AWS Cloud WAN

ataccama

Agenda

- AWS Cloud WAN introduction
- Building blocks
- User interface
- Cloud WAN deployment
- Ataccama and AWS Cloud WAN
- Q&A

About me

Daniel Pospíšil

- Over 14 years of experience in networking and Linux infrastructure

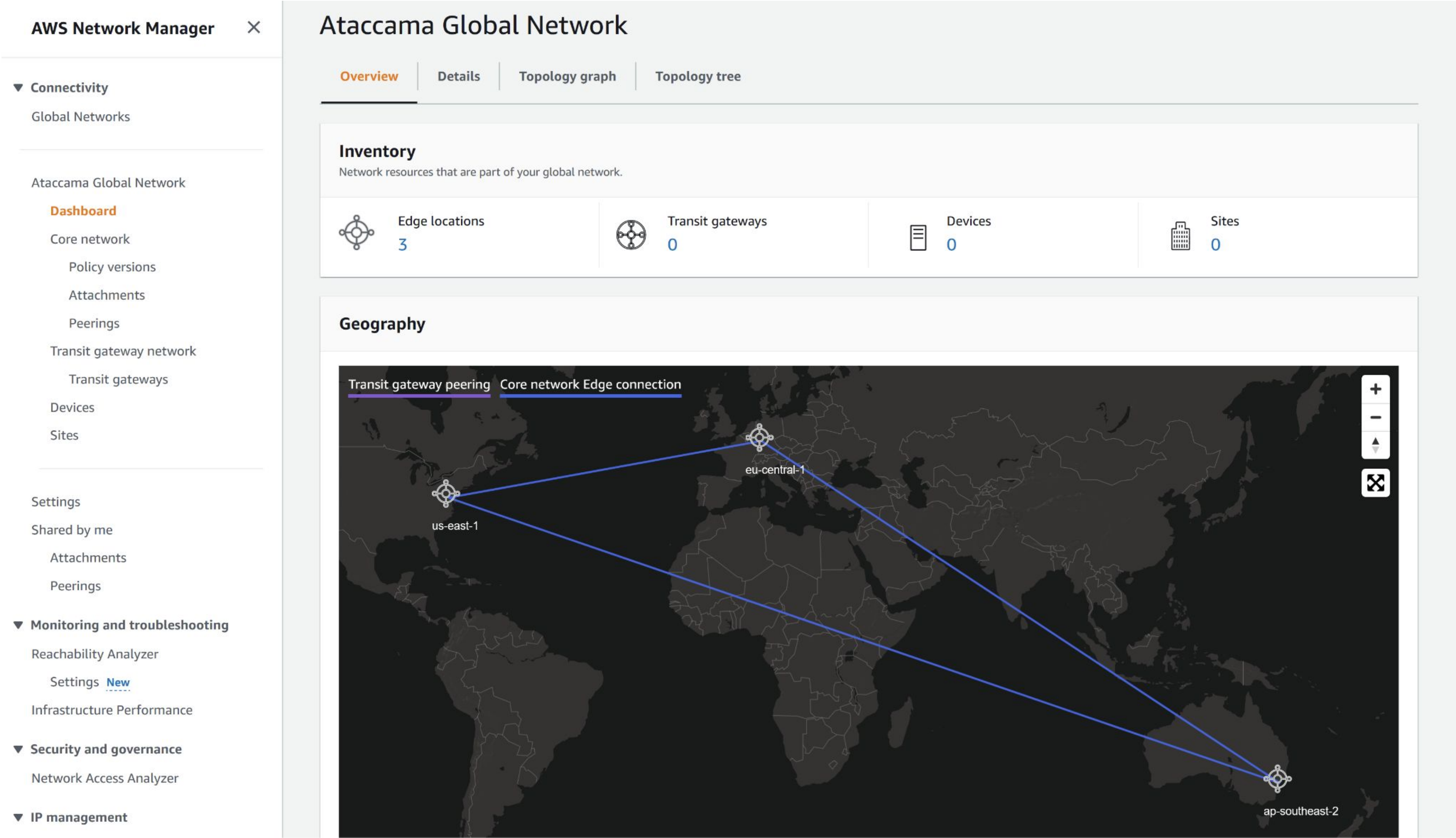
- Over 2 years at Ataccama
  - Internal network and secops lead

AWS Cloud WAN introduction

What is Cloud WAN?

- Managed global network
- Layer 3 IP VPN over MPLS
- Central dashboard for management across all regions
- Segmentation by design
- Managed by policy
- Throughputs similar to transit gateways (eg. 50 Gbit/s per VPC attached to Cloud WAN)
- Easy way how to interconnect VPCs, onprem datacenters, branch offices…

What is Cloud WAN?



AWS Network Manager

Connectivity

Global Networks

Ataccama Global Network

Dashboard

Core network

Policy versions

Attachments

Peerings

Transit gateway network

Transit gateways

Devices

Sites

Settings

Shared by me

Attachments

Peerings

Monitoring and troubleshooting

Reachability Analyzer

Settings New

Infrastructure Performance

Security and governance

Network Access Analyzer

IP management

Ataccama Global Network

Overview | Details | Topology graph | Topology tree

Inventory

Network resources that are part of your global network.

Edge locations	Transit gateways	Devices	Sites
3	0	0	0

Geography

Building blocks

AWS Cloud WAN BBs

- Global network and core network
- Policies
- Segments
- Attachments
- Routing

Global network and core network

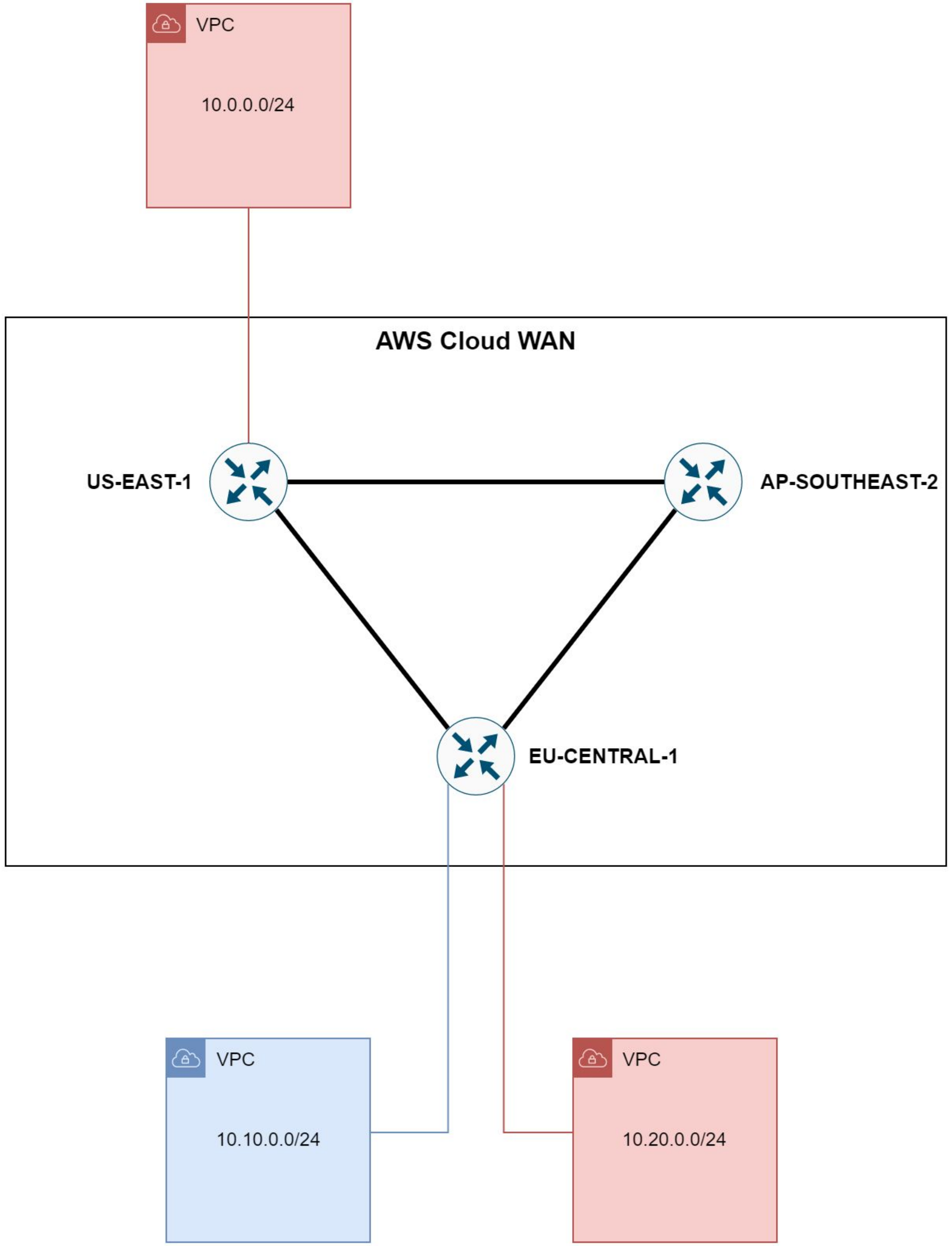
- **Global network**
  - Root level container for network objects
  - You can have multiple global networks
- **Core network**
  - Global network managed by AWS
  - You can have one core network per global network

