EMnify

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

Steffen Gebert (@StGebert)

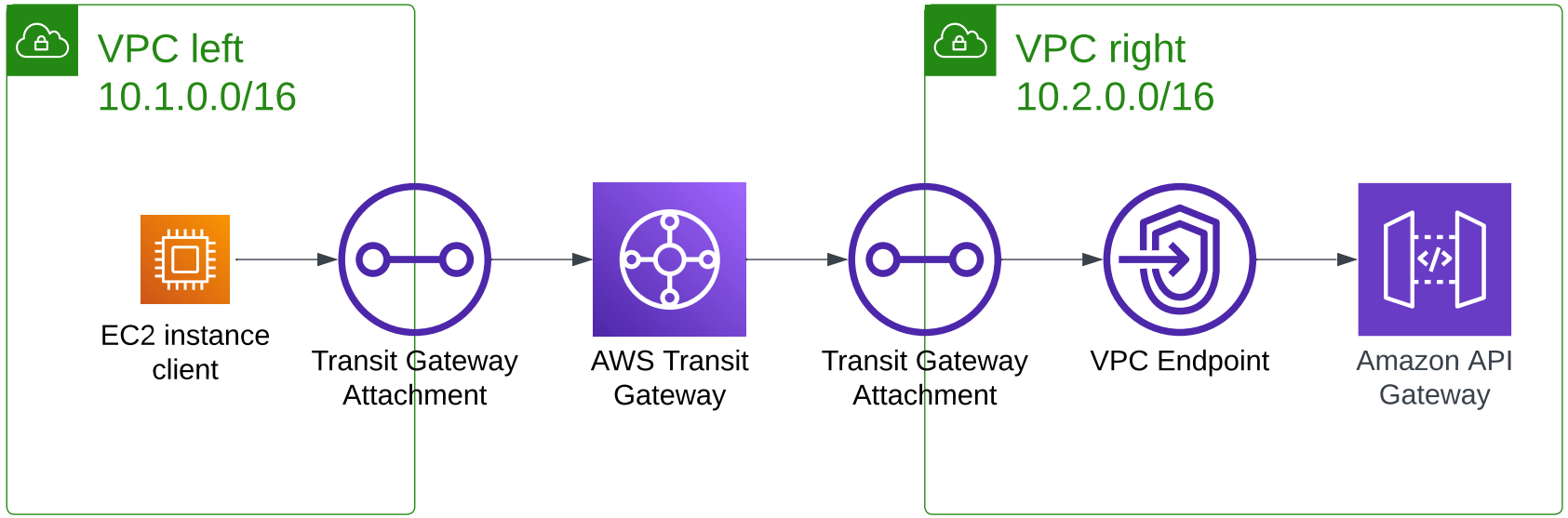
Wolfgang Schäfer (@wo_wue)

AWS Community Day DACH in Dresden

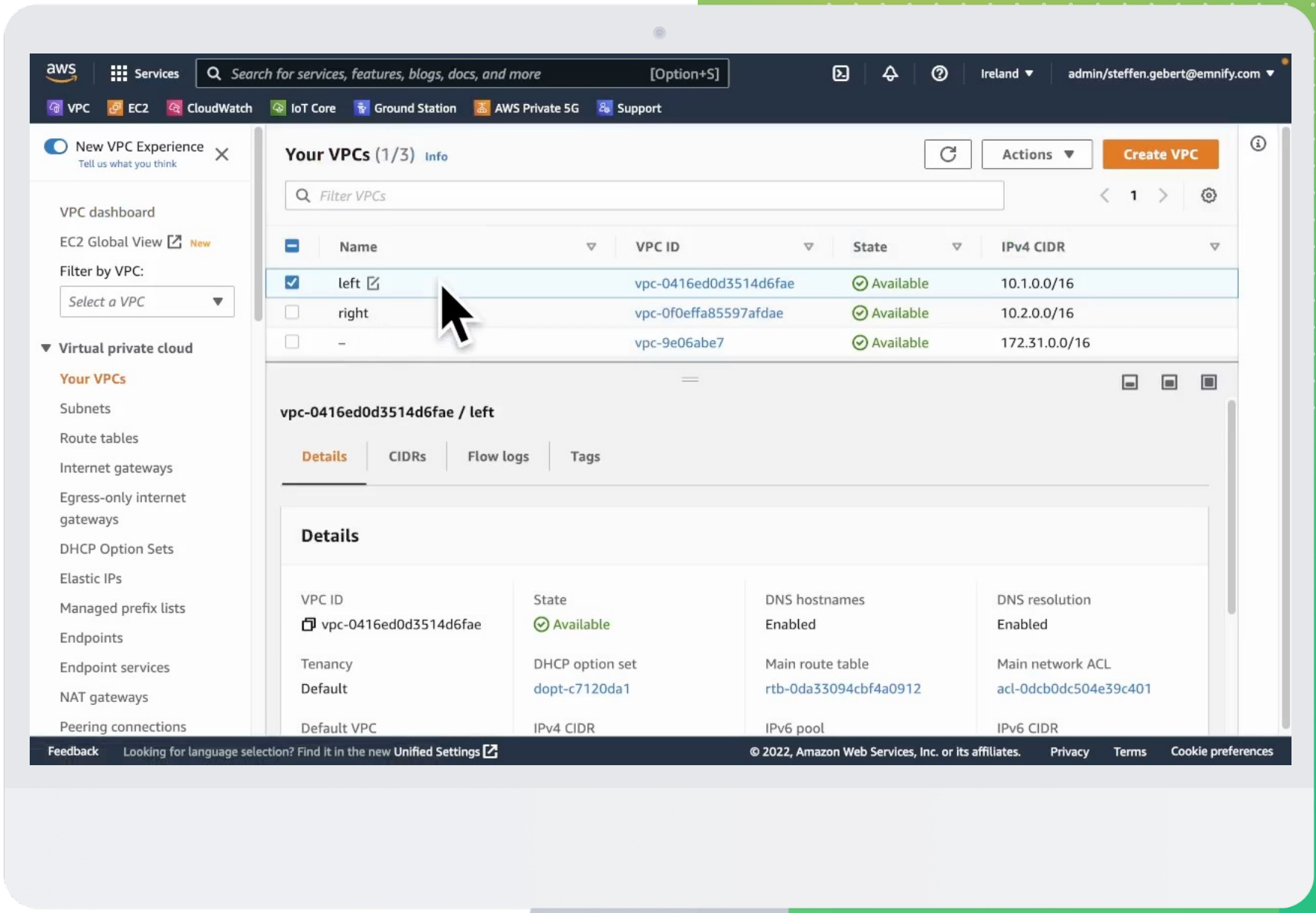
19.10.2022

UNSERE SPONSOREN

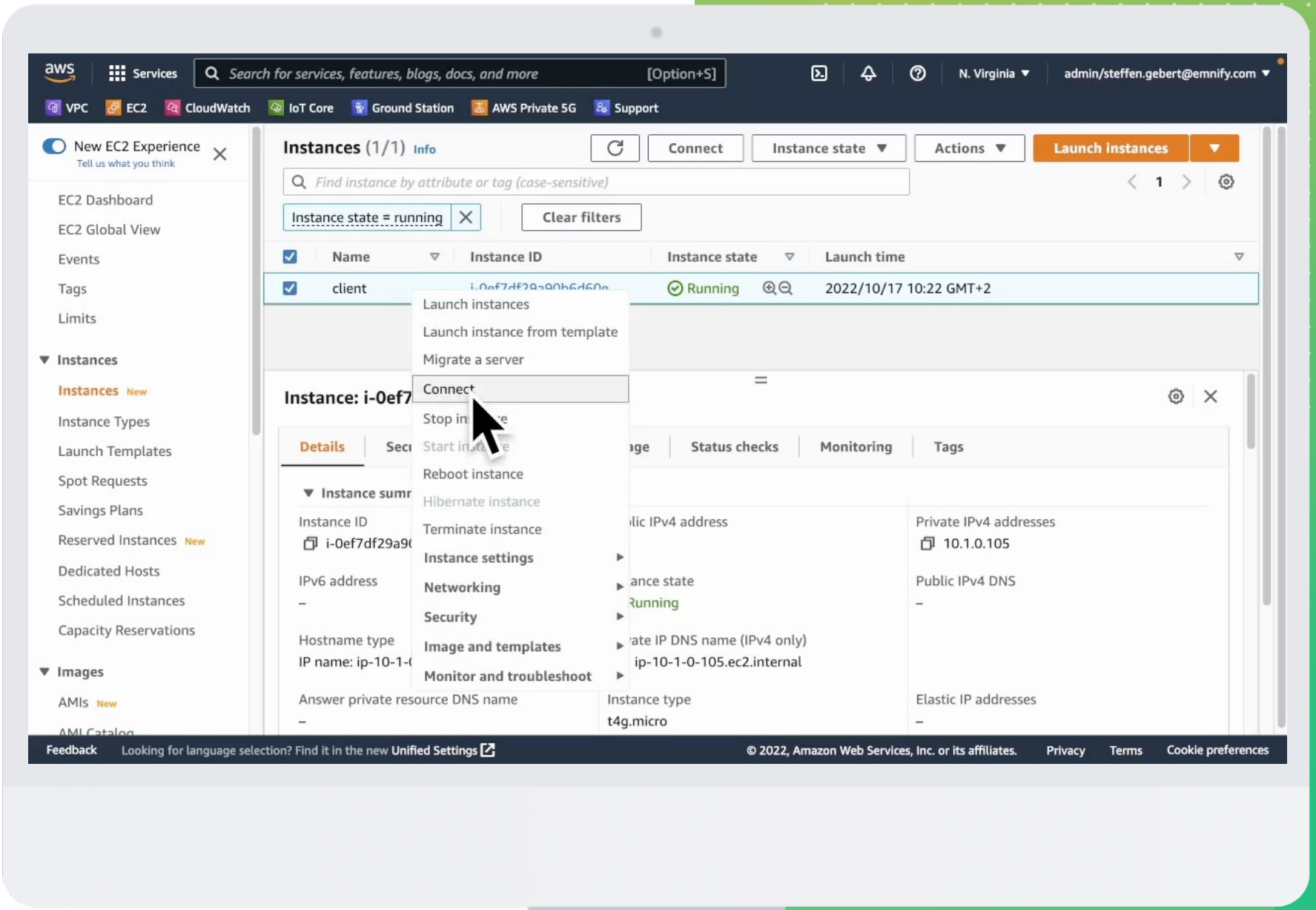
This is Our Architecture



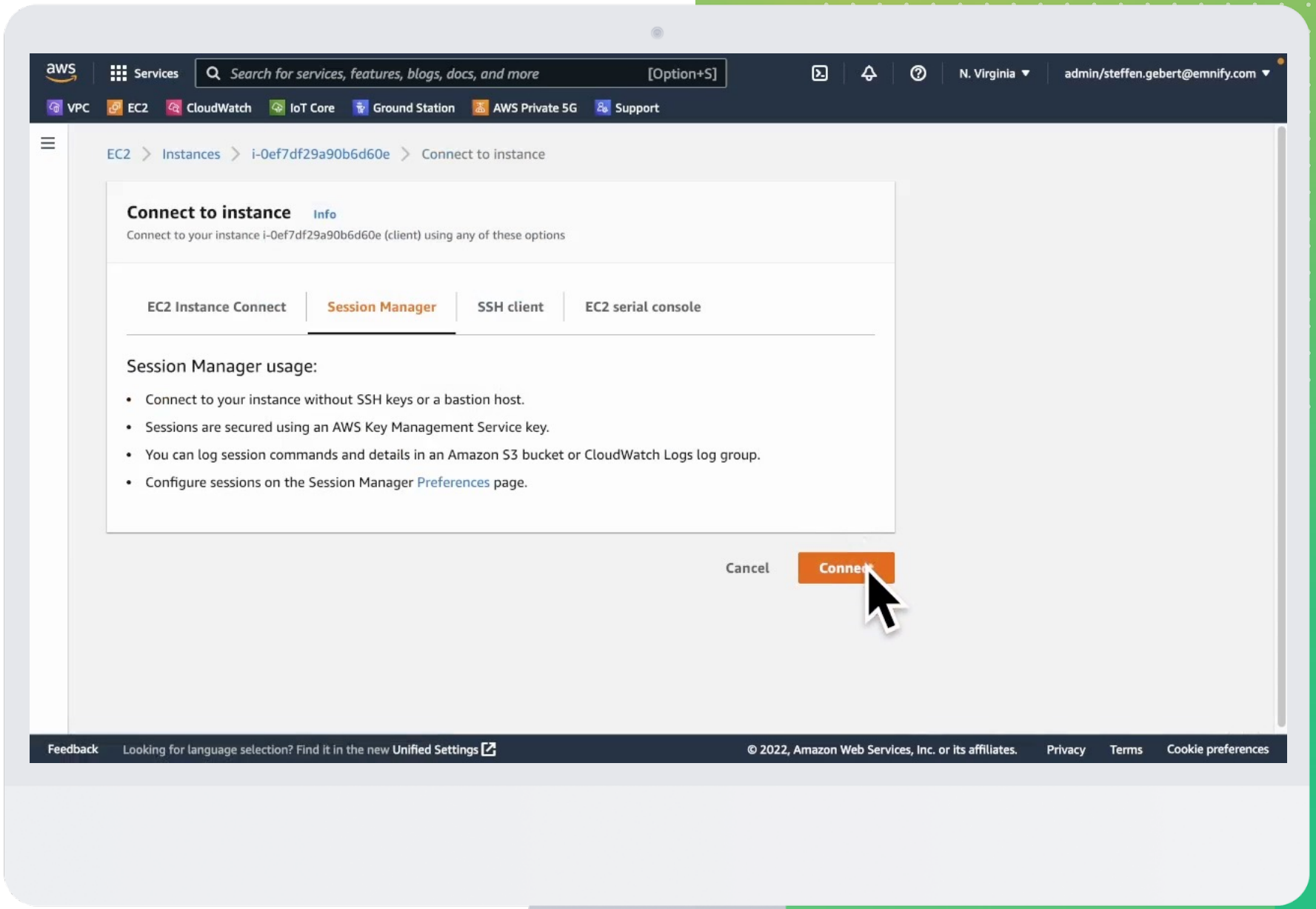
Problem


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Ireland
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
New VPC Experience
Tell us what you think
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP Option Sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Your VPCs (1/3) Info
Actions
Create VPC
Filter VPCs
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
CIDRs
Flow logs
Tags
Details
VPC ID
vpc-0416ed0d3514d6fae
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-c7120da1
Main route table
rtb-0da33094cbf4a0912
Main network ACL
acl-0dcb0dc504e39c401
Default VPC
IPv4 CIDR
IPv6 pool
IPv6 CIDR
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

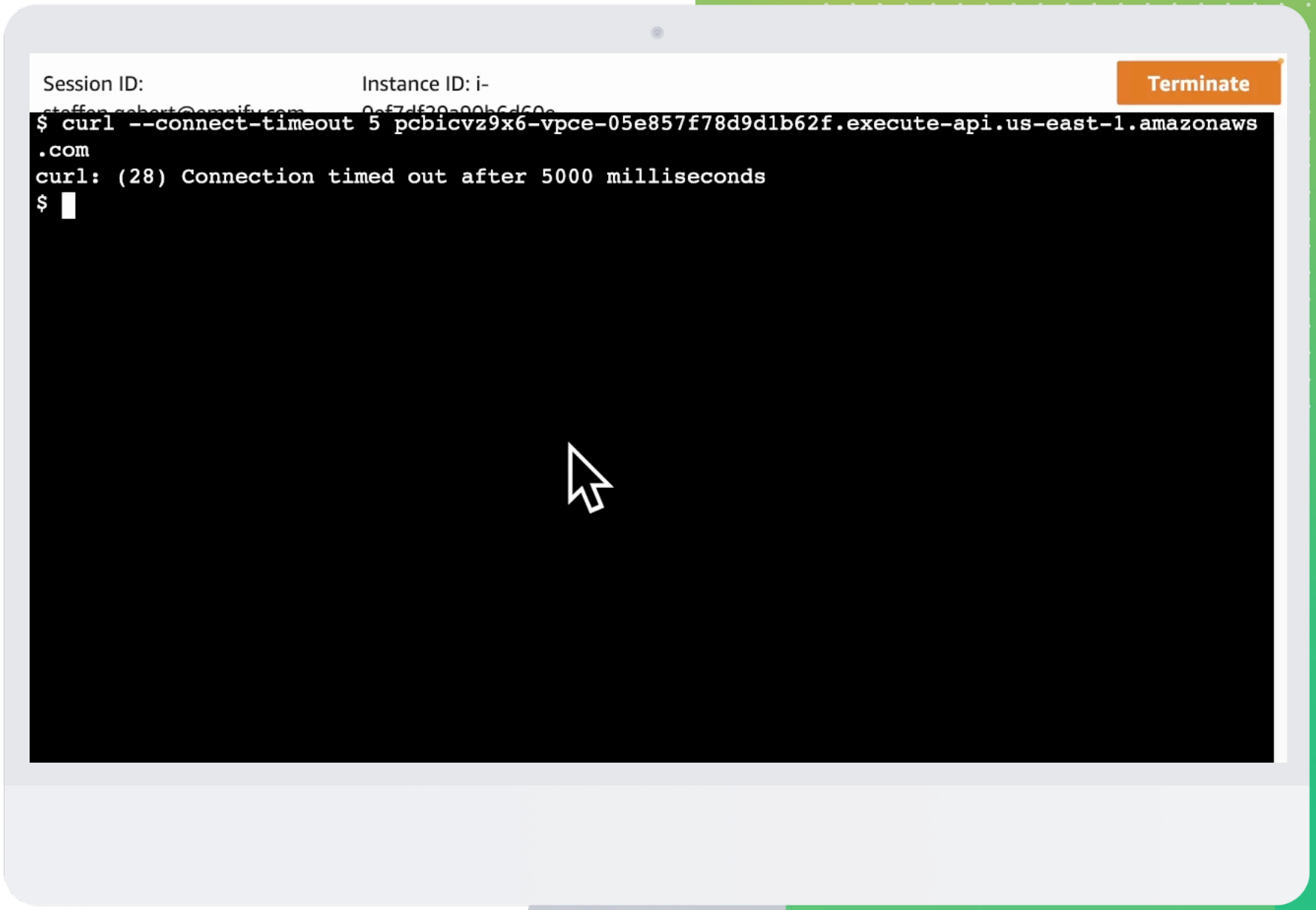
Problem


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
N. Virginia
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs New
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Instance state = running
Clear filters
Name
Instance ID
Instance state
Launch time
client
Running
2022/10/17 10:22 GMT+2
Launch instances
Launch instance from template
Migrate a server
Connect
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate instance
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Instance: i-0ef7
Details
Status checks
Monitoring
Tags
Instance ID
Private IPv4 addresses
10.1.0.105
IPv6 address
Public IPv4 DNS
Hostname type
ip-10-1-0-105.ec2.internal
Answer private resource DNS name
Instance type
t4g.micro
Elastic IP addresses
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

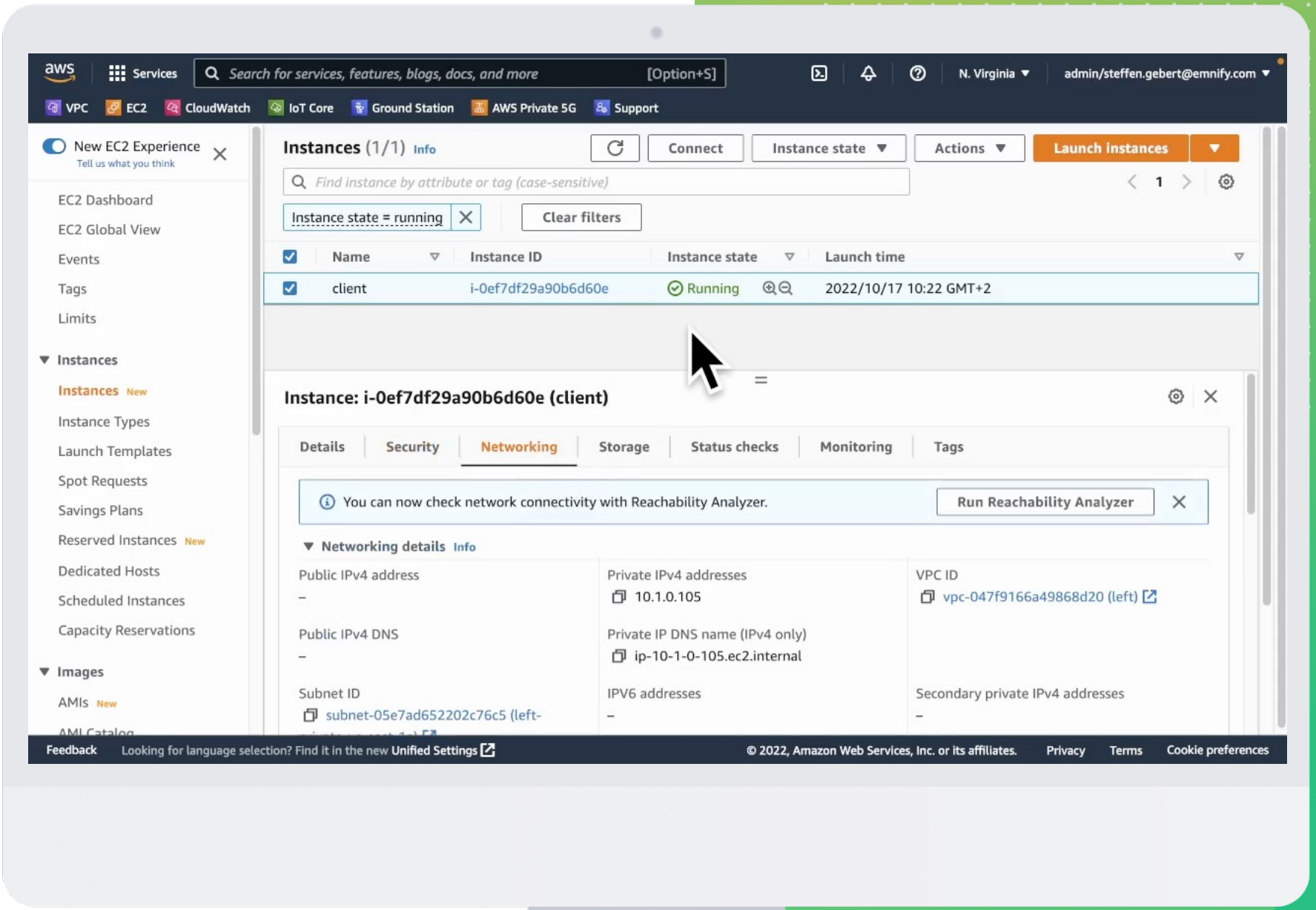
Problem


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
N. Virginia
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
EC2 > Instances > i-0ef7df29a90b6d60e > Connect to instance
Connect to instance
Info
Connect to your instance i-0ef7df29a90b6d60e (client) using any of these options
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Session Manager usage:
Connect to your instance without SSH keys or a bastion host.
Sessions are secured using an AWS Key Management Service key.
You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
Configure sessions on the Session Manager Preferences page.
Cancel
Connect
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

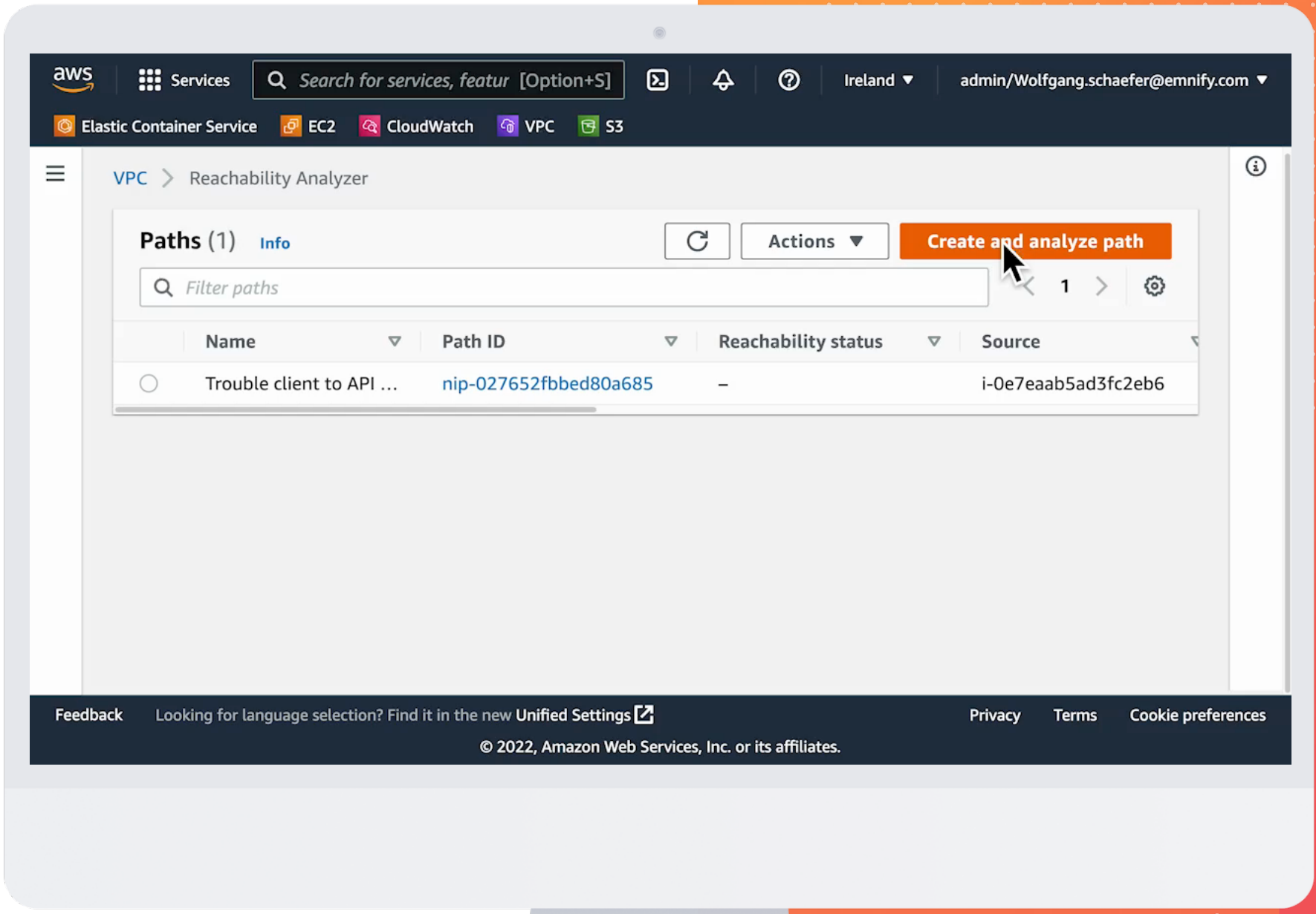
Problem


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
$

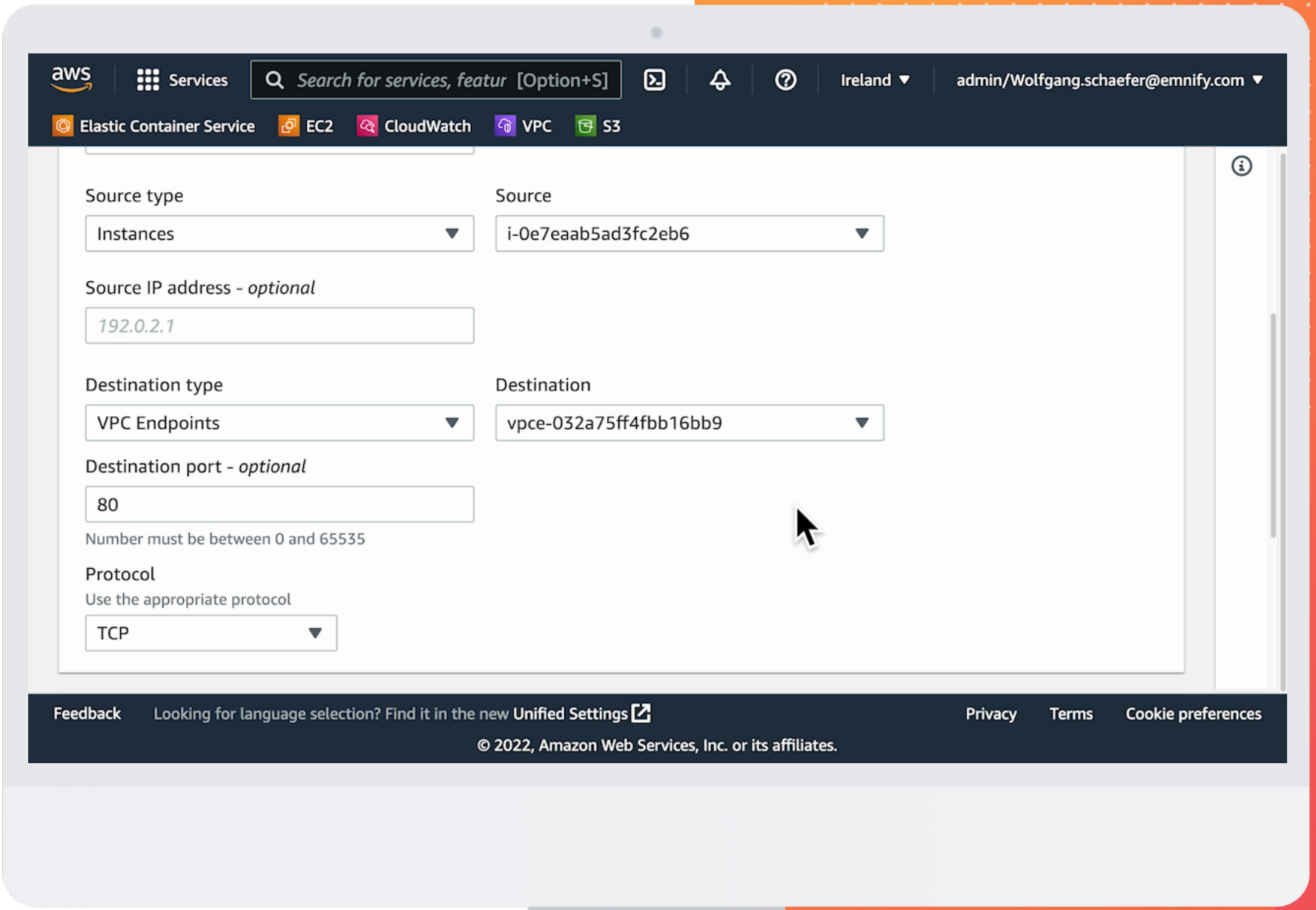
Problem


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
N. Virginia
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs New
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
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 Info
Public IPv4 address
–
Private IPv4 addresses
10.1.0.105
VPC ID
vpc-047f9166a49868d20 (left)
Public IPv4 DNS
–
Private IP DNS name (IPv4 only)
ip-10-1-0-105.ec2.internal
Subnet ID
subnet-05e7ad652202c76c5 (left-
IPV6 addresses
–
Secondary private IPv4 addresses
–
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

