CLOUD NETWORK SEGMENTATION IN PURSUIT OF ZERO TRUST

Atif Siddiqui

Source: https://www.cyberrescue.co.uk/library/cartoons#&gid=1&pid=1

AGENDA

- Emergence of Zero Trust
- Network Segmentation Concepts and Transit Gateway
- Cloud Network Segmentation Design

ZERO TRUST HISTORY

- Zero Trust term introduced in 1994
- Zero Trust Model coined in 2010 in Forrester Research paper
  - Build Security Into Your Network's DNA: The Zero Trust Network Architecture
- NIST publication served as the endorsement

ZERO TRUST PRINCIPLES

'Never Trust, Always Verify' instead of 'Trust but Verify'

- Verify explicitly
- Use least privilege access
- Minimize blast radius and segment access

Source: Powell/ Amoroso

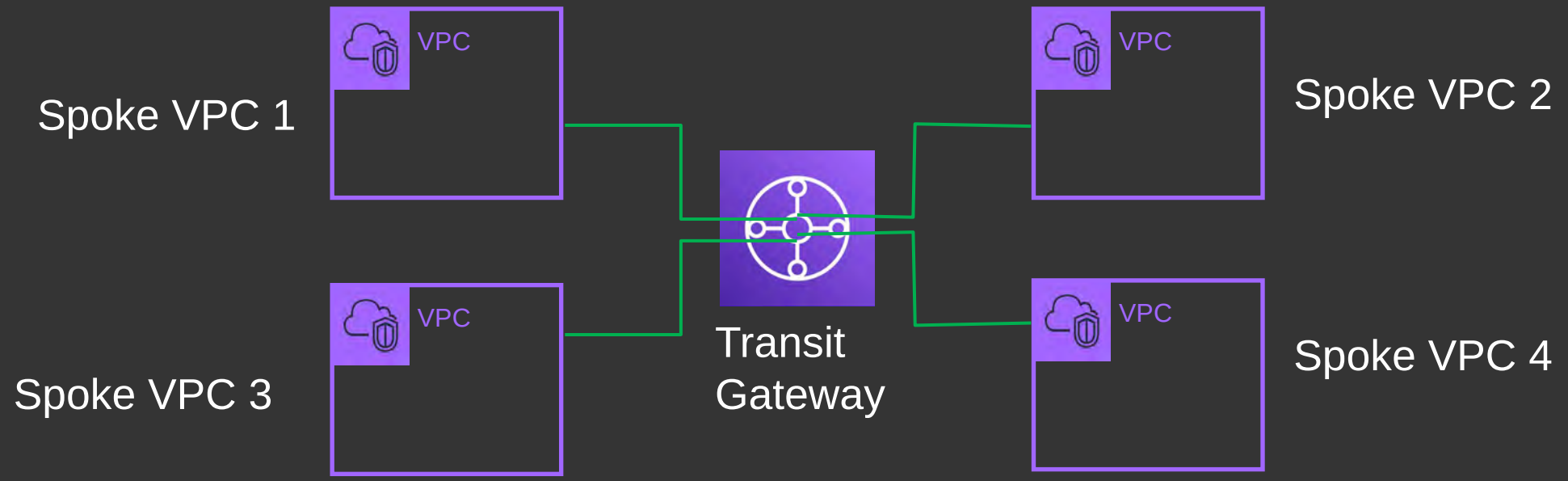
NETWORK SEGMENTATION

- Architectural approach to split network into multiple smaller segments
  - Stronger network security by reducing attack plane
  - Prevent lateral movement
  - Reduce compliance scope

TRANSIT GATEWAY (TGW)

- Announced in November 2018
- Layer 3 Router provided as a managed service by AWS
- Tight integration with Hyperplane allows Transit Gateway to be highly scalable
- Hub and Spoke model