Policy

- Single document that defines your core network
    - Regions
    - Segments
    - Routing rules
    - Attachment rules
- Versioned with rollback support

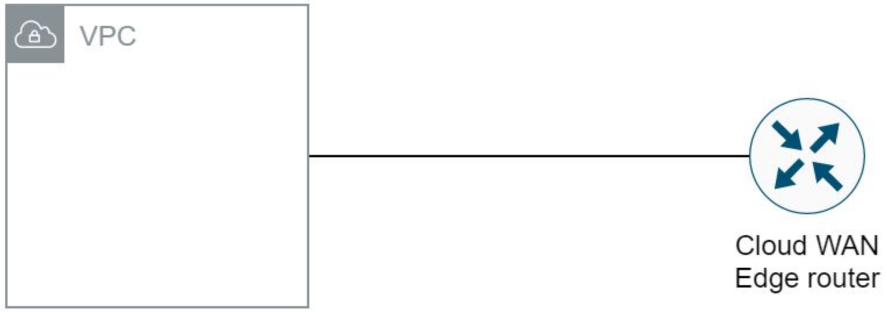
Segments

- Like VRFs
- Provide network isolation
- Driven by policies
- Attaching by tags

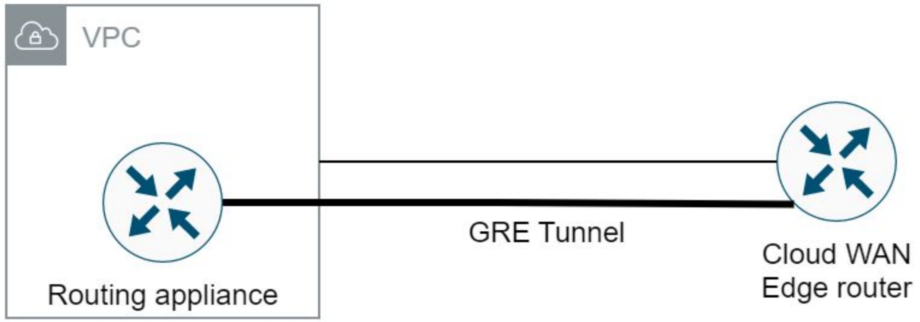


Attachments

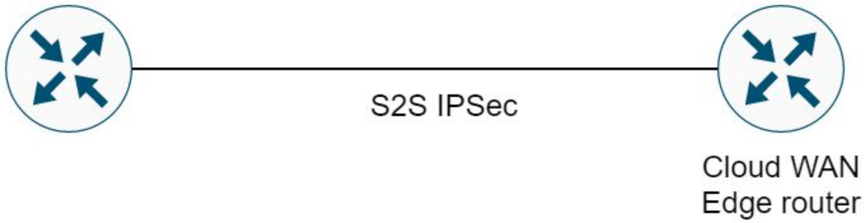
- VPC Attachment



