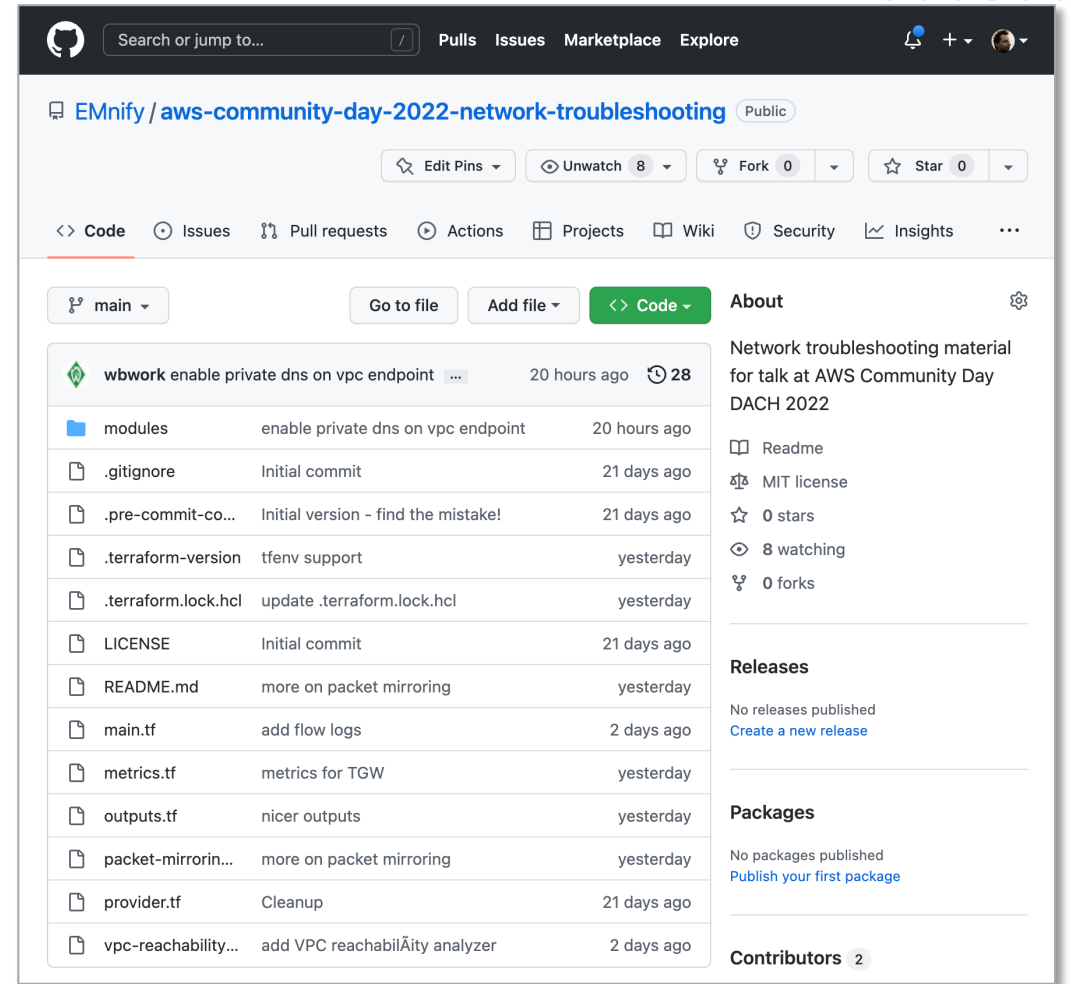




# Learn from our mistakes!

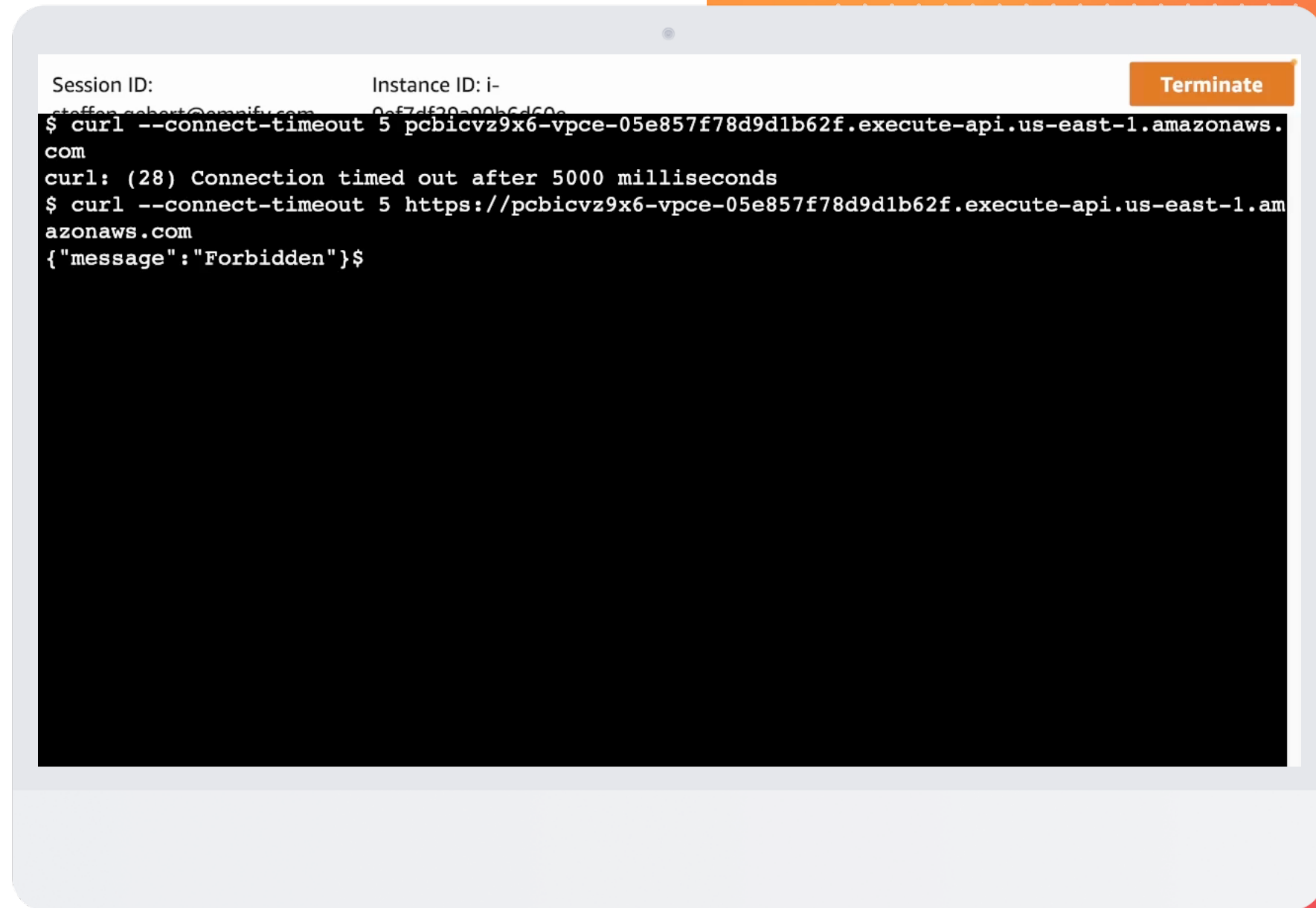
- IaC definition of the setup used in this talk
  - Terraform
  - incl. Reachability Analyzer and Traffic Mirroring

■ [github.com/EMnify/](https://github.com/EMnify/)



# One More Try

Oh.. Layer 8 issues 😊





# Agenda

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