AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

NET209-R2

Improve your network monitoring

Christian Elsen
Principal Networking Solutions Architect
Amazon Web Services

Rashpal Kler
Senior Solutions Architect
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Monitoring: Why, how, what?

AWS service monitoring:

- Amazon Virtual Private Cloud – 15 min (Amazon VPC)
- Multi-VPC – 10 min
- Hybrid connectivity – 20 min

Chalk Talk: Ask us questions!


Single VPC


Flow logs


Traffic mirroring


VPC Reachability Analyzer


AWS Transit Gateway


Transit Gateway Route Analyzer


Amazon CloudWatch metrics


AWS Direct Connect


AWS Site-to-Site VPN


CloudWatch metrics


AWS Personal Health Dashboard

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Monitoring: Why, how, what?

- Why monitor?
  - Health, availability, performance, utilization . . .
- How?
  - Active vs. passive
  - Dashboards vs. alarms
- What?
  - Within a VPC, across VPCs, hybrid networking

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC



Flow logs

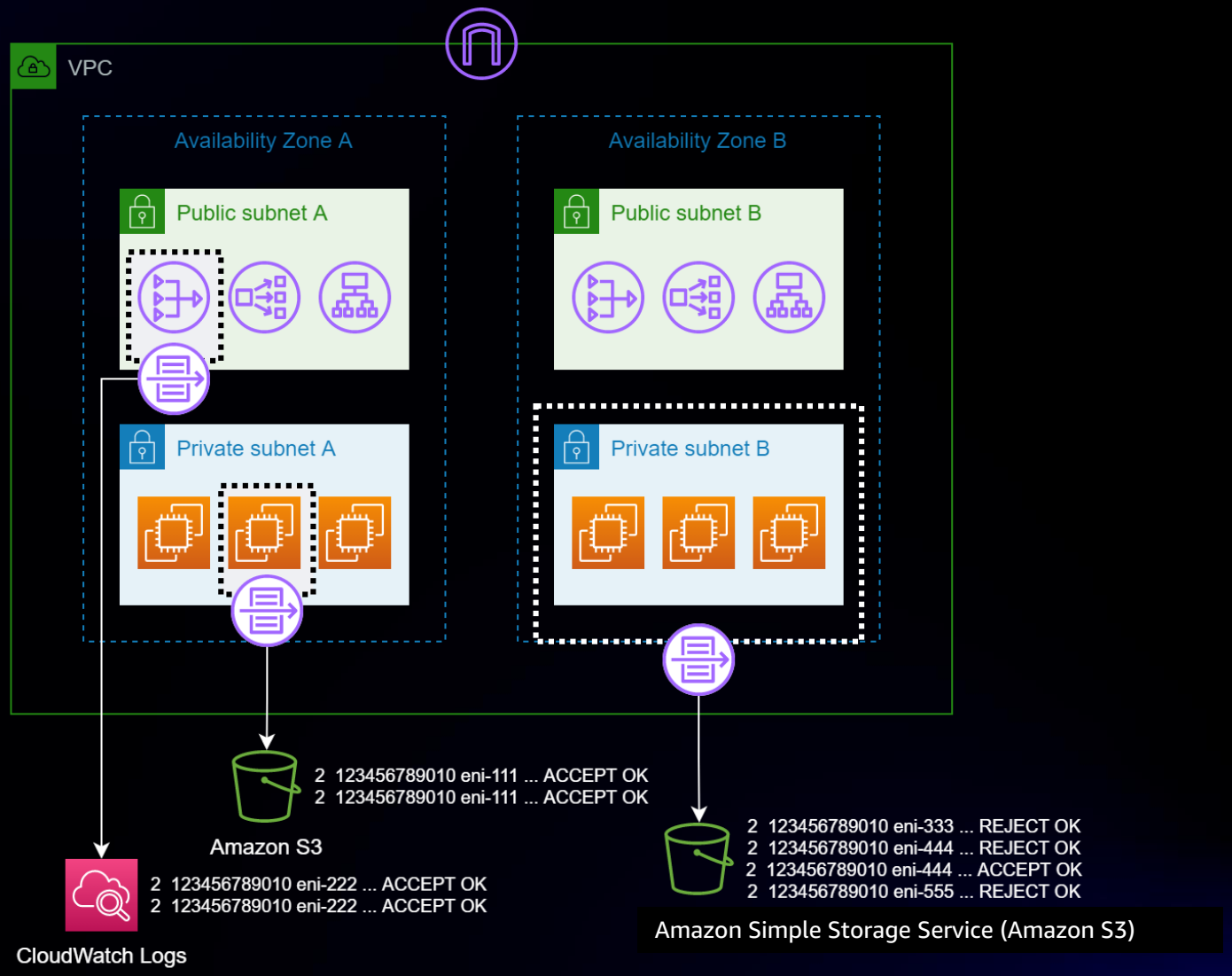
Traffic mirroring

Reachability Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Flow Logs

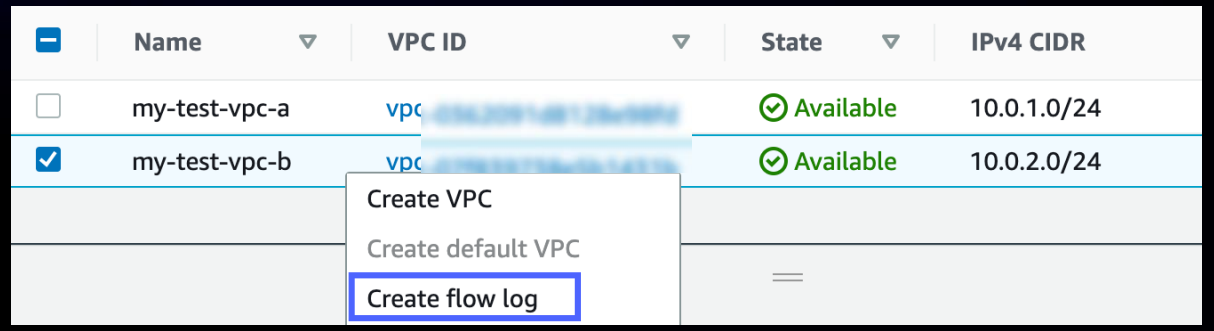
Flow logs



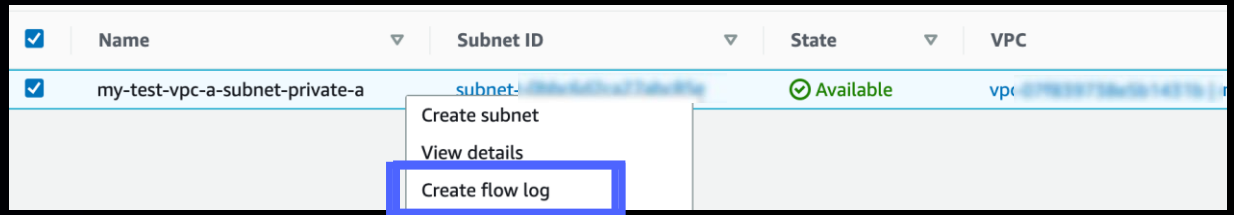
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Flow logs – VPC, subnet, interface

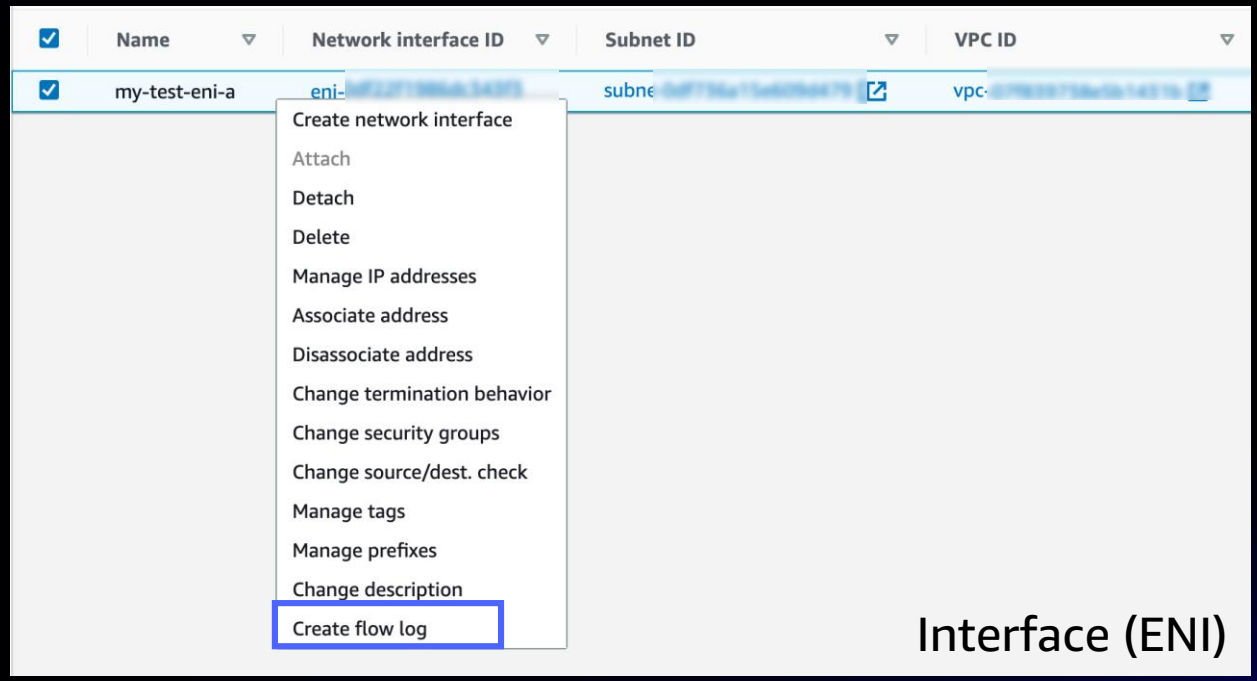




VPC



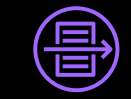
Subnet



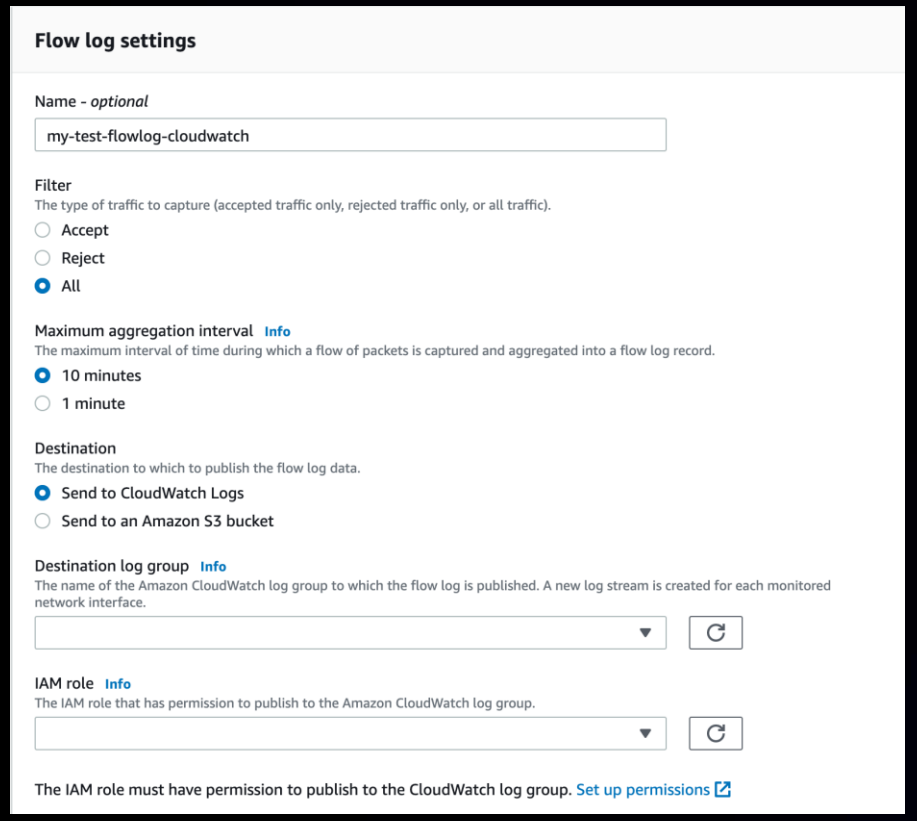
Interface (ENI)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