- Connect Attachment



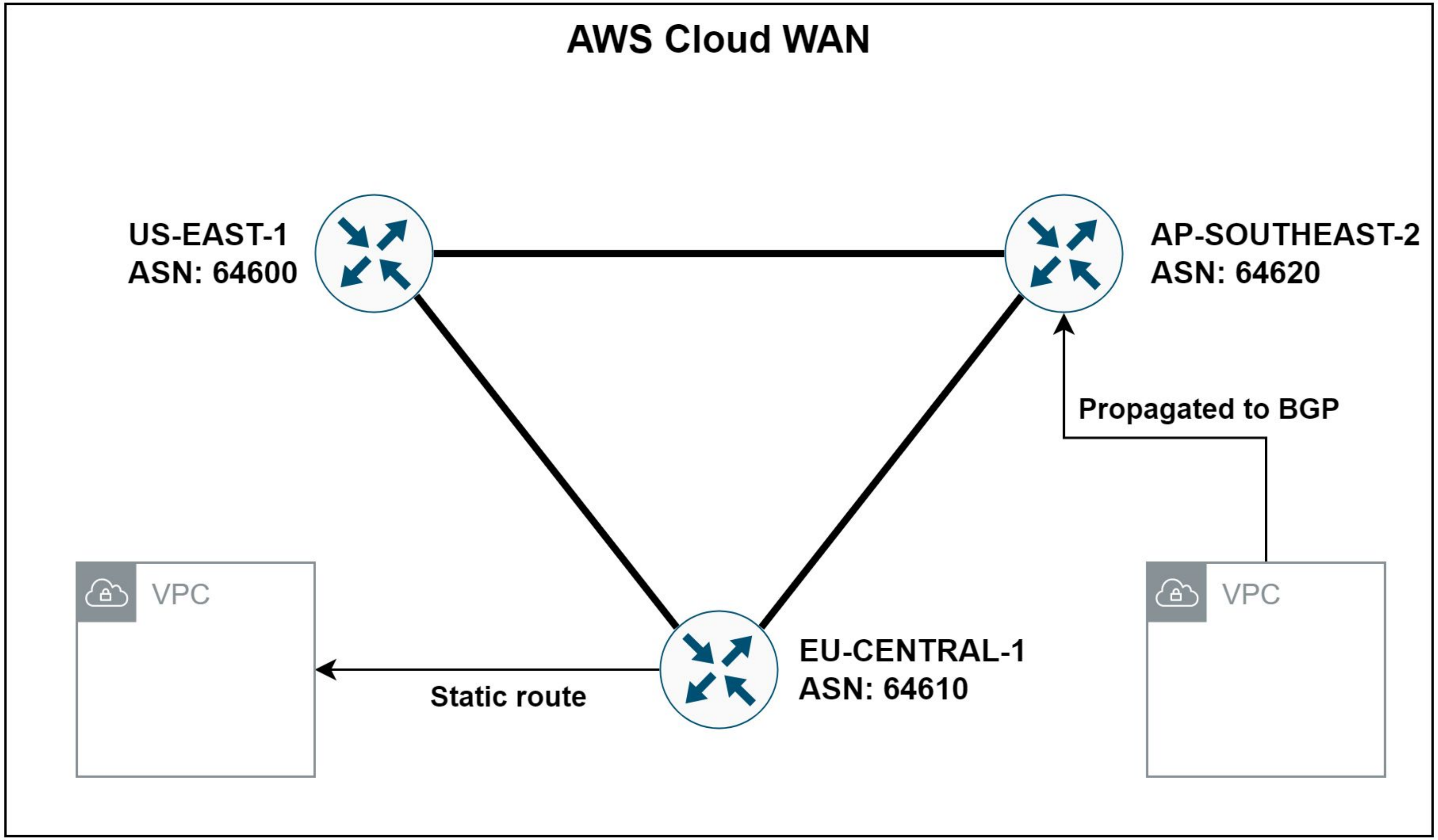
- S2S VPN Attachment



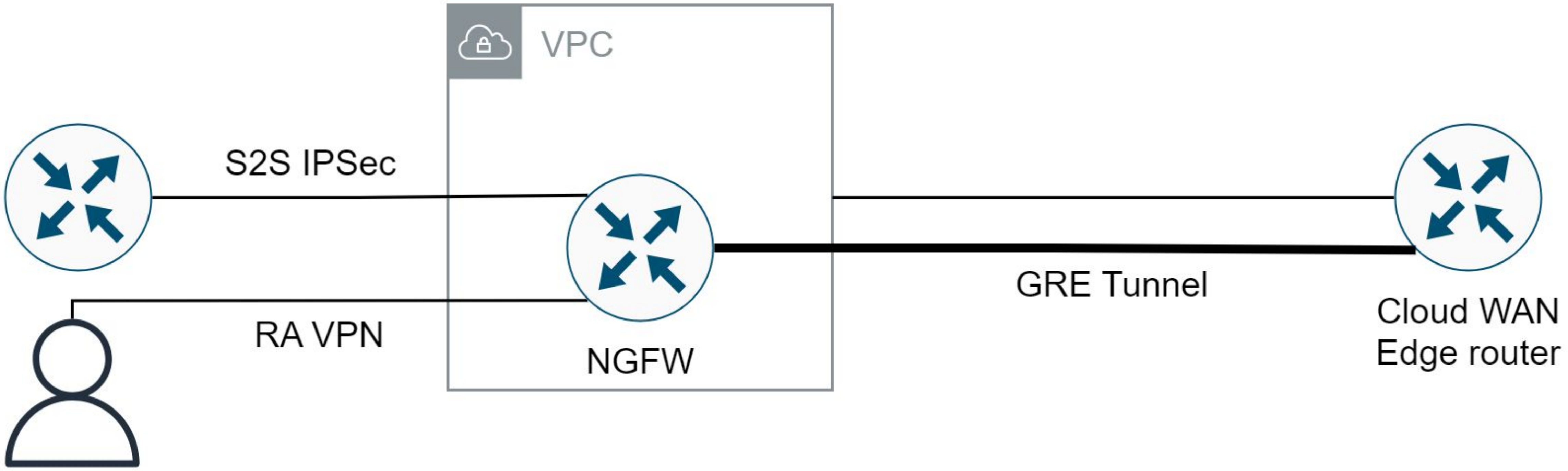
Routing

- BGP (EBGP)
- Static routing propagated to BGP
- BGP Metrics
  - AS PATH
  - MED
- Beware of asymmetric routing

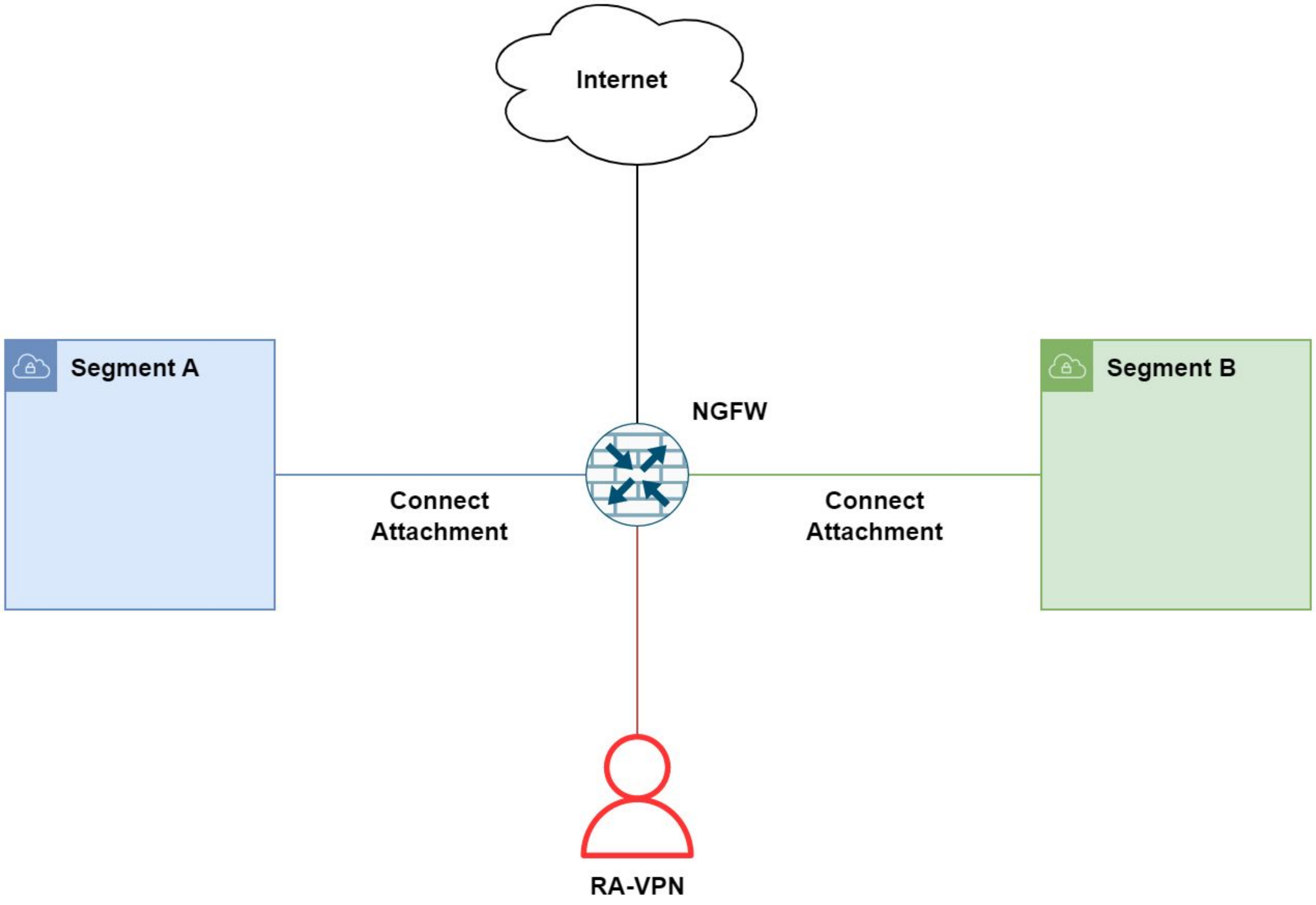
Routing


AWS Cloud WAN
US-EAST-1
ASN: 64600
AP-SOUTHEAST-2
ASN: 64620
Propagated to BGP
VPC
VPC
Static route
EU-CENTRAL-1
ASN: 64610