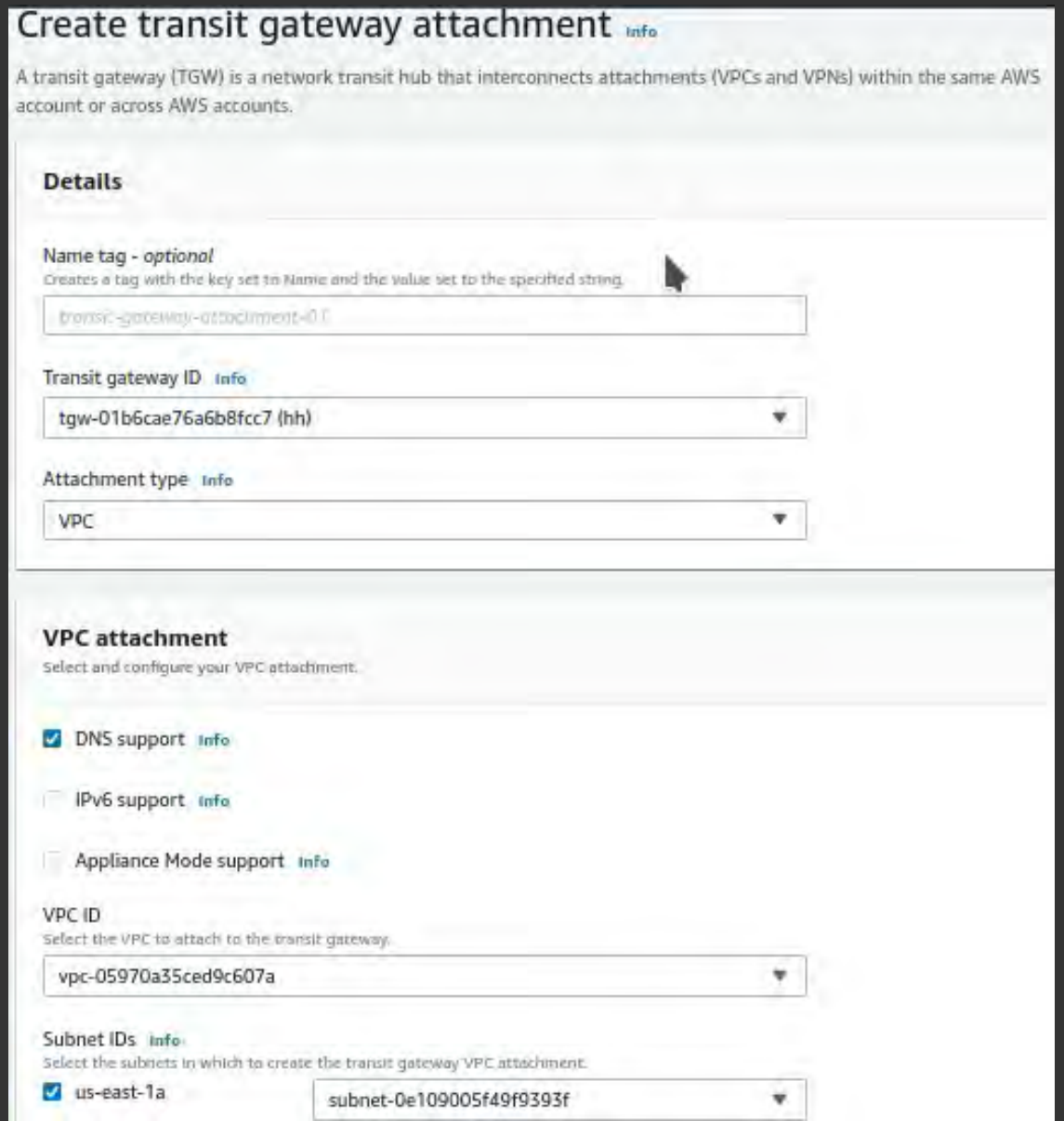
HUB AND SPOKE MODEL

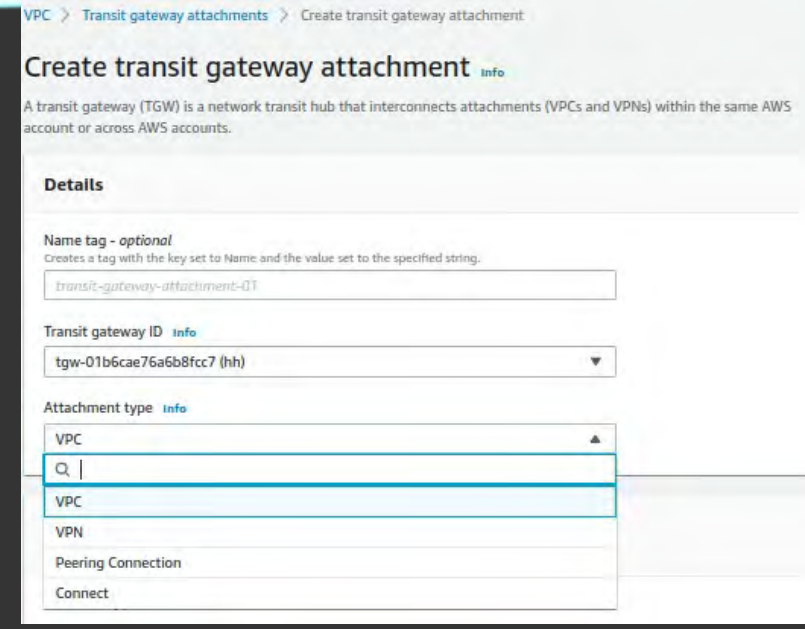


KEY CONCEPTS OF TRANSIT GATEWAY

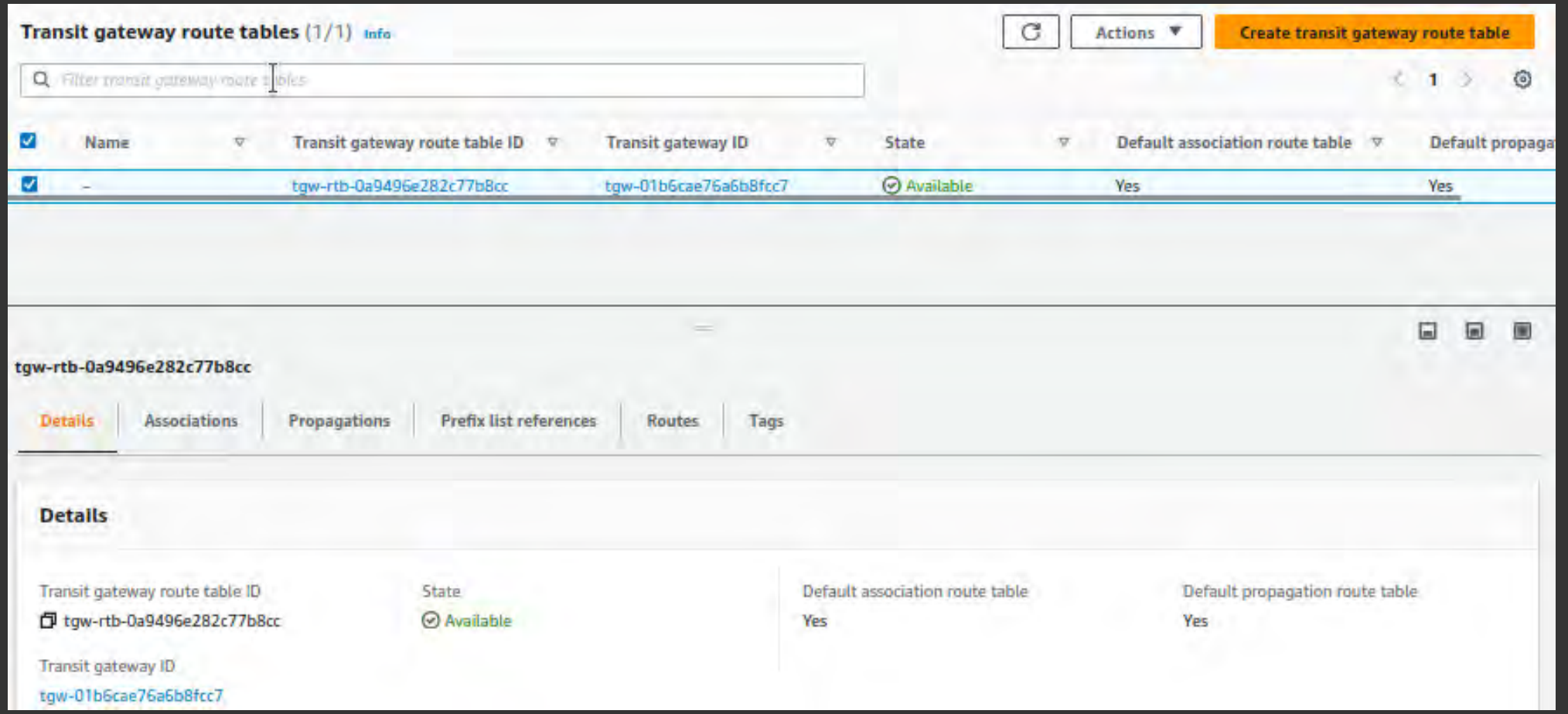
- Attachment
- Route Table
- Association
- Route propagation
- Route