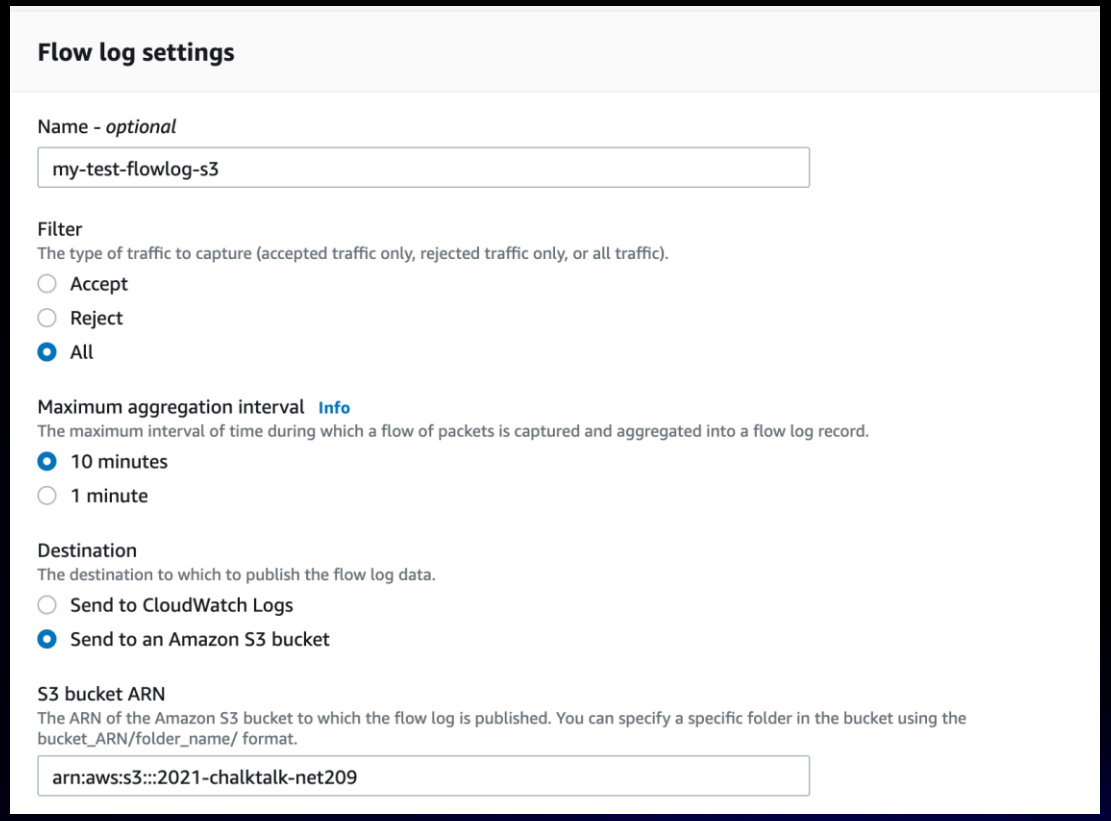
Publish flow logs



- Publish to CloudWatch

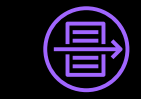


- Publish to Amazon S3

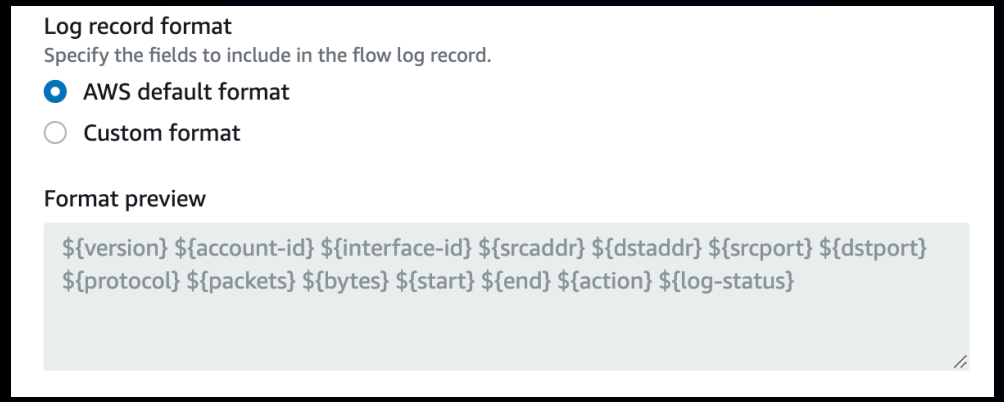


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

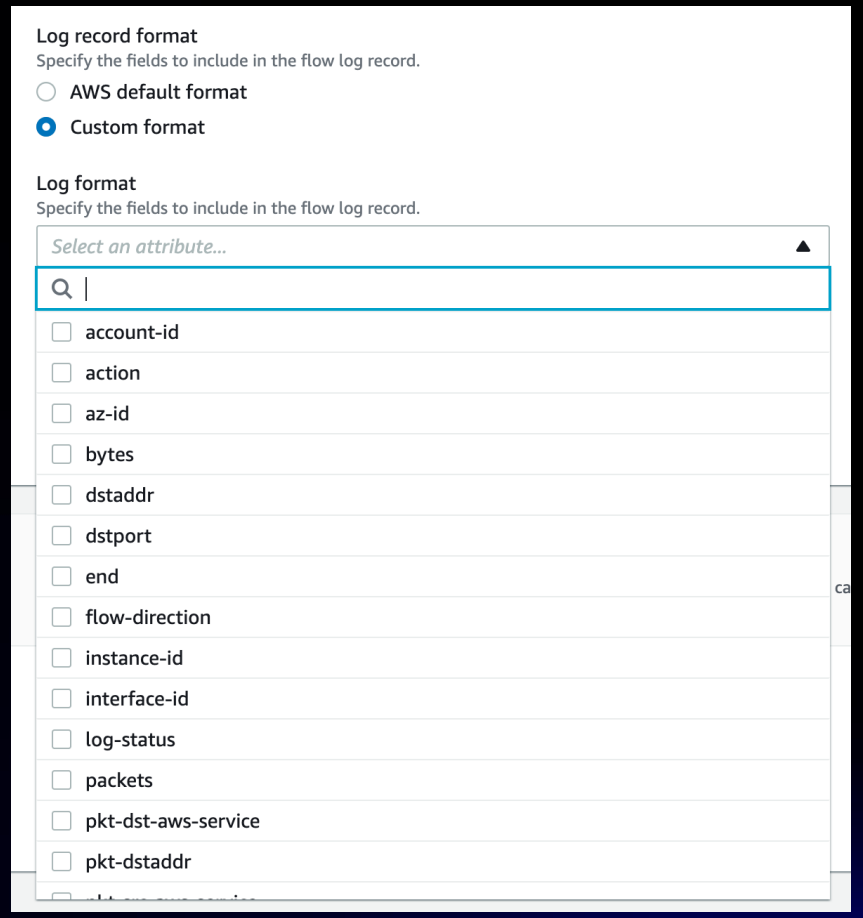
Flow log fields



- Default flow log fields



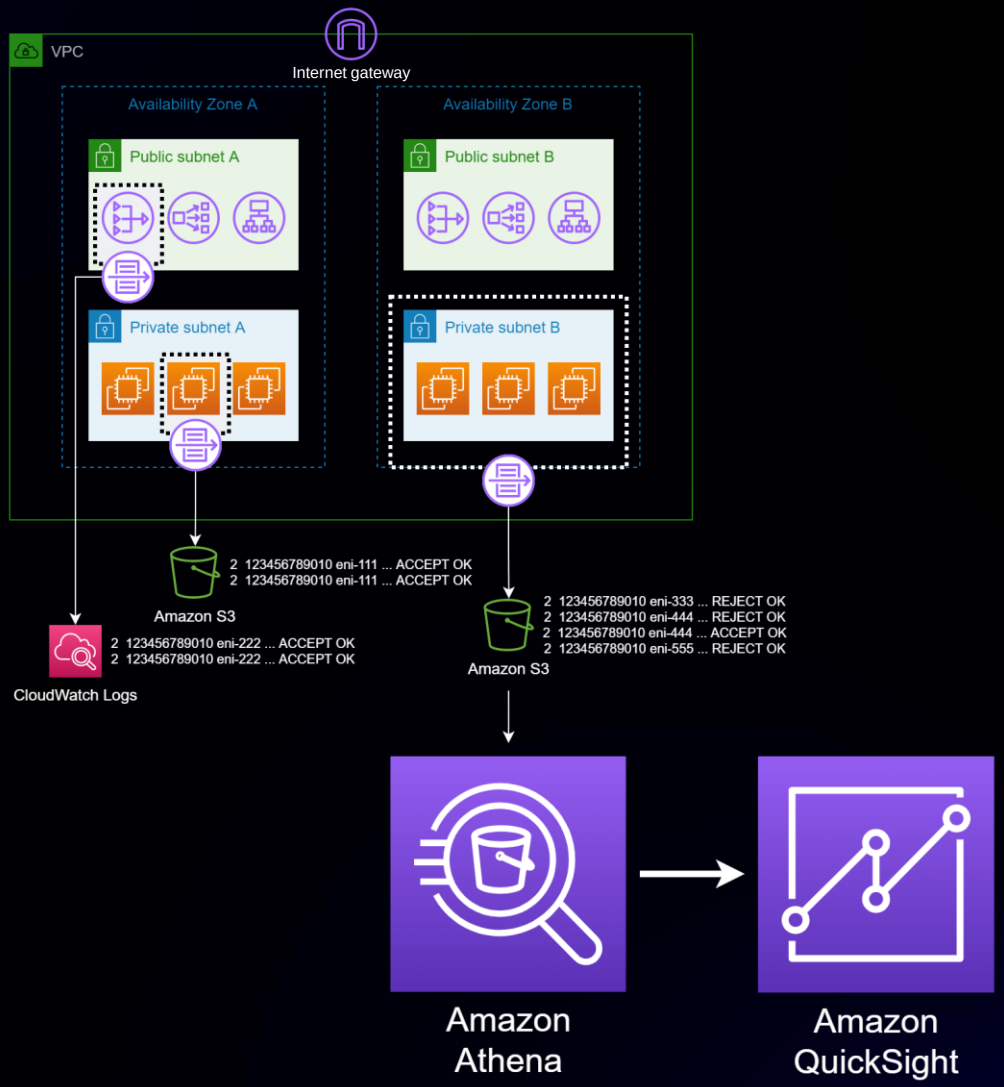
- Custom flow log fields



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: Visualize VPC Flow Logs

Flow logs