Next Gen firewalls integration



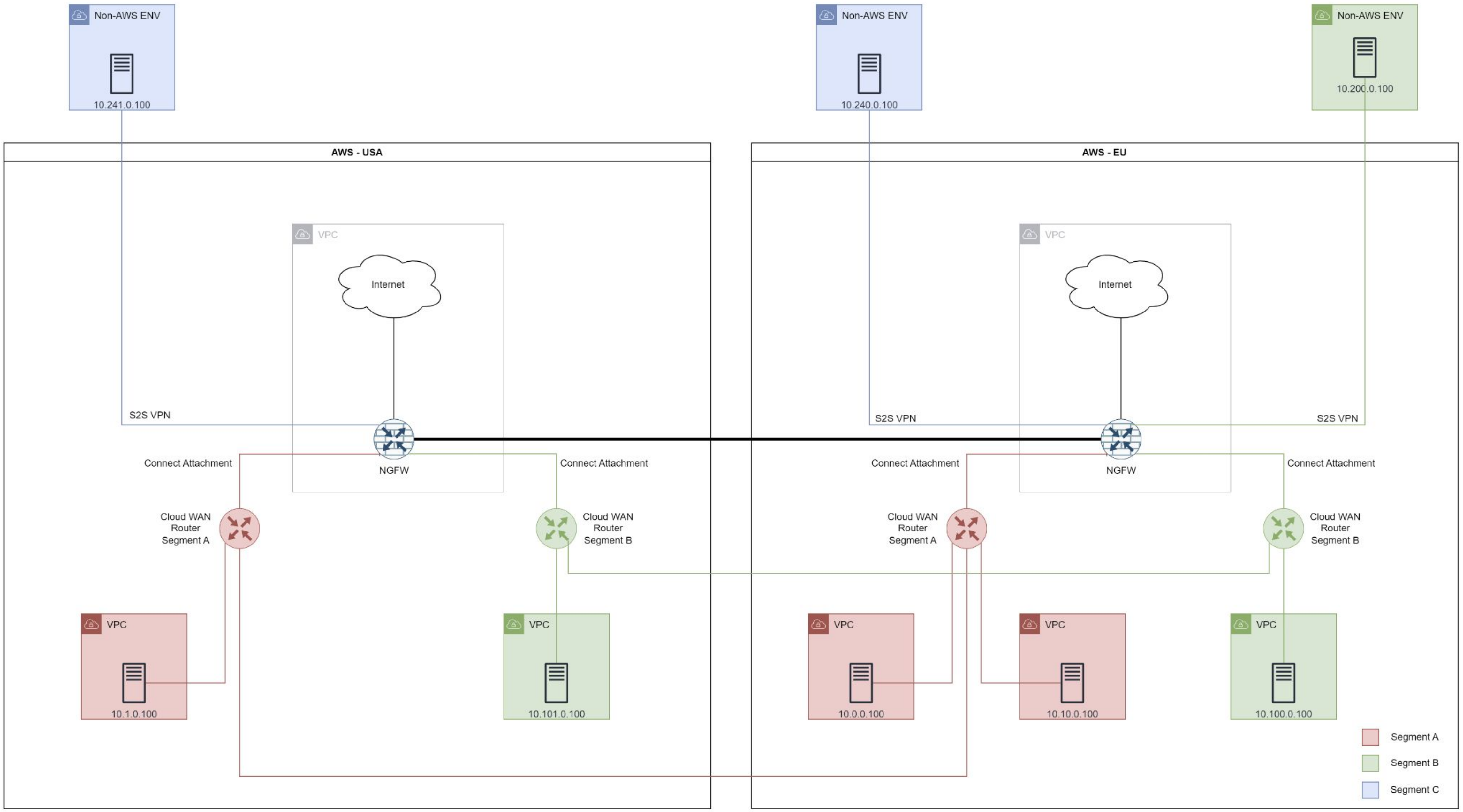
Next Gen firewalls integration



BGP Tricks

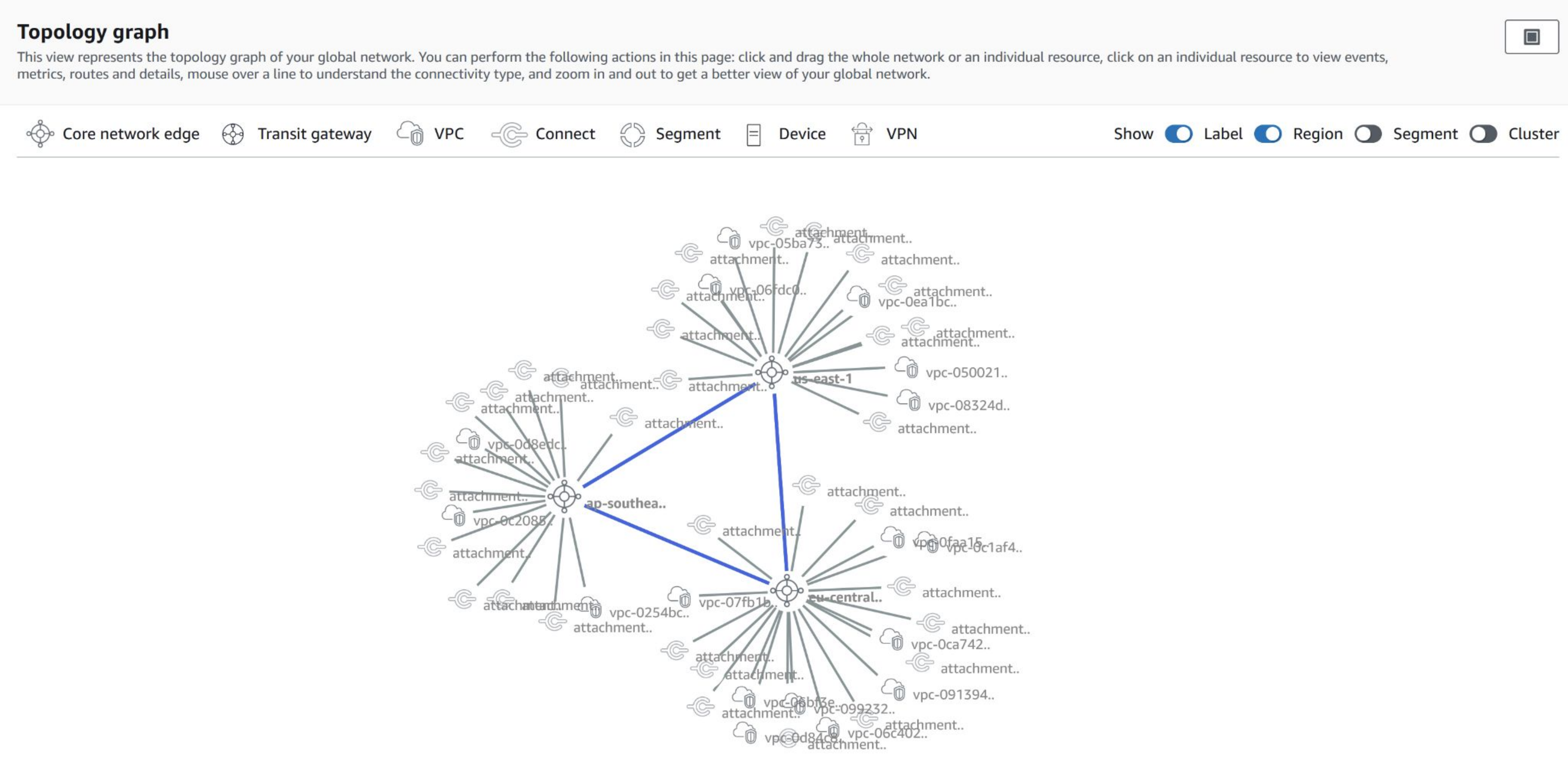
- Announce least specific and 0.0.0.0/0 routes to segments only
    - eg. 10.0.0.0/8
- Use separated segment for interconnecting NGFWs (transit) with all learned routes
- Design transit segment routes propagation properly to eliminate asymmetric routing
    - Prefer inter-region routes learned from transit segment to routes learned from other segments
    - Think about failover (depends on NGFW capabilities)
        - AS prepending with MED, conditional routes propagating