TRANSIT GATEWAY ATTACHMENT

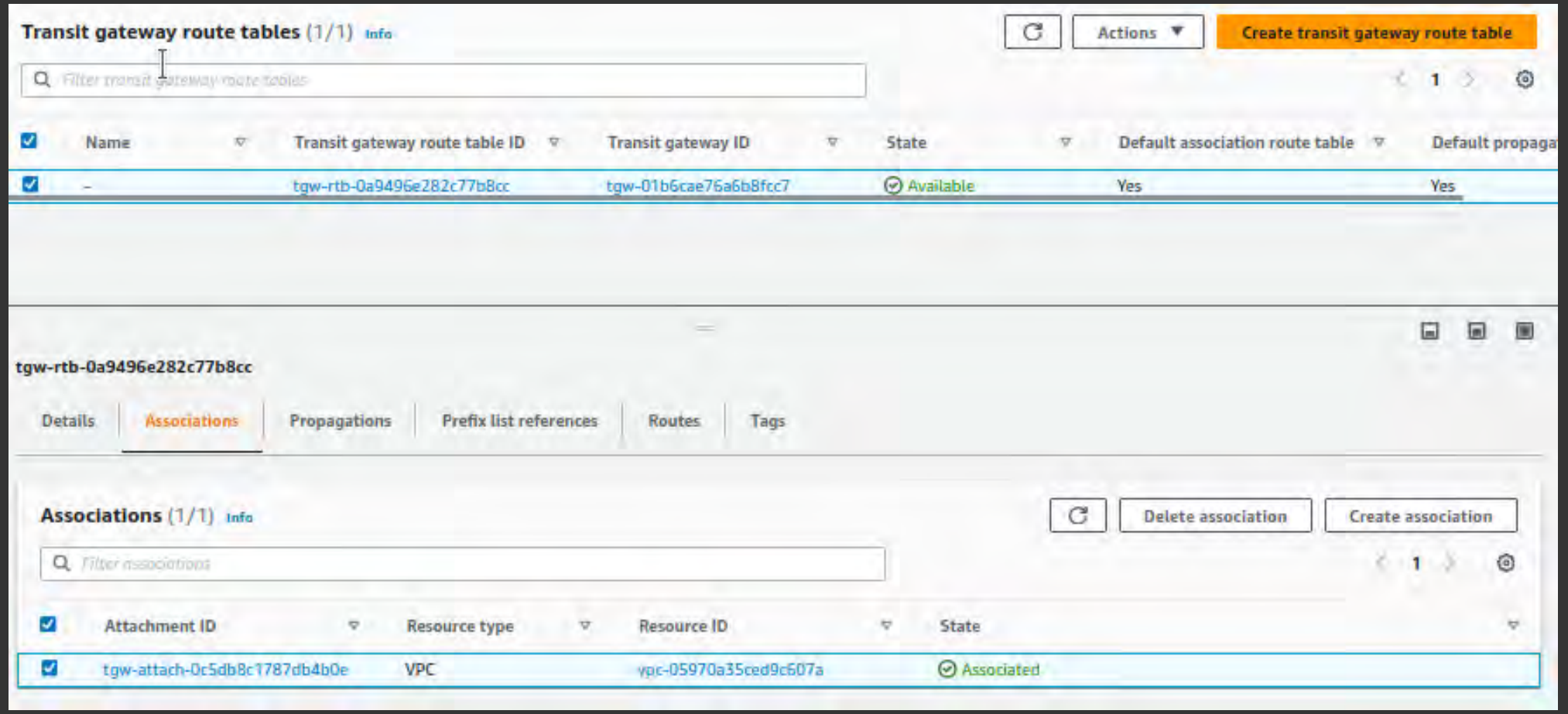




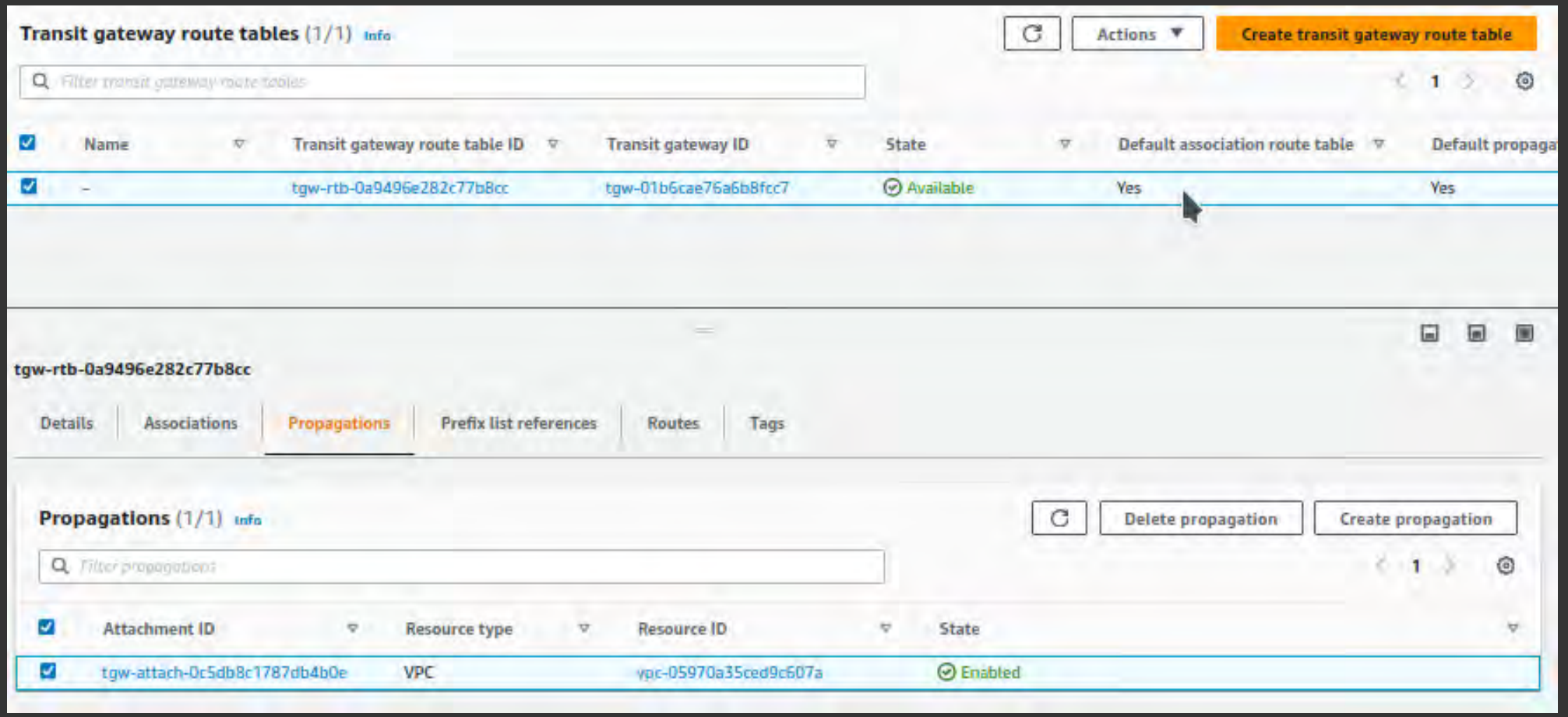
TRANSIT GATEWAY ROUTE TABLE



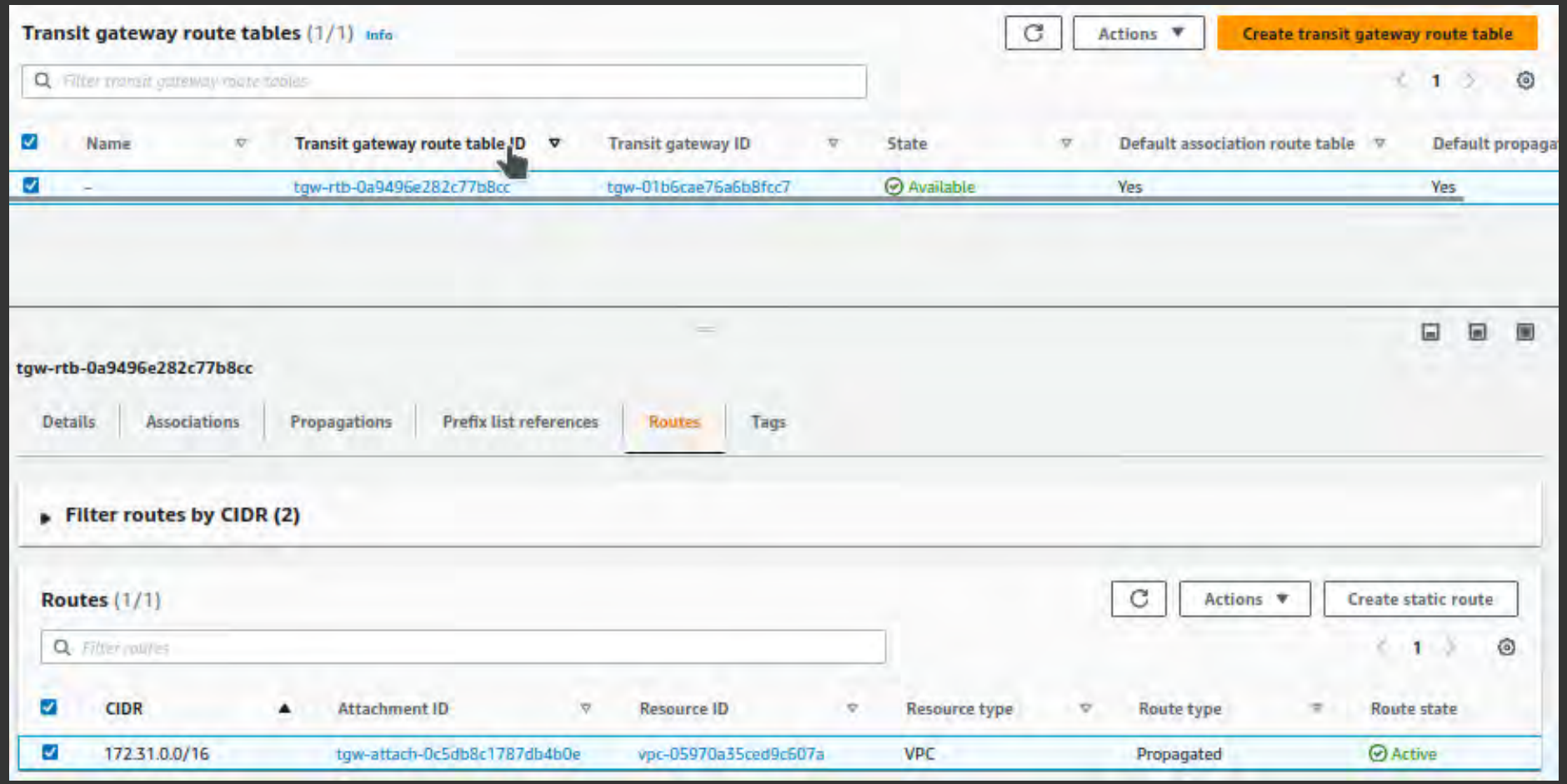
TRANSIT GATEWAY ASSOCIATION



TRANSIT GATEWAY PROPAGATION



TRANSIT GATEWAY ROUTE



NETWORK DESIGN

- Considerations
  - AWS Accounts' landscape
  - Environments: Dev, QA, UAT and Prod
  - Traffic patterns
  - Inspection model

DESIGN CONSIDERATION - ISOLATION OF ACCOUNTS