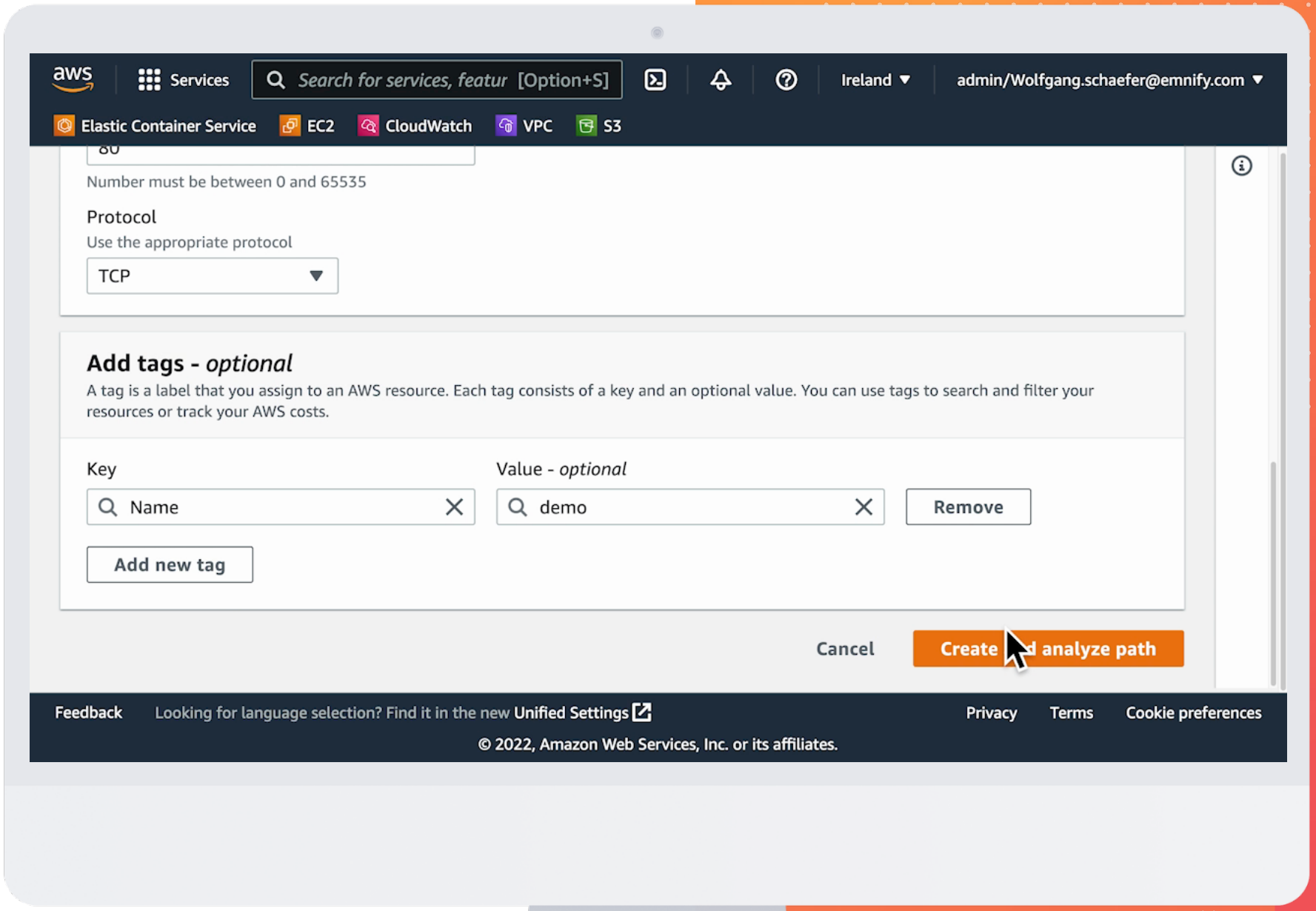
VPC Reachability Analyzer



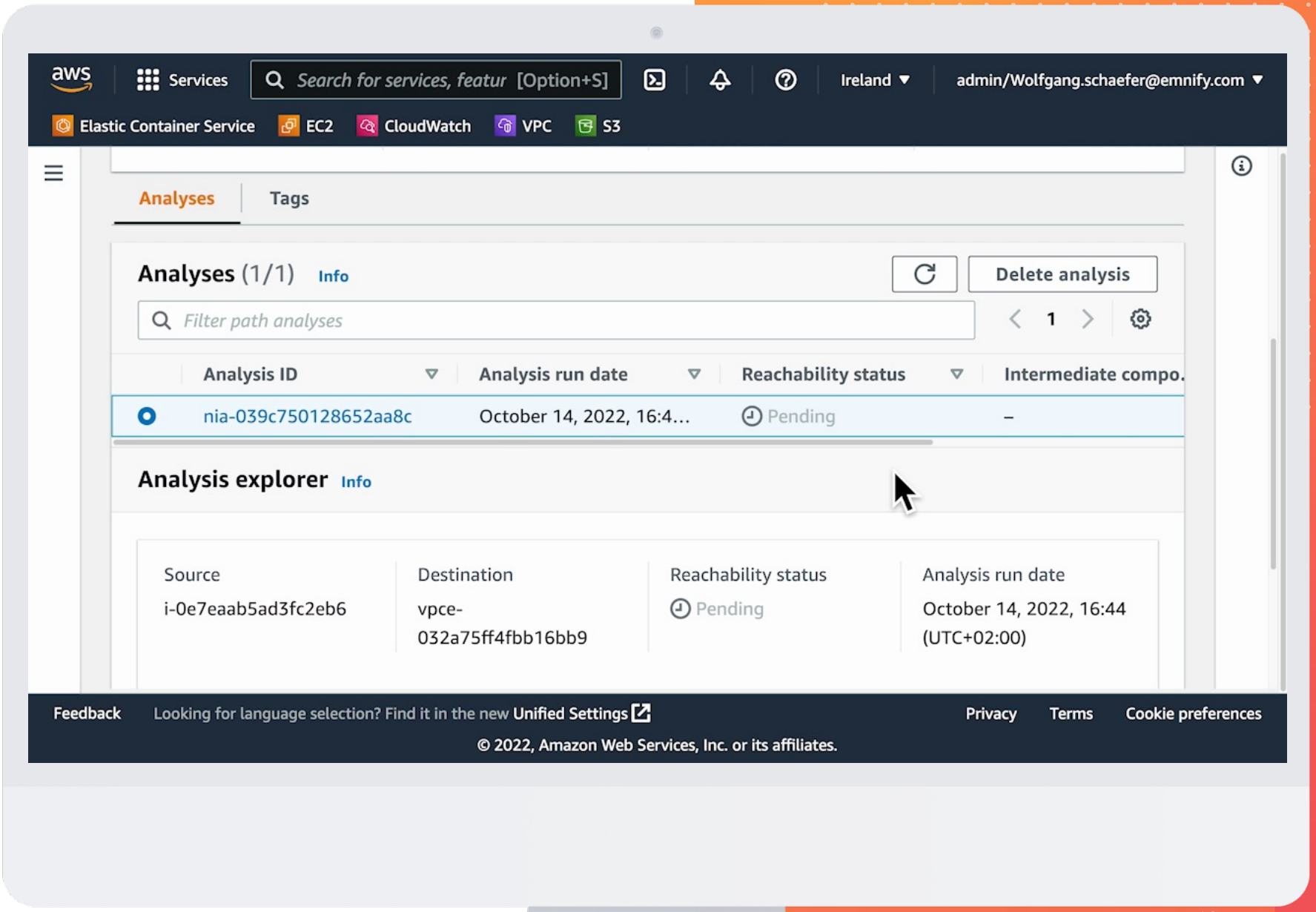
VPC Reachability Analyzer



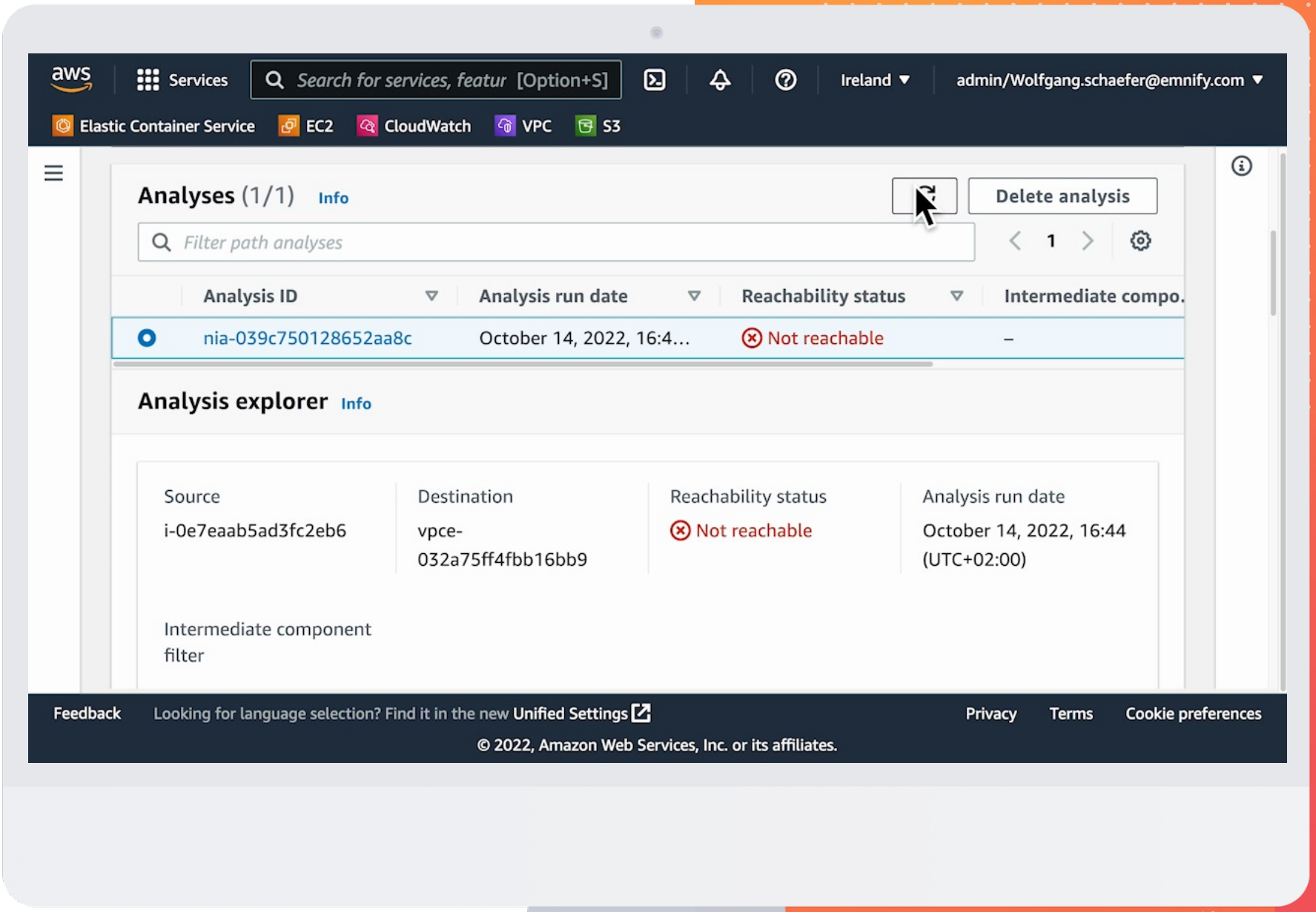
VPC Reachability Analyzer



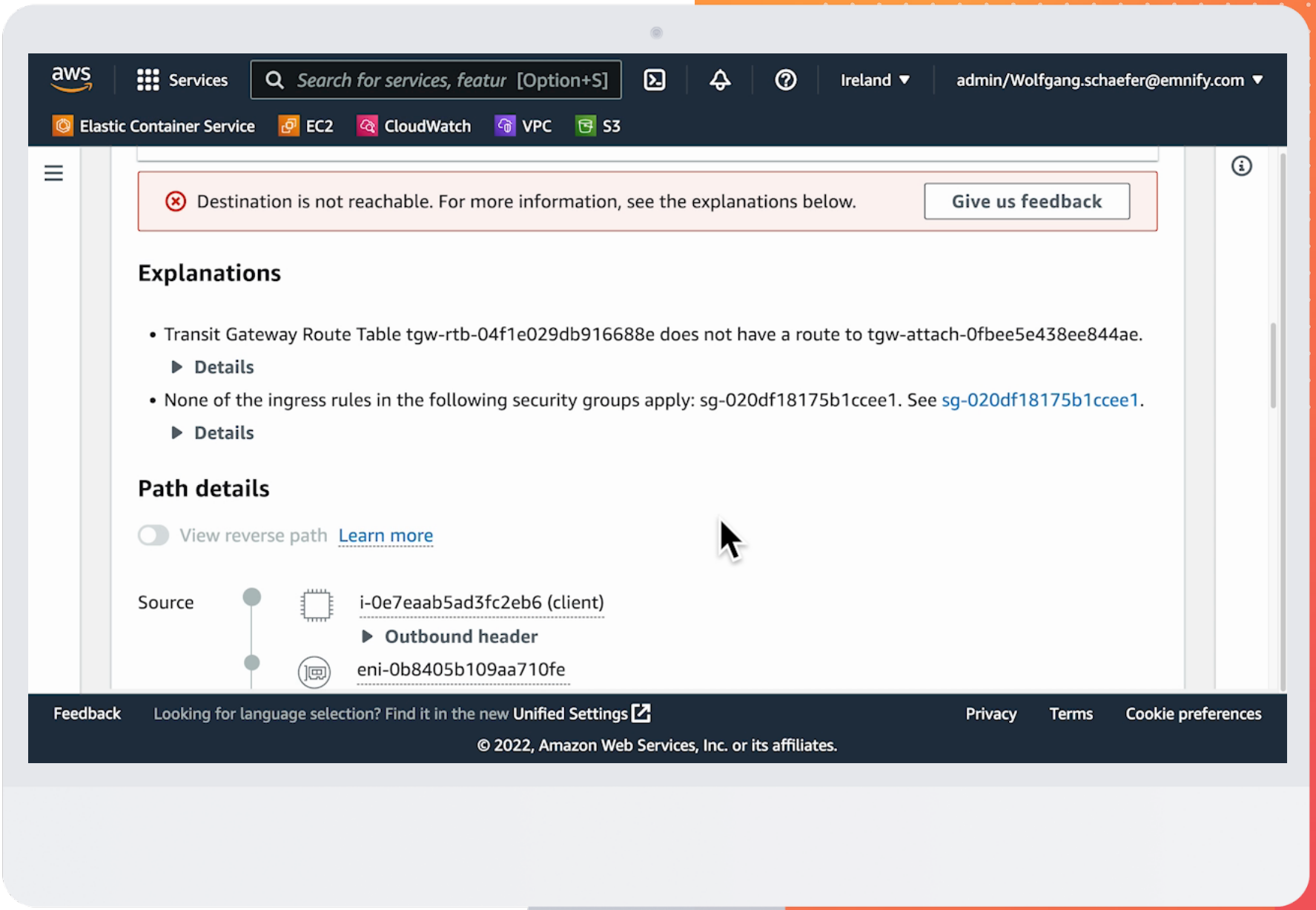
VPC Reachability Analyzer



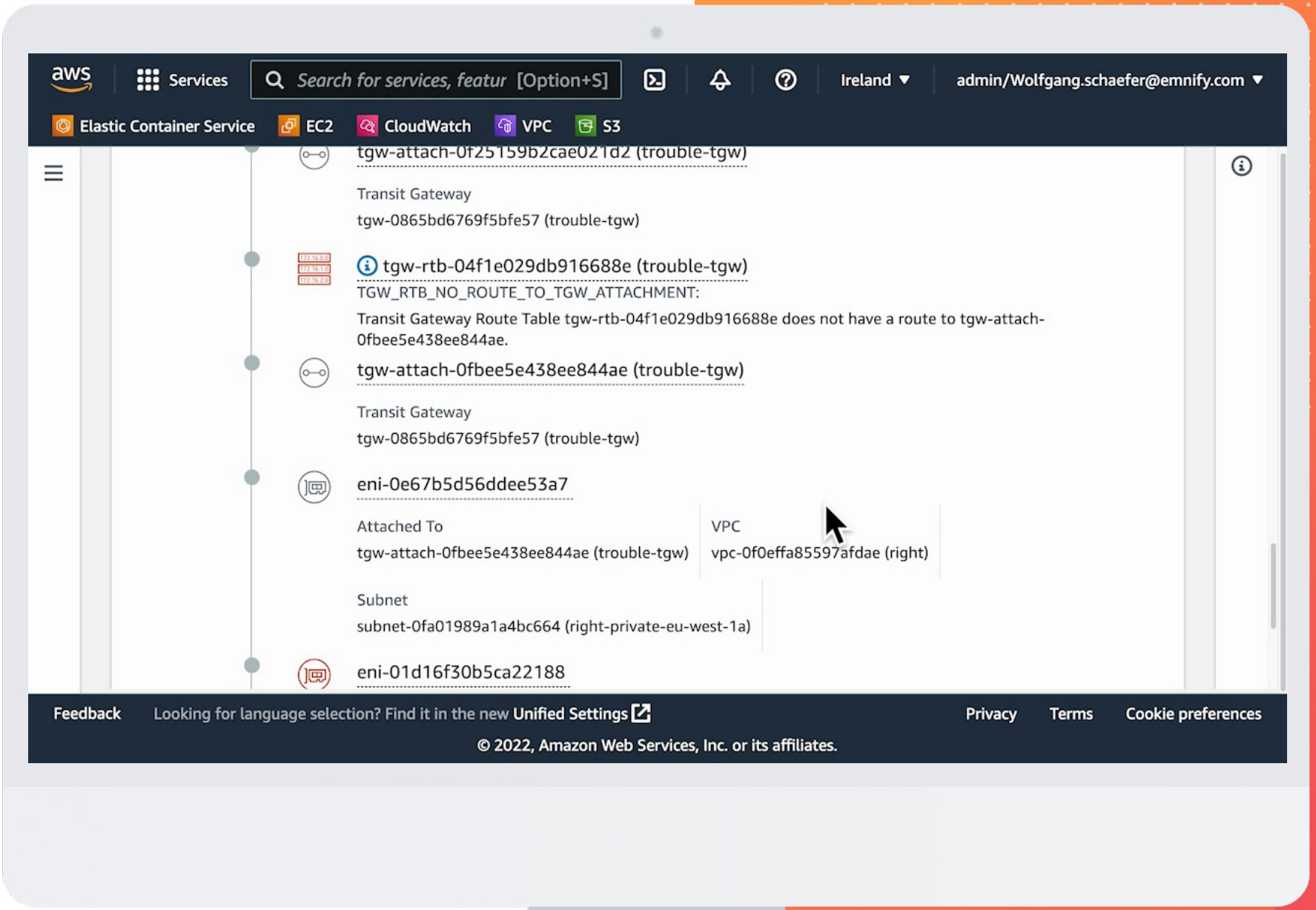
VPC Reachability Analyzer



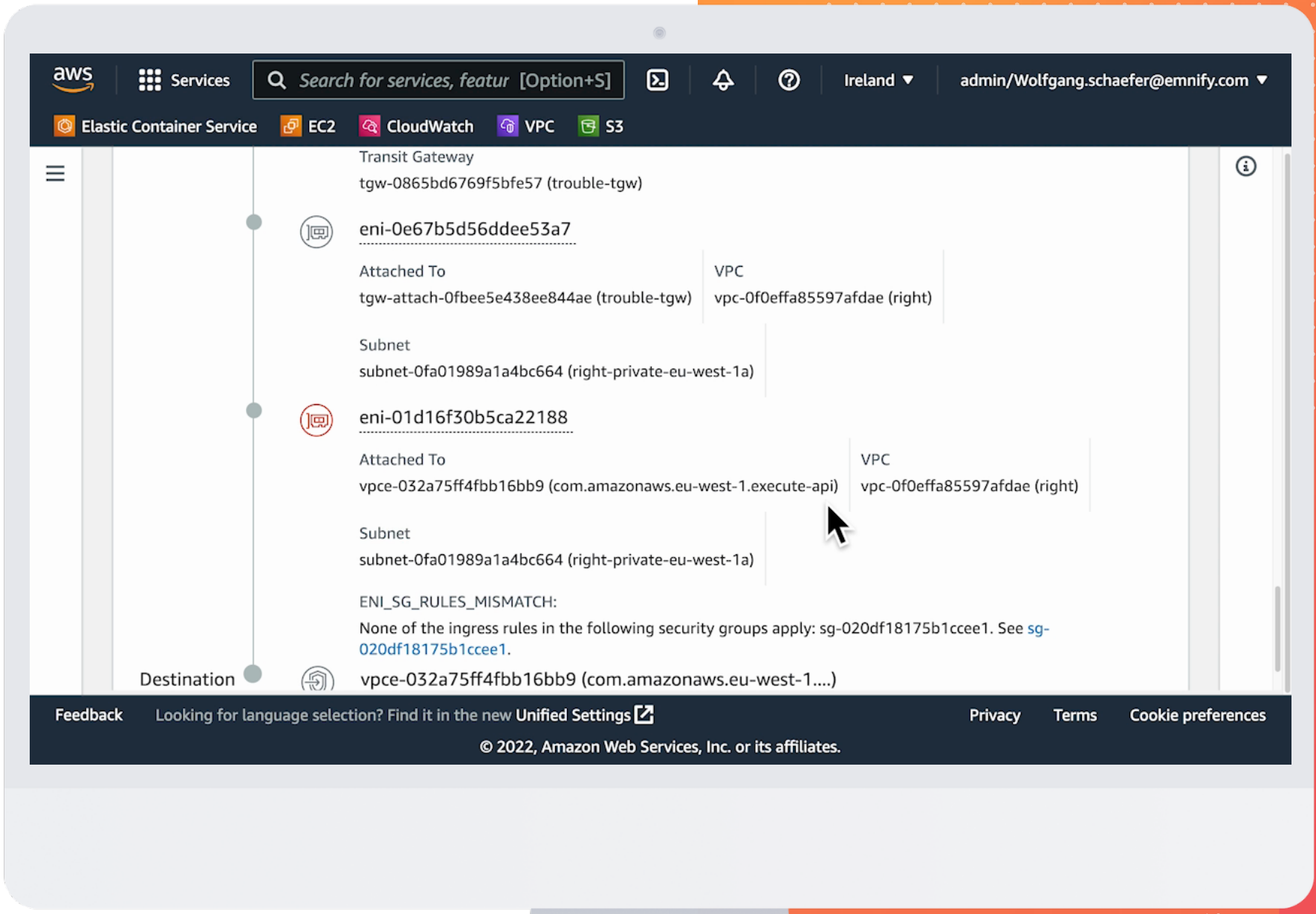
VPC Reachability Analyzer



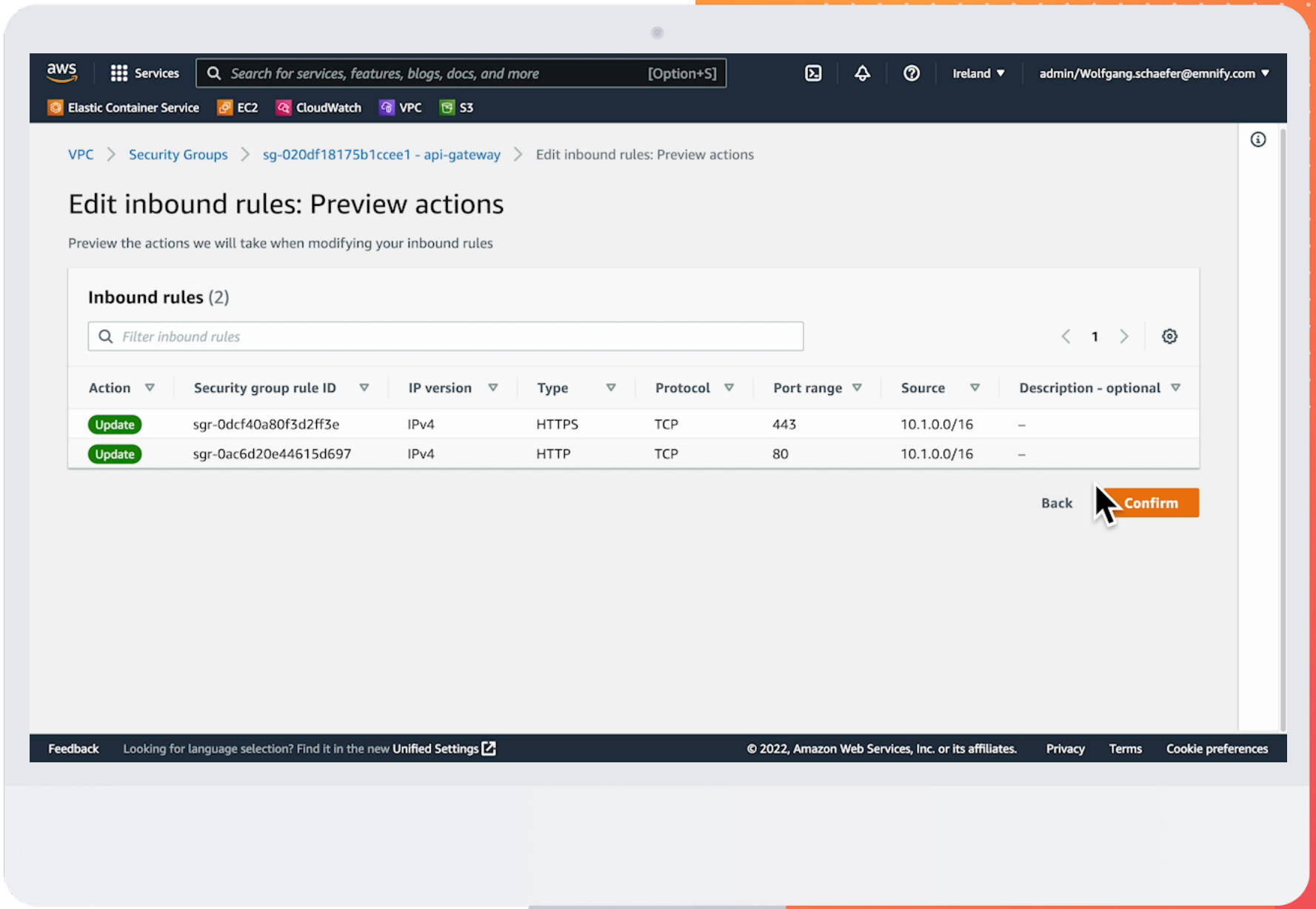
VPC Reachability Analyzer



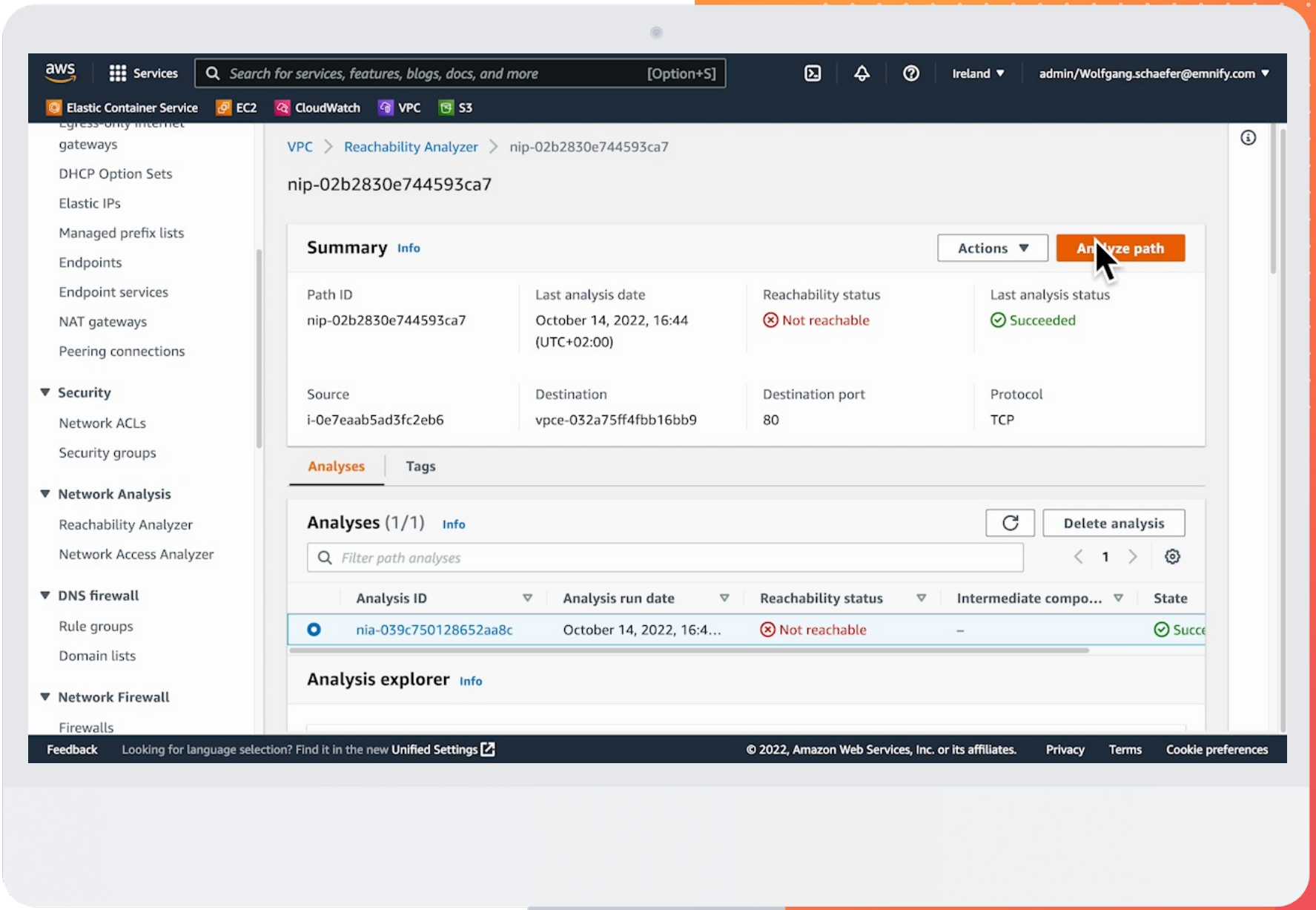
VPC Reachability Analyzer



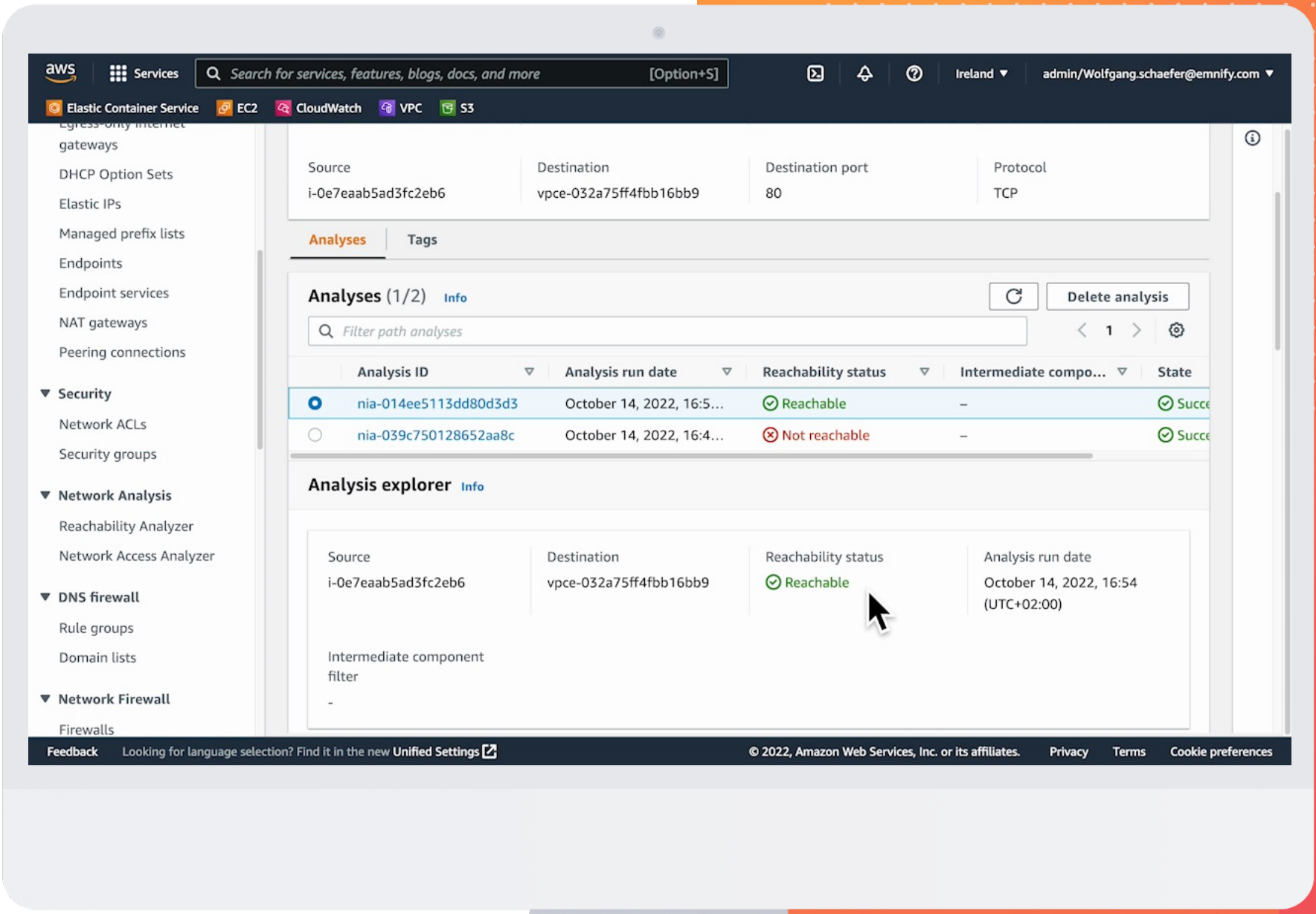
Fixing Connectivity



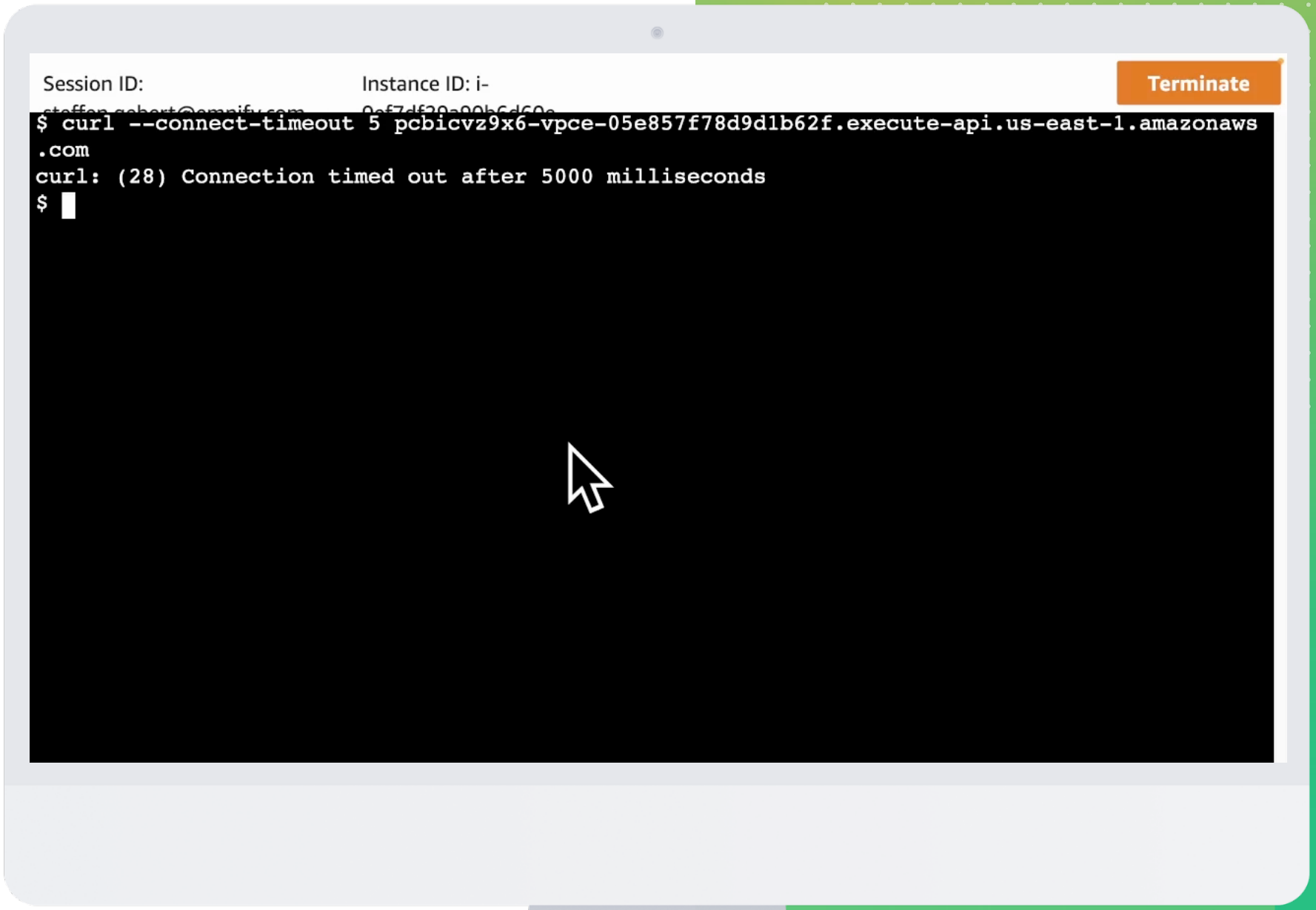
VPC Reachability Analyzer



VPC Reachability Analyzer



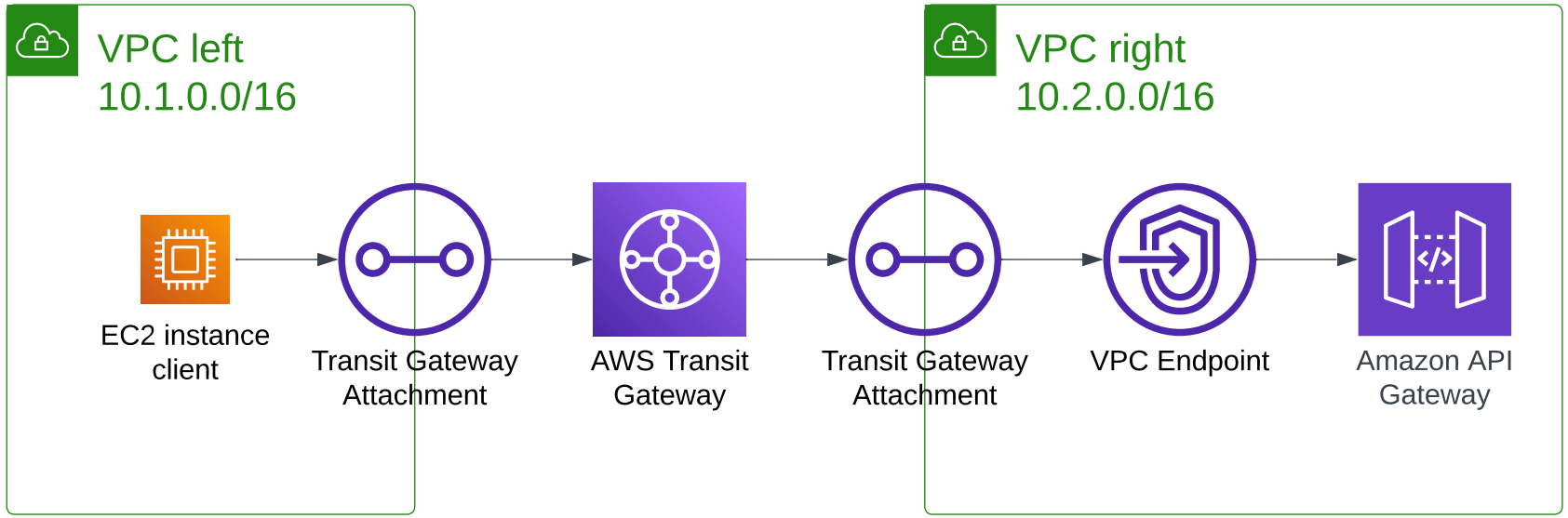
Connectivity Test



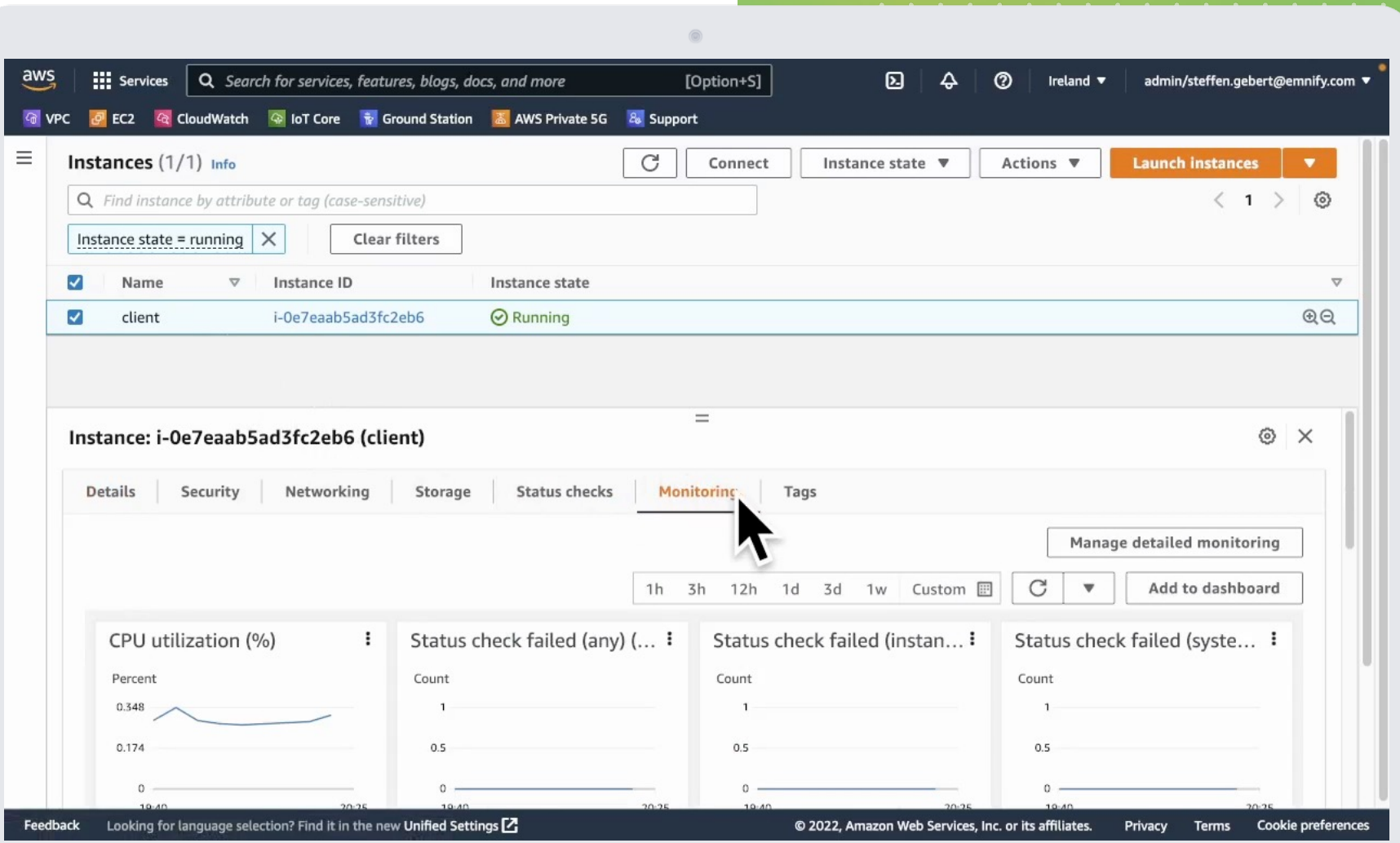
EMnify

Metrics

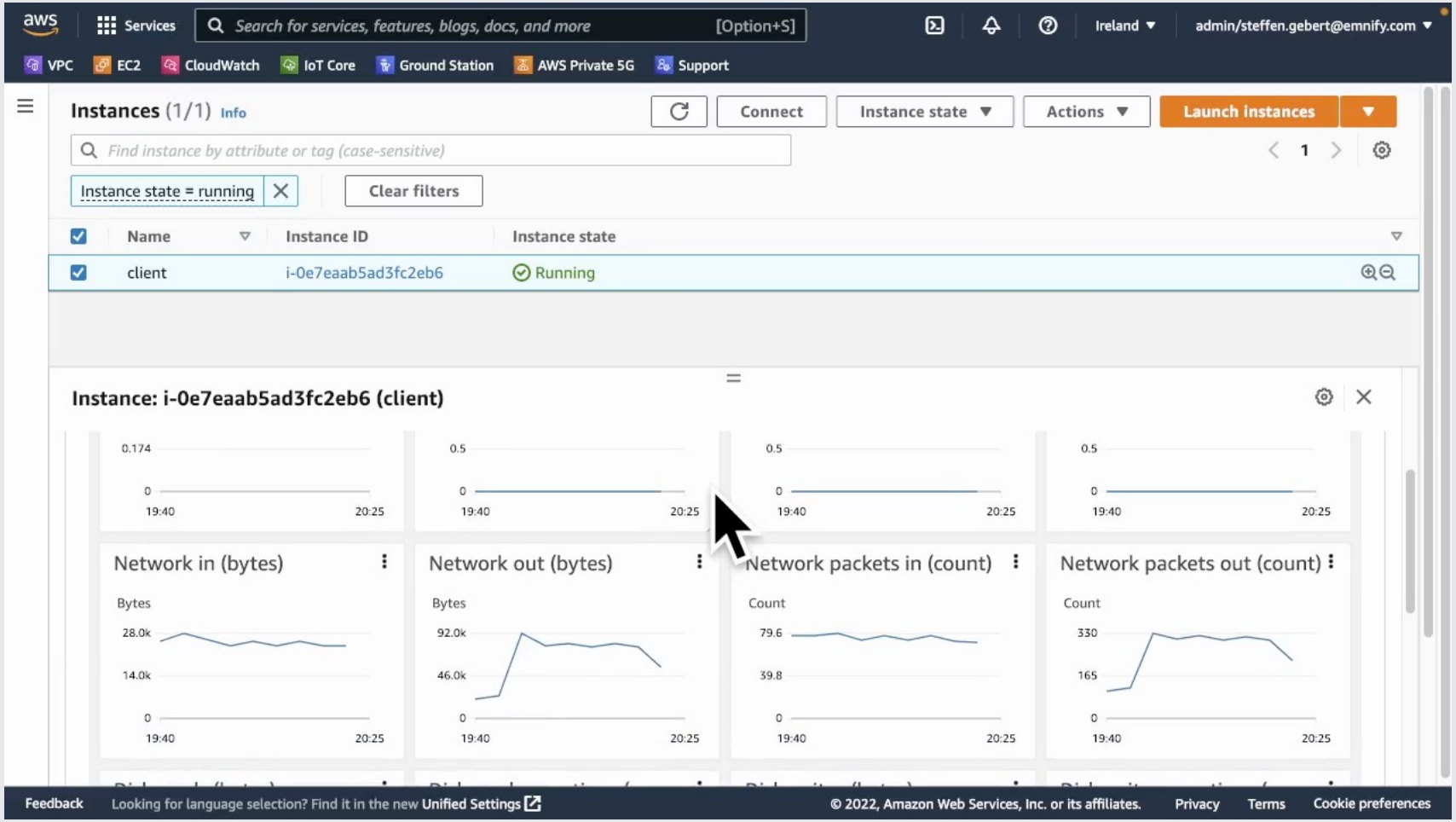
This is Our Architecture



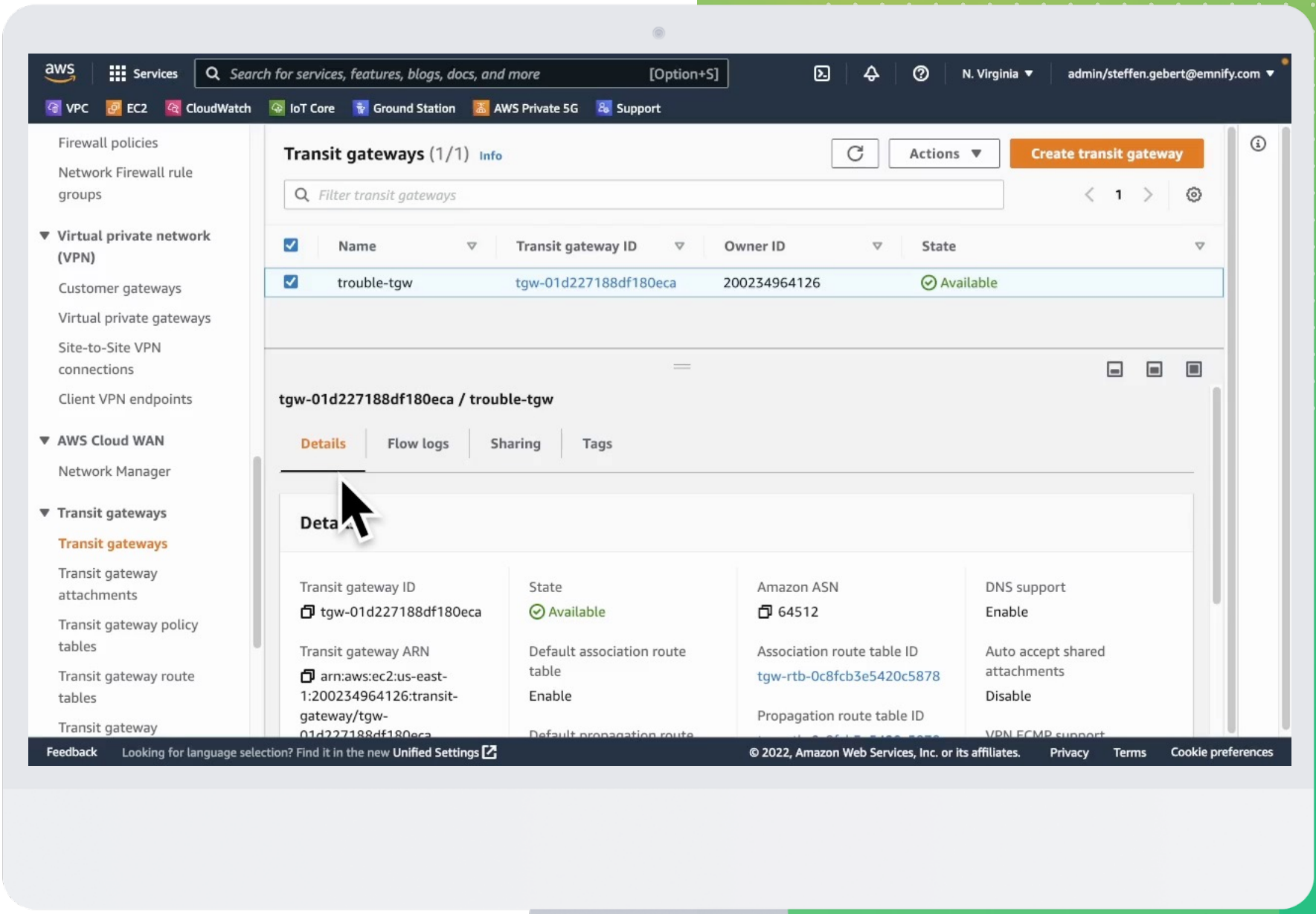
Metrics


aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Ireland
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
1
Instance state = running
Clear filters
Name