Everything together



AWS Cloud WAN UI

Cloud WAN UI - Topology



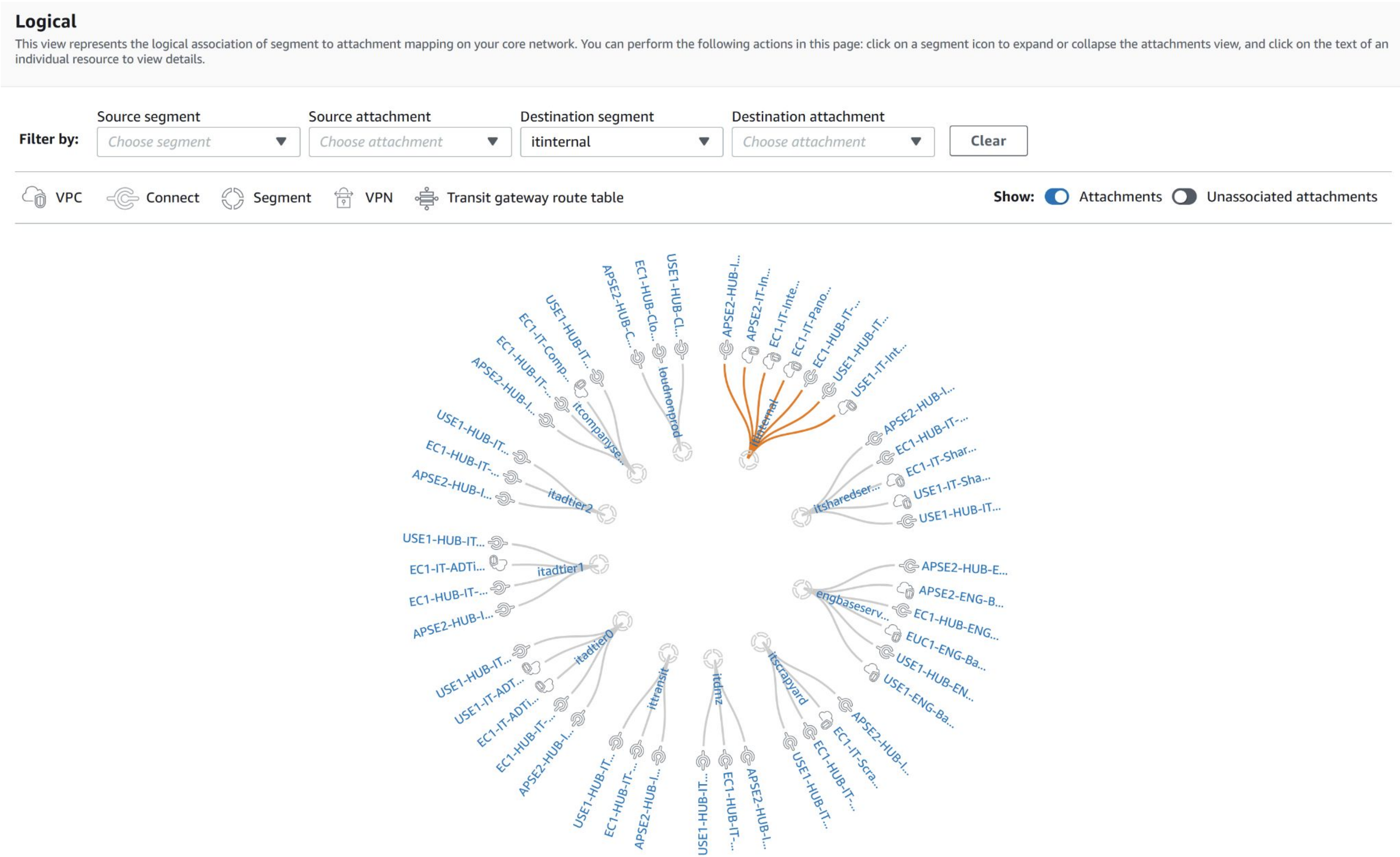
Topology graph

This view represents the topology graph of your global network. You can perform the following actions in this page: click and drag the whole network or an individual resource, click on an individual resource to view events, metrics, routes and details, mouse over a line to understand the connectivity type, and zoom in and out to get a better view of your global network.

Core network edge   Transit gateway   VPC   Connect   Segment   Device   VPN

Show ● Label ● Region ○ Segment ○ Cluster

Cloud WAN UI - Logical graph



Logical

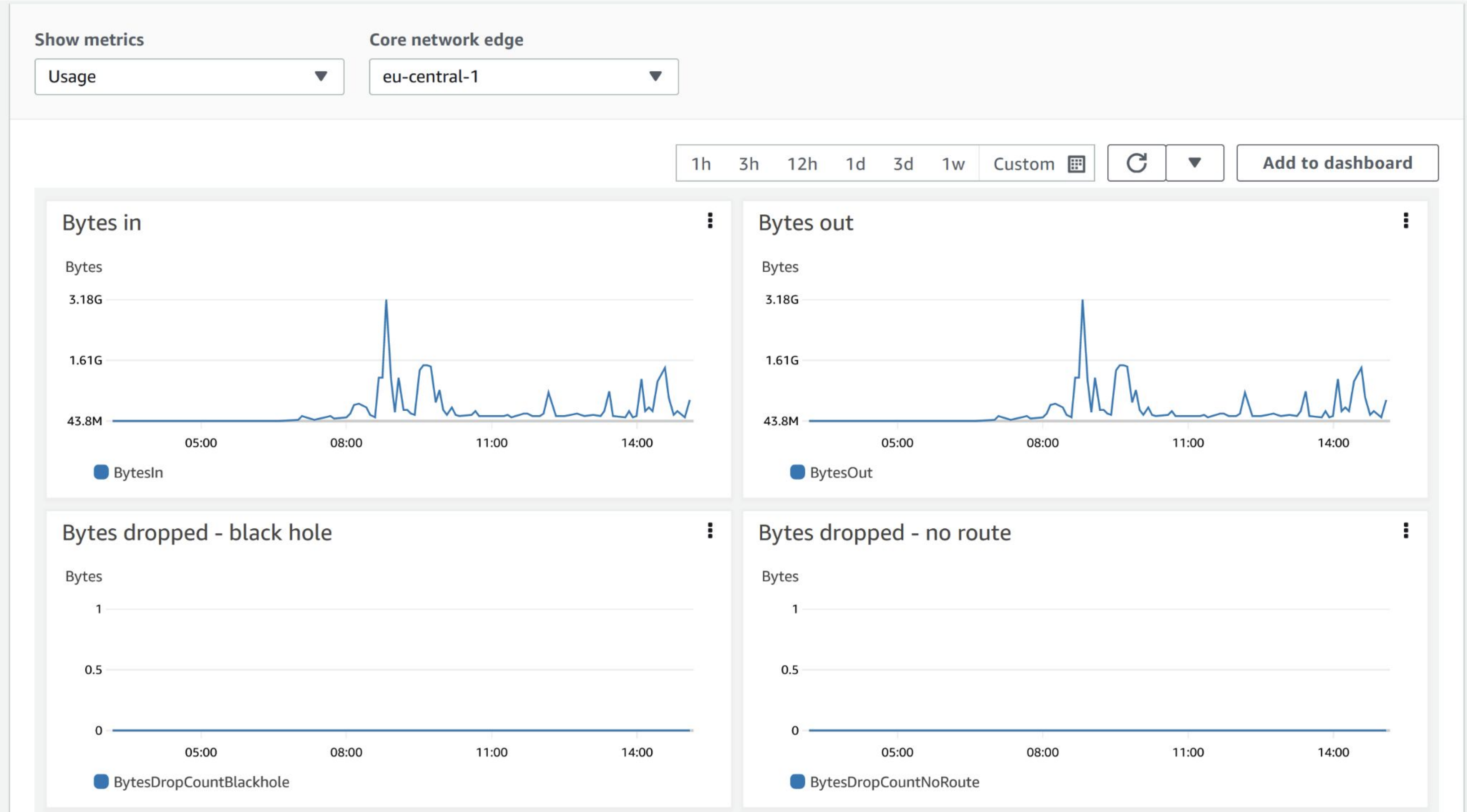
This view represents the logical association of segment to attachment mapping on your core network. You can perform the following actions in this page: click on a segment icon to expand or collapse the attachments view, and click on the text of an individual resource to view details.

Filter by: Source segment: Choose segment ▼ | Source attachment: Choose attachment ▼ | Destination segment: itinternal ▼ | Destination attachment: Choose attachment ▼ | Clear