- With an application having four environments (dev, qa, uat and prod), each environment is in its own AWS account
- VPCs (virtual private cloud) are connected via AWS Transit Gateway

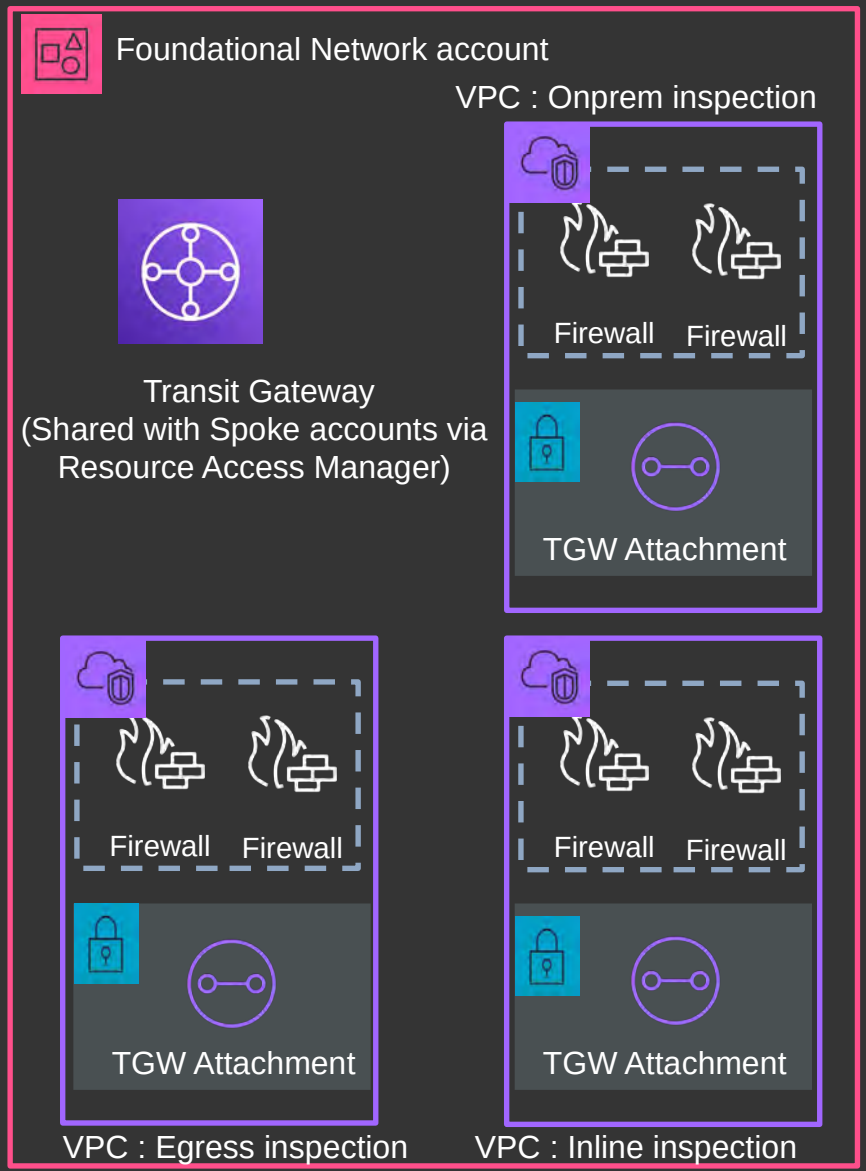
DESIGN CONSIDERATION – TGW ROUTE TABLES

- Routing is driven by Transit Gateway
- Two key Transit Gateway Route tables
  - Route table 1 named *Spoke*
  - Route table 2 named *Inspection*

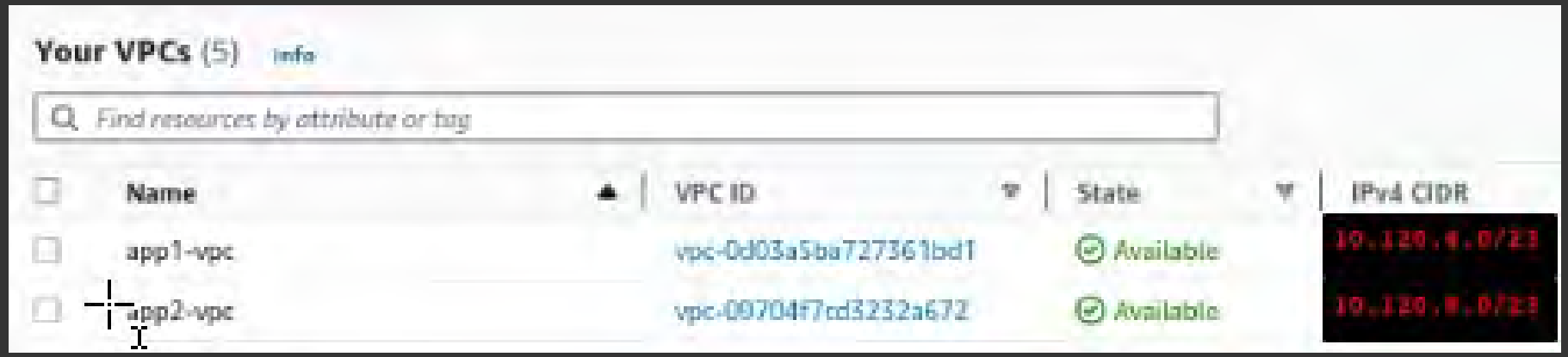
DESIGN CONSIDERATION - TRAFFIC INSPECTION PATTERNS