Instance ID
Instance state
client
i-0e7eaab5ad3fc2eb6
Running
Instance: i-0e7eaab5ad3fc2eb6 (client)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Manage detailed monitoring
1h
3h
12h
1d
3d
1w
Custom
Add to dashboard
CPU utilization (%)
Percent
0.348
0.174
0
Status check failed (any) (...
Count
1
0.5
0
Status check failed (instan...
Count
1
0.5
0
Status check failed (syste...
Count
1
0.5
0
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Metrics

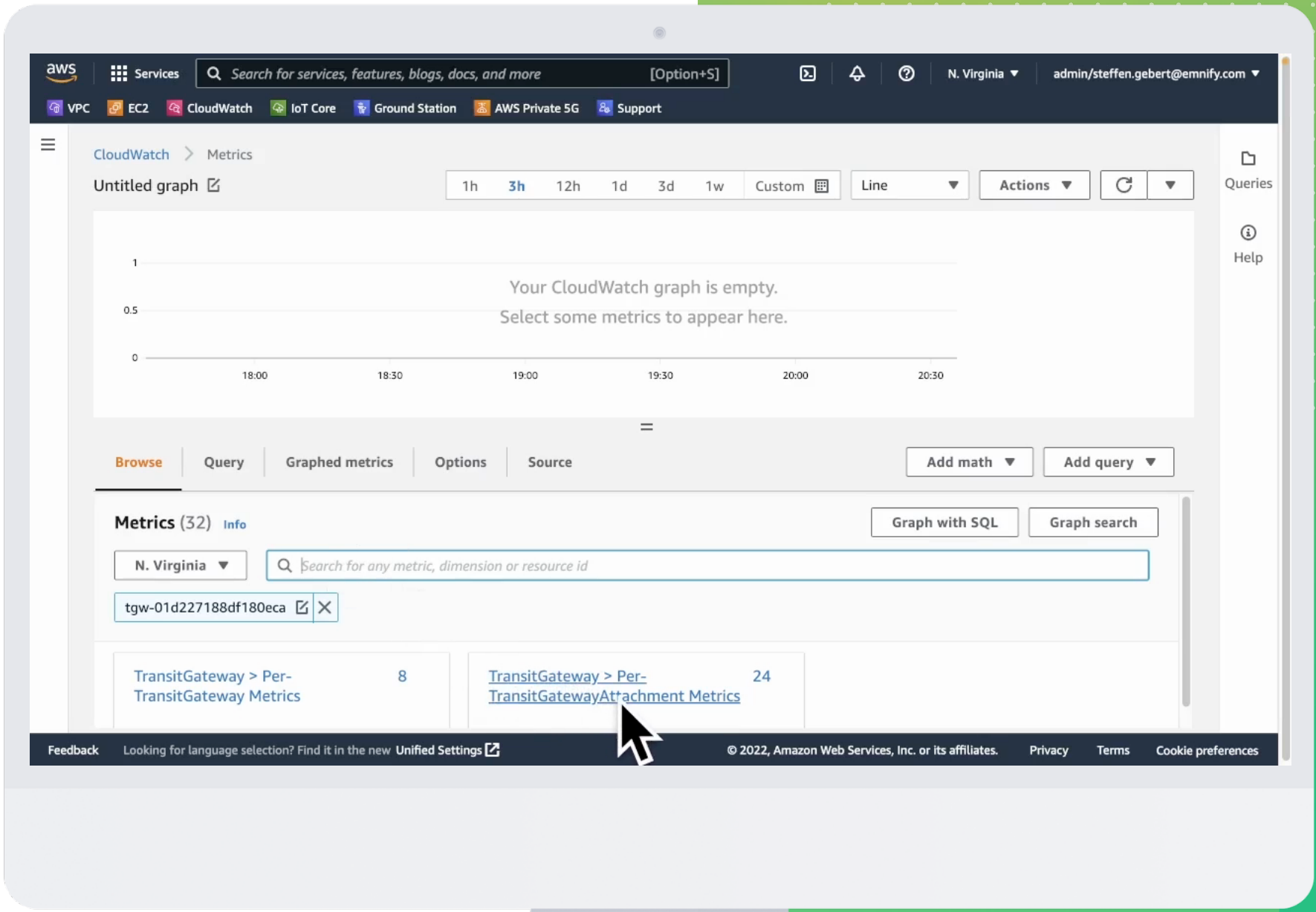

aws
Services
Search for services, features, blogs, docs, and more
[Option+S]
Ireland
admin/steffen.gebert@emnify.com
VPC
EC2
CloudWatch
IoT Core
Ground Station
AWS Private 5G
Support
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
1
Instance state = running
Clear filters
Name
Instance ID
Instance state
client
i-0e7eaab5ad3fc2eb6
Running
Instance: i-0e7eaab5ad3fc2eb6 (client)
Network in (bytes)
Bytes
28.0k
14.0k
0
19:40
20:25
Network out (bytes)
Bytes
92.0k
46.0k
Network packets in (count)
Count
79.6
39.8
Network packets out (count)
Count
330
165
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Metrics Transit GW