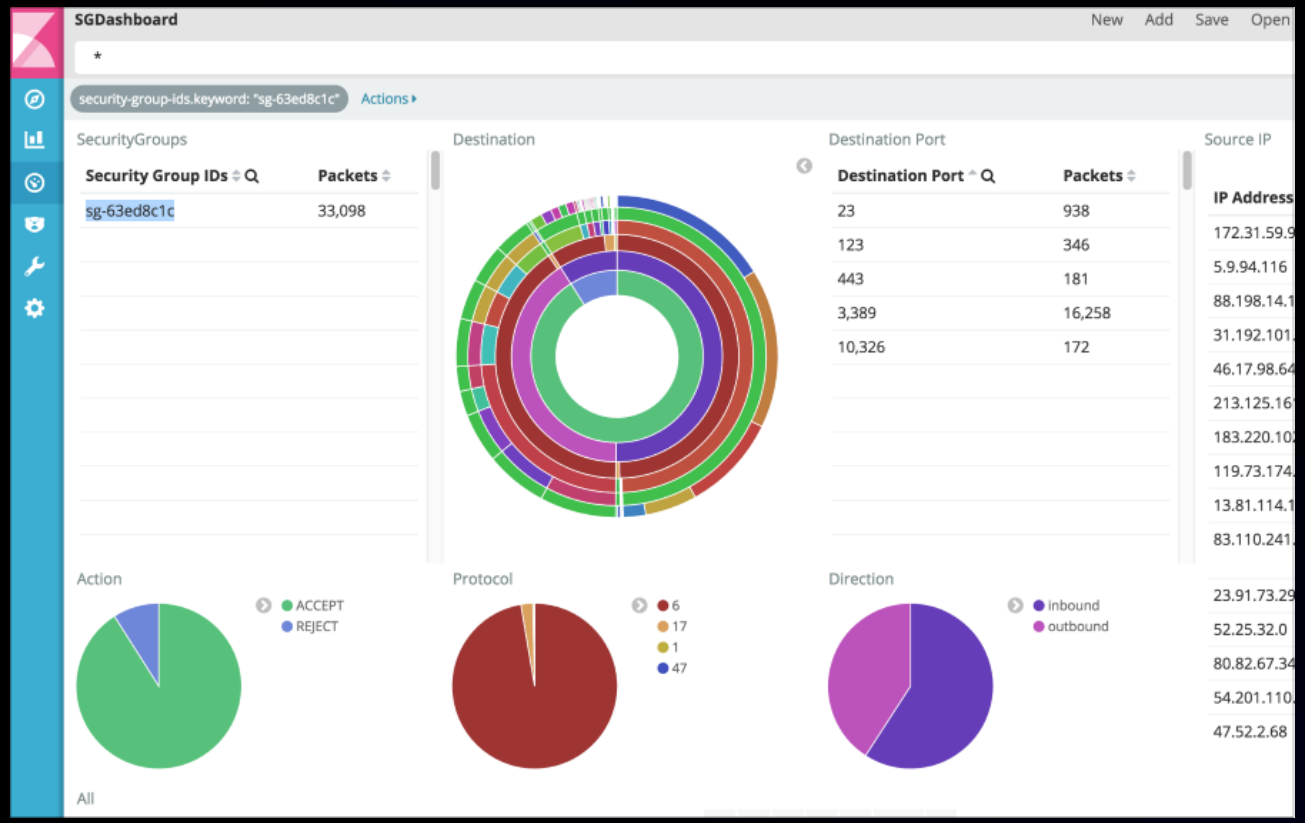


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: Visualize VPC Flow Logs



- AWS Blog: How to Visualize and Refine Your Network's Security by Adding Security Group IDs to Your VPC Flow Logs

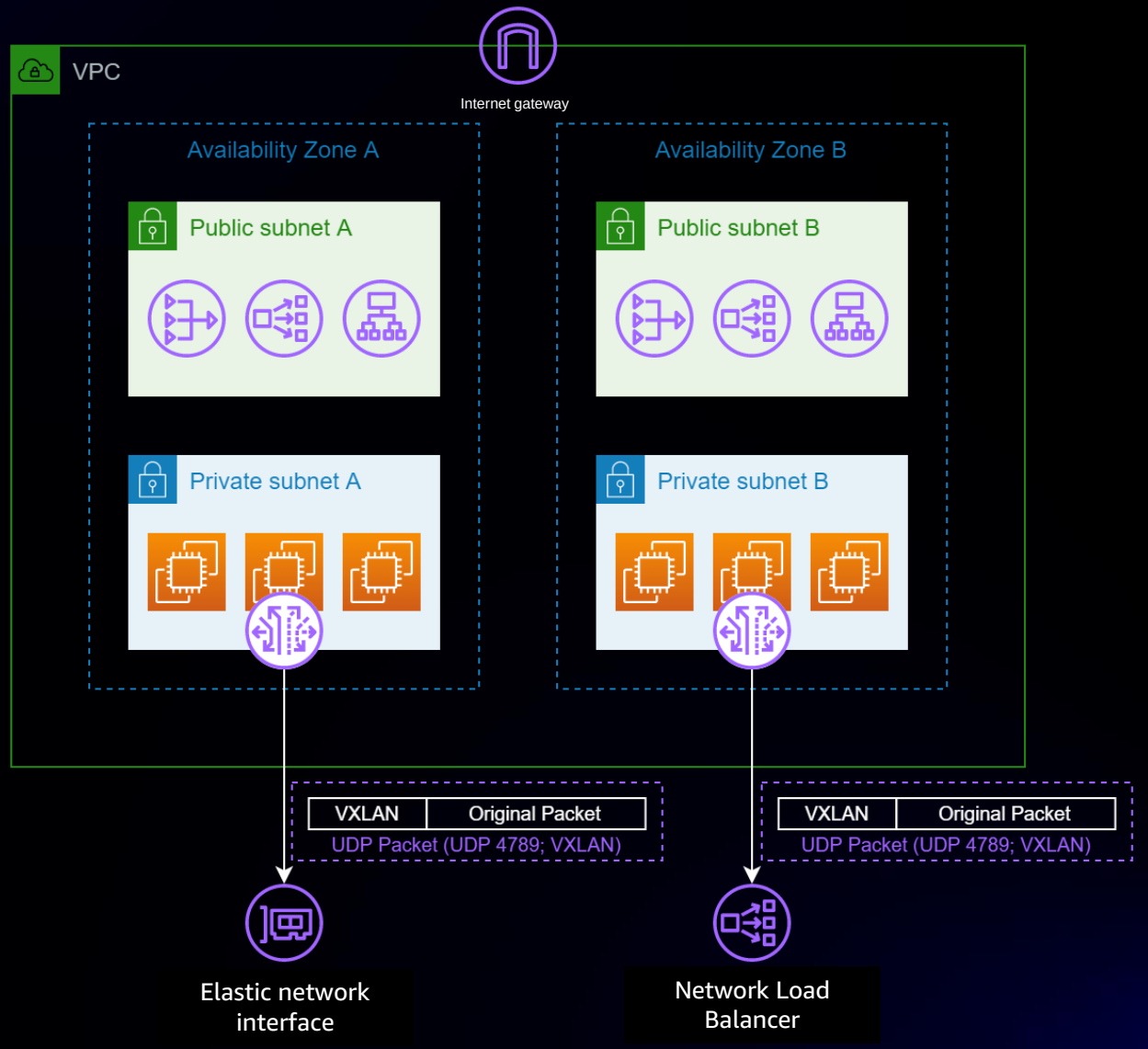




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC traffic mirroring

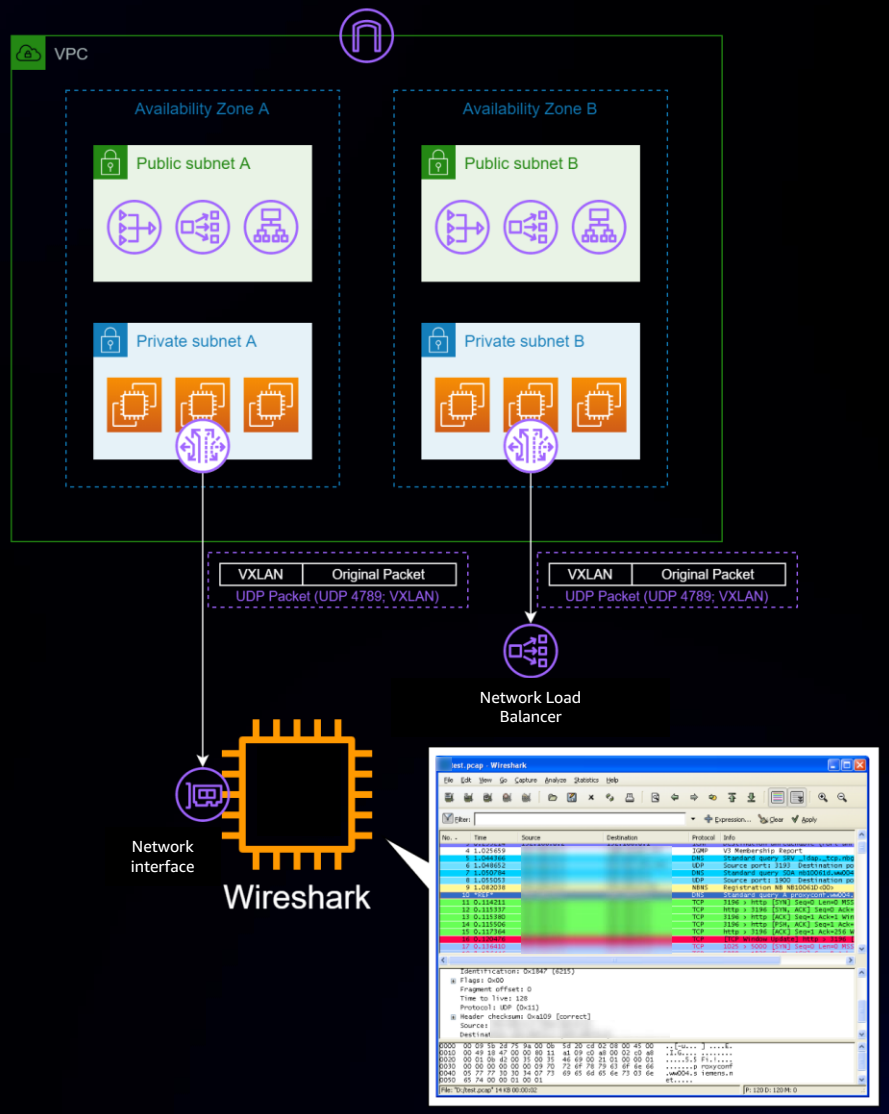
Traffic mirroring



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Troubleshooting with Wireshark