- Onprem
- Inline
- Egress

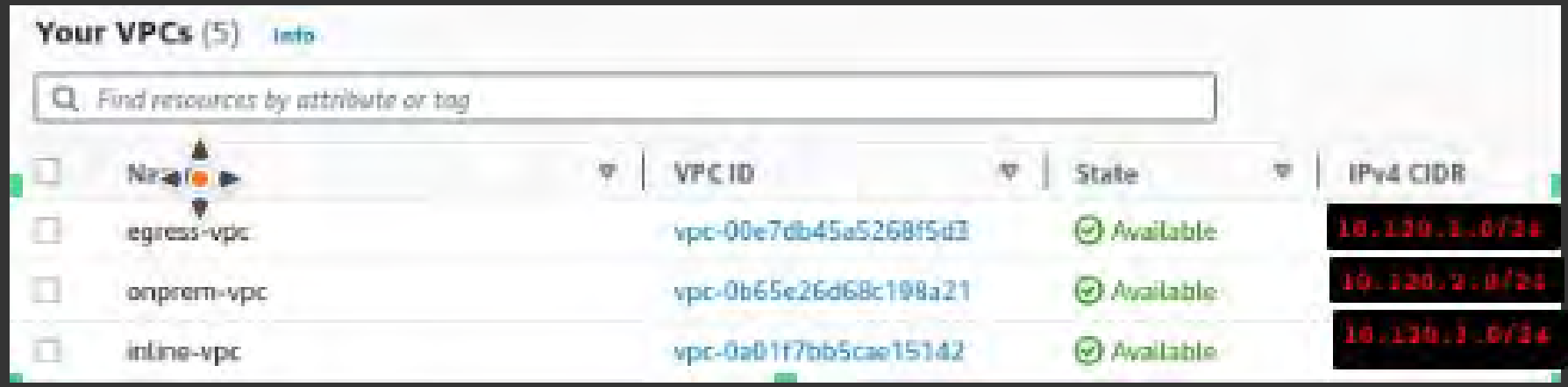
NOTE: Any traffic crossing VPC boundary must be inspected regardless of the destination