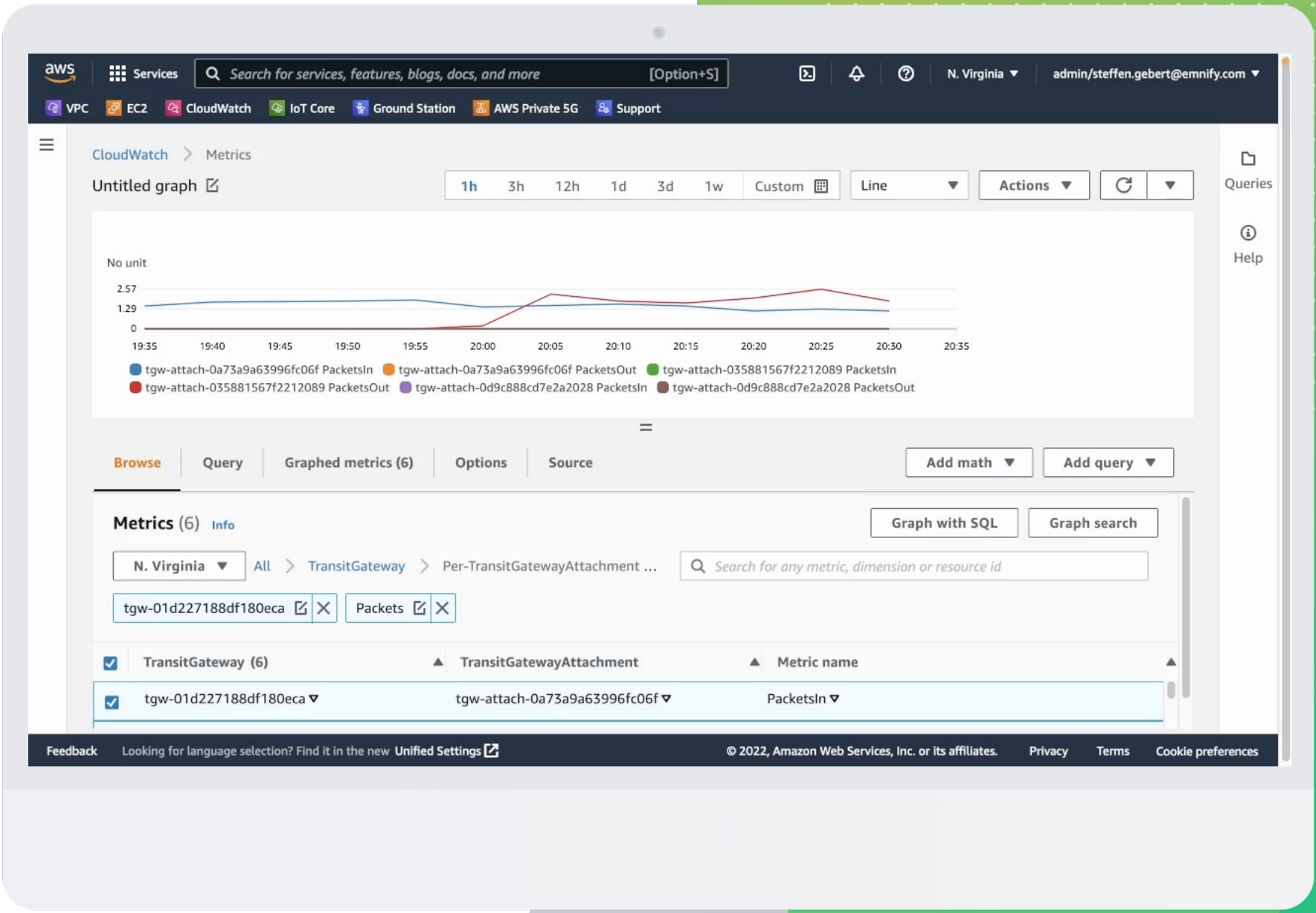
Metrics Transit GW

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



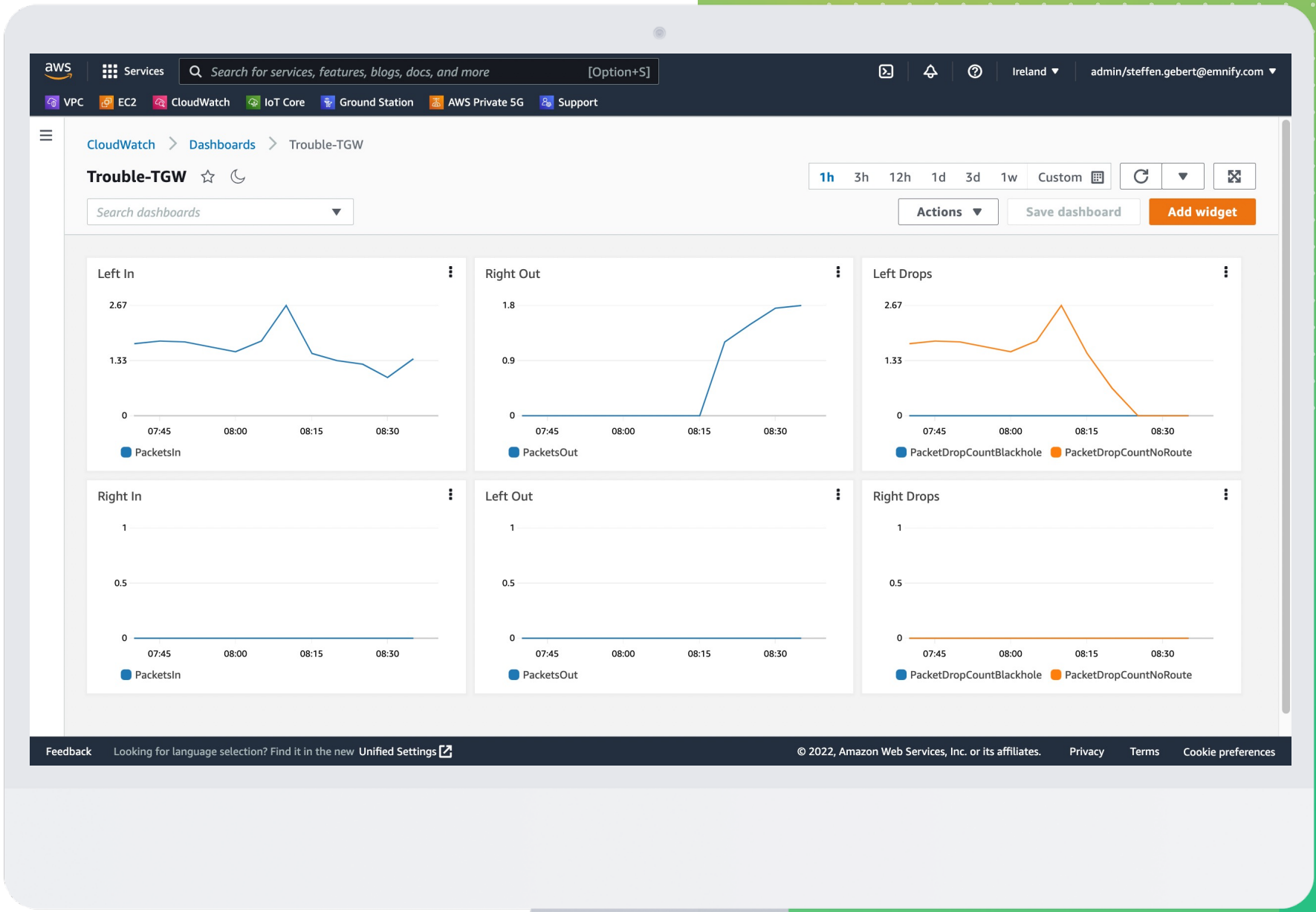
Metrics Transit GW

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



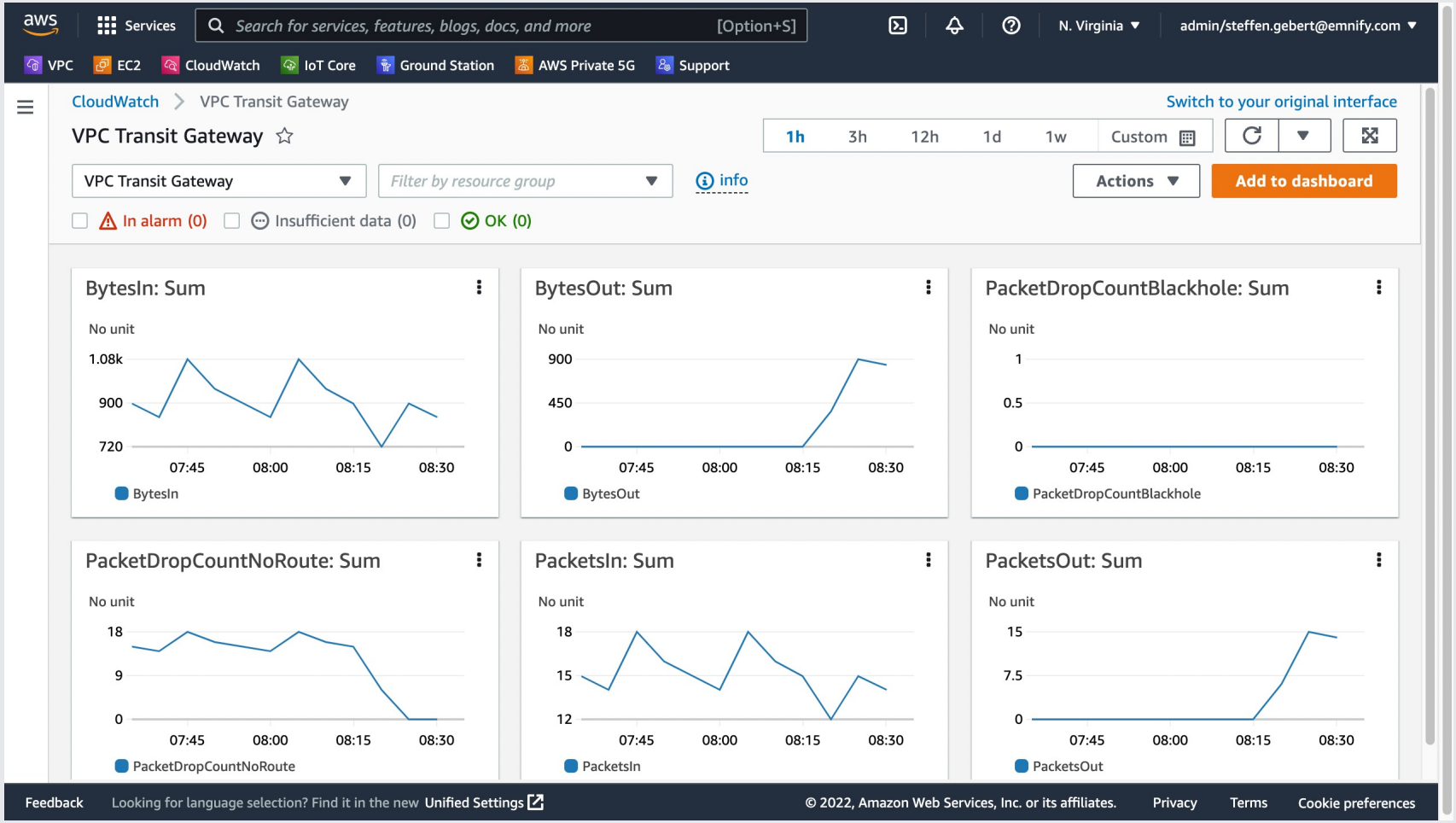
Metrics Transit GW

- Custom Dashboard



Metrics Transit GW

- Automatic Dashboard “VPC Transit Gateway”

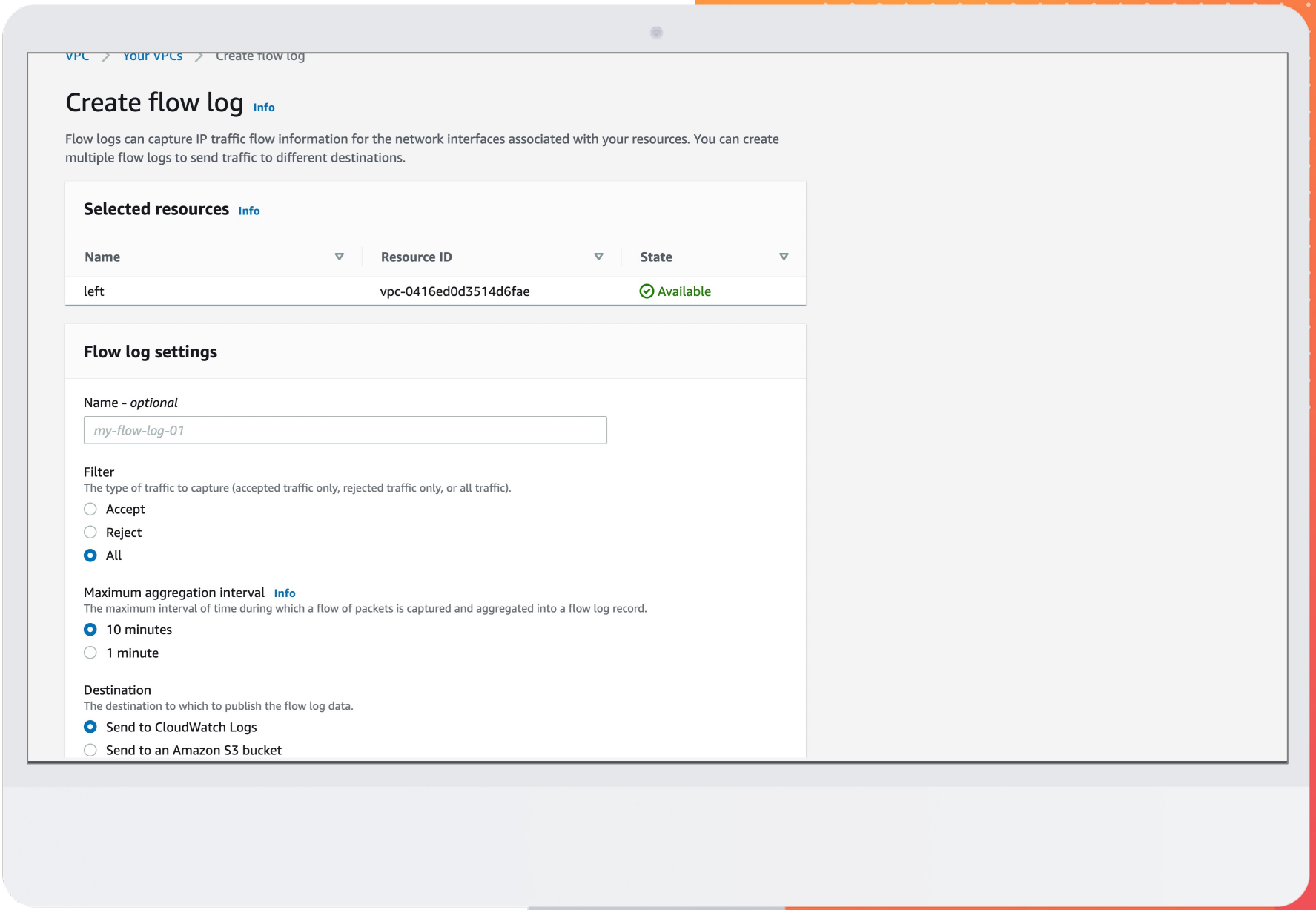


EMnify

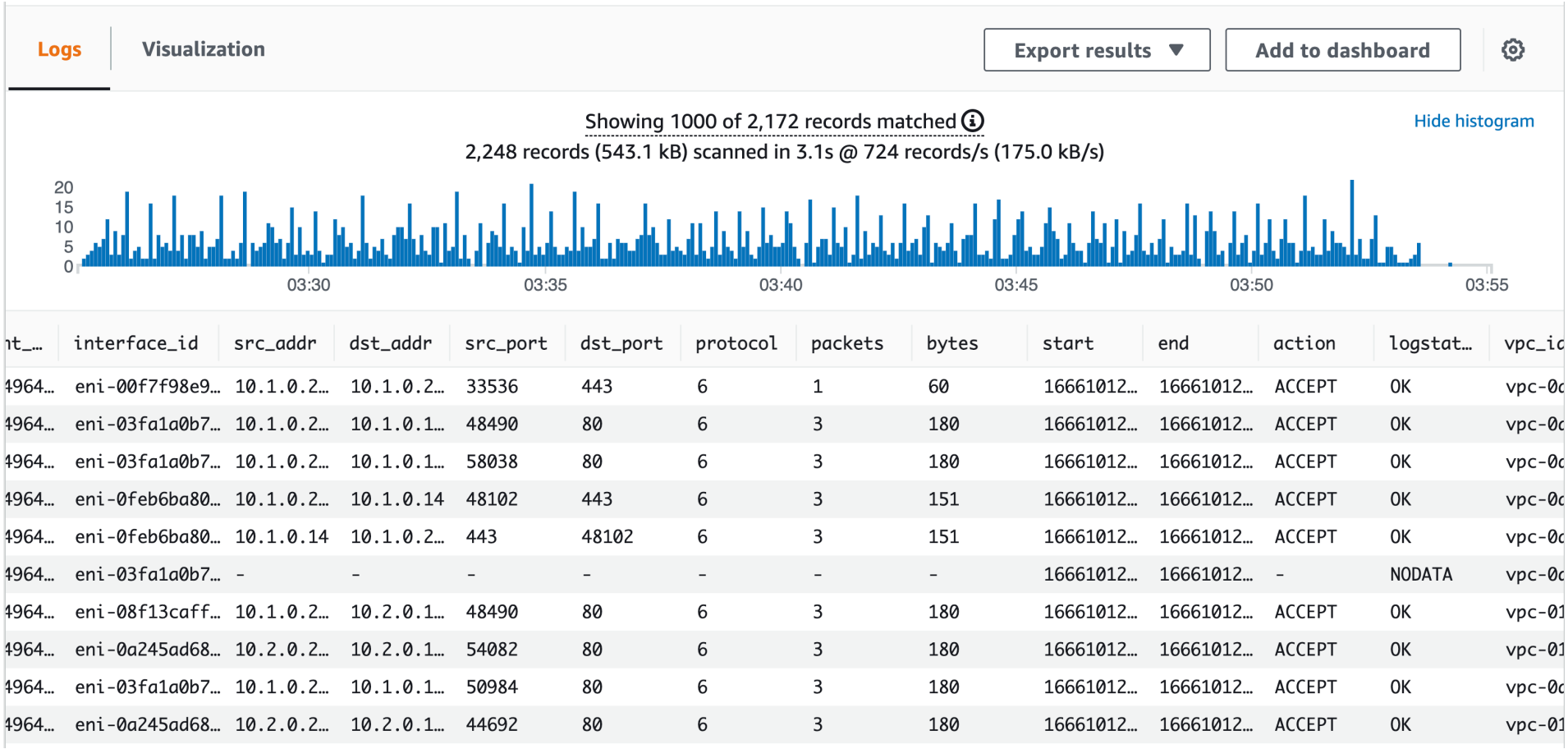
Flow Logs

Flow Logs

- VPC Flow Logs
- TGW Flow Logs new

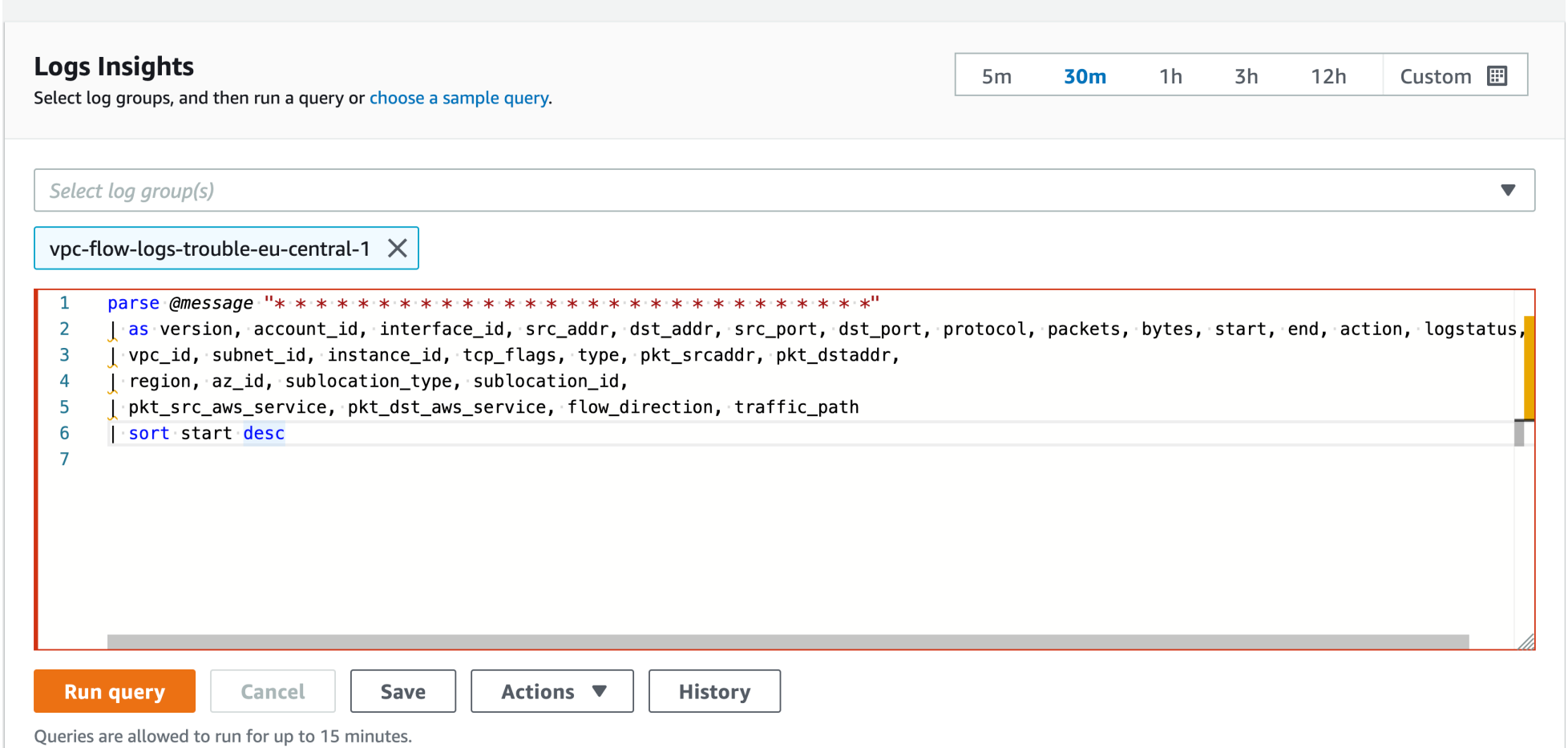


CloudWatch Logs Insights

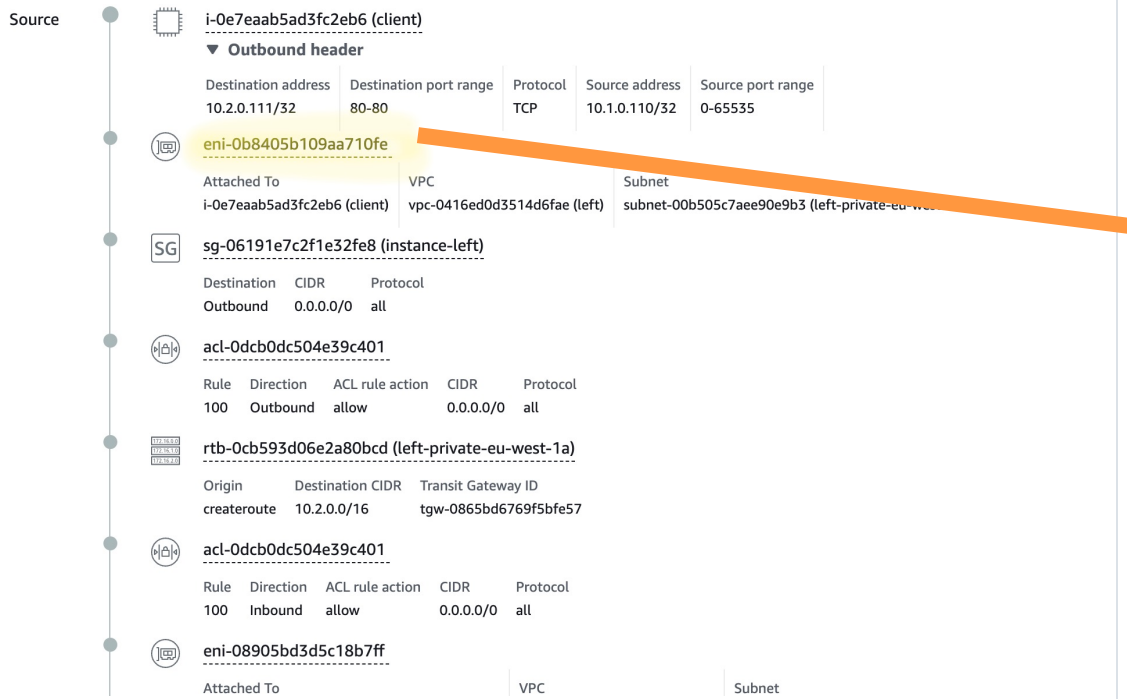


ıt_…	interface_id	src_addr	dst_addr	src_port	dst_port	protocol	packets	bytes	start	end	action	logstat…	vpc_ic
4964…	eni-00f7f98e9…	10.1.0.2…	10.1.0.2…	33536	443	6	1	60	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-03fa1a0b7…	10.1.0.2…	10.1.0.1…	48490	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-03fa1a0b7…	10.1.0.2…	10.1.0.1…	58038	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-0feb6ba80…	10.1.0.2…	10.1.0.14	48102	443	6	3	151	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-0feb6ba80…	10.1.0.14	10.1.0.2…	443	48102	6	3	151	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-03fa1a0b7…	-	-	-	-	-	-	-	16661012…	16661012…	-	NODATA	vpc-0c
4964…	eni-08f13caff…	10.1.0.2…	10.2.0.1…	48490	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-01
4964…	eni-0a245ad68…	10.2.0.2…	10.2.0.1…	54082	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-01
4964…	eni-03fa1a0b7…	10.1.0.2…	10.1.0.1…	50984	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-0c
4964…	eni-0a245ad68…	10.2.0.2…	10.2.0.1…	44692	80	6	3	180	16661012…	16661012…	ACCEPT	OK	vpc-01