VPC | Connect | Segment | VPN | Transit gateway route table

Show: ● Attachments ○ Unassociated attachments

Cloud WAN UI - Metrics



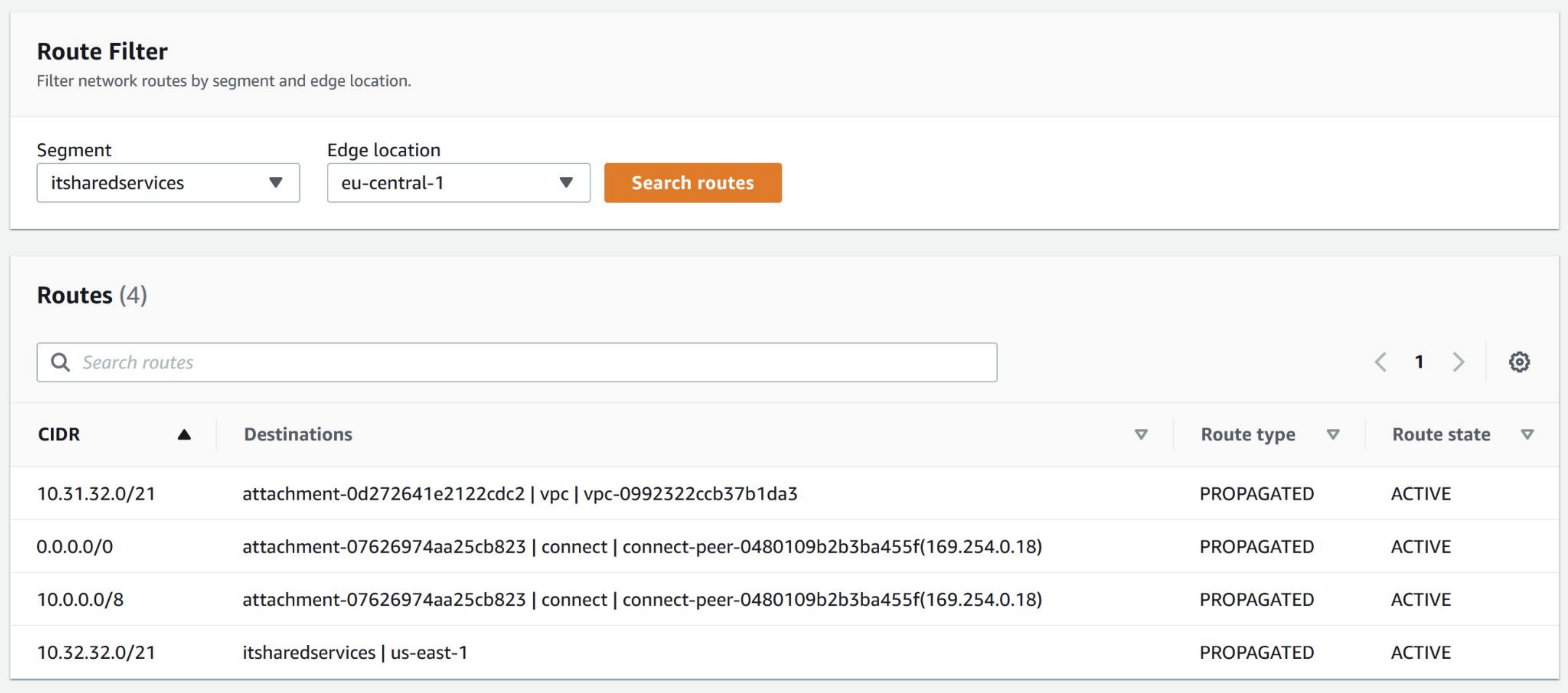
Show metrics

Usage

Core network edge

eu-central-1

Cloud WAN UI - Routing



Route Filter

Filter network routes by segment and edge location.

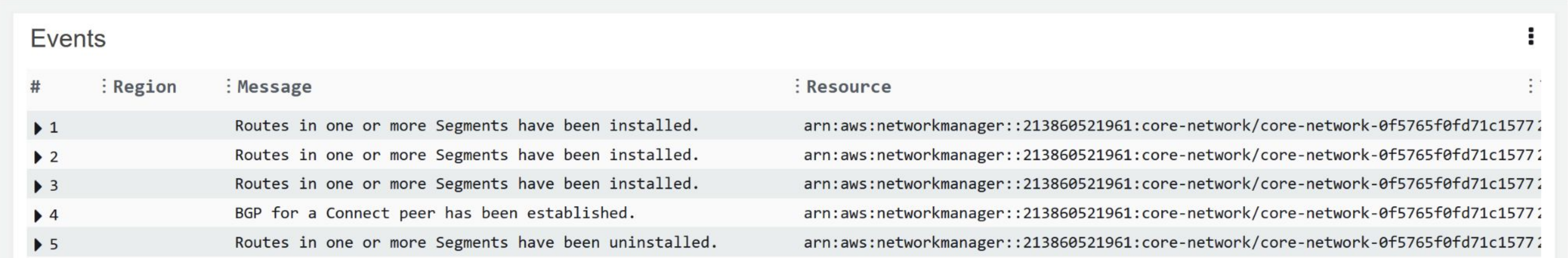
Segment: itsharedservices

Edge location: eu-central-1

Routes (4)

CIDR	Destinations	Route type	Route state
10.31.32.0/21	attachment-0d272641e2122cdc2 | vpc | vpc-0992322ccb37b1da3	PROPAGATED	ACTIVE
0.0.0.0/0	attachment-07626974aa25cb823 | connect | connect-peer-0480109b2b3ba455f(169.254.0.18)	PROPAGATED	ACTIVE
10.0.0.0/8	attachment-07626974aa25cb823 | connect | connect-peer-0480109b2b3ba455f(169.254.0.18)	PROPAGATED	ACTIVE
10.32.32.0/21	itsharedservices | us-east-1	PROPAGATED	ACTIVE

Cloud WAN UI - Events



Events

#	Region	Message	Resource
▶ 1		Routes in one or more Segments have been installed.	arn:aws:networkmanager::213860521961:core-network/core-network-0f5765f0fd71c1577
▶ 2		Routes in one or more Segments have been installed.	arn:aws:networkmanager::213860521961:core-network/core-network-0f5765f0fd71c1577
▶ 3		Routes in one or more Segments have been installed.	arn:aws:networkmanager::213860521961:core-network/core-network-0f5765f0fd71c1577
▶ 4		BGP for a Connect peer has been established.	arn:aws:networkmanager::213860521961:core-network/core-network-0f5765f0fd71c1577
▶ 5		Routes in one or more Segments have been uninstalled.	arn:aws:networkmanager::213860521961:core-network/core-network-0f5765f0fd71c1577

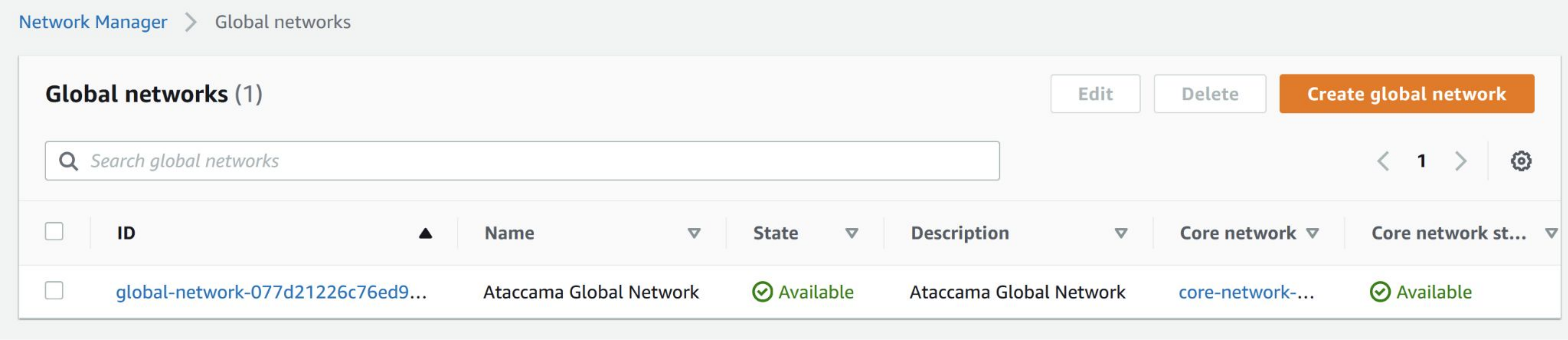
Cloud WAN deployment

Cloud WAN deployment 101

- Clickops
- JSON
- CloudFormation
- Terraform

Cloud WAN deployment 101

- Open Network Manager
- Create a global network for your core network
- Create a core network
- Create your first policy version



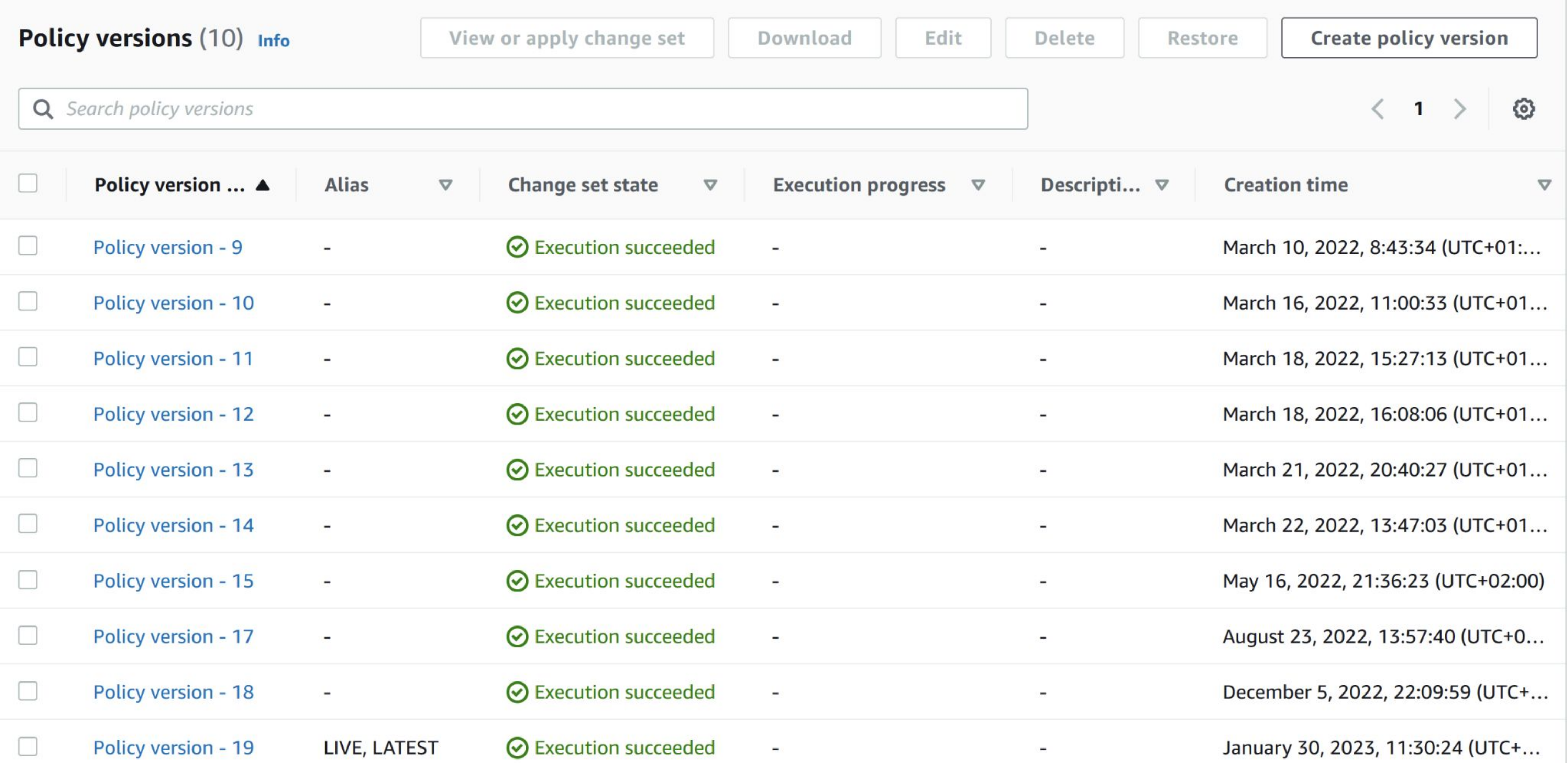
Global networks (1)