VPC DETAILS

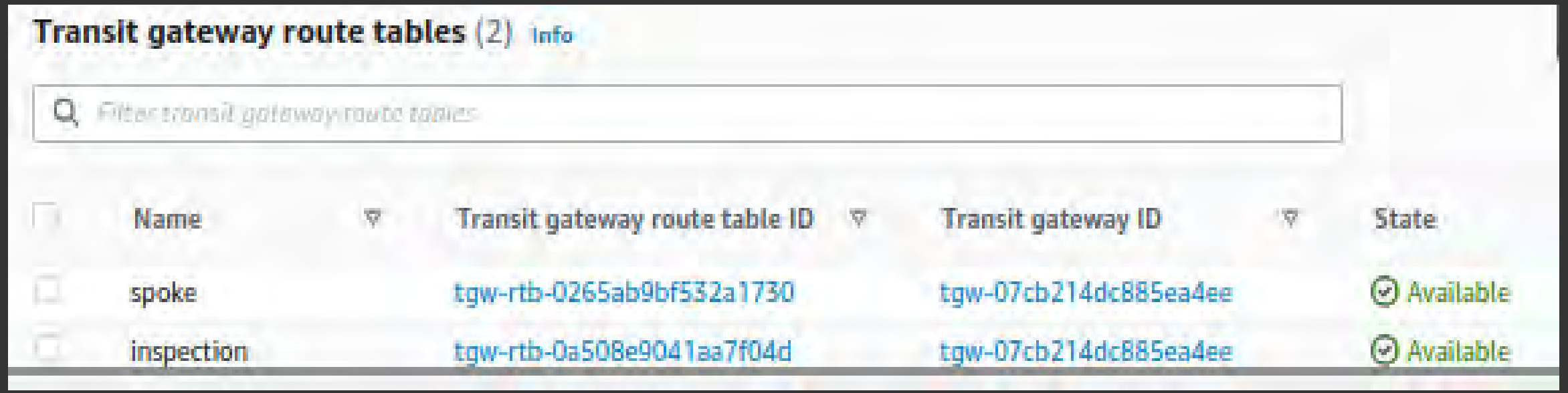


Spoke VPCs



Inspection VPCs

TRANSIT GATEWAY ROUTE TABLES

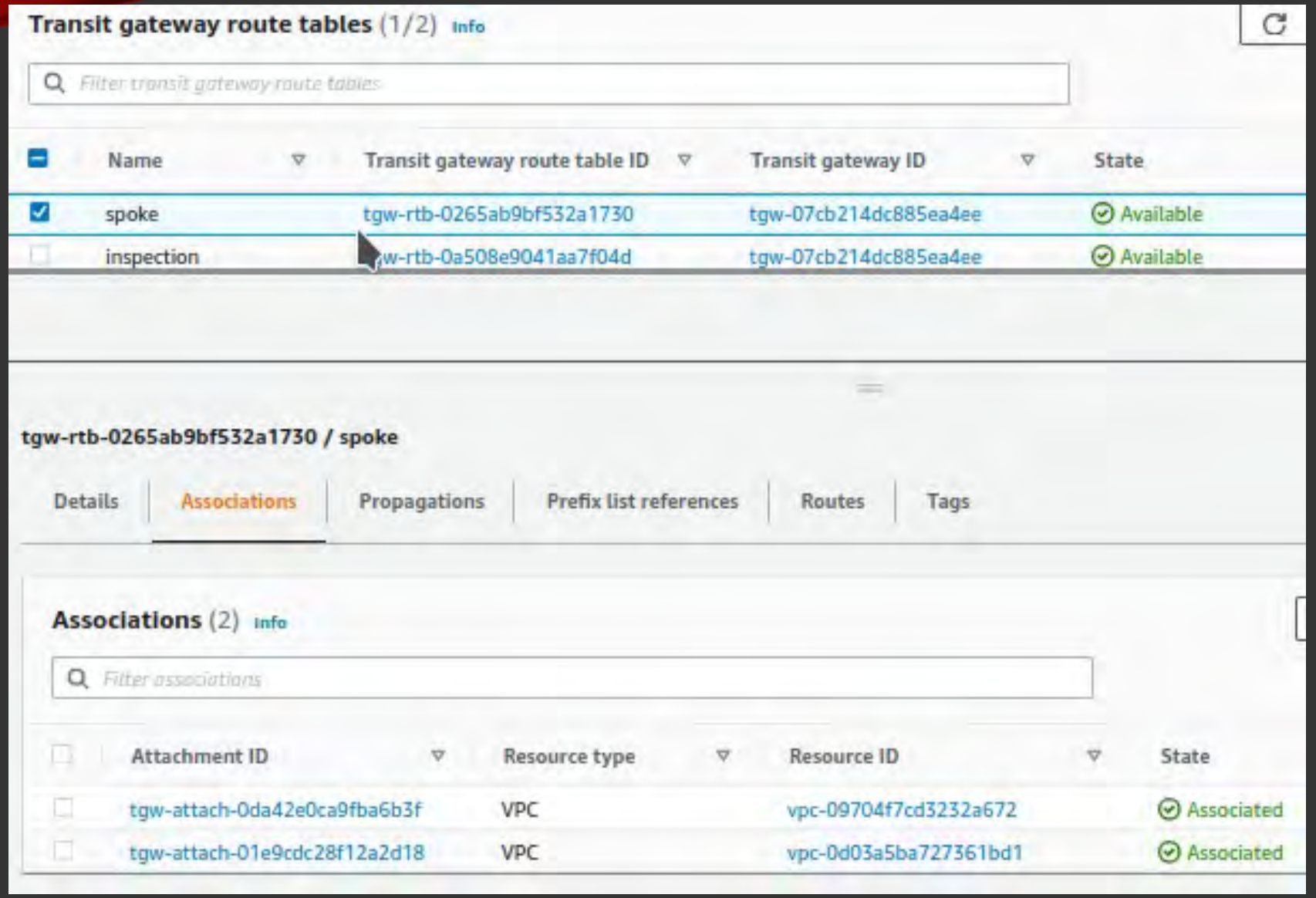


Transit gateway route tables (2) Info

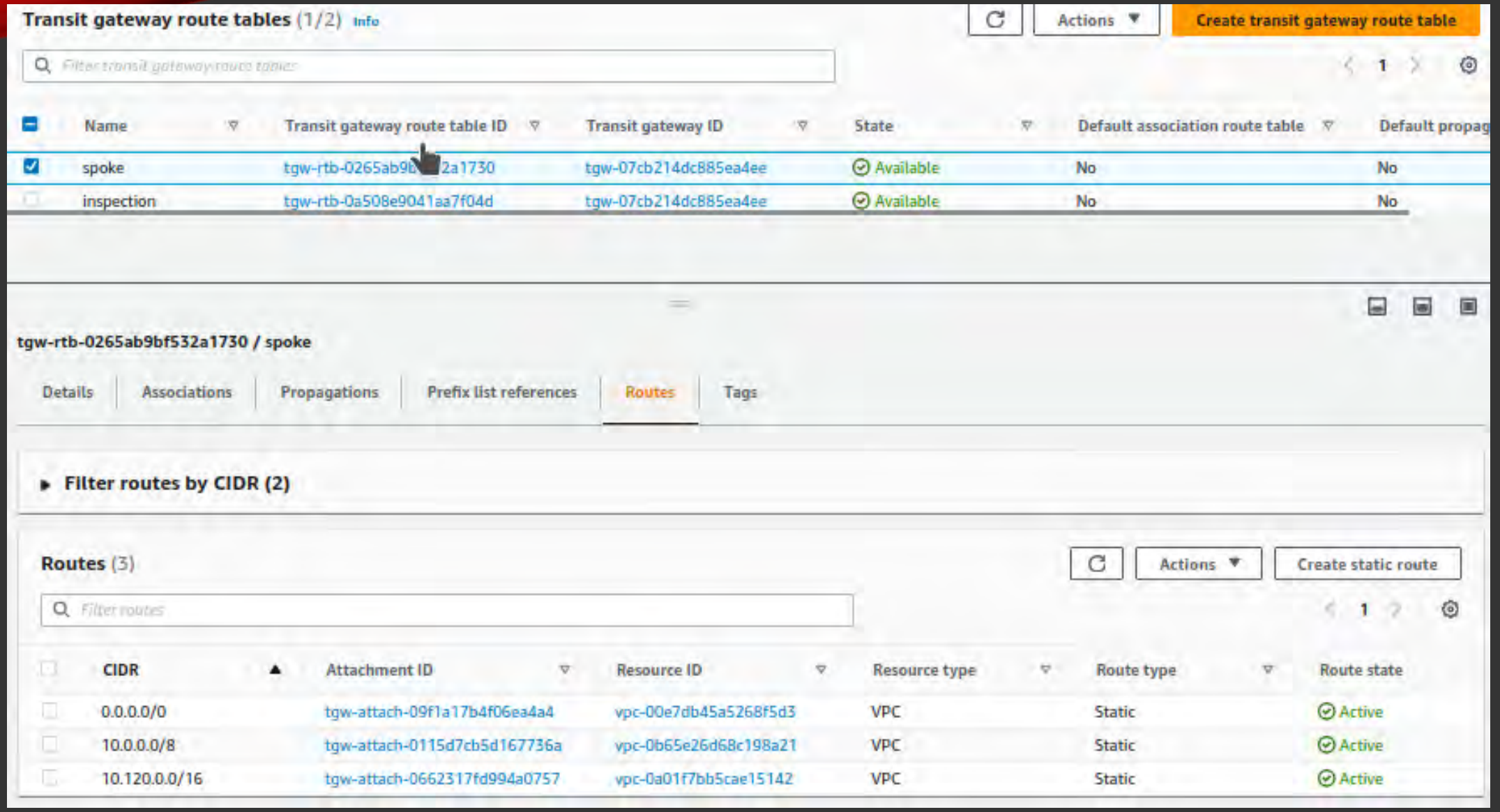
Filter transit gateway route tables

Name	Transit gateway route table ID	Transit gateway ID	State
spoke	tgw-rtb-0265ab9bf532a1730	tgw-07cb214dc885ea4ee	Available
inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available

TGW ASSOCIATIONS (SPOKE)



TGW ROUTES (SPOKE)



Transit gateway route tables (1/2) Info

Actions ▼ | Create transit gateway route table

Filter transit gateway route tables

1

Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table	Default propag
spoke	tgw-rtb-0265ab9b[illegible]2a1730	tgw-07cb214dc885ea4ee	Available	No	No
inspection	tgw-rtb-0a508e9041aa7f04d	tgw-07cb214dc885ea4ee	Available	No	No

tgw-rtb-0265ab9bf532a1730 / spoke

Details | Associations | Propagations | Prefix list references | Routes | Tags

▶ **Filter routes by CIDR (2)**

Routes (3)