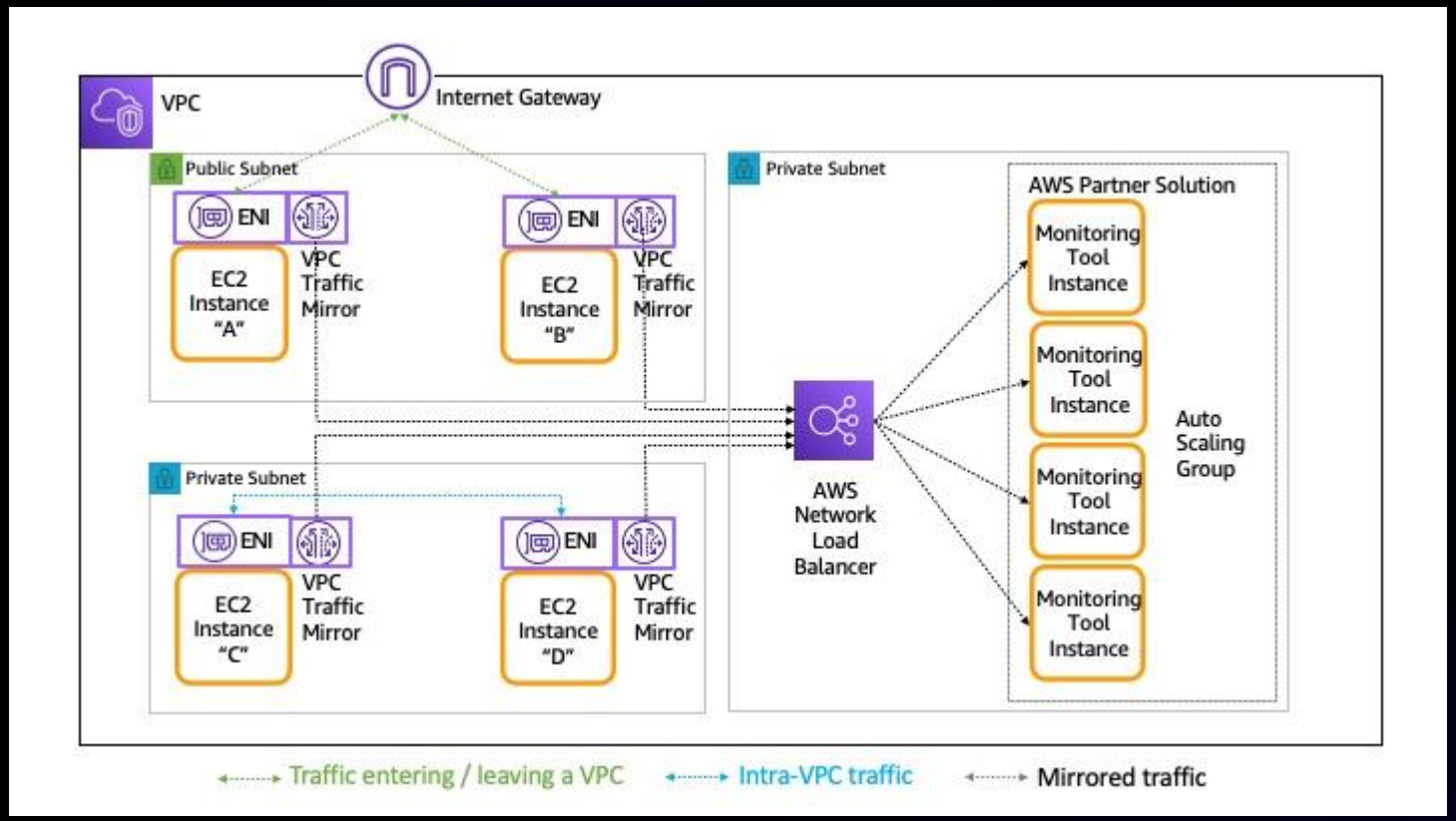
Traffic mirroring



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: Partner Solutions

- AWS Blog: Using VPC Traffic Mirroring to monitor and secure your AWS infrastructure

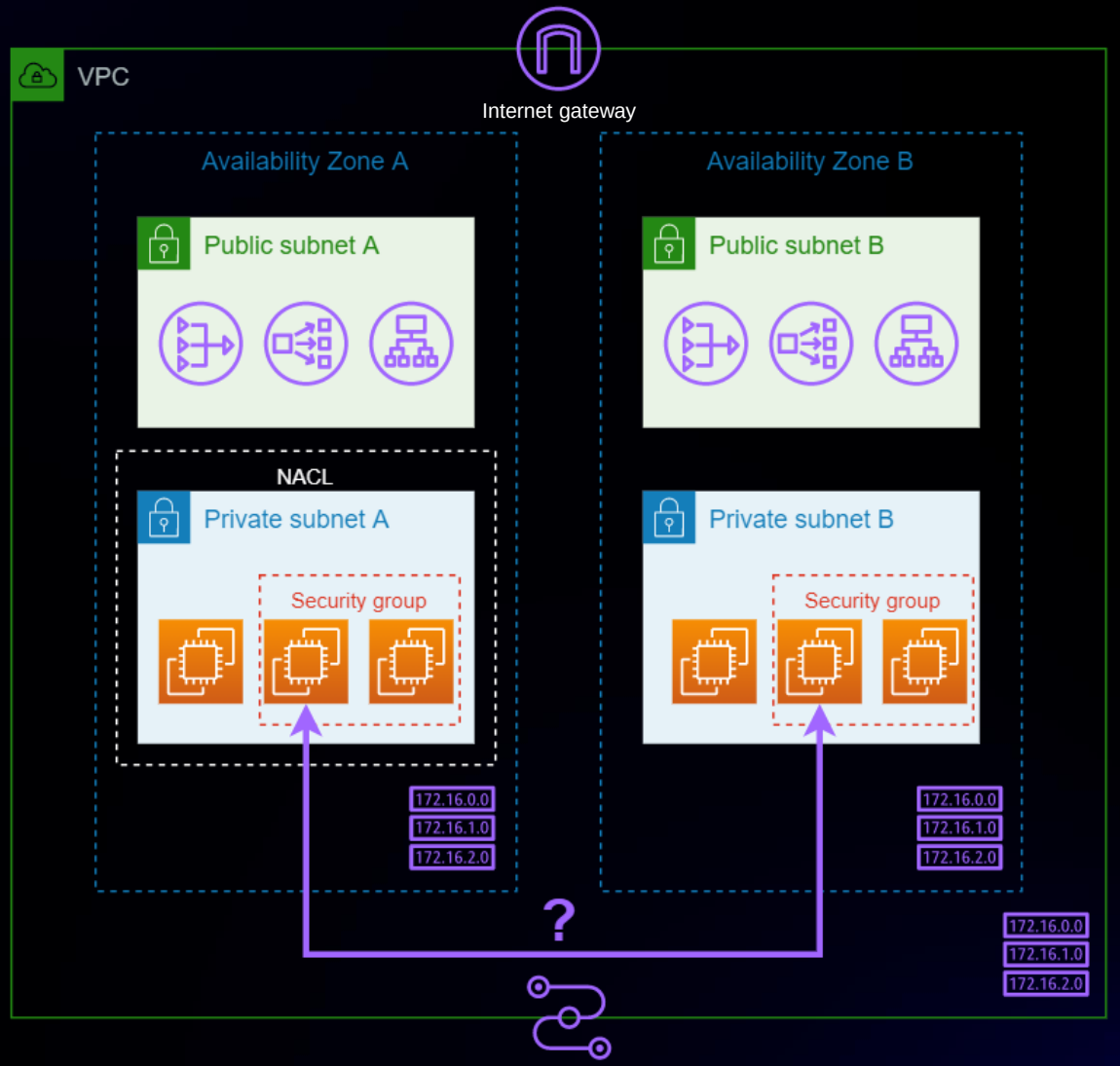




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Reachability Analyzer

Reachability Analyzer

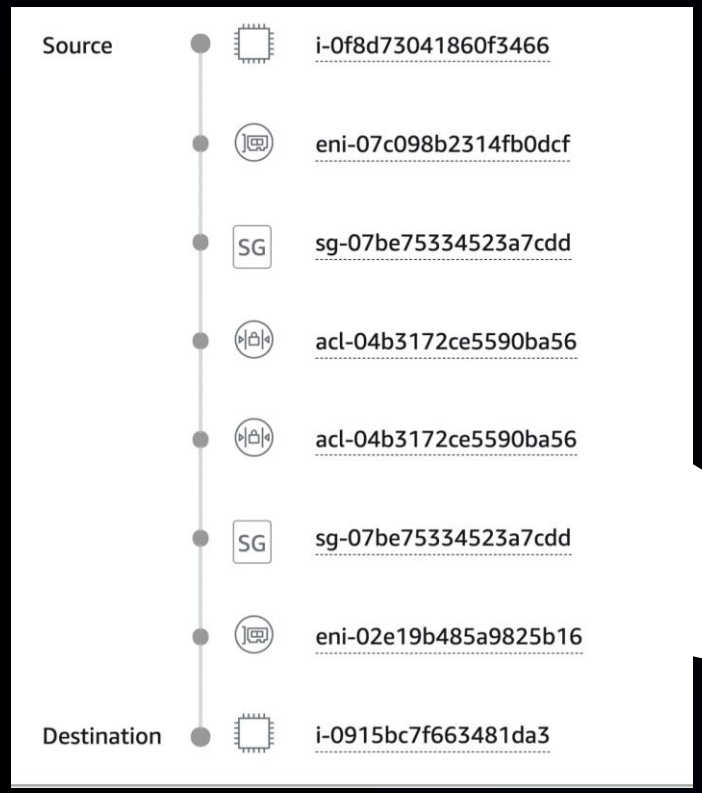


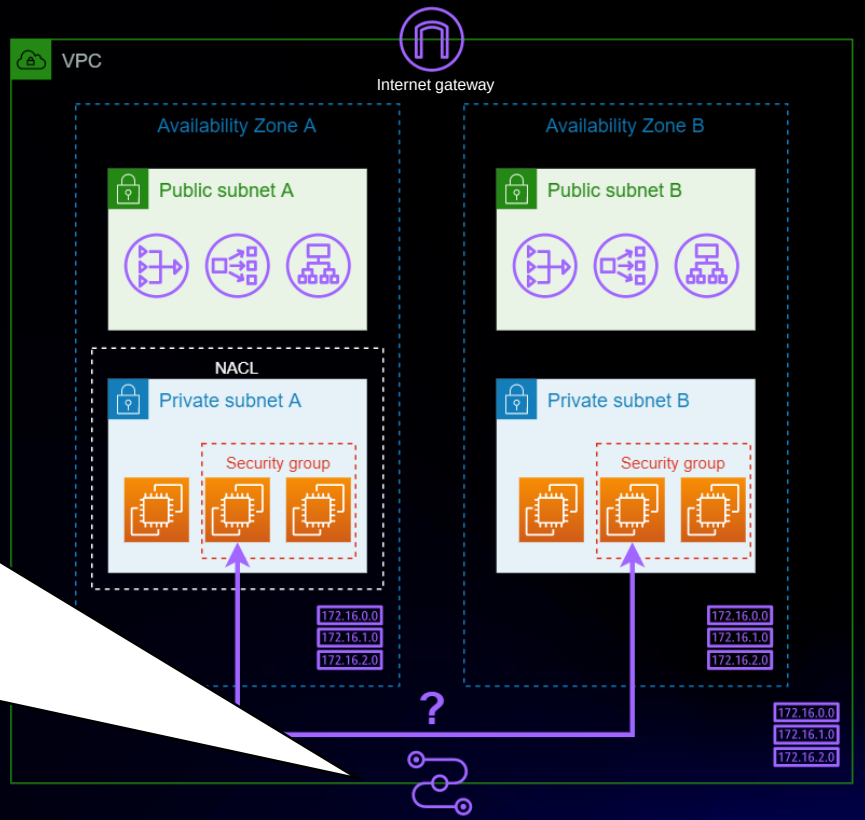
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC Reachability Analyzer

Reachability Analyzer

- Network diagnostics tool that troubleshoots reachability between two endpoints in a VPC, or within multiple VPCs