CloudWatch Logs Insights

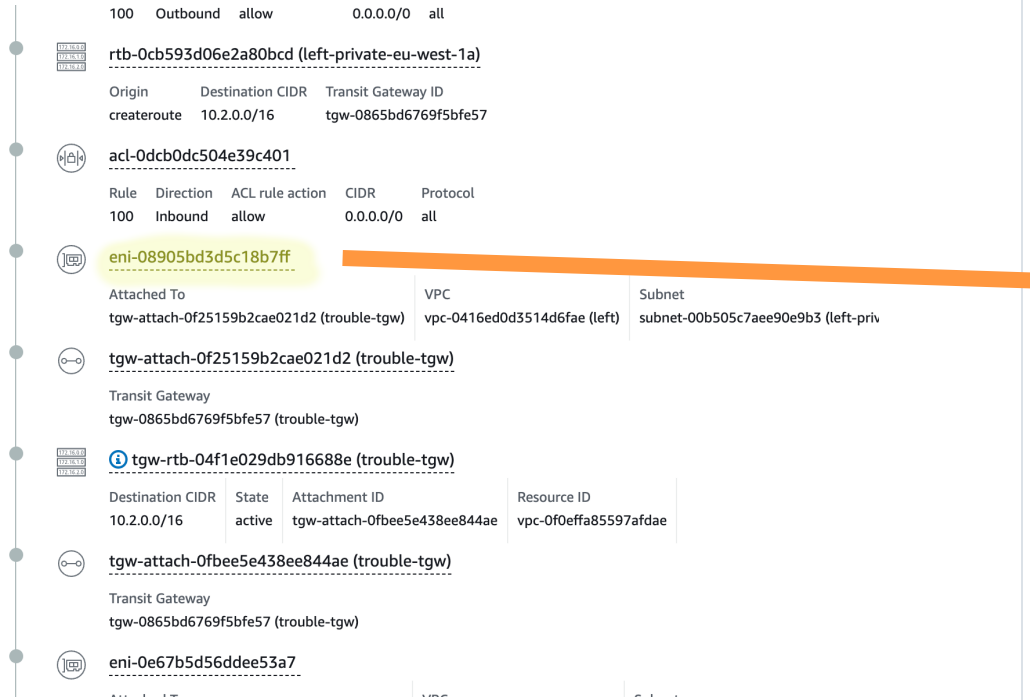


Reachability Analyzer zu Flow Logs



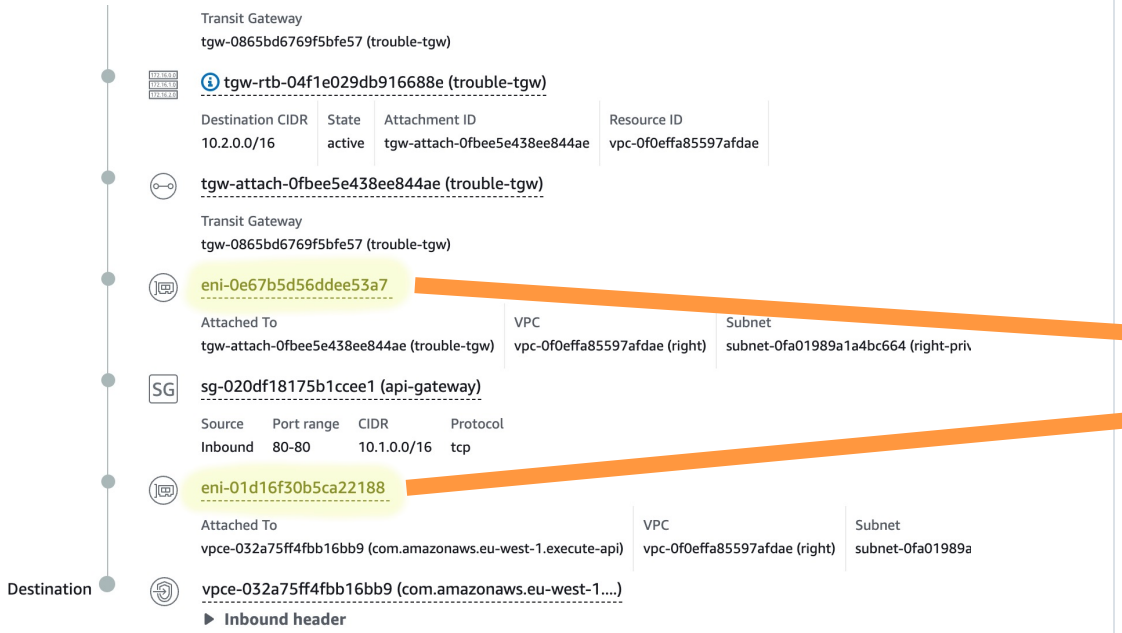
interface_id	vpc_id	src_port	dst_port	action	flow_di…
eni-0b8405b10…	vpc-0416ed…	12345	80	ACCEPT	egress
eni-08905bd3d…	vpc-0416ed…	12345	80	ACCEPT	ingress
eni-0e67b5d56…	vpc-0f0eff…	12345	80	ACCEPT	egress
eni-01d16f30b…	vpc-0f0eff…	12345	80	ACCEPT	ingress
eni-01d16f30b…	vpc-0f0eff…	12345	80	REJECT	ingress