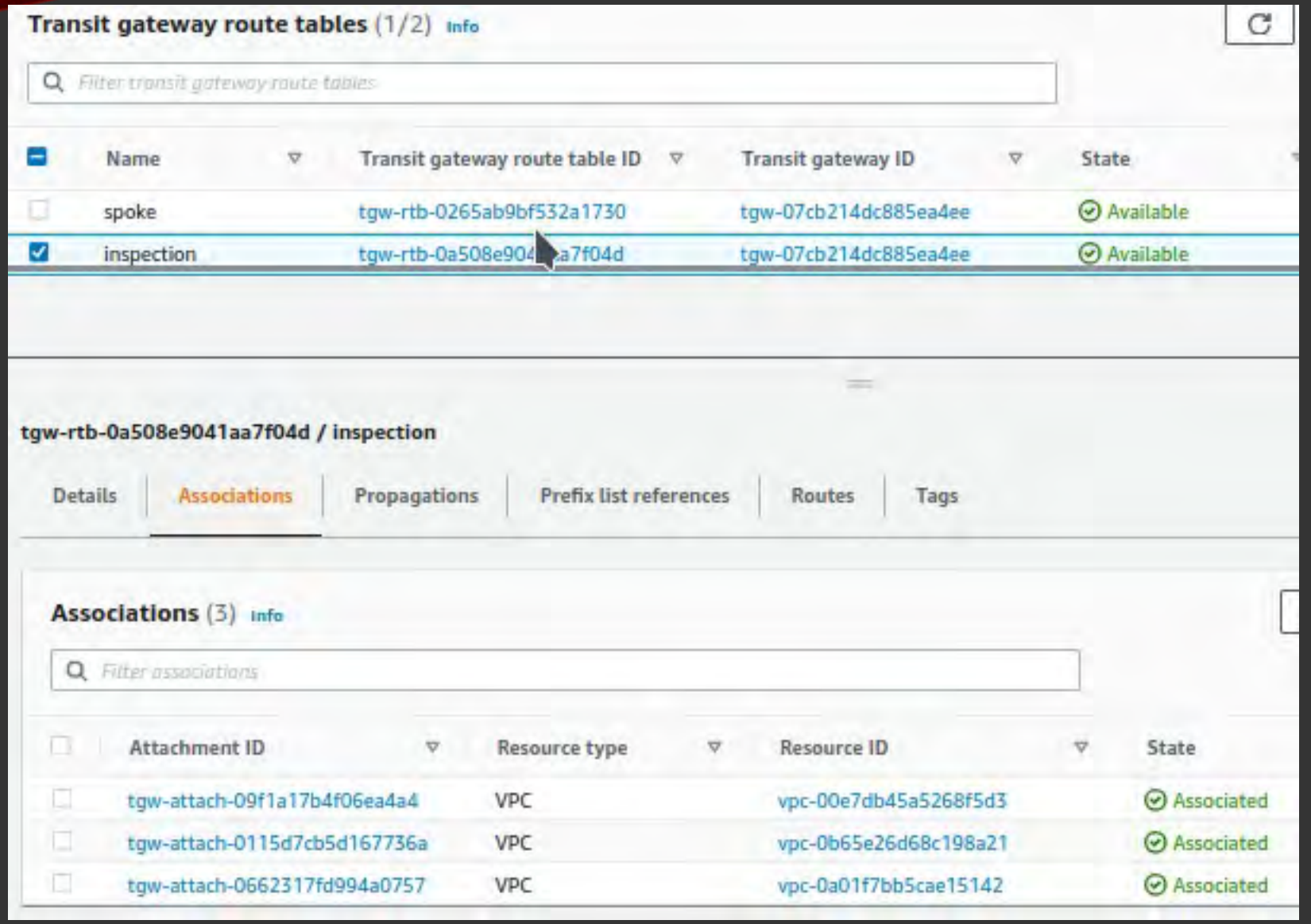
Actions ▼ | Create static route

Filter routes

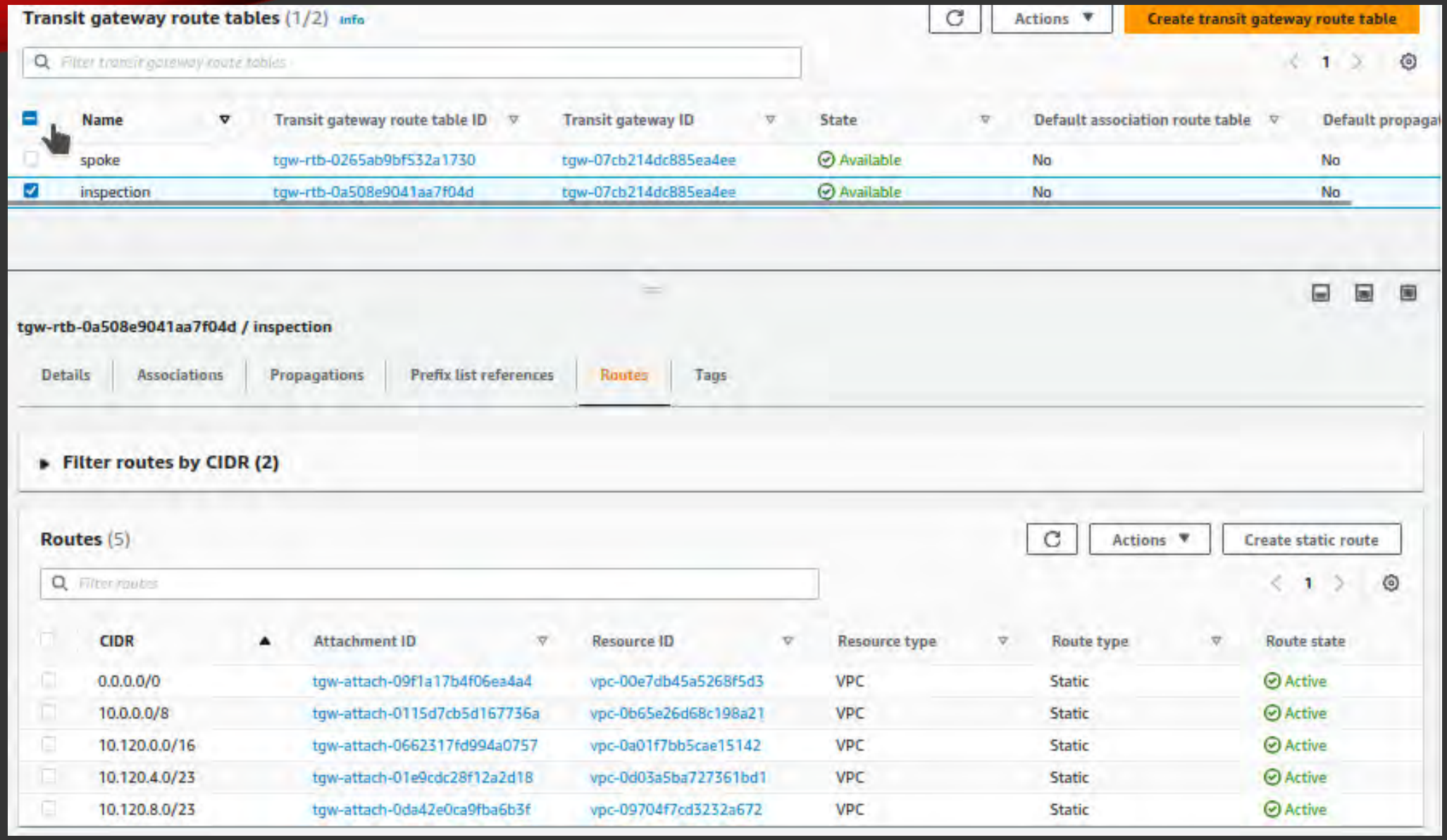
1

CIDR ▲	Attachment ID	Resource ID	Resource type	Route type	Route state
0.0.0.0/0	tgw-attach-09f1a17b4f06ea4a4	vpc-00e7db45a5268f5d3	VPC	Static	Active
10.0.0.0/8	tgw-attach-0115d7cb5d167736a	vpc-0b65e26d68c198a21	VPC	Static	Active
10.120.0.0/16	tgw-attach-0662317fd994a0757	vpc-0a01f7bb5cae15142	VPC	Static	Active