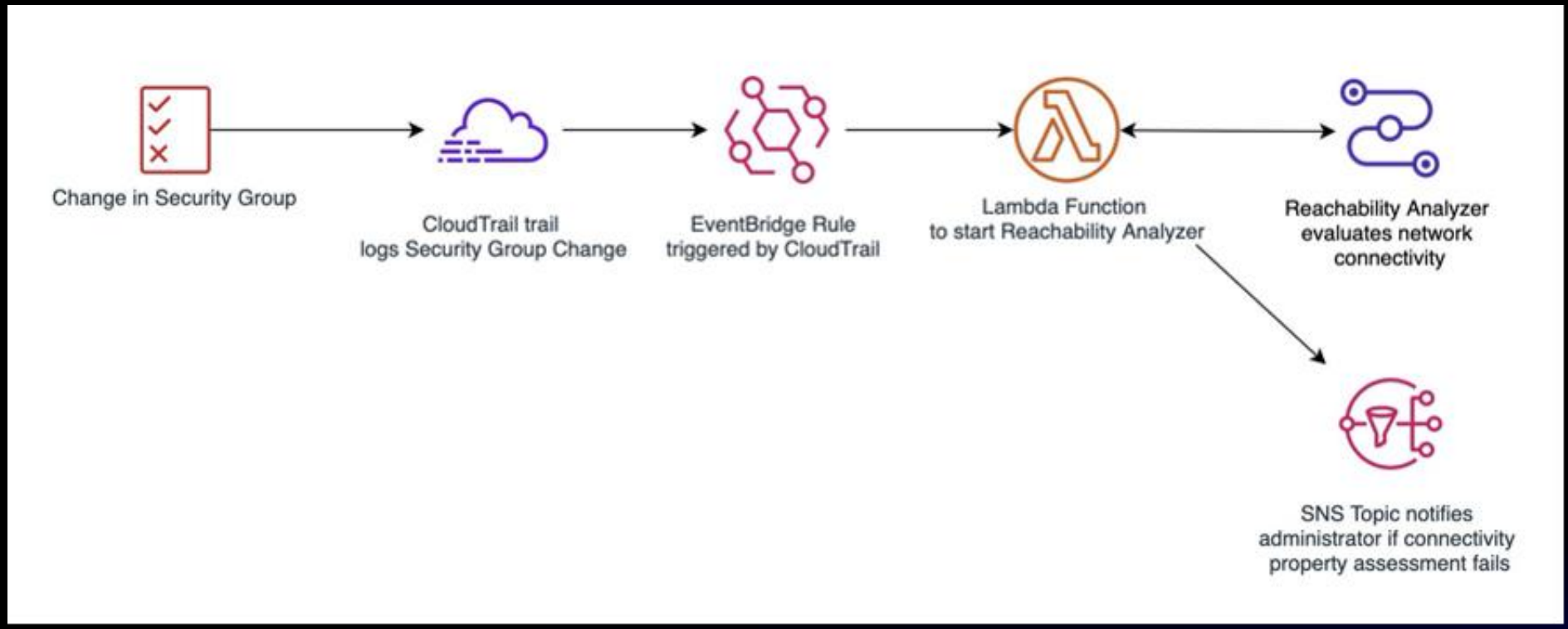


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example: Deployment pipeline

Reachability Analyzer

- AWS Blog: Automating connectivity assessments with VPC Reachability Analyzer



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Questions?

- Amazon VPC


Single VPC


Flow logs

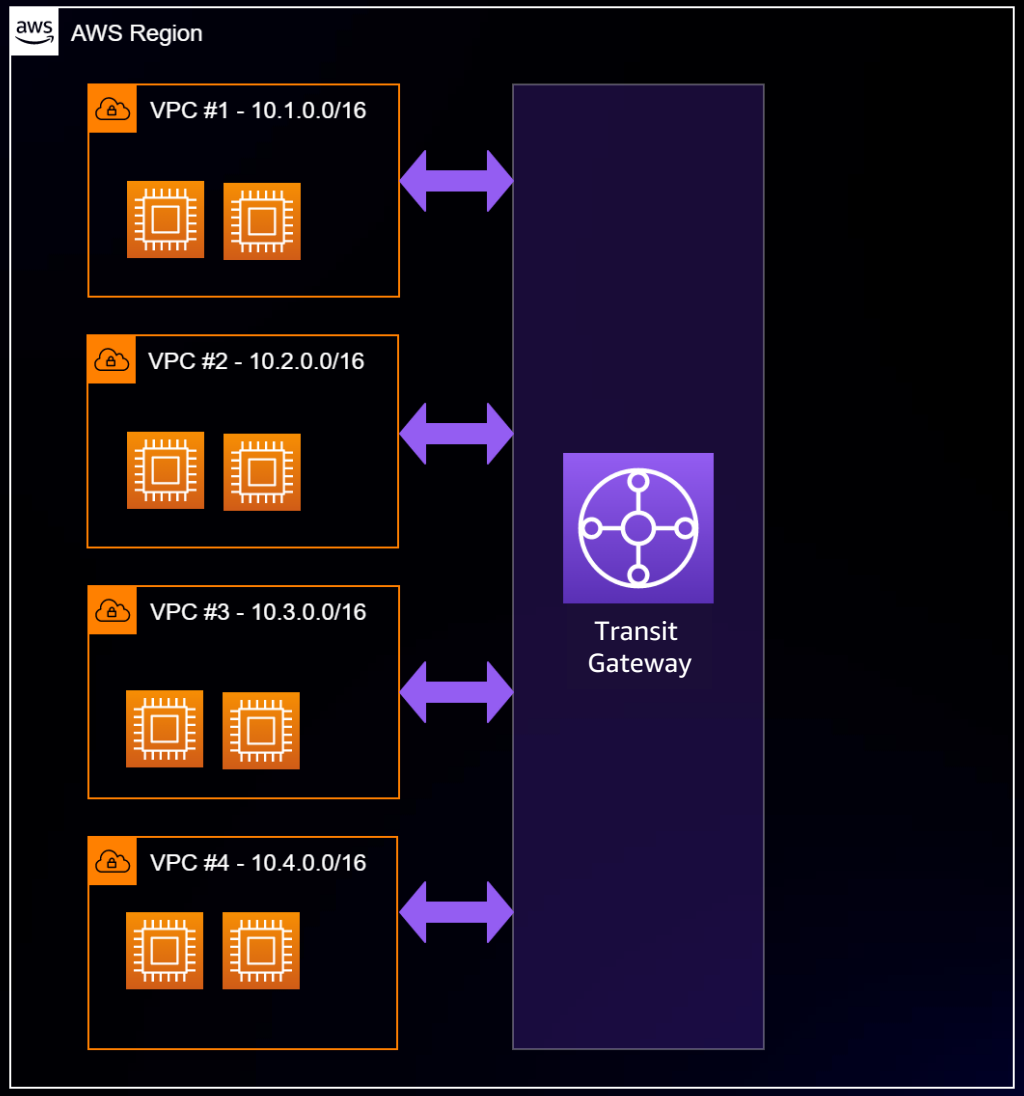

Traffic mirroring


Reachability Analyzer



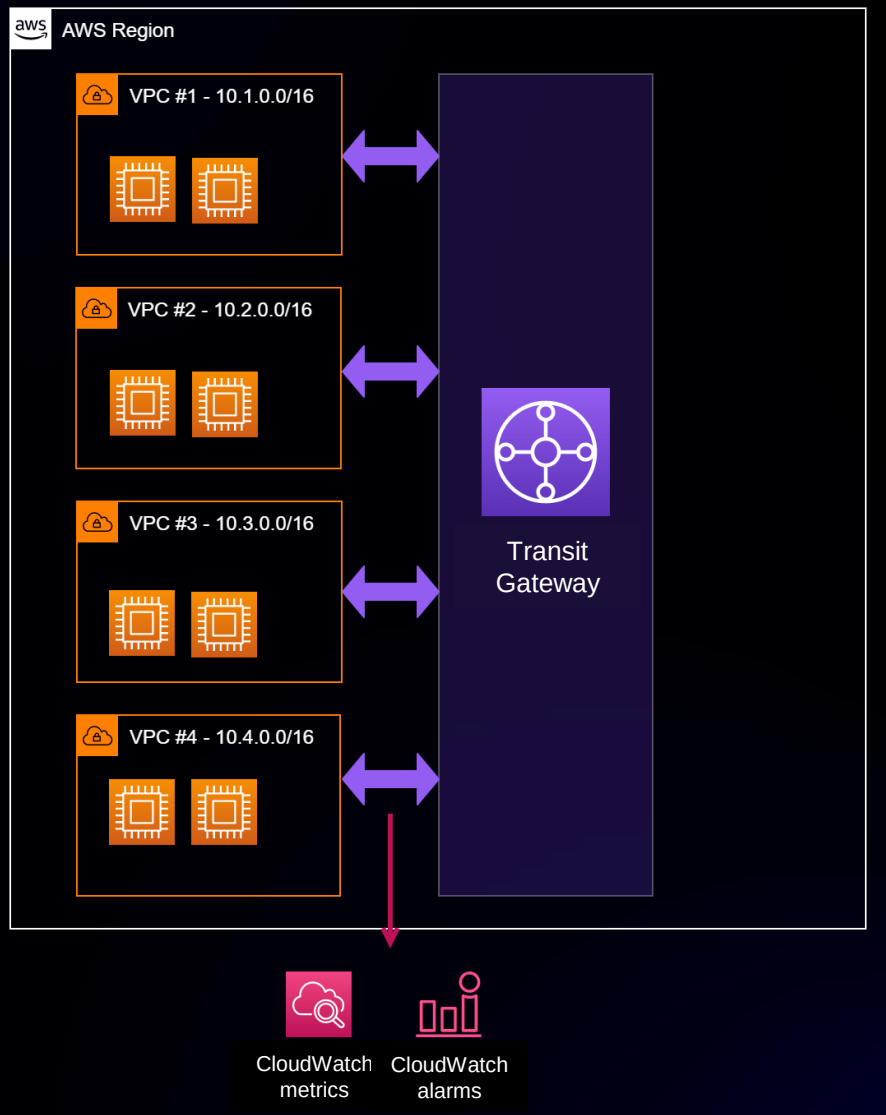
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-VPC