☐	ID ▲	Name ▽	State ▽	Description ▽	Core network ▽	Core network st... ▽
☐	global-network-077d21226c76ed9...	Ataccama Global Network	✓ Available	Ataccama Global Network	core-network-...	✓ Available

Cloud WAN deployment 101 - policy

- Define ASN ranges
- For GRE - define internal core network CIDR block
- Choose your regions
- Define your segments and attachment acceptance
- Define attachment policies
  - tags that will assign attachments to corresponding segments
  - auto approval / manual approval
- Create policy and apply it

Cloud WAN deployment 101 - policy



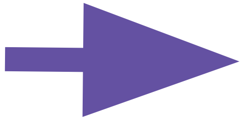
□	Policy version ... ▲	Alias	Change set state	Execution progress	Descripti...	Creation time
□	Policy version - 9	-	✓ Execution succeeded	-	-	March 10, 2022, 8:43:34 (UTC+01:...
□	Policy version - 10	-	✓ Execution succeeded	-	-	March 16, 2022, 11:00:33 (UTC+01...
□	Policy version - 11	-	✓ Execution succeeded	-	-	March 18, 2022, 15:27:13 (UTC+01...
□	Policy version - 12	-	✓ Execution succeeded	-	-	March 18, 2022, 16:08:06 (UTC+01...
□	Policy version - 13	-	✓ Execution succeeded	-	-	March 21, 2022, 20:40:27 (UTC+01...
□	Policy version - 14	-	✓ Execution succeeded	-	-	March 22, 2022, 13:47:03 (UTC+01...
□	Policy version - 15	-	✓ Execution succeeded	-	-	May 16, 2022, 21:36:23 (UTC+02:00)
□	Policy version - 17	-	✓ Execution succeeded	-	-	August 23, 2022, 13:57:40 (UTC+0...
□	Policy version - 18	-	✓ Execution succeeded	-	-	December 5, 2022, 22:09:59 (UTC+...
□	Policy version - 19	LIVE, LATEST	✓ Execution succeeded	-	-	January 30, 2023, 11:30:24 (UTC+...

Cloud WAN pricing

- Hourly rate per network edge
  - cca $366 / month per region
- Hourly rate per attachment
  - varies per region
  - around $40 / month
- Data transfers
  - varies on source and target, much more complicated to calculate
  - around $20 / 1 TB inside AWS
  - around $90 / 1 TB to the internet

Ataccama and AWS Cloud WAN

The goal



Issues we had

- Teams started to be scattered all around the world
- Not enough people to build onprem infrastructure
- Different technologies
- Dozens of cloud accounts that needed access to something
- Security requirements
- Chip shortage
- Crappy RA-VPN solution
- Limited HA

How did we solve it?

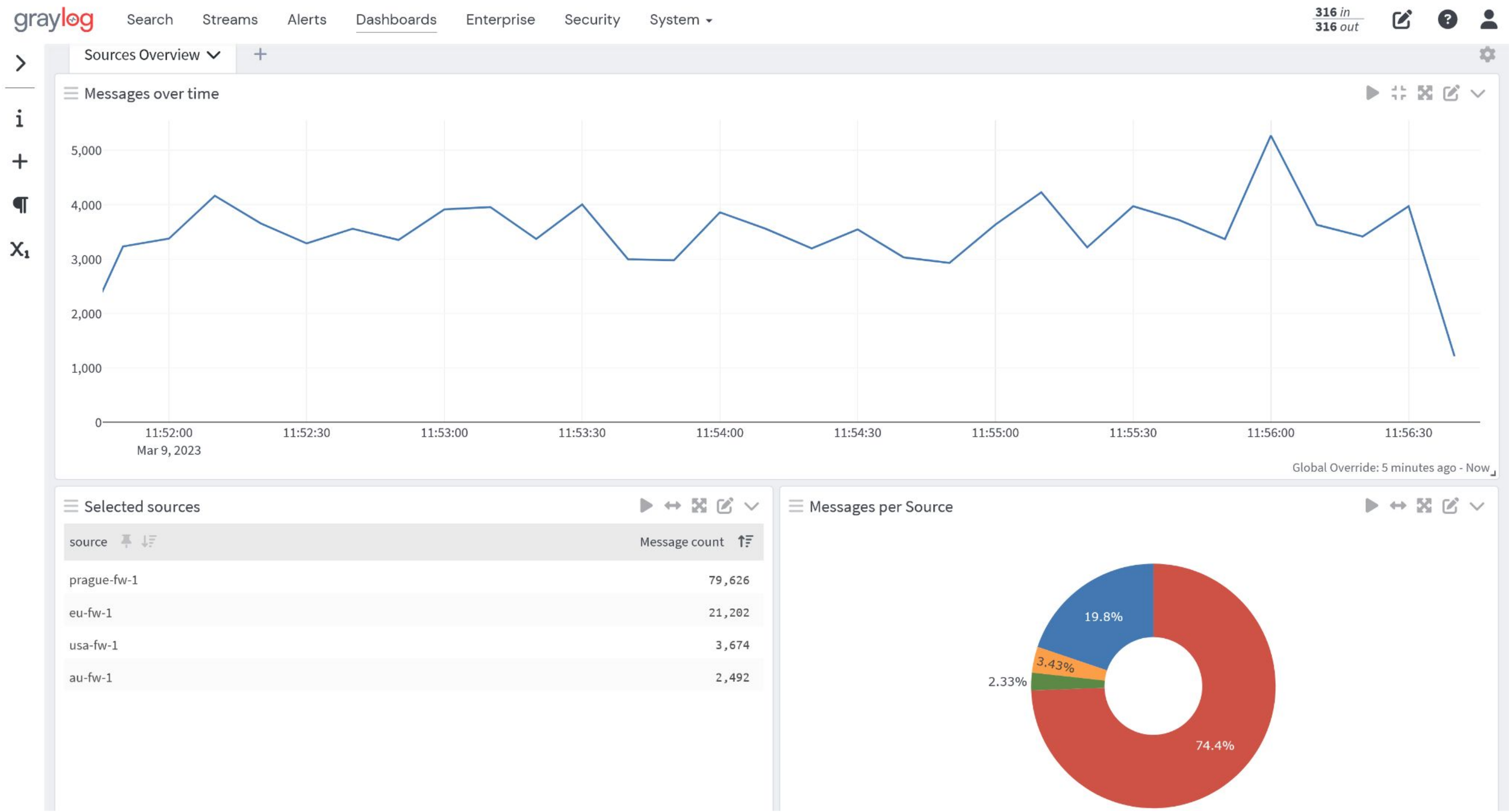
- We decided to skip creating our own onprem infrastructure
- We selected AWS to be the main provider due to the Cloud WAN
    - In December 2021 …
- 3 regions, 11 segments
- All our offices connected to the Cloud WAN (via NGFWs)
- All our IT services in the cloud and interconnected via Cloud WAN
    - Really, all of them
    - DNS, Cisco WLC, Cisco DNAC, logging solution, Active Directory, S2S to partners, backups, firewall management and so on…