Reachability Analyzer zu Flow Logs



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

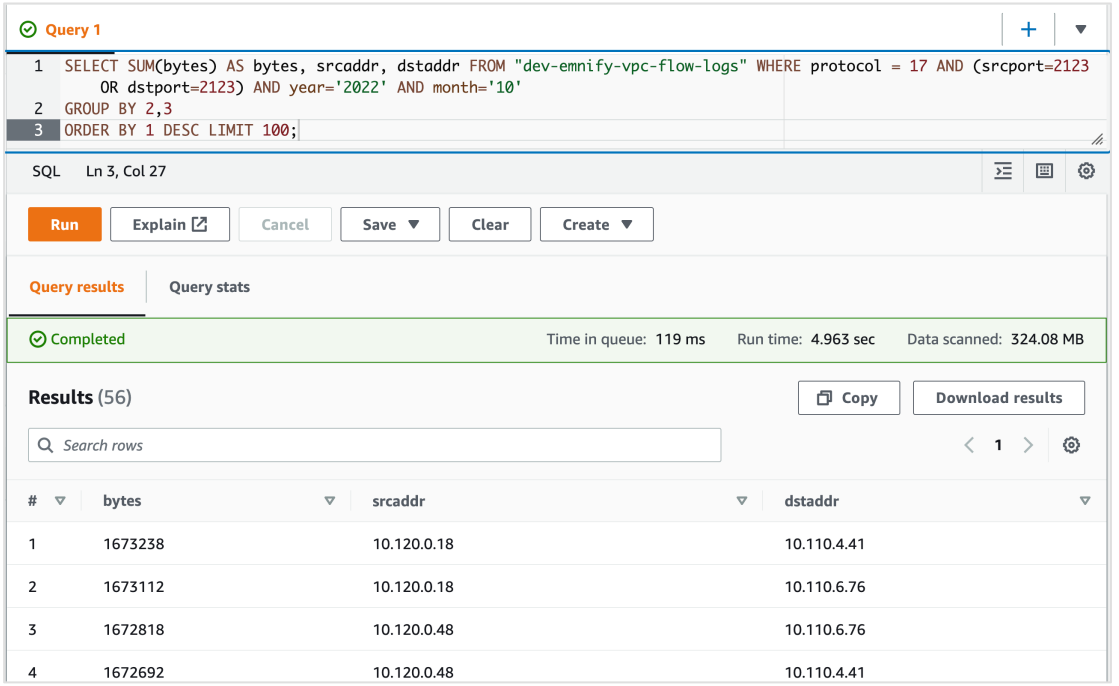
Reachability Analyzer zu Flow Logs



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

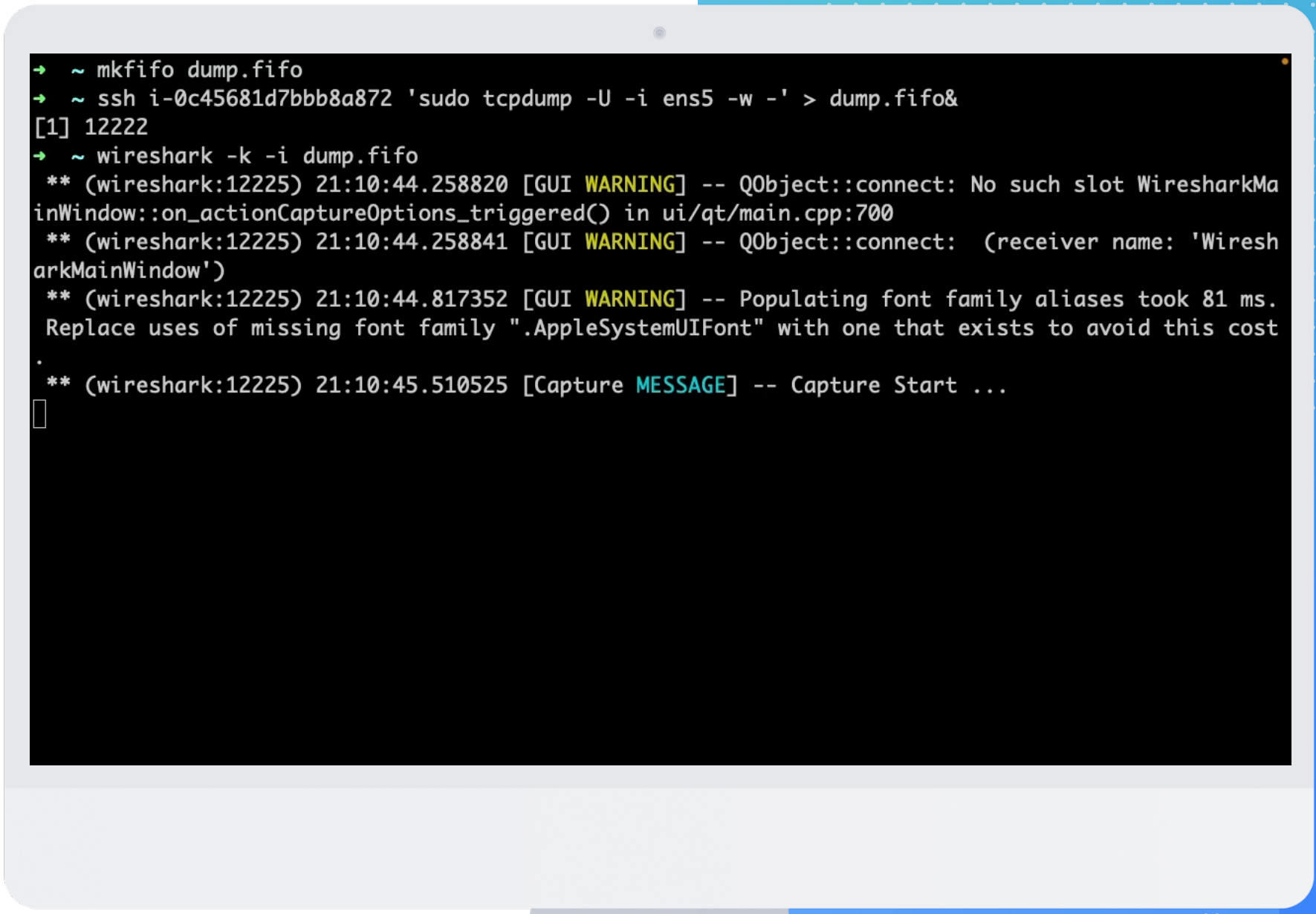


EMnify

Packet Capture

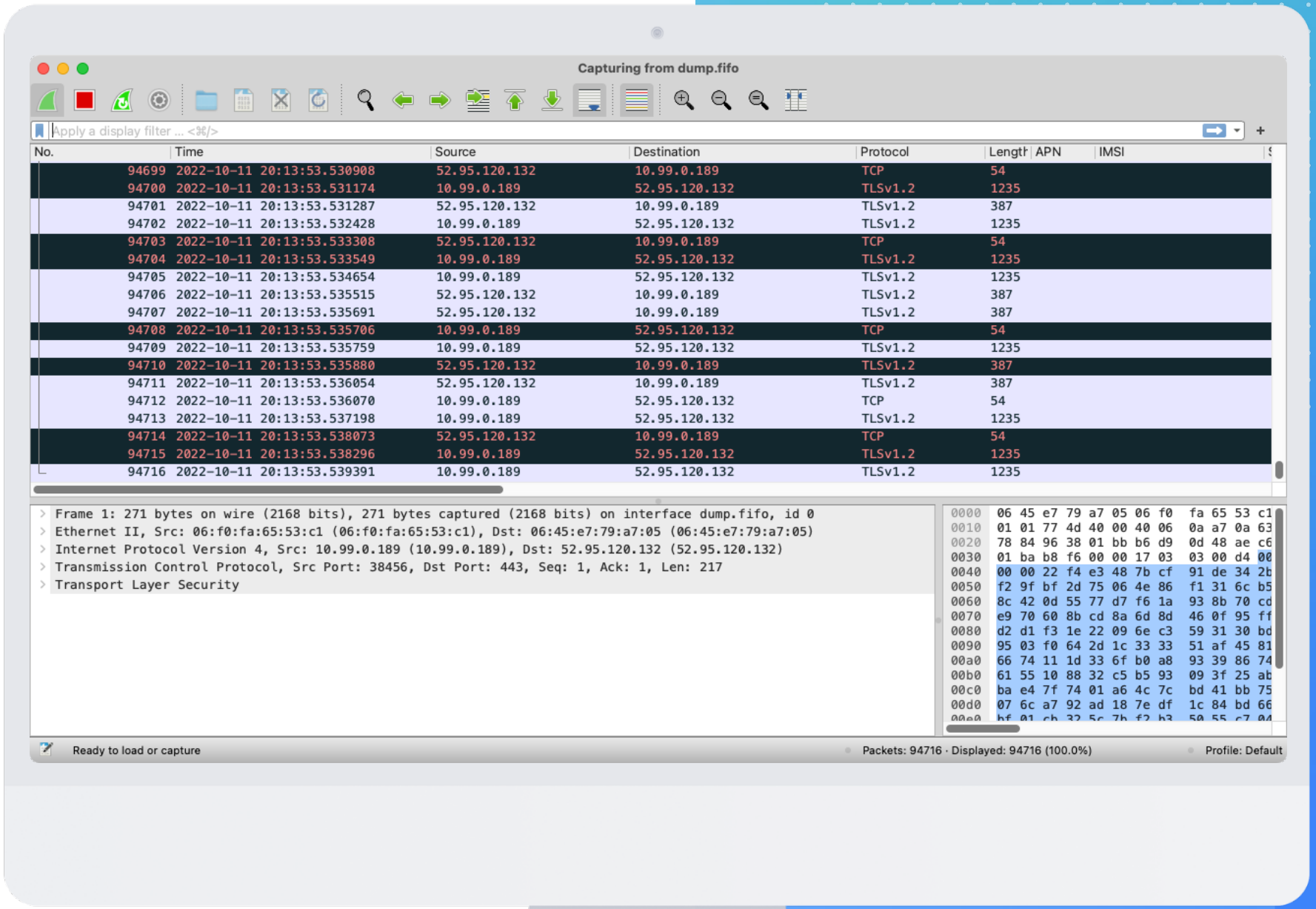
Wireshark

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



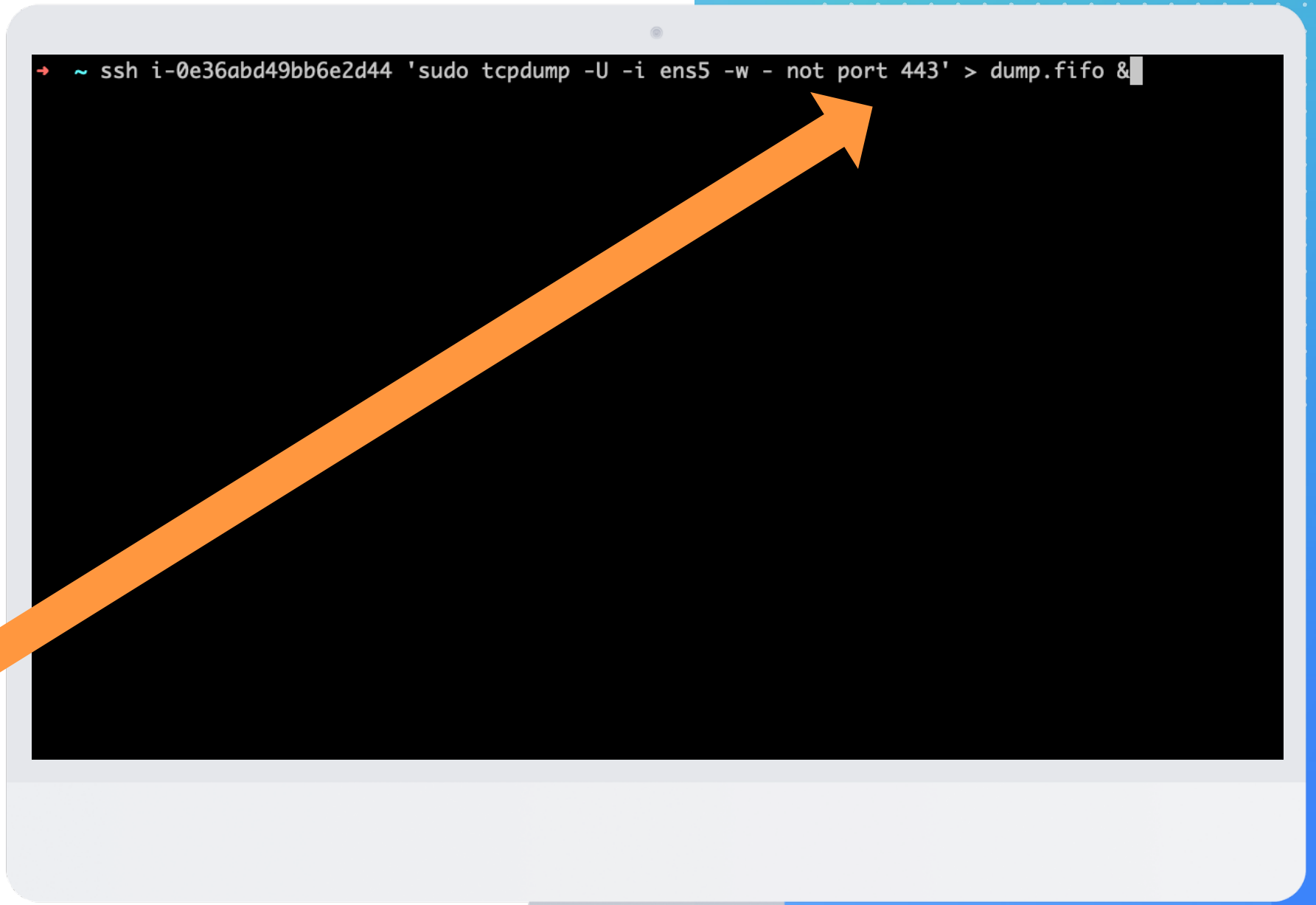
Wireshark

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



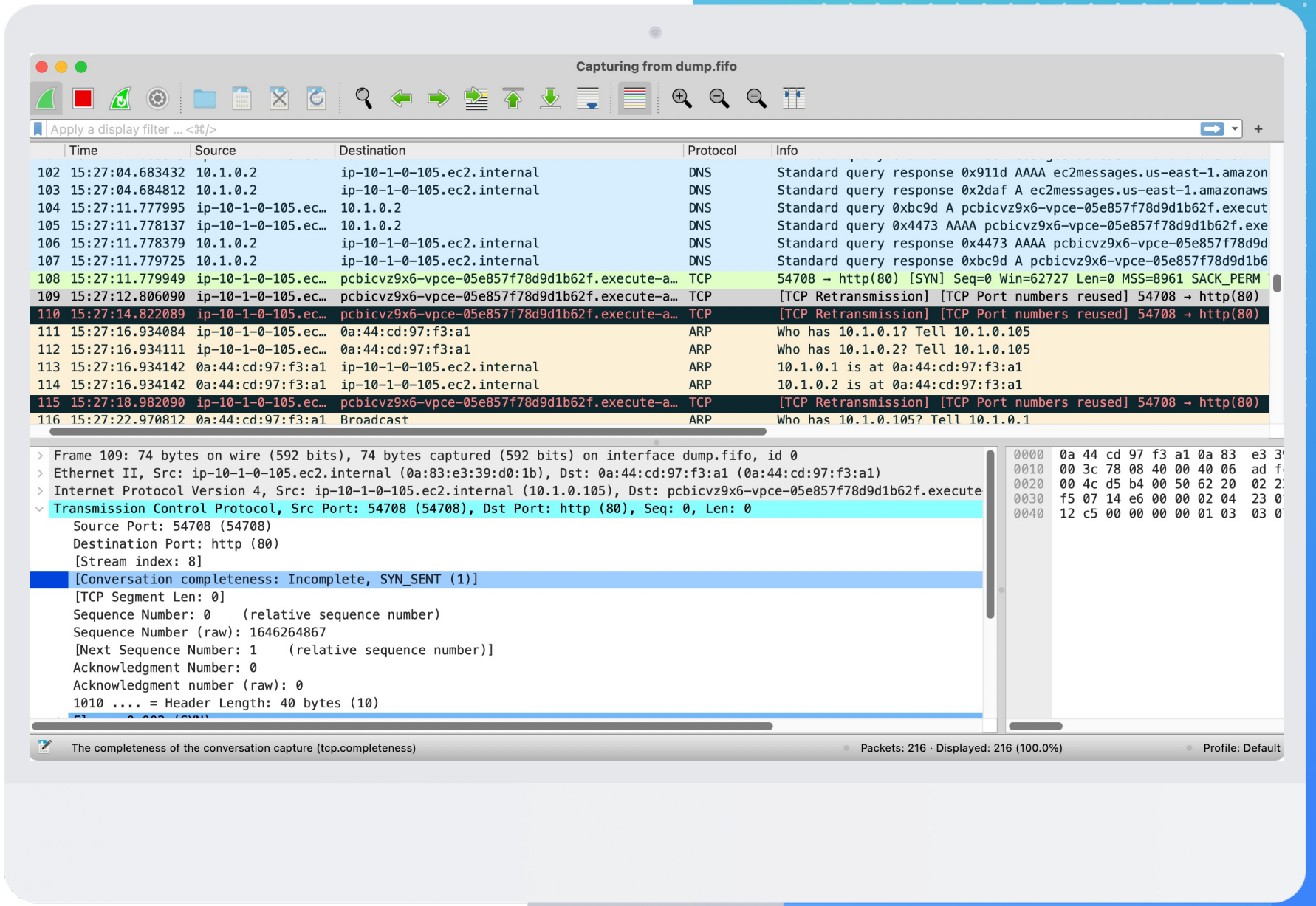
Wireshark

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

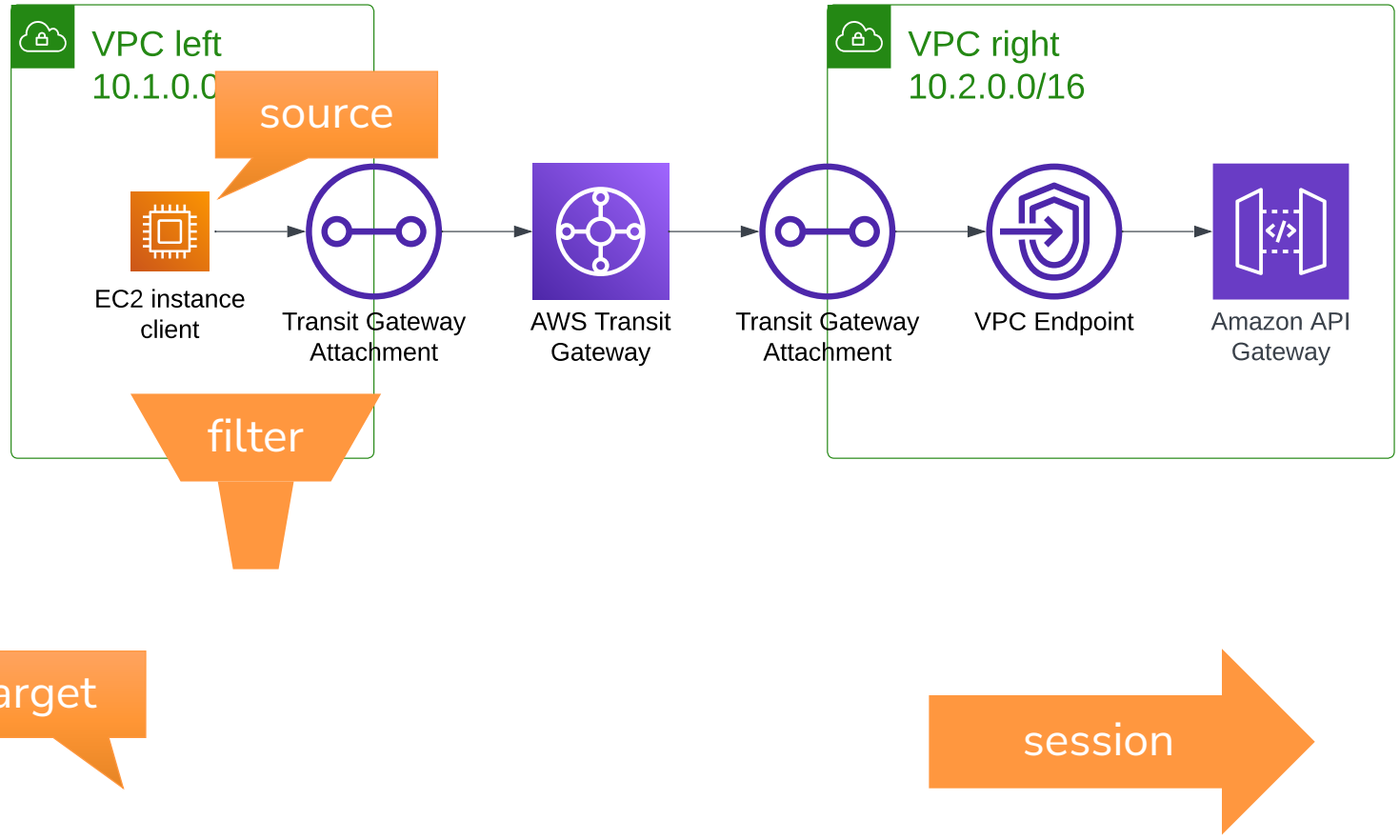


Wireshark

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

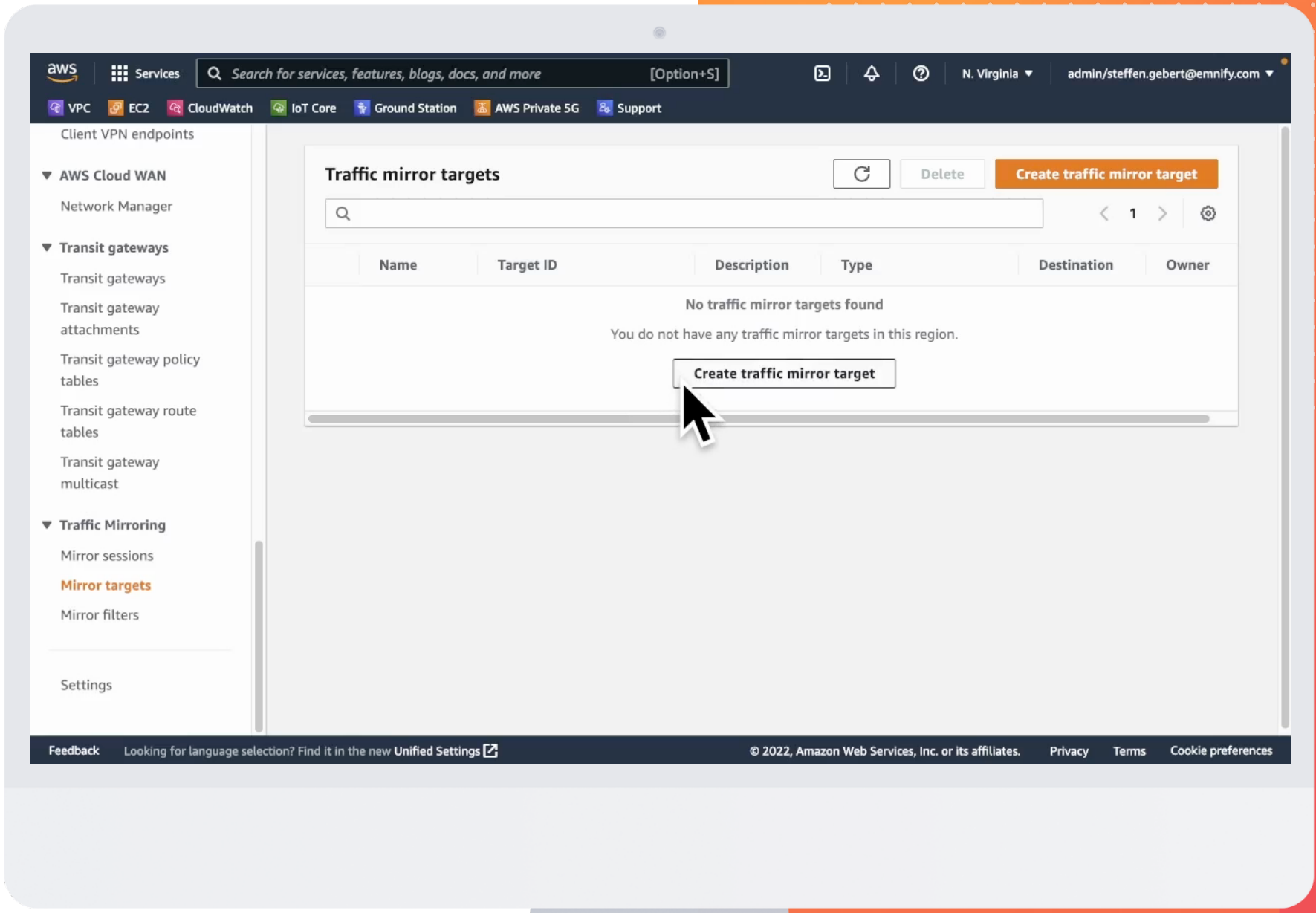


VPC Traffic Mirroring



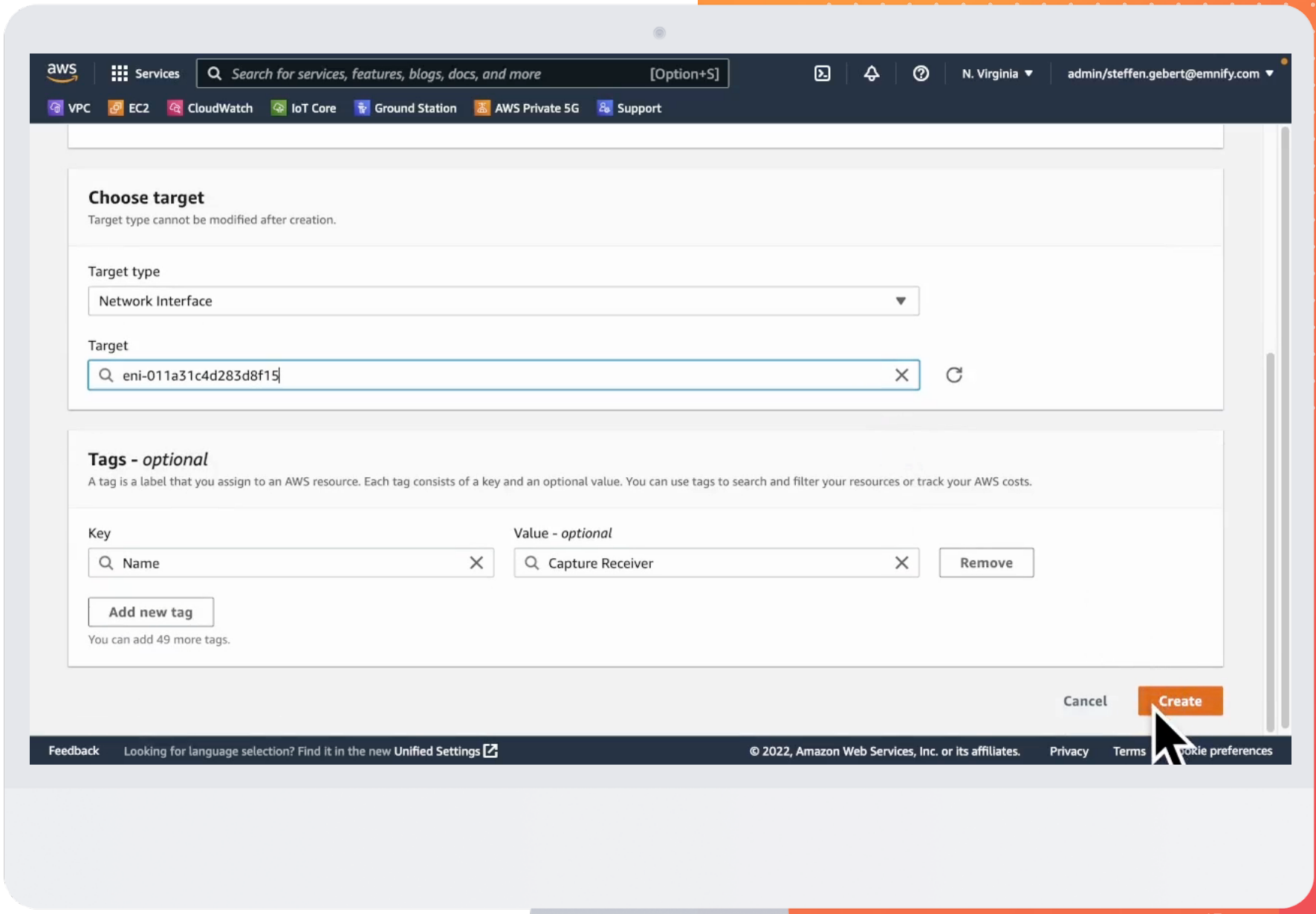
VPC Traffic Mirroring

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



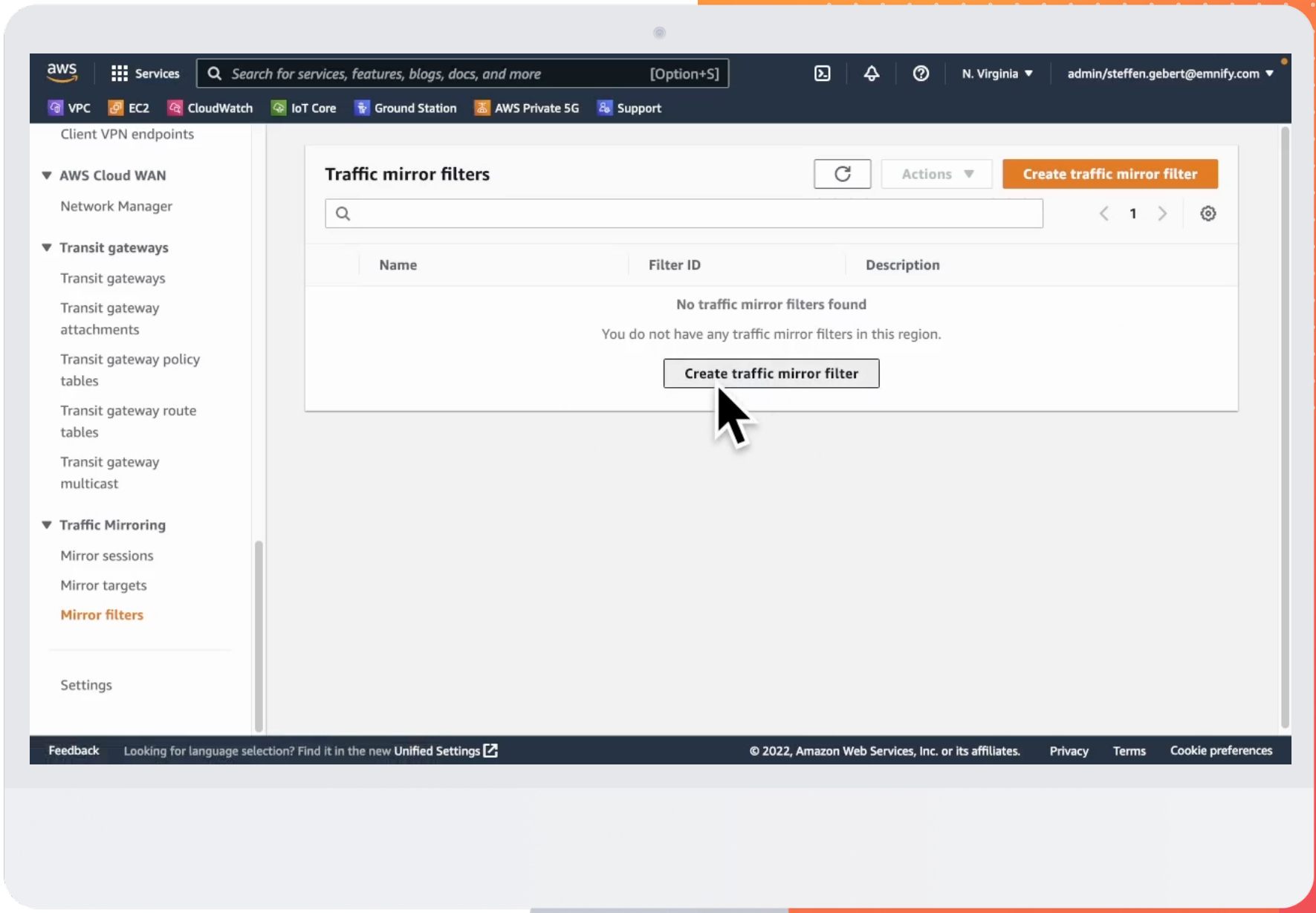
VPC Traffic Mirroring

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



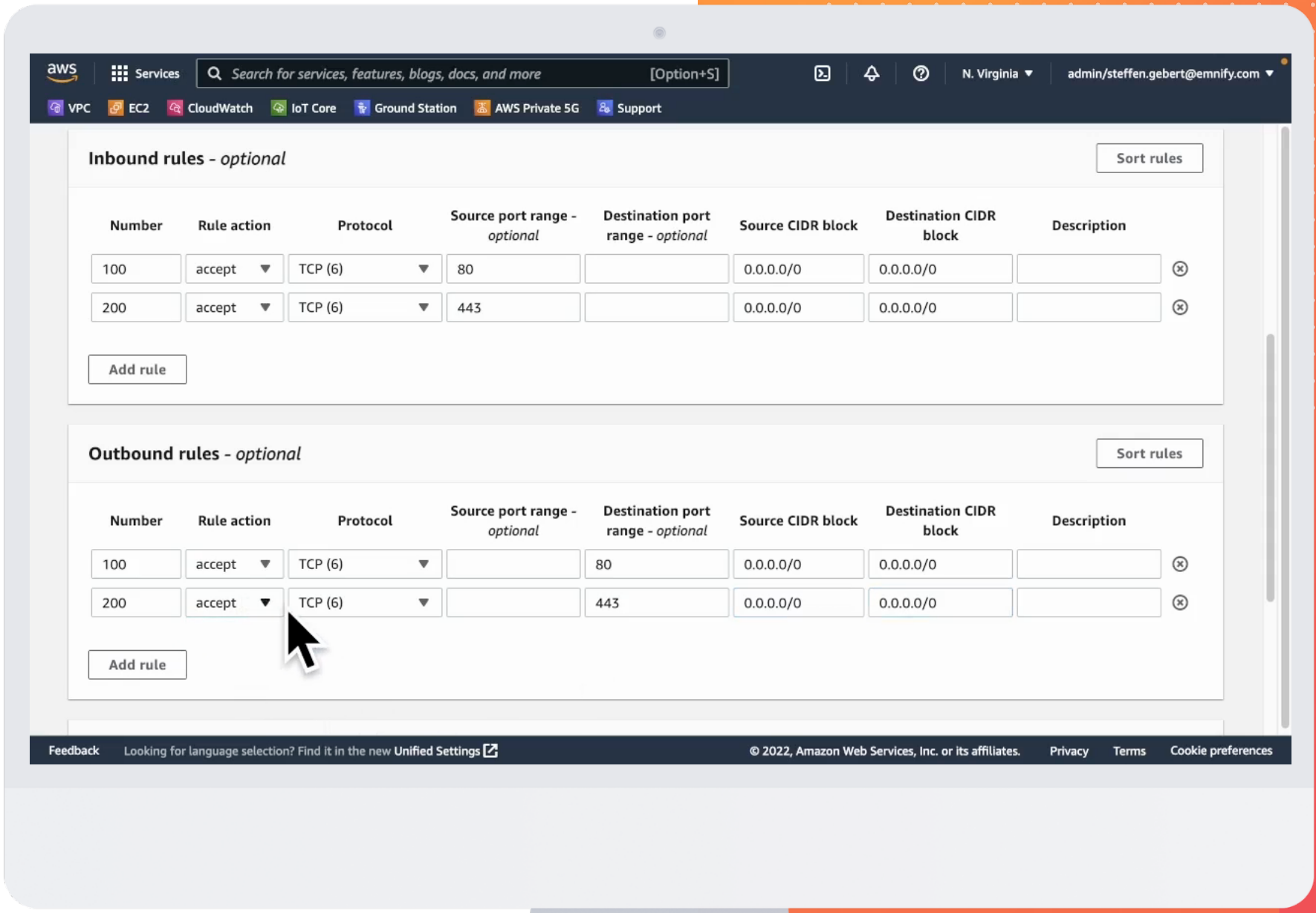
VPC Traffic Mirroring

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



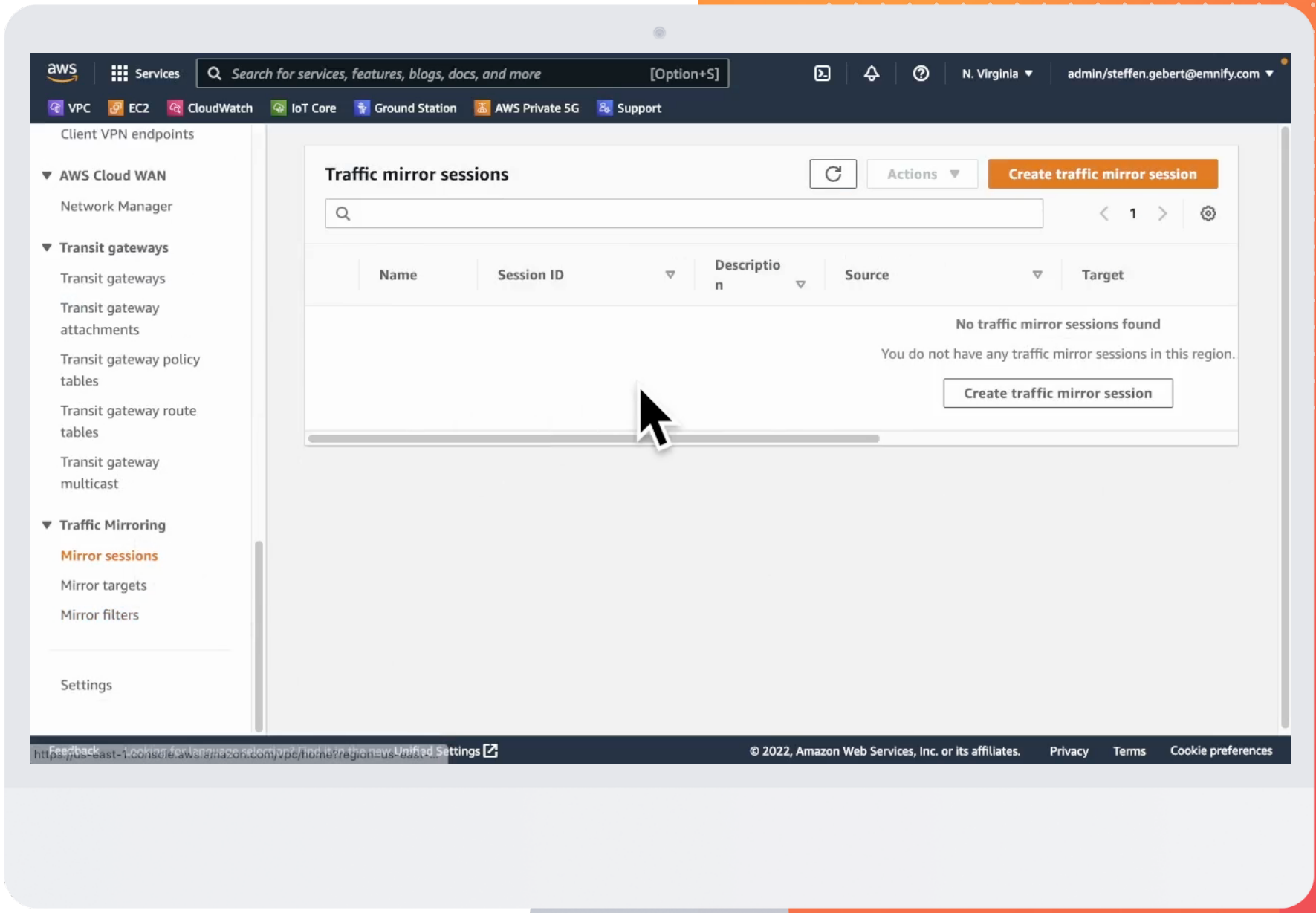
VPC Traffic Mirroring

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



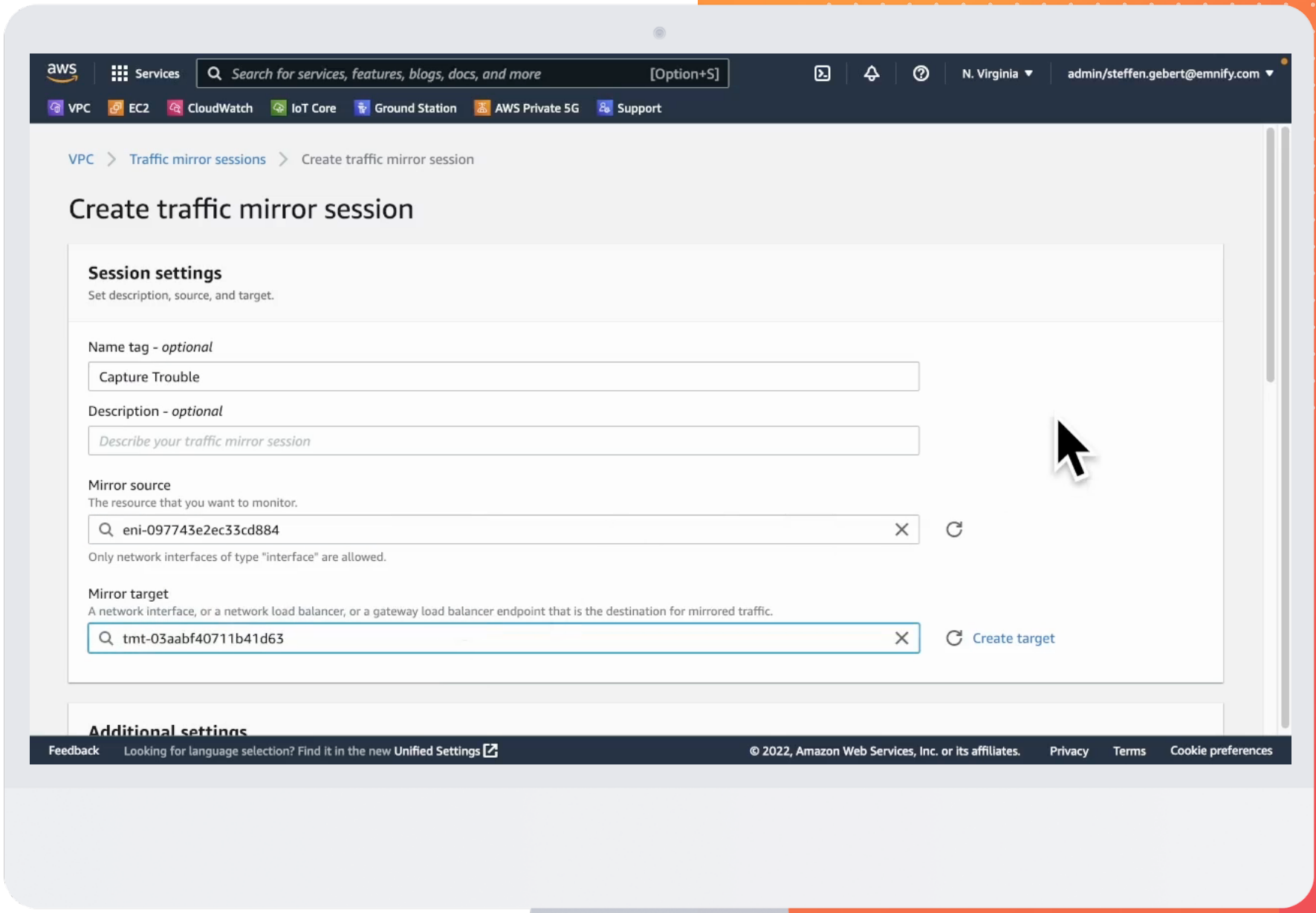
VPC Traffic Mirroring