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway: CloudWatch metrics



Transit Gateway

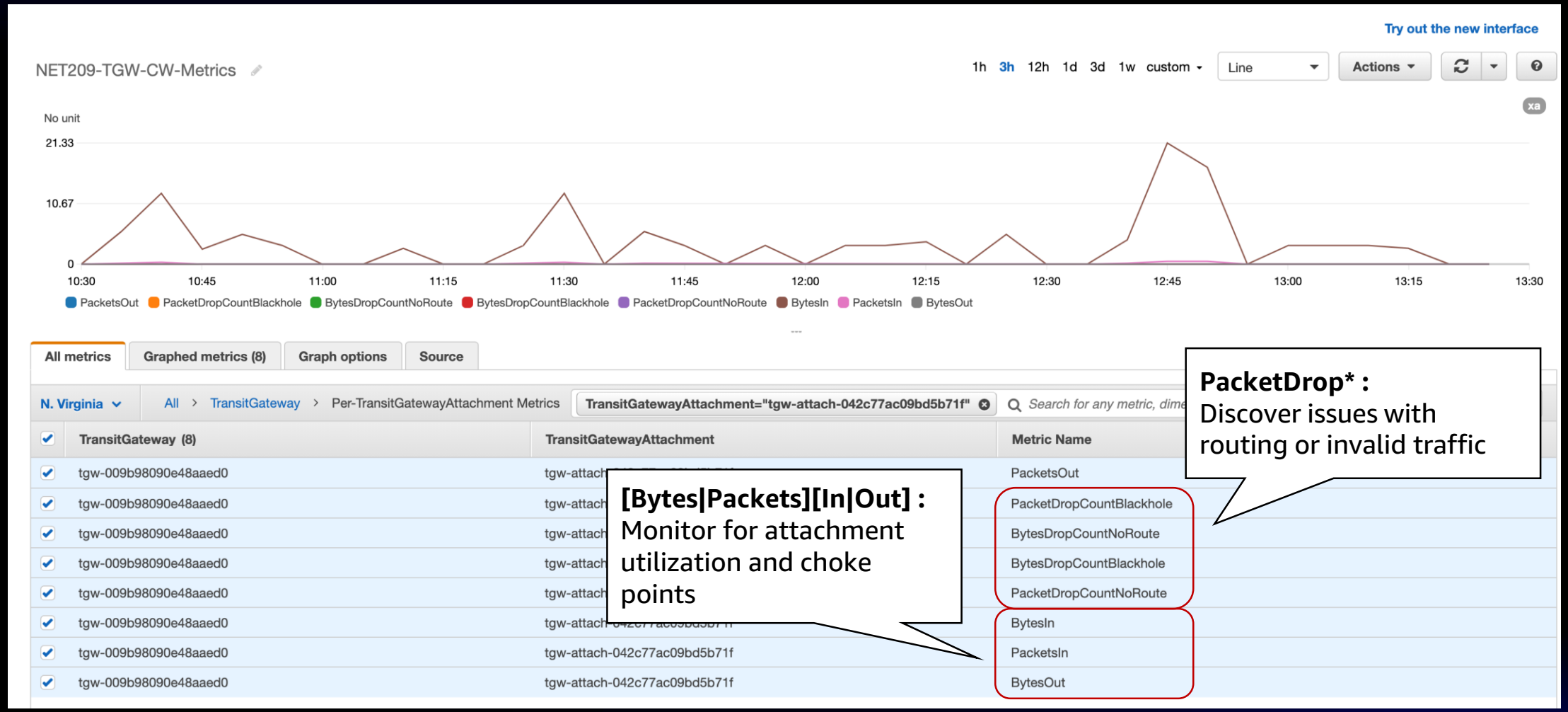
CloudWatch metrics

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway CloudWatch Metrics

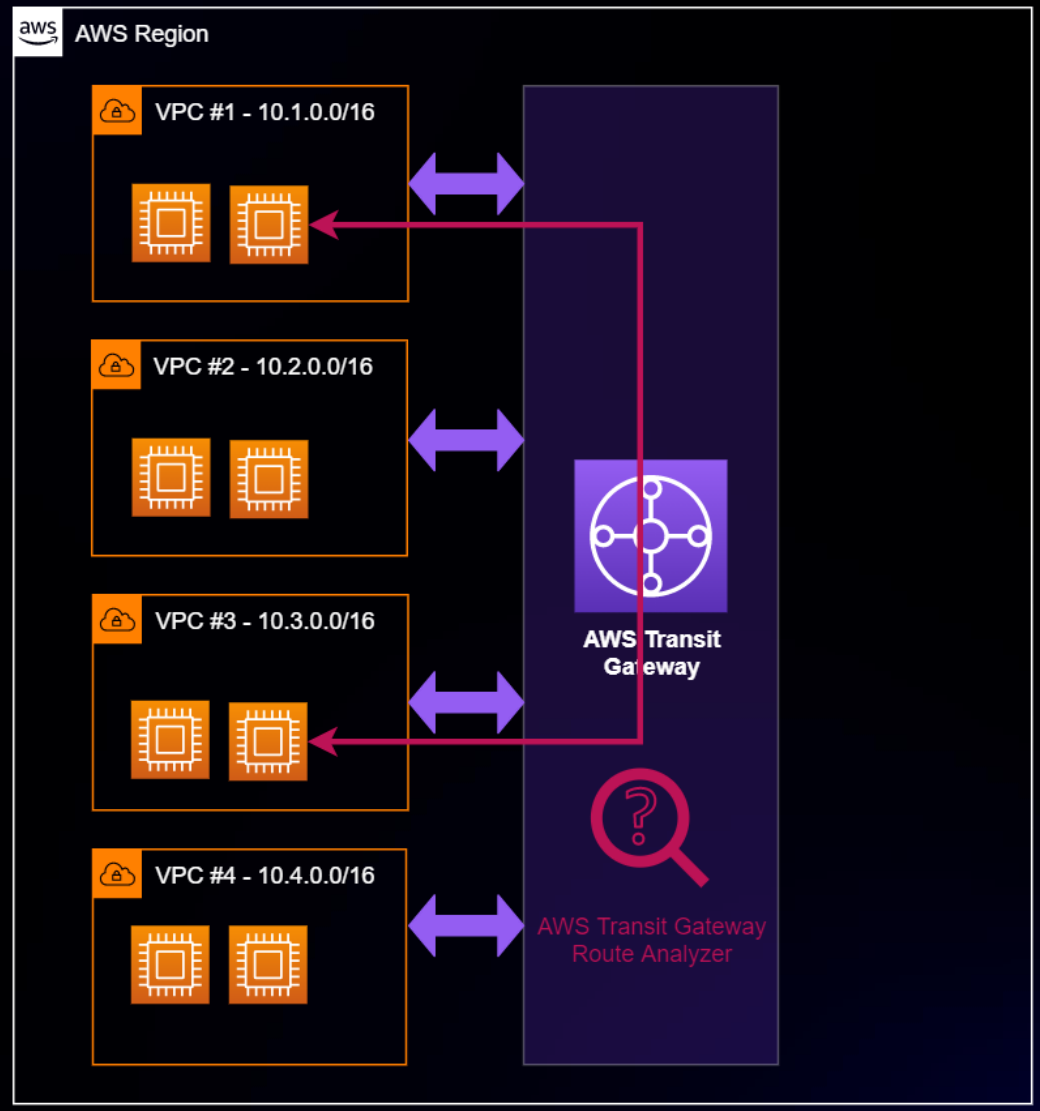
Transit Gateway

CloudWatch metrics



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway Route Analyzer



Transit Gateway Route Analyzer

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transit Gateway Route Analyzer

Transit Gateway Route Analyzer

Results of route analysis

The result of source and destination route is displayed here. You can update either the source and/or destination and re-run the analysis for updated results.

Forward path

Source	Destination	Status
tgw-attach-0a51f6605300339b7	tgw-attach-03567f73fbc68c402	Connected

Return path

Source	Destination	Status
tgw-attach-03567f73fbc68c402	tgw-attach-0a51f6605300339b7	Connected

Source
[redacted]
palo-on-prem-vpn (tgw-attach-0a51f6605300339b7)
VPN us-east-2

tgw-rtb-078951e783d453a8b
Transit Gateway route table us-east-2 tgw-08b4d2b50b457e6fc

Destination
[redacted]
acct4-8-0 (tgw-attach-03567f73fbc68c402)
VPC us-east-2

tgw-rtb-04933e869da9c2715
Transit Gateway route table us-east-2 tgw-08b4d2b50b457e6fc

Source
[redacted]
ECMP group
VPN us-east-2

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Questions?