Network security

- **Palo Alto Next Generation firewalls between segments**
  - Providing internet access to the whole network
  - IPS, IDS, Threat Prevention, DNS security
  - RA-VPN, S2S to offices
  - Identity firewalling based on Azure AD utilizing Cloud Identity Engine
    - Onprem Active Directory will be soon obsolete
- **Communication within segment**
  - Still relying on security groups
  - Flow logs + Prisma Cloud

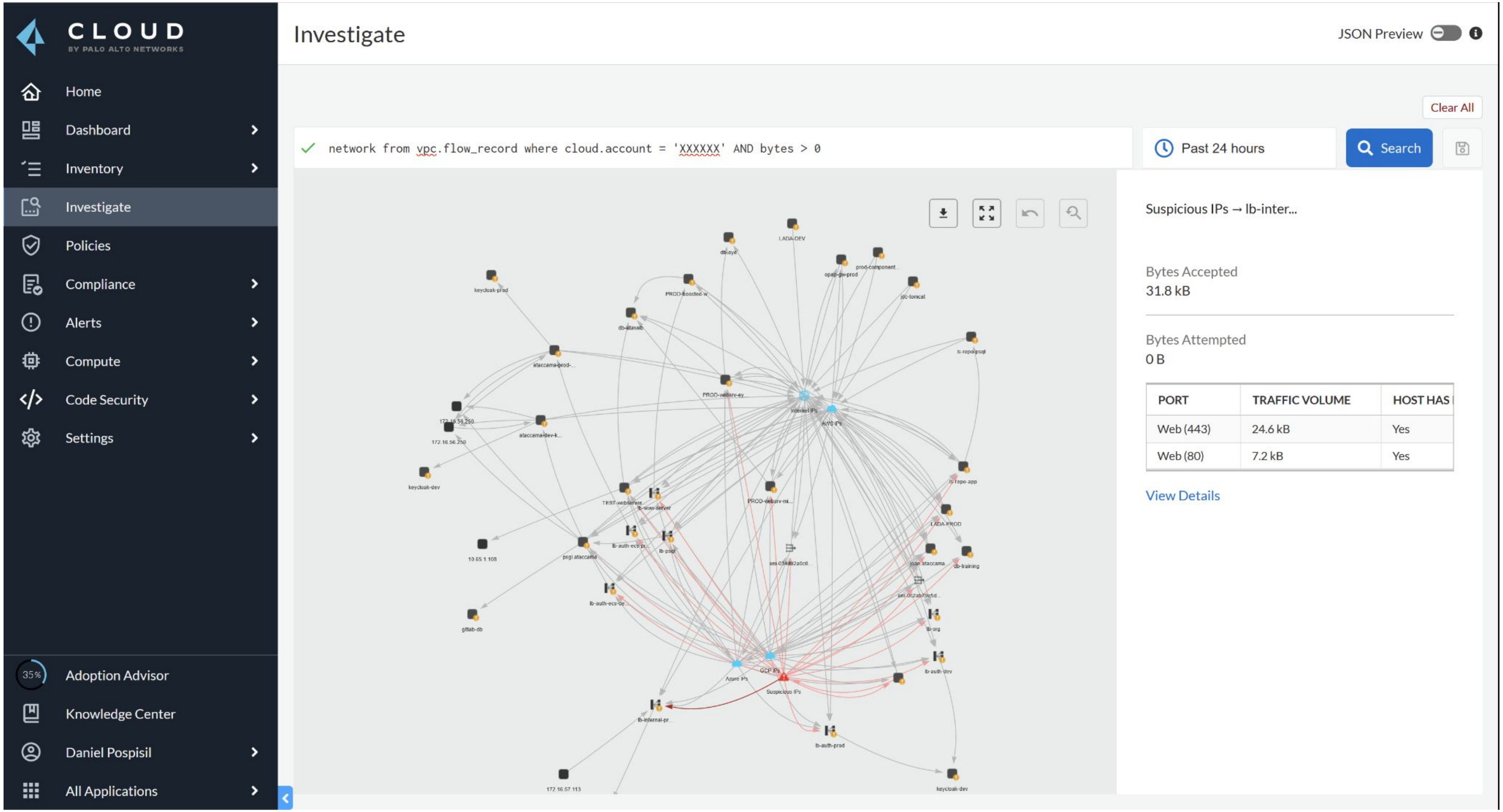
Network visibility

- All traffic logged and forwarded to logging solution
- All discovered threats logged as well



source	Message count
prague-fw-1	79,626
eu-fw-1	21,202
usa-fw-1	3,674
au-fw-1	2,492

Network visibility



```
network from vpc.flow_record where cloud.account = 'XXXXXX' AND bytes > 0
```

Suspicious IPs → lb-inter...

Bytes Accepted
31.8 kB

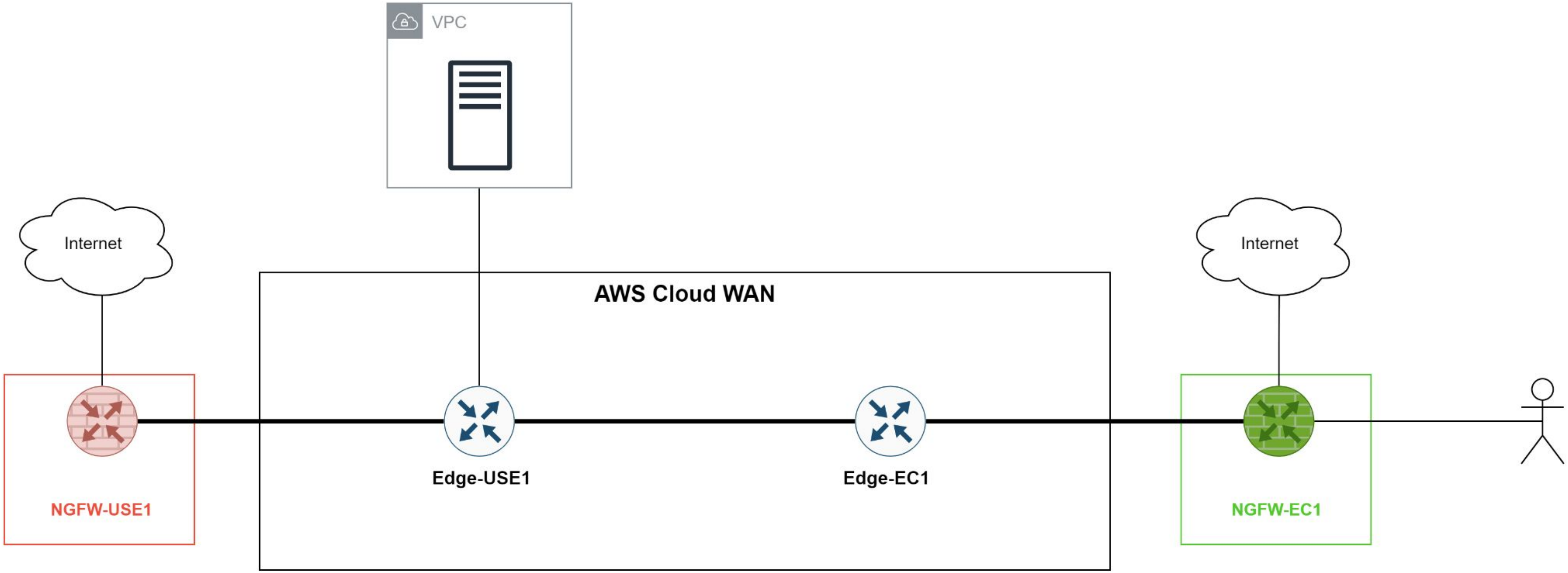
Bytes Attempted
0 B

PORT	TRAFFIC VOLUME	HOST HAS
Web (443)	24.6 kB	Yes
Web (80)	7.2 kB	Yes

View Details

High availability

DEMO TIME



Q&A