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



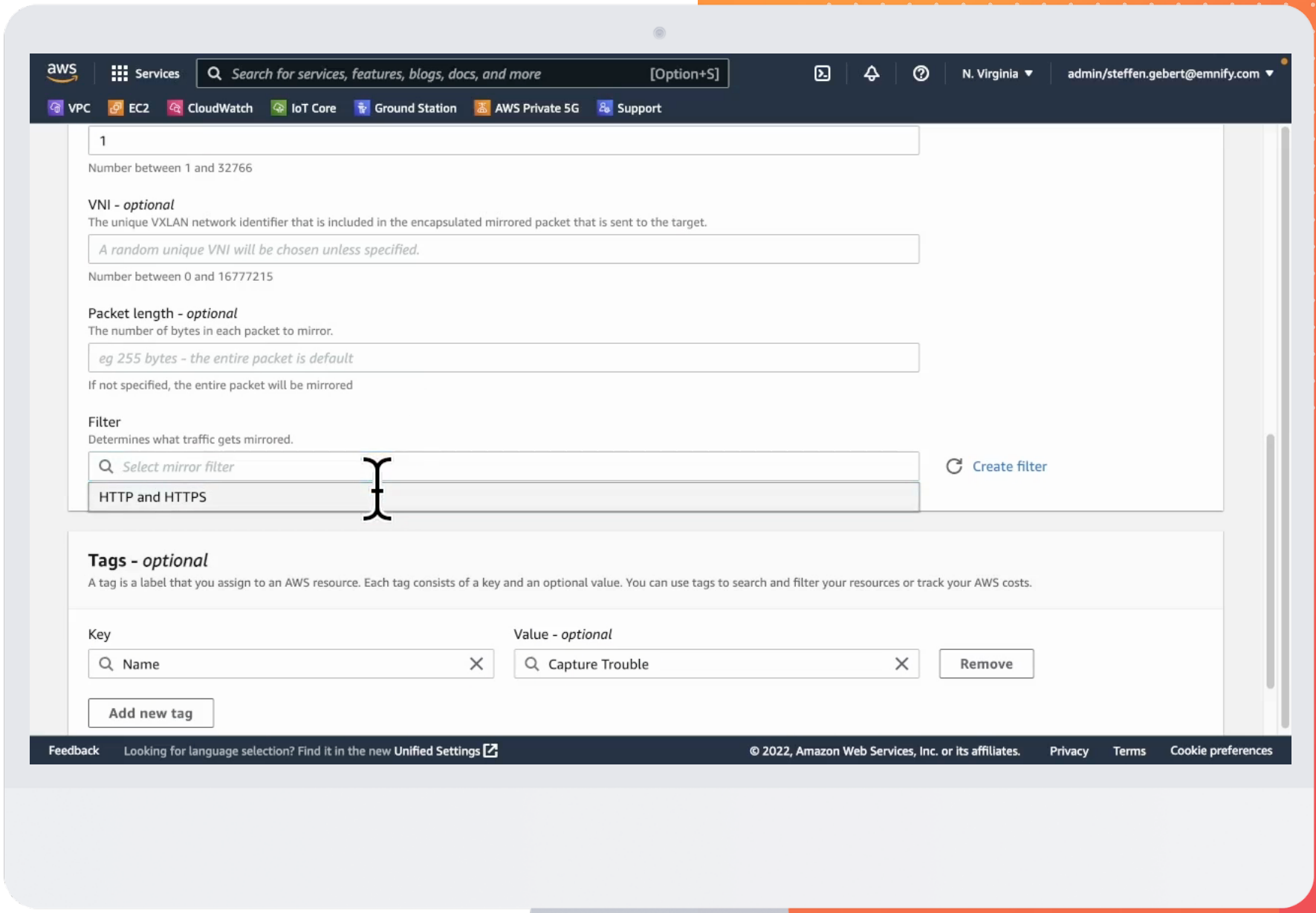
VPC Traffic Mirroring

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



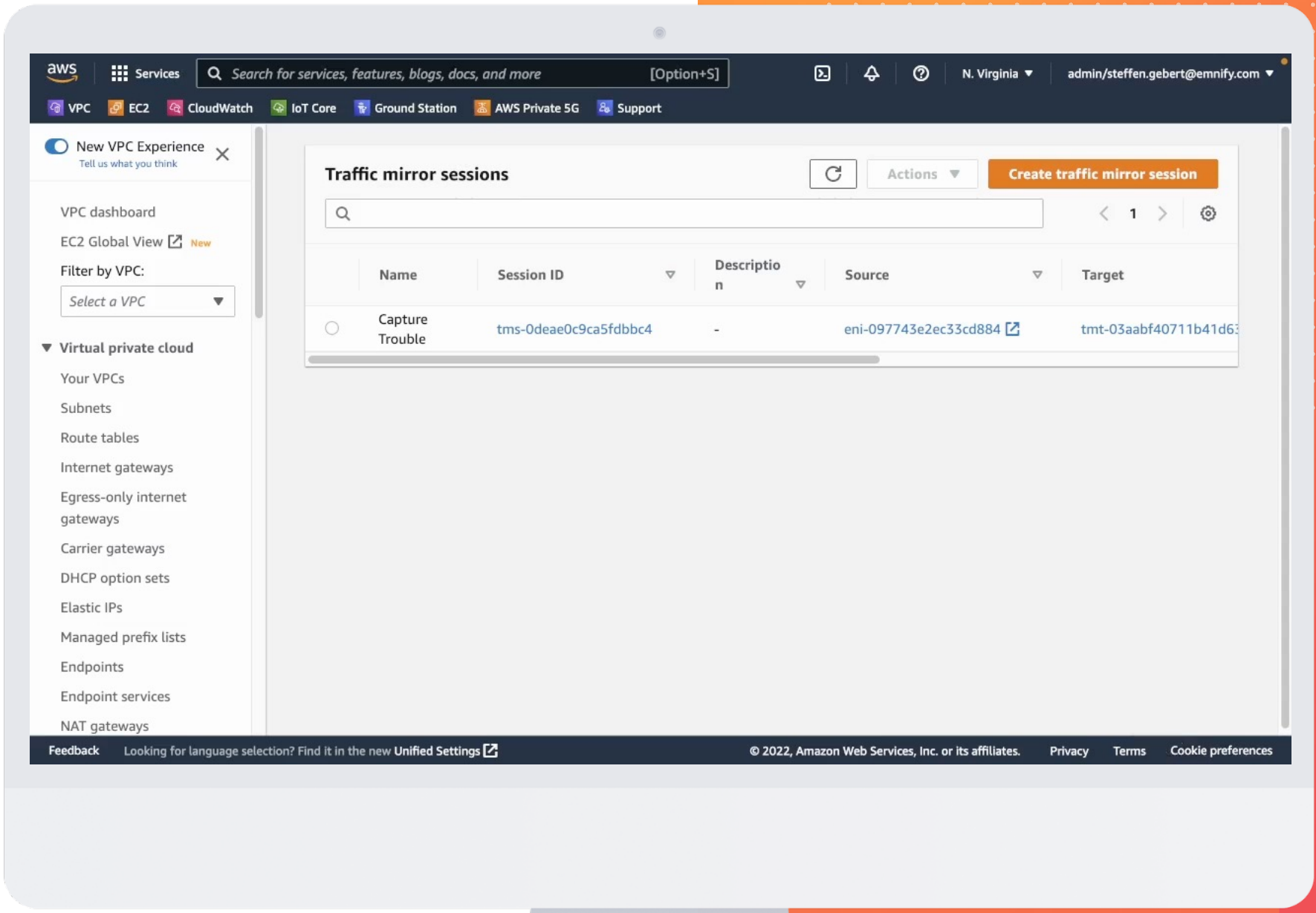
VPC Traffic Mirroring

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



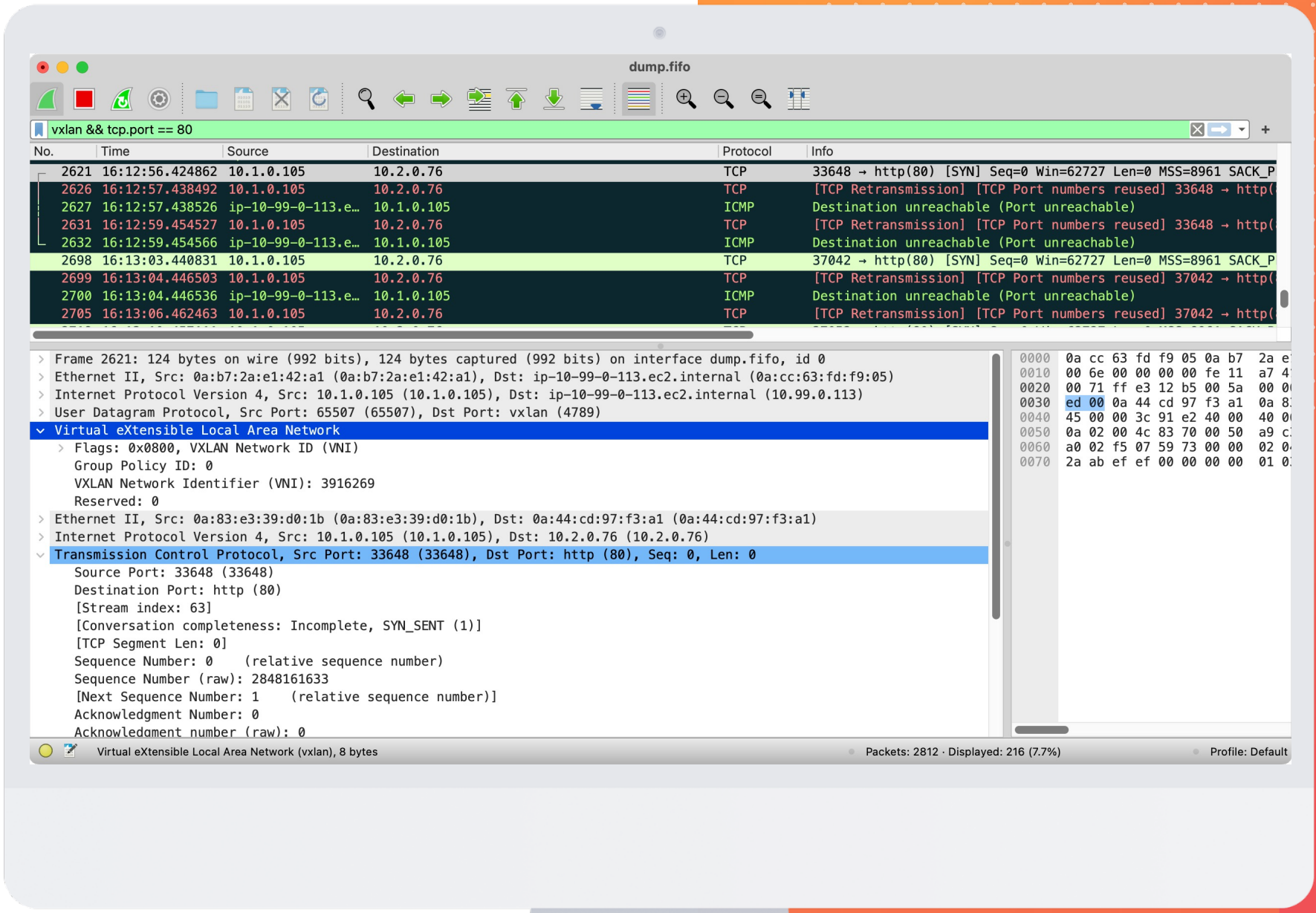
VPC Traffic Mirroring

- 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

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

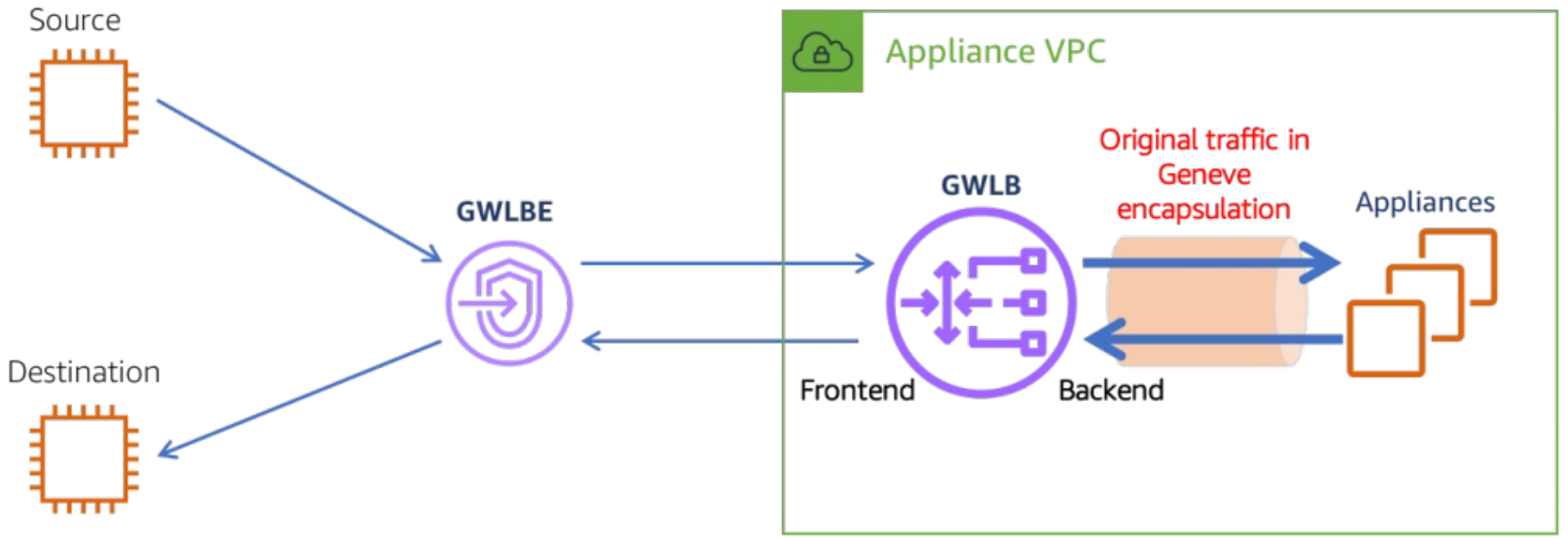


That’s fun!

NOBODY EVER DOING THIS

Can it be easier?

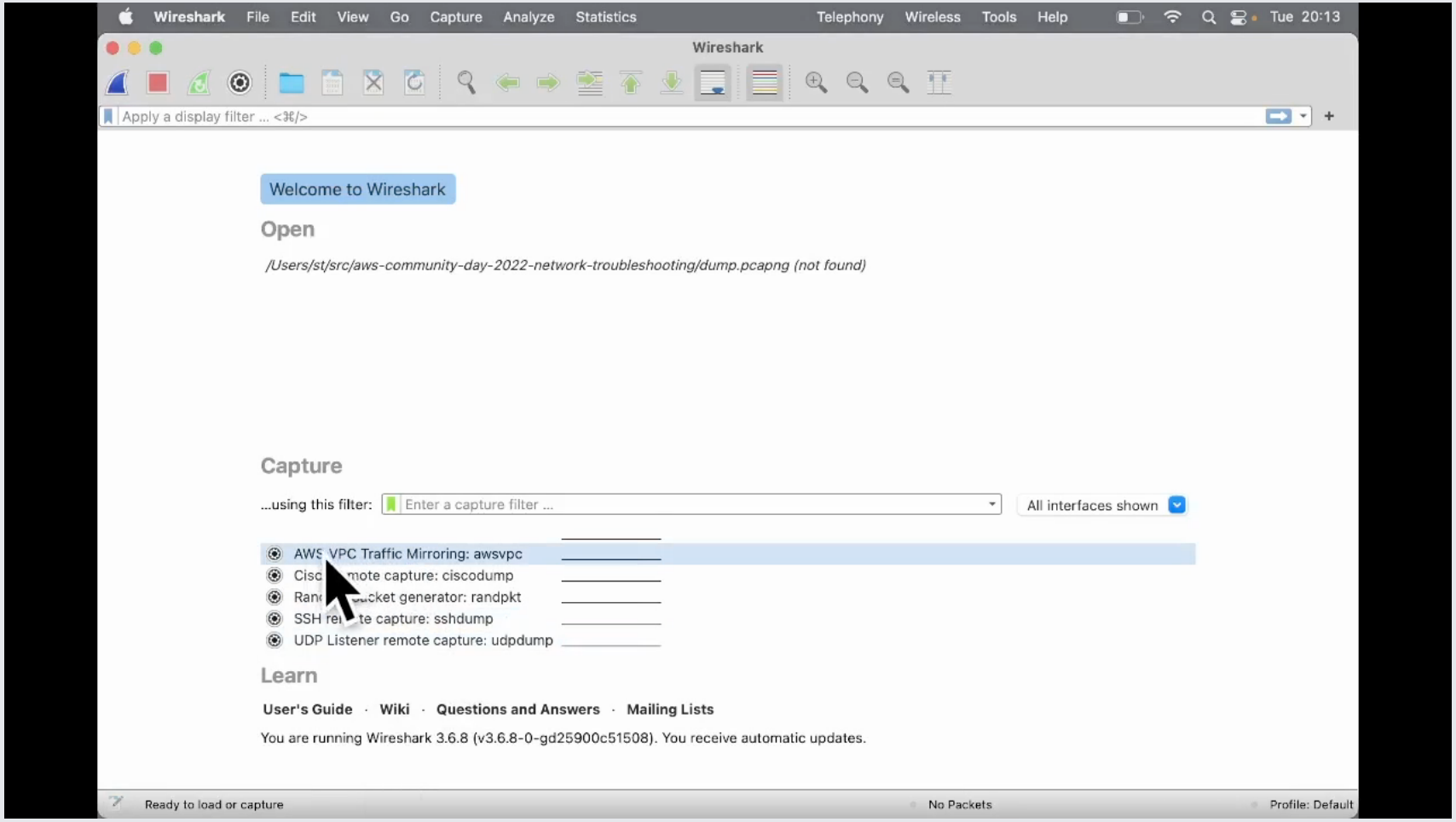
- Aidan Steele's projects
  - flowdogshark (GWLB)



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

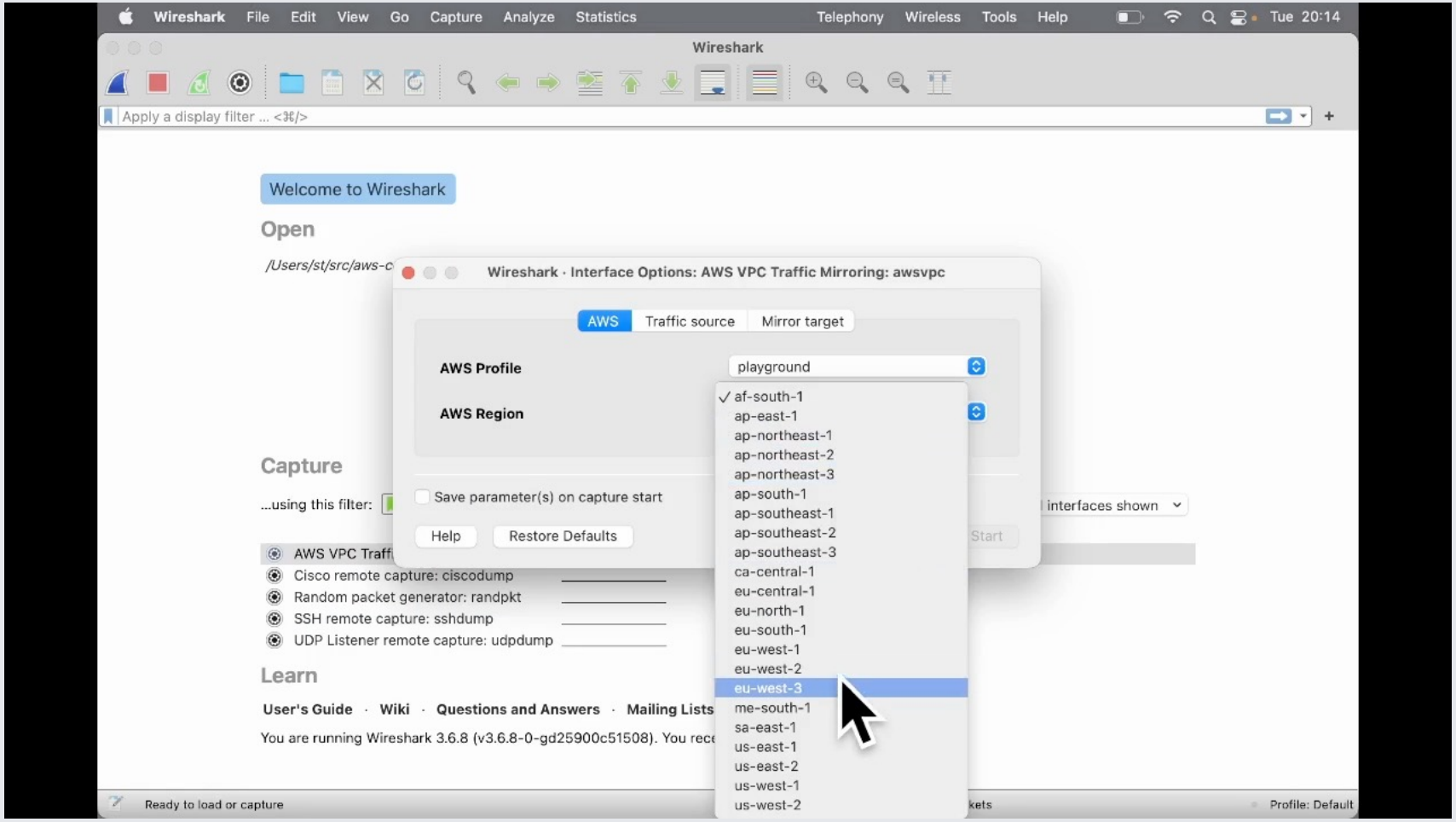


https://github.com/aidansteele/flowdog
https://github.com/aidansteele/vpcshark (* not yet publicly released)

Can it be easier?

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

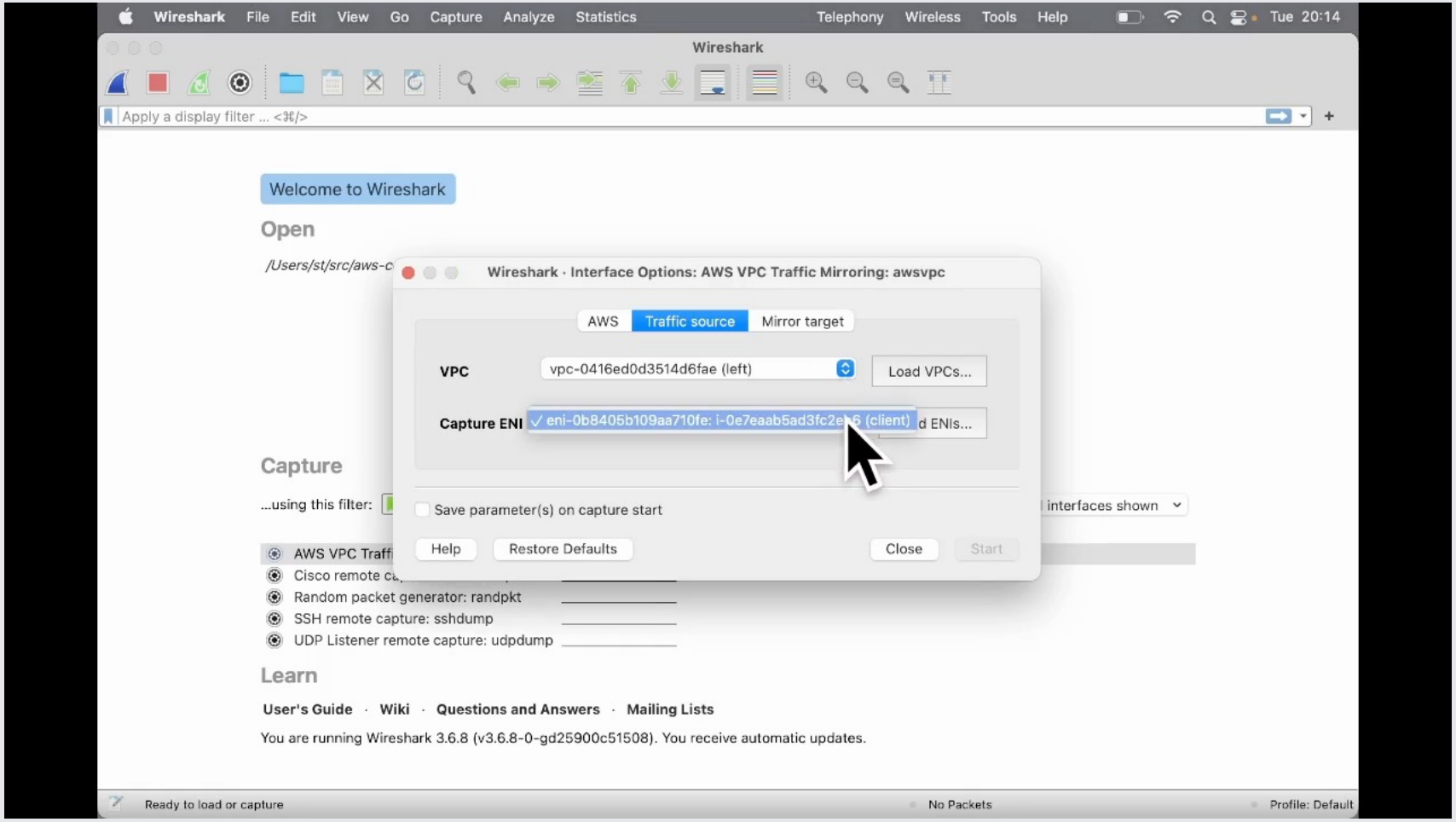
Aidan W Steele
@_steele Follows you



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

Can it be easier?

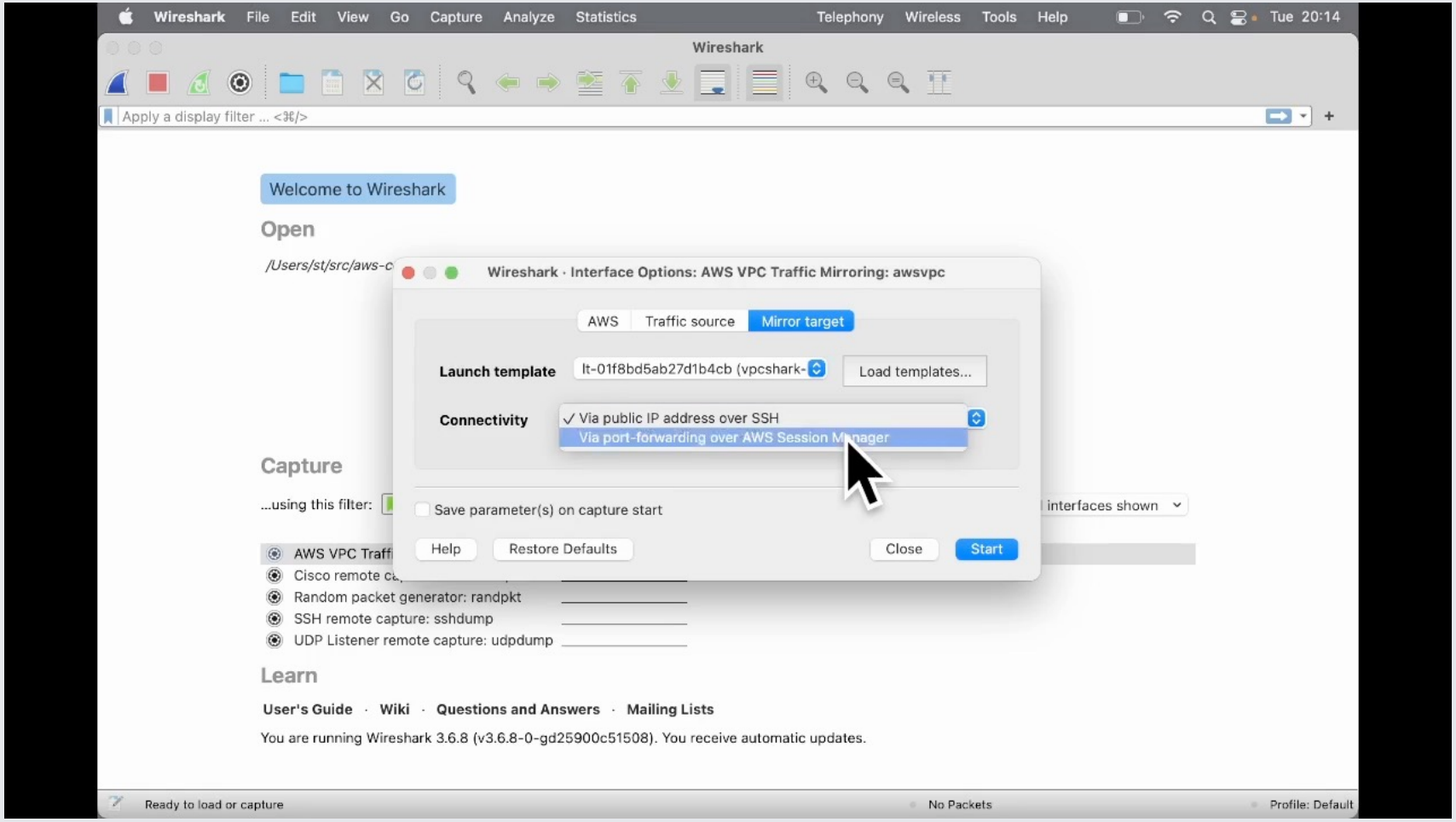
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

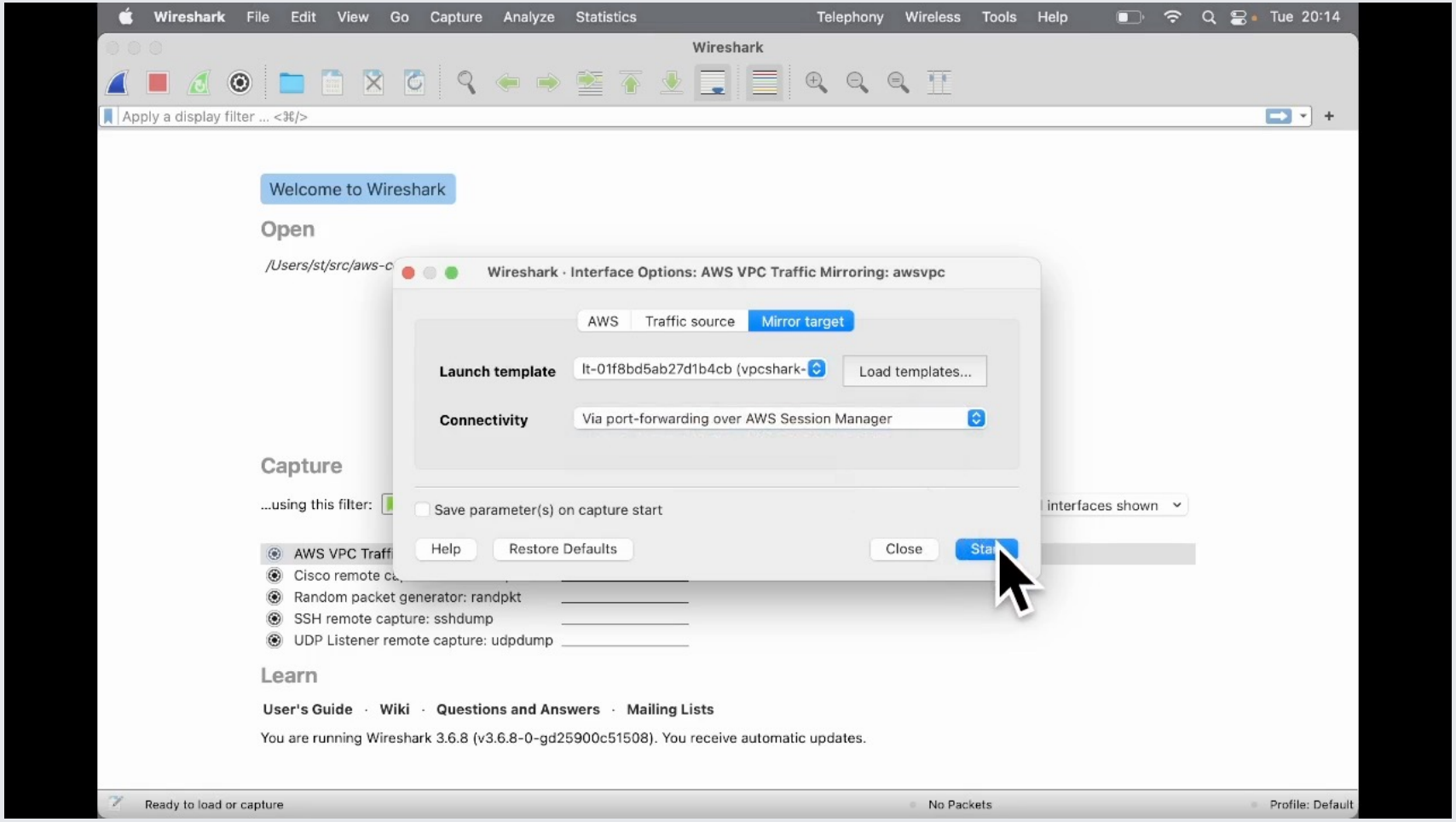
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

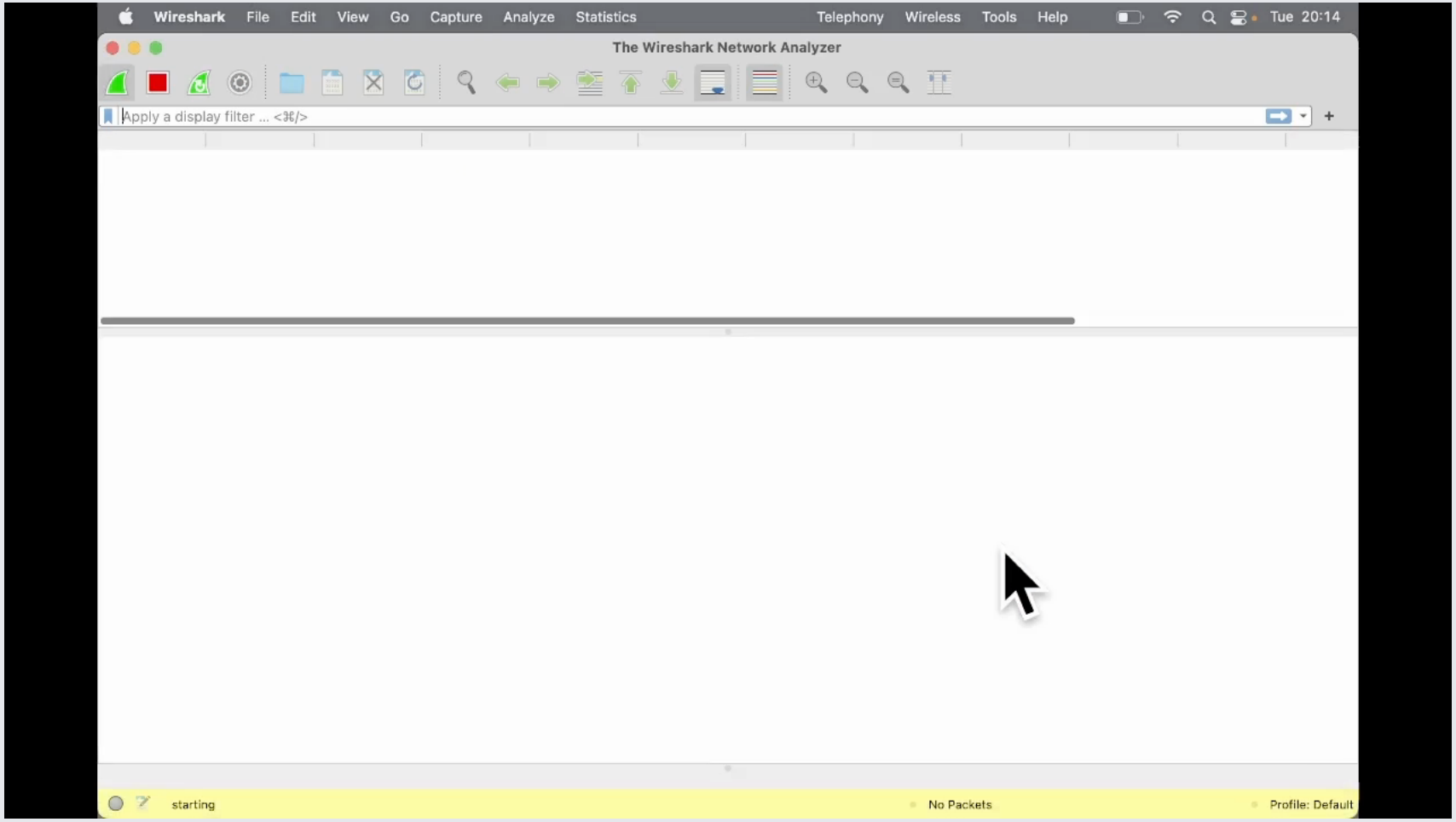
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