- Multi-VPC


Transit Gateway

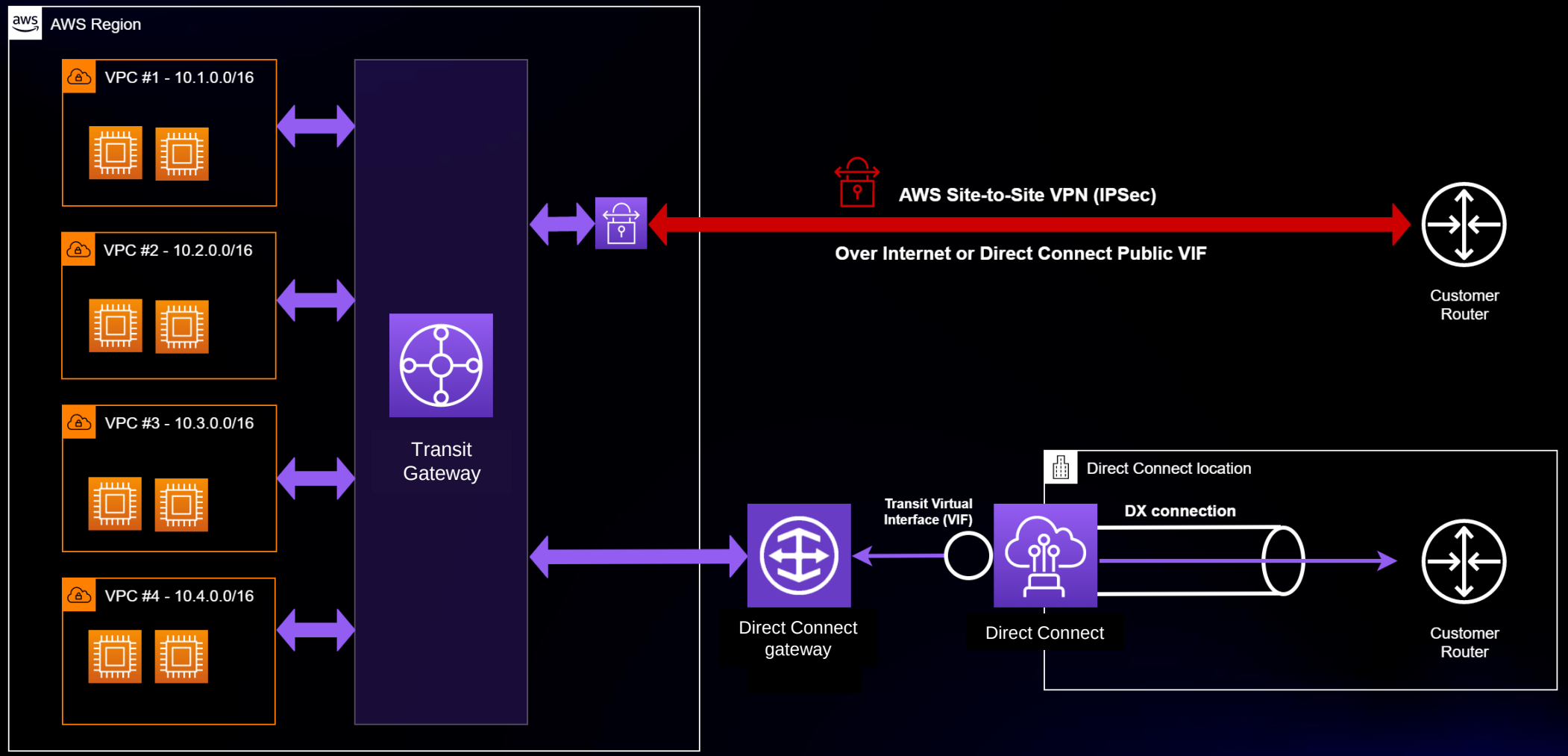

Transit Gateway Route Analyzer


CloudWatch metrics



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

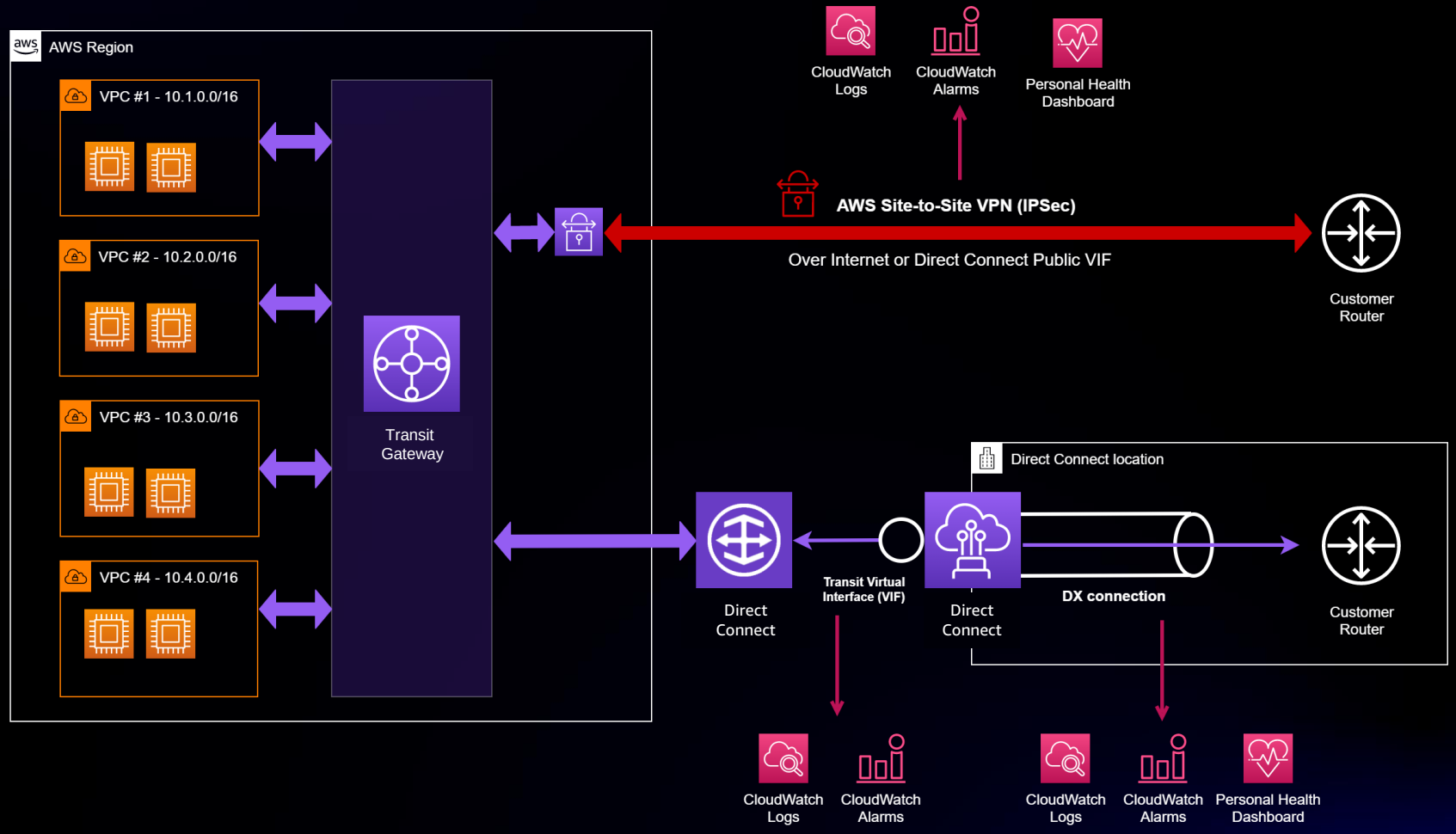
Hybrid Connectivity



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

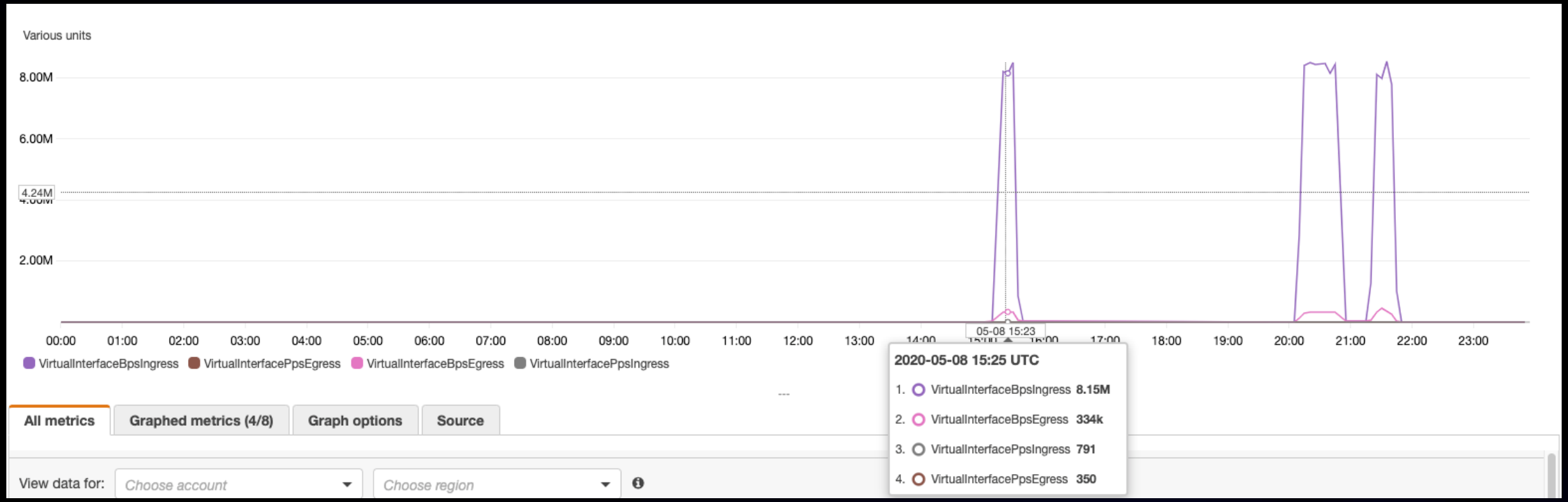
Direct Connect & VPN CloudWatch Metrics

Direct Connect | Site-to-Site VPN | CloudWatch metrics | Personal Health Dashboard



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect CloudWatch metrics

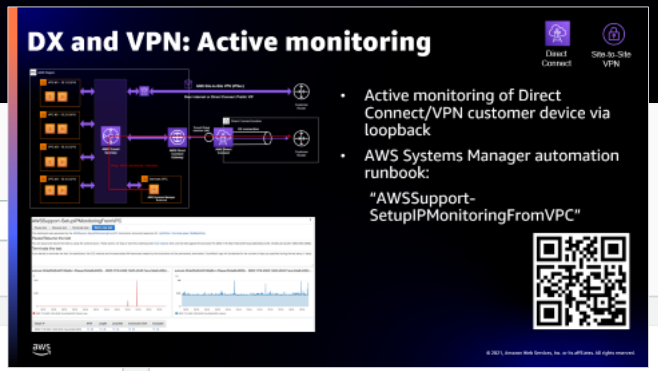


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPN CloudWatch metrics





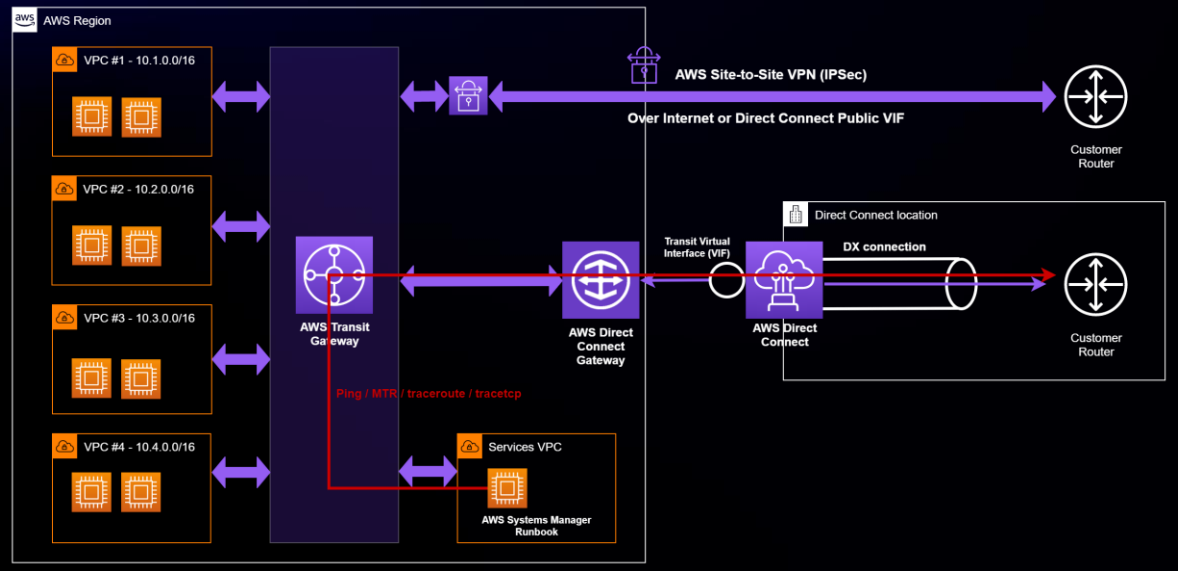


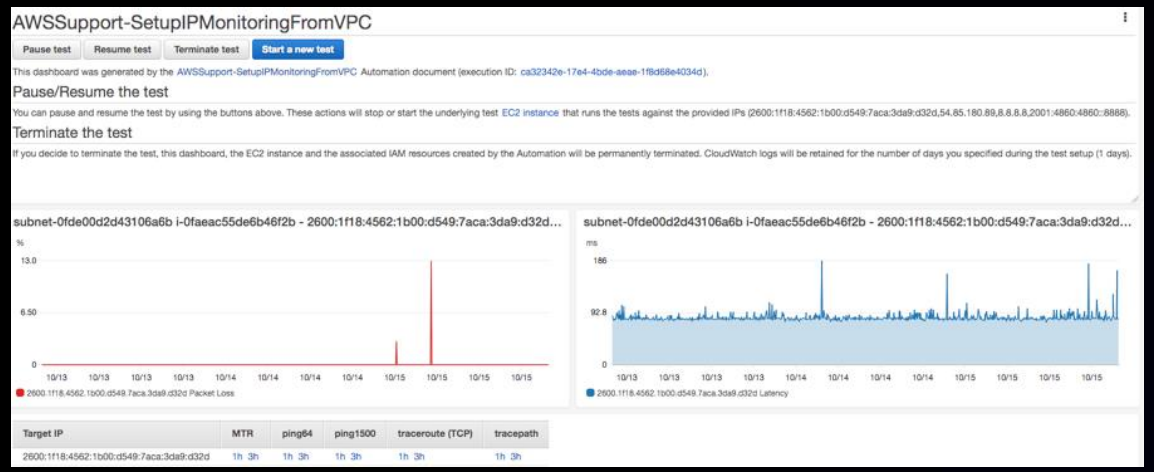
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DX and VPN: Active monitoring

Direct Connect

Site-to-Site VPN





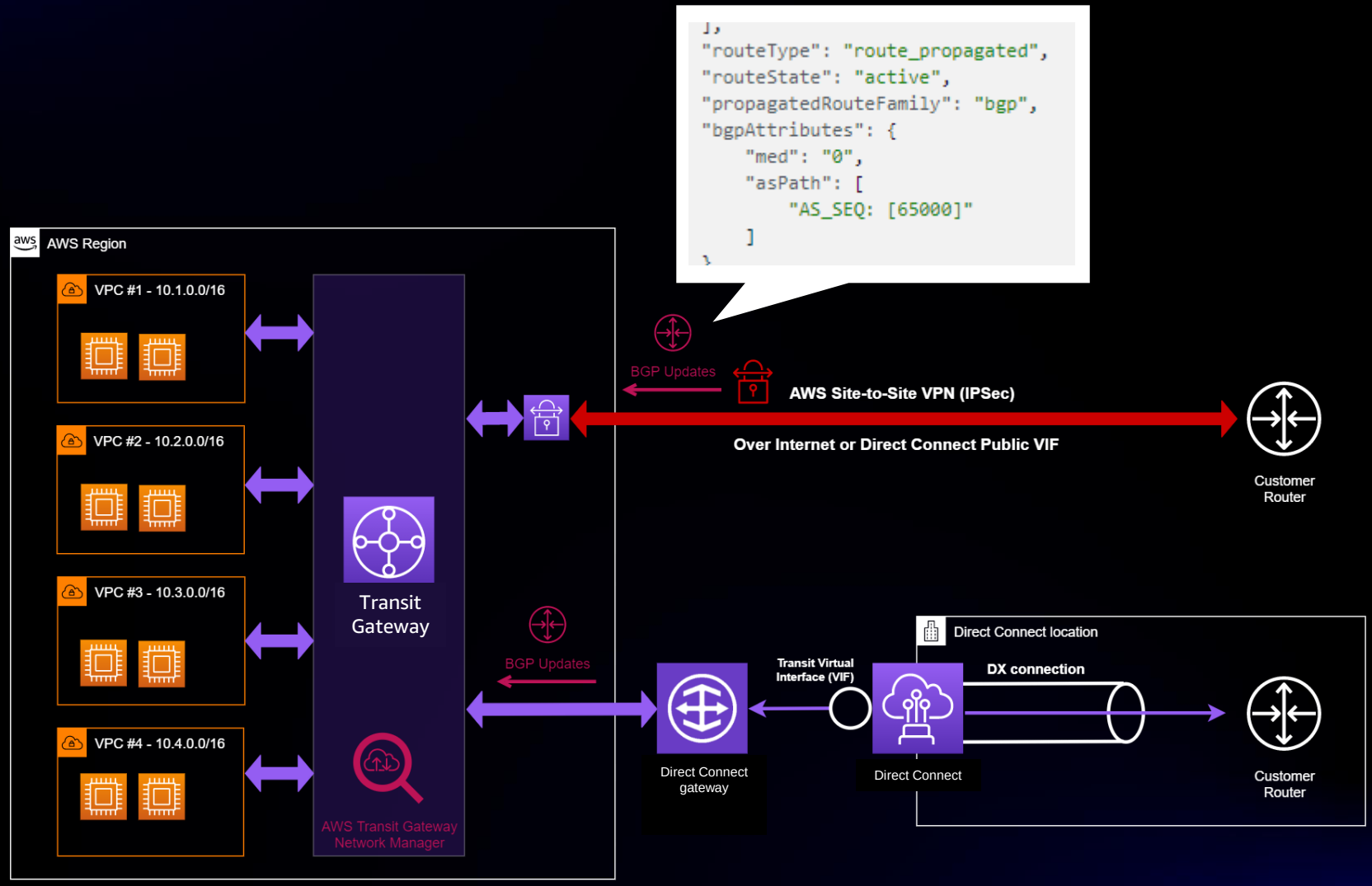
- Active monitoring of Direct Connect/VPN customer device via loopback
- AWS Systems Manager automation runbook:

  “AWSSupport-SetupIPMonitoringFromVPC”

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

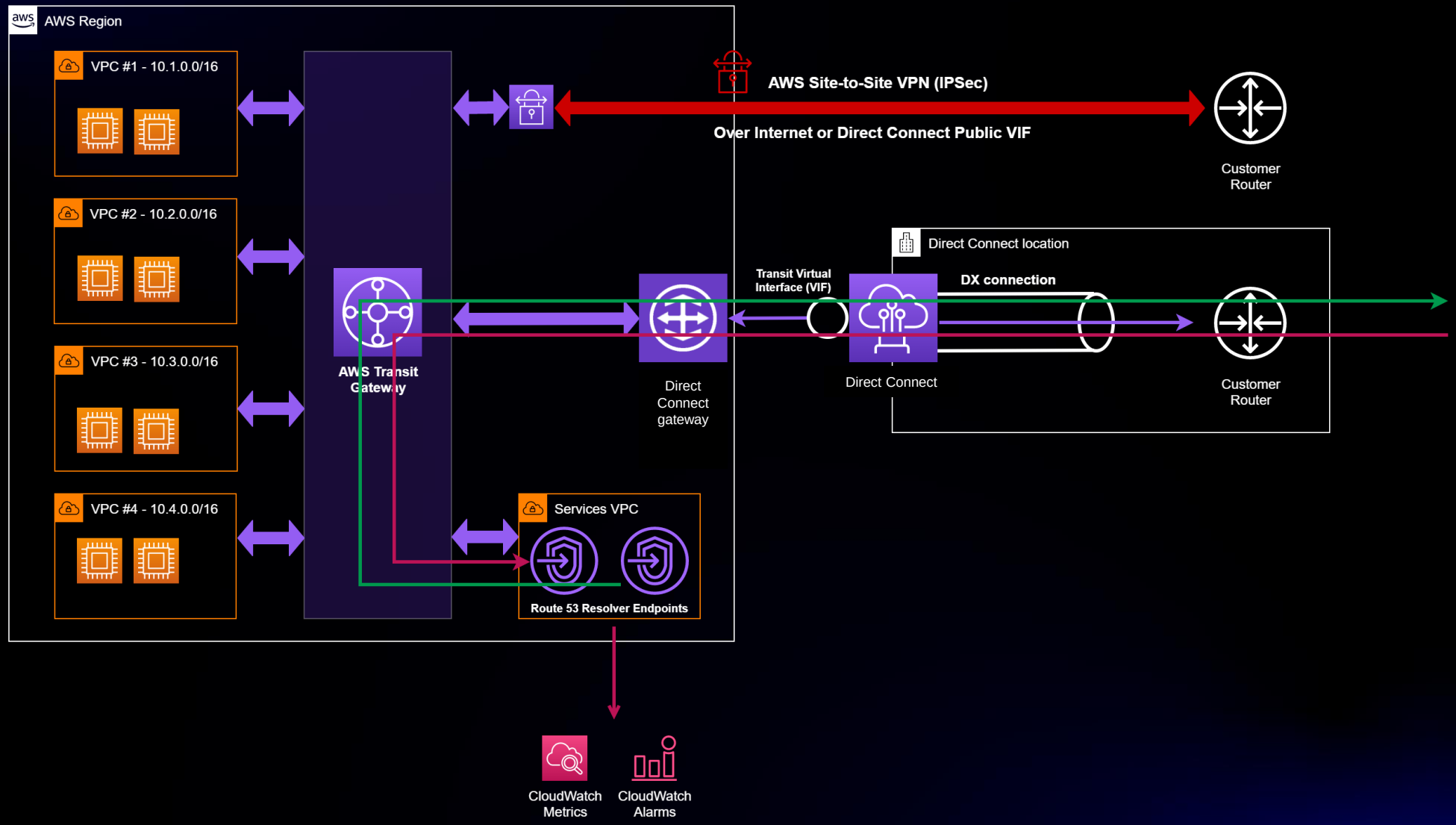
Transit Gateway Network Manager

Direct Connect | Site-to-Site VPN | CloudWatch Logs



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

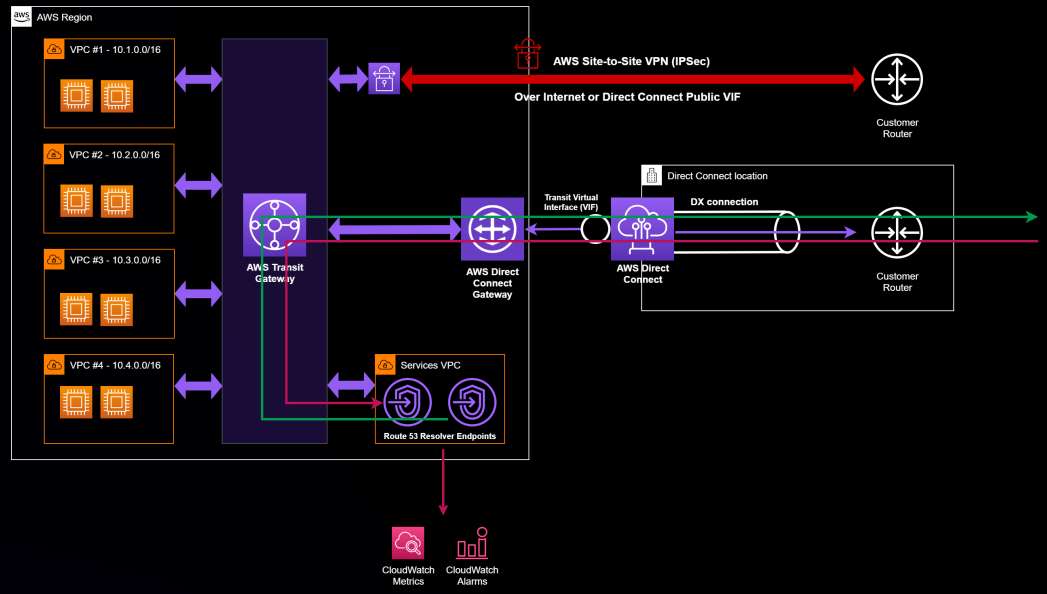
Amazon Route 53 Resolver endpoints



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Resolver endpoints

- Each endpoint network interface can process up to 10,000 DNS queries per second (QPS)
- Add more network interfaces to increase the endpoint capacity
- Use CloudWatch metrics to monitor current utilization
- Action item: Setup CloudWatch alarm on 50% utilization

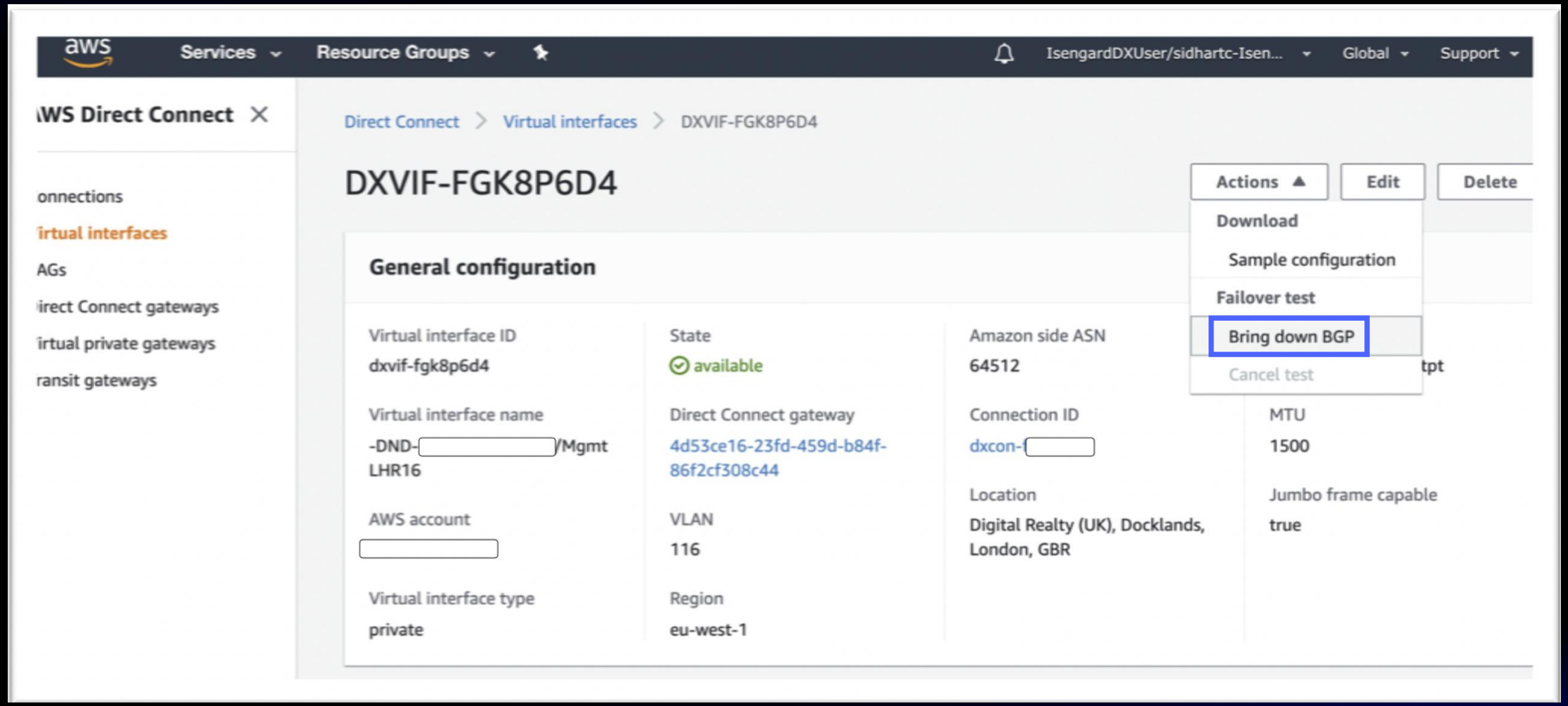


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Test and validation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Direct Connect Resiliency Toolkit



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Questions?

- Hybrid Connectivity


Direct Connect


Site-to-Site VPN


CloudWatch metrics


Personal Health Dashboard



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Christian Elsen
elsenc@amazon.com

Rashpal Kler
kler@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.