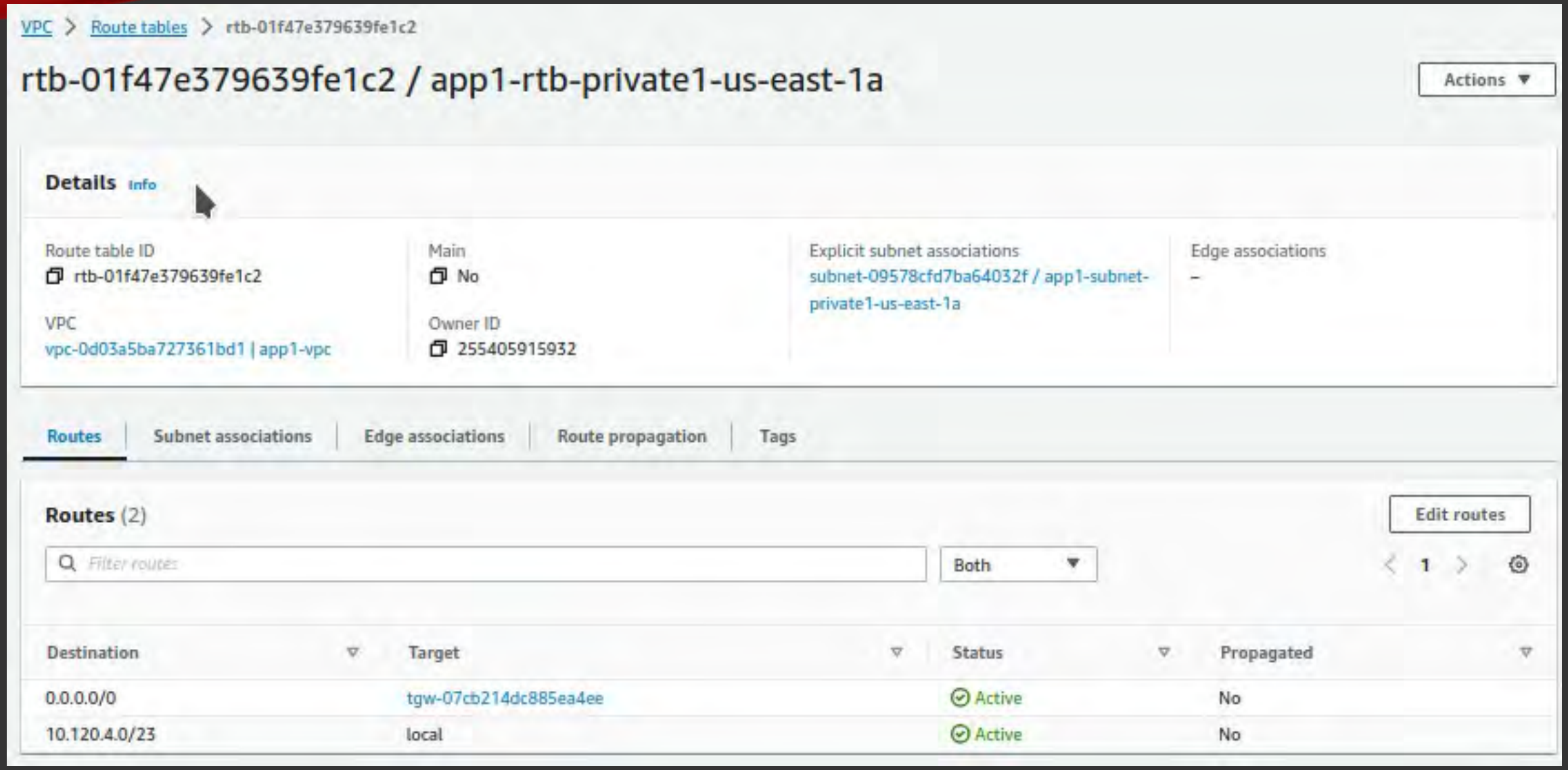
TGW ASSOCIATIONS (INSPECTION)



TGW ROUTES (INSPECTION)



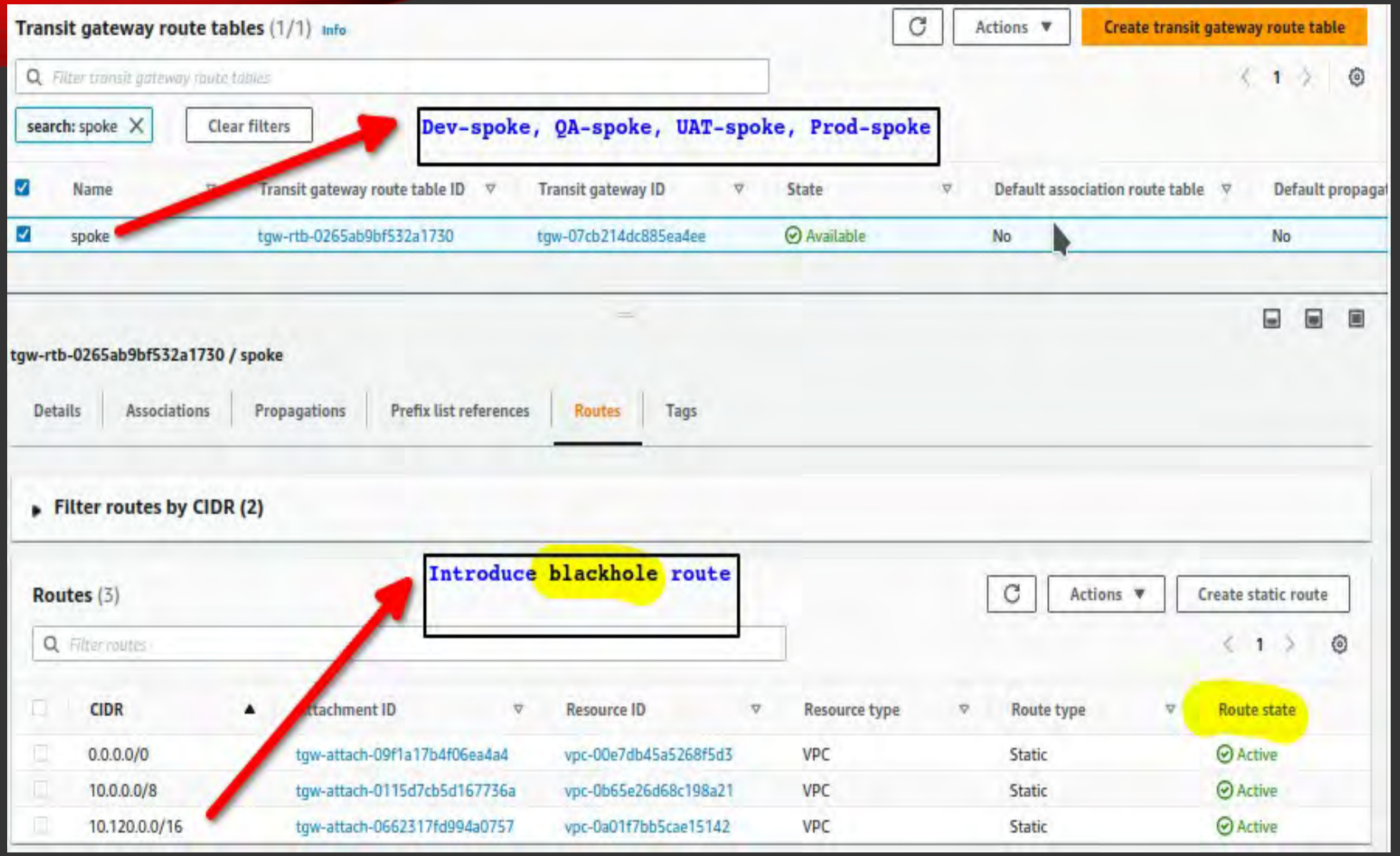
APPLICATION VPC ROUTES

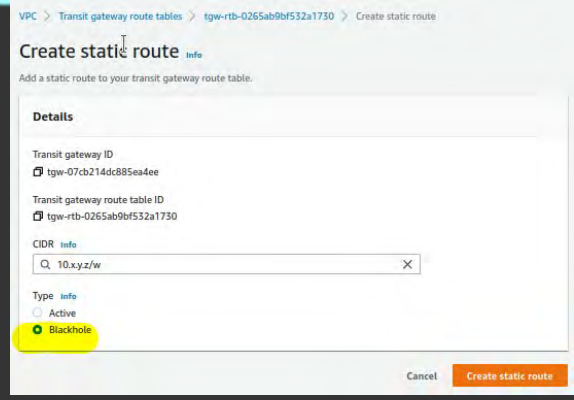


TAKING DESIGN FURTHER

- Isolating traffic at the routing level
  - Dev traffic can only get routed to other Dev environments
  - QA traffic can only get routed to other QA environments
  - UAT traffic can only get routed to other UAT environments
  - Prod traffic can only get routed to other Prod environments

ISOLATION AT ENVIRONMENT TYPE





THANK YOU

References

- https://www.ibm.com/reports/data-breach
- https://www.ndm.net/firewall/pdf/palo_alto/Forrester-Build-Security-Into-Your-Network.pdf
- https://aws.amazon.com/transit-gateway/
- https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/