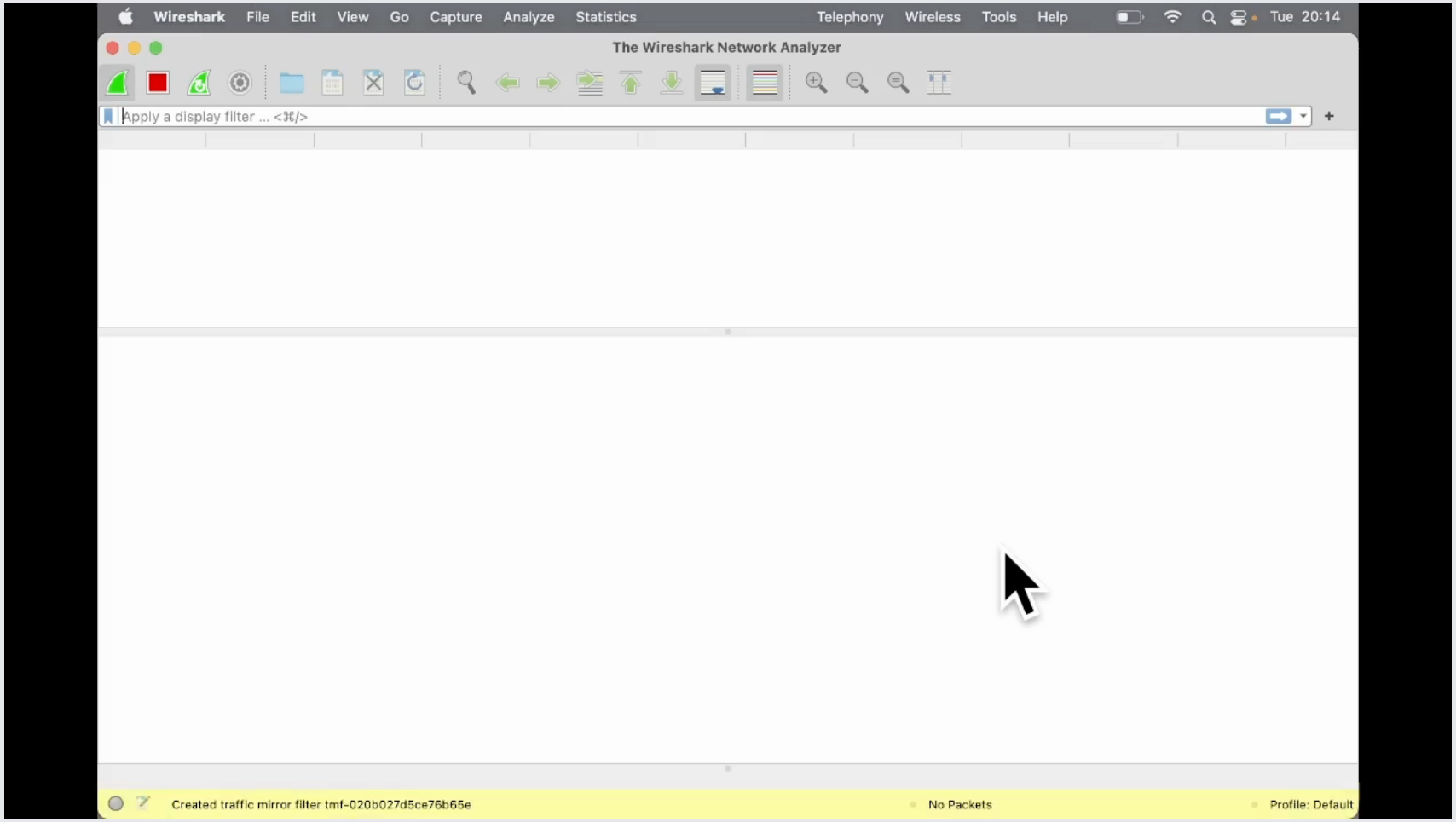
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

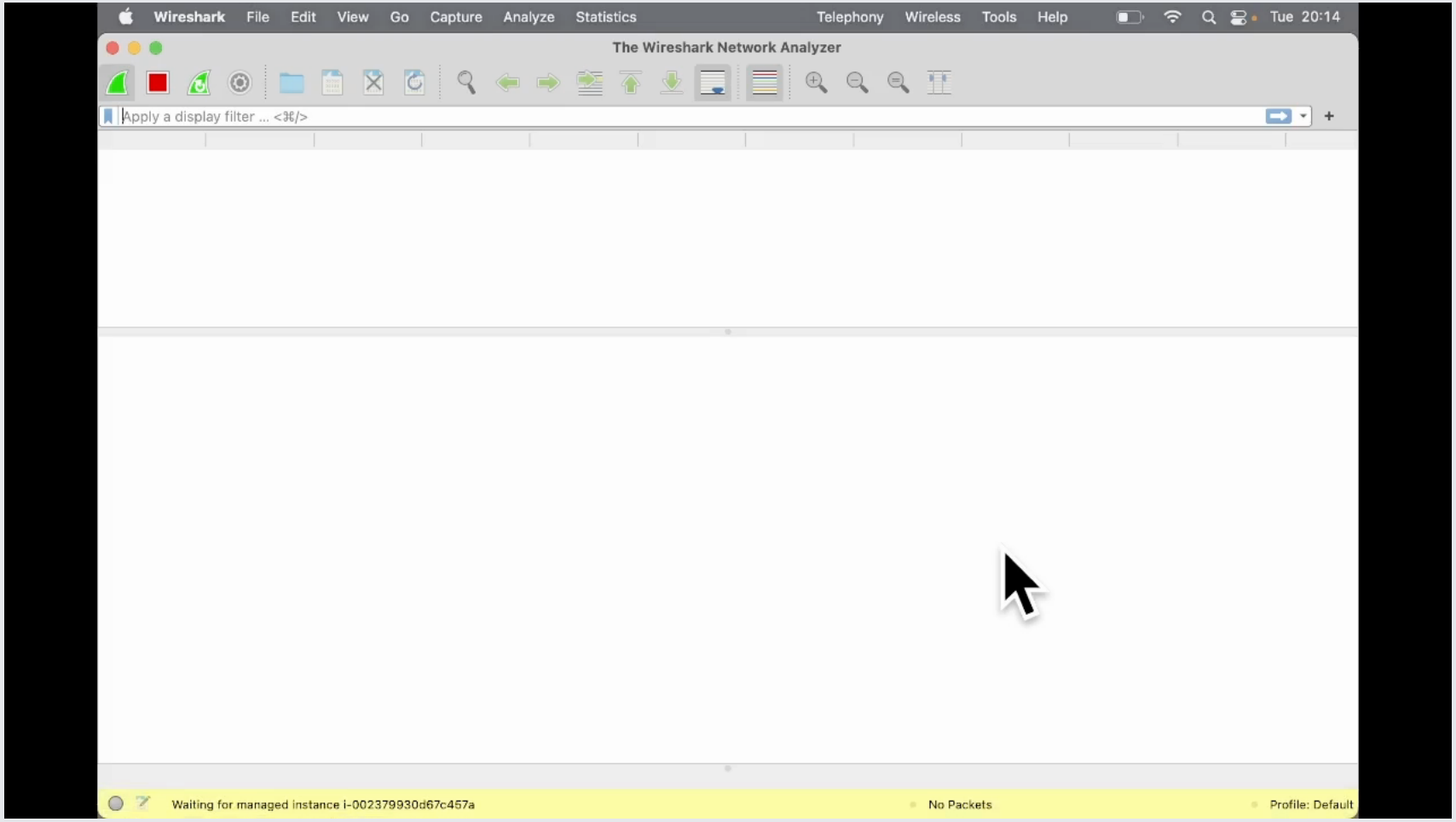
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

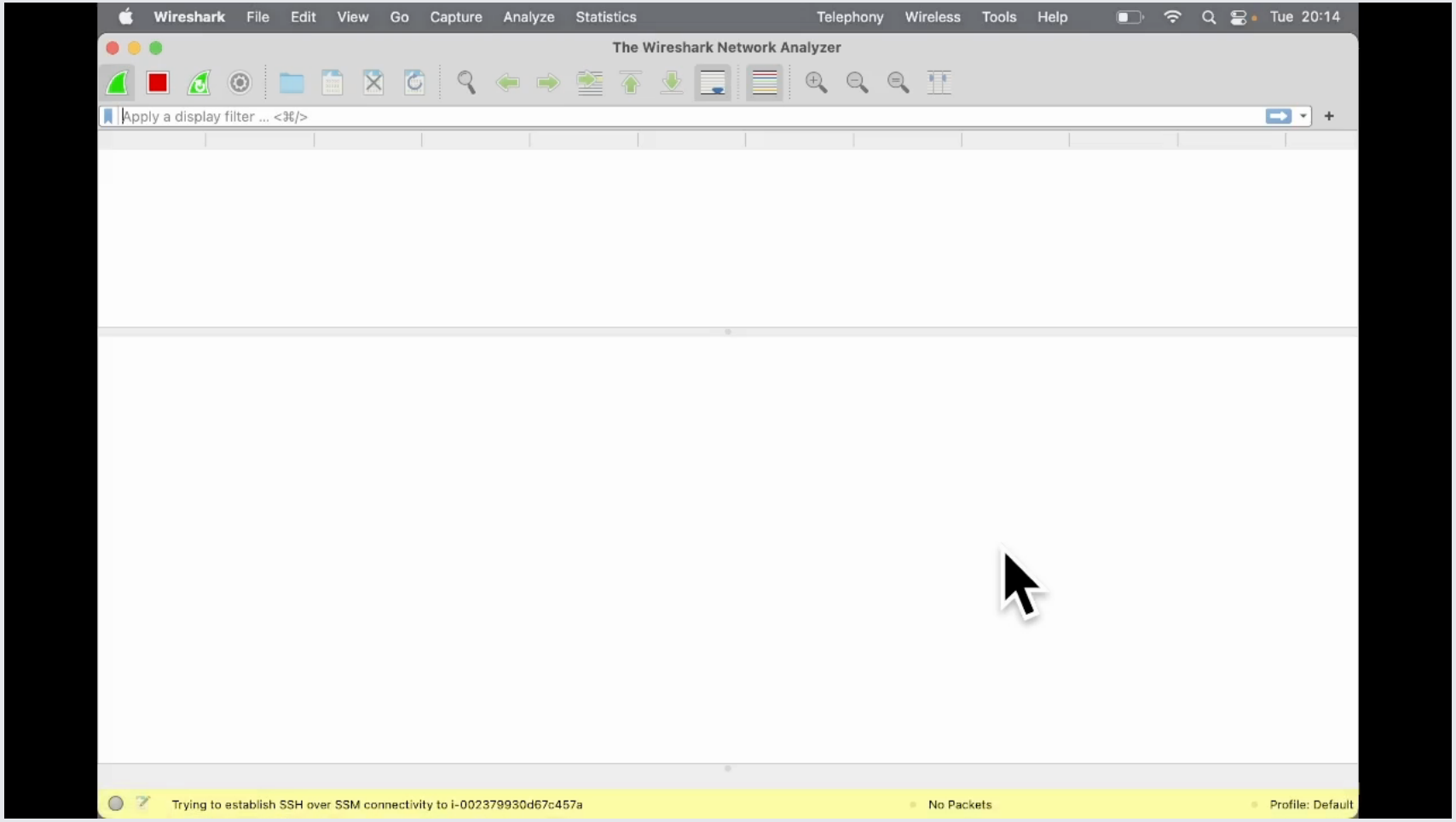
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

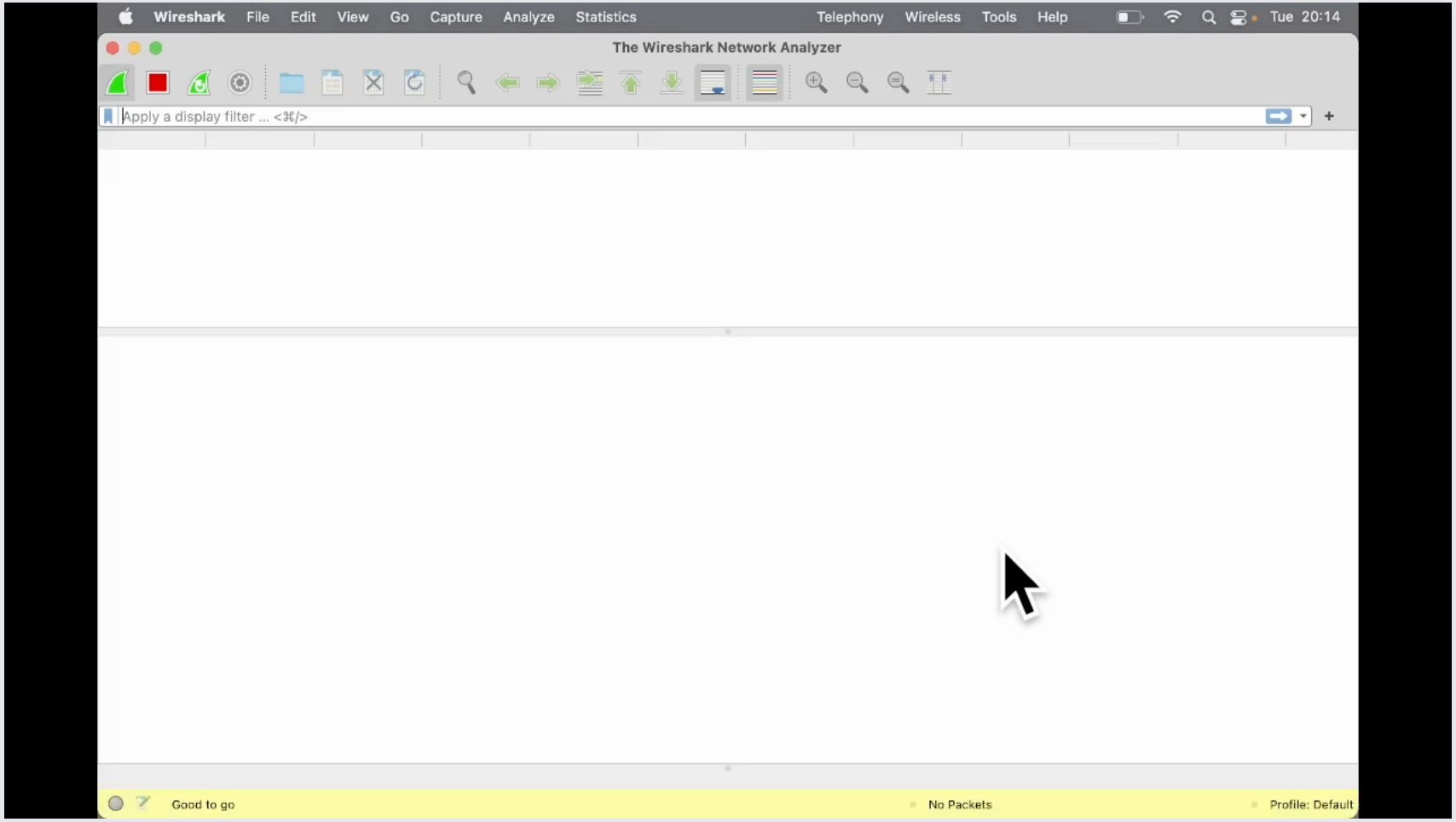
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

Can it be easier?

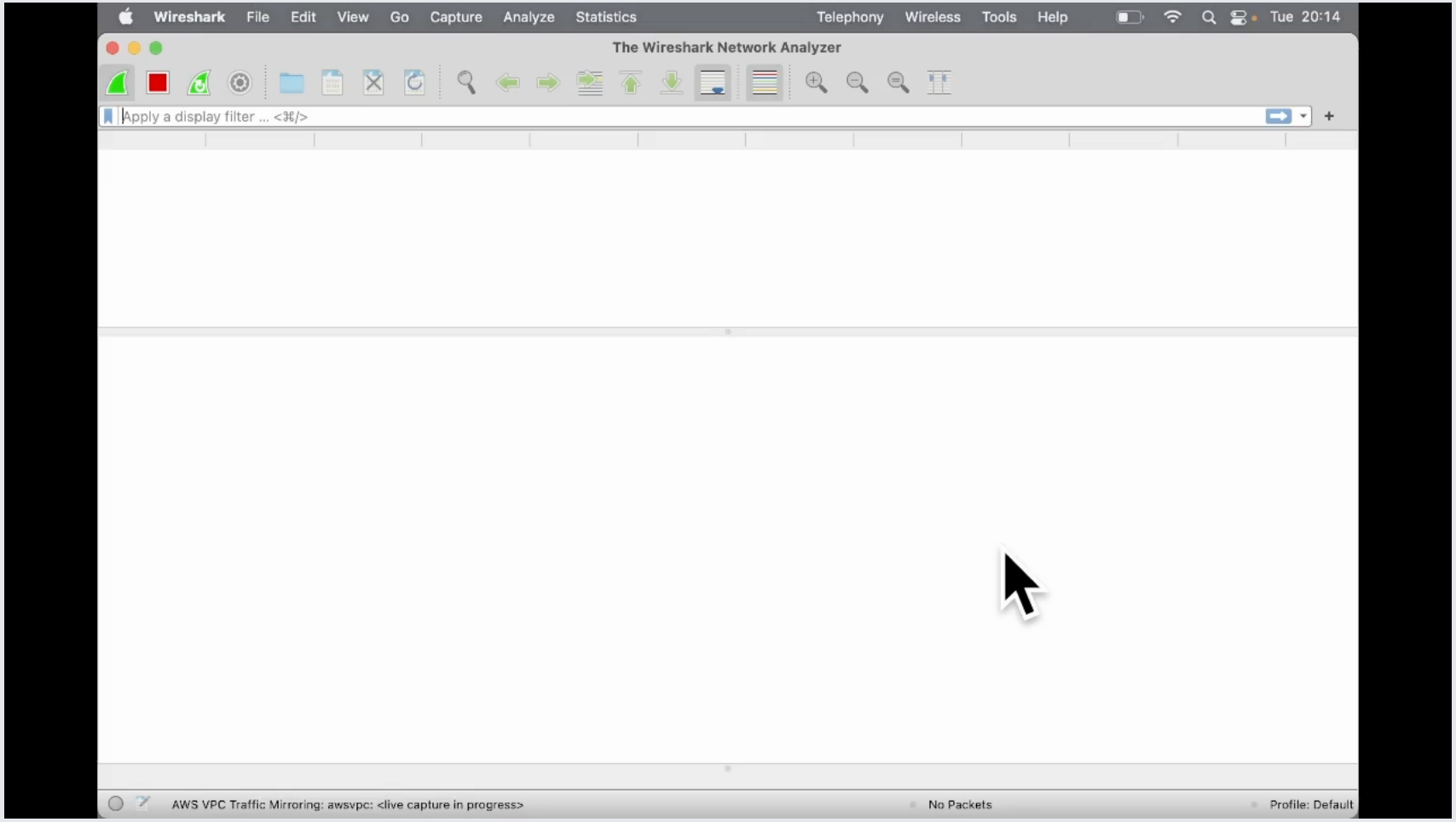
- Aidan Steele's projects
  - flowdogshark (GWLB)
  - vpcshark *
- More concept studies than for production



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

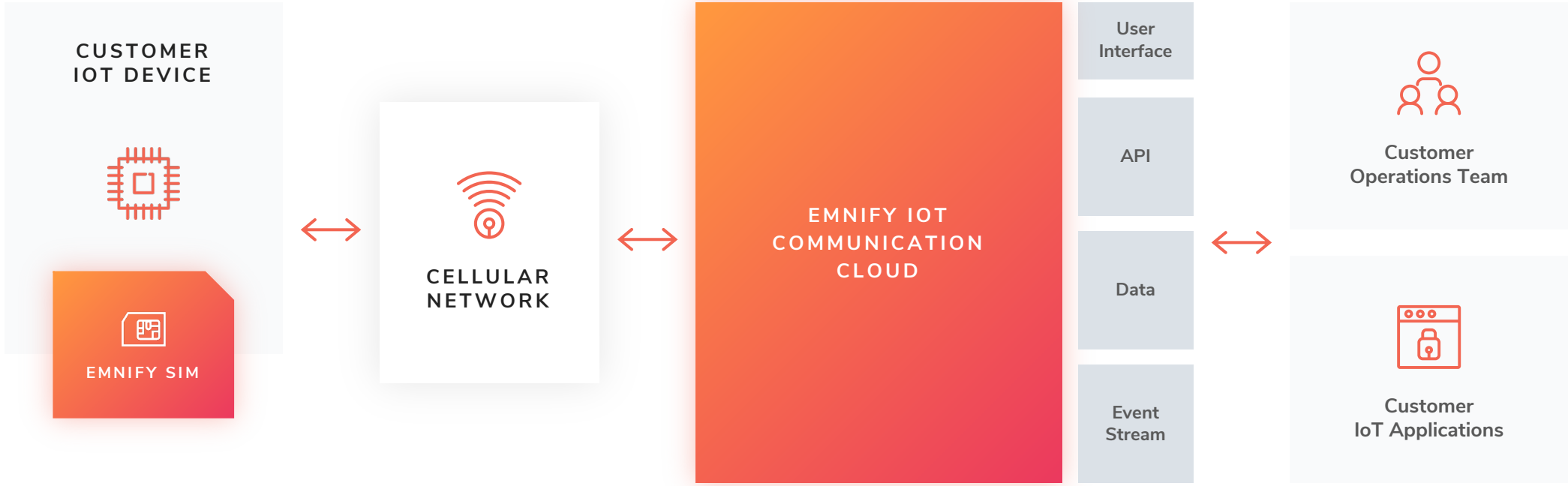


https://github.com/aidansteele/flowdog
https://github.com/aidansteele/vpcshark (* not yet publicly released)

When nothing helps...
Ask your AWS Account Team

THANKS Karl!

EMnify IoT Communication Cloud



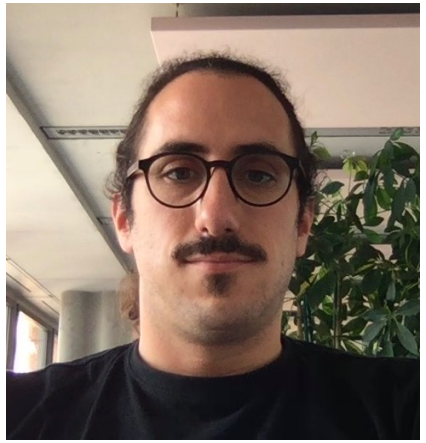
Your Trouble Shooters

Dr. **Steffen** Gebert

- Director Technology, Infrastructure
- @StGebert

Wolfgang Schäfer

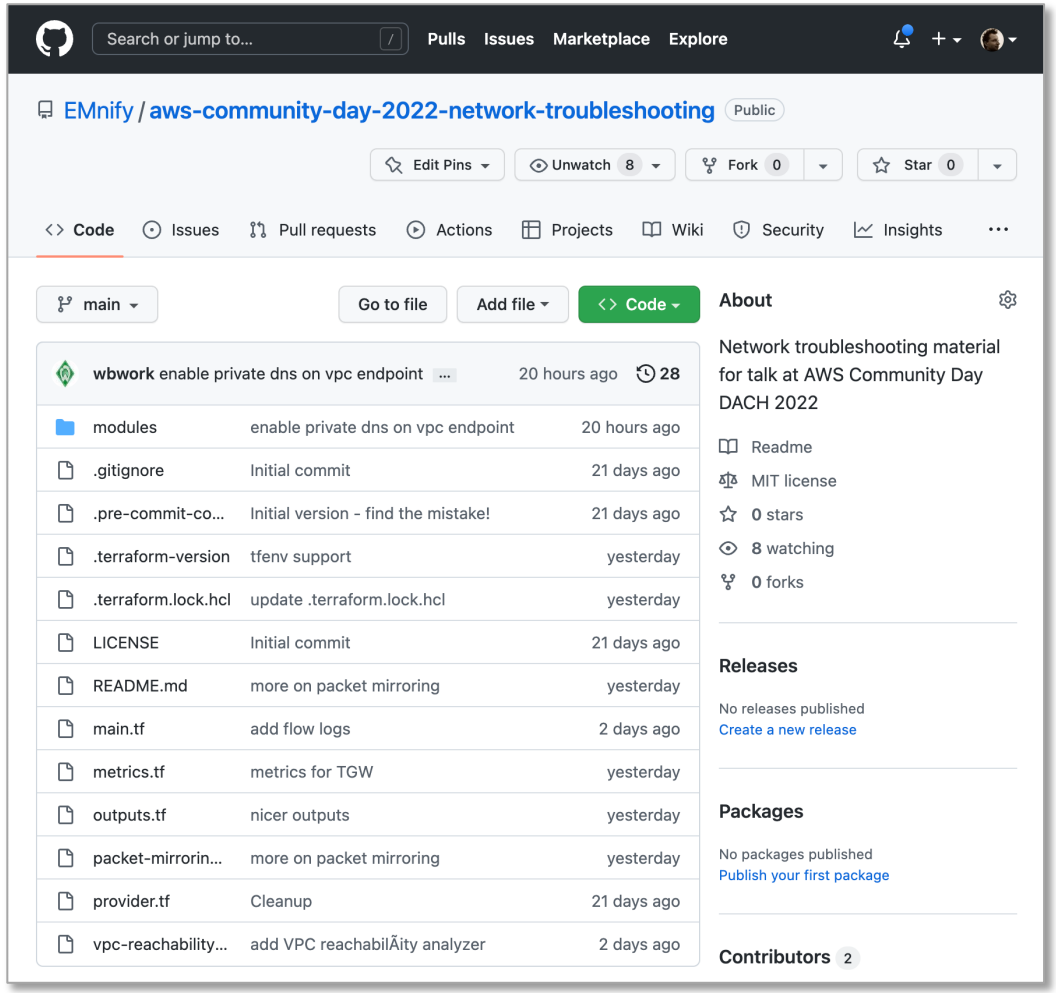
- Senior Core Network Engineer
- @wo_wue



Learn from our mistakes!

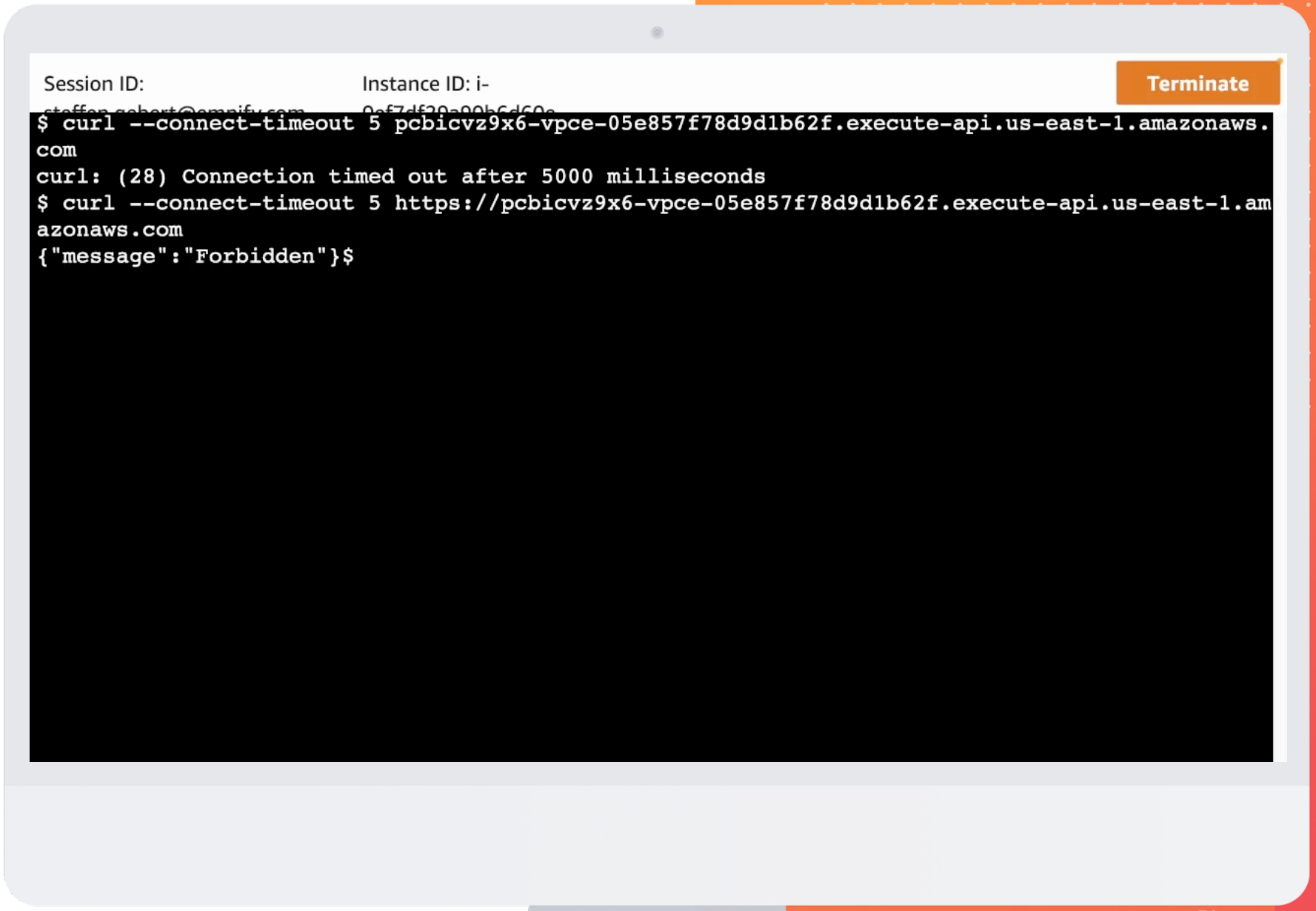
- IaC definition of the setup used in this talk
  - Terraform
  - incl. Reachability Analyzer and Traffic Mirroring

- **github.com/EMnify/**



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!