
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET321

Choosing the right firewall for your hybrid network

Nolan Chen (he/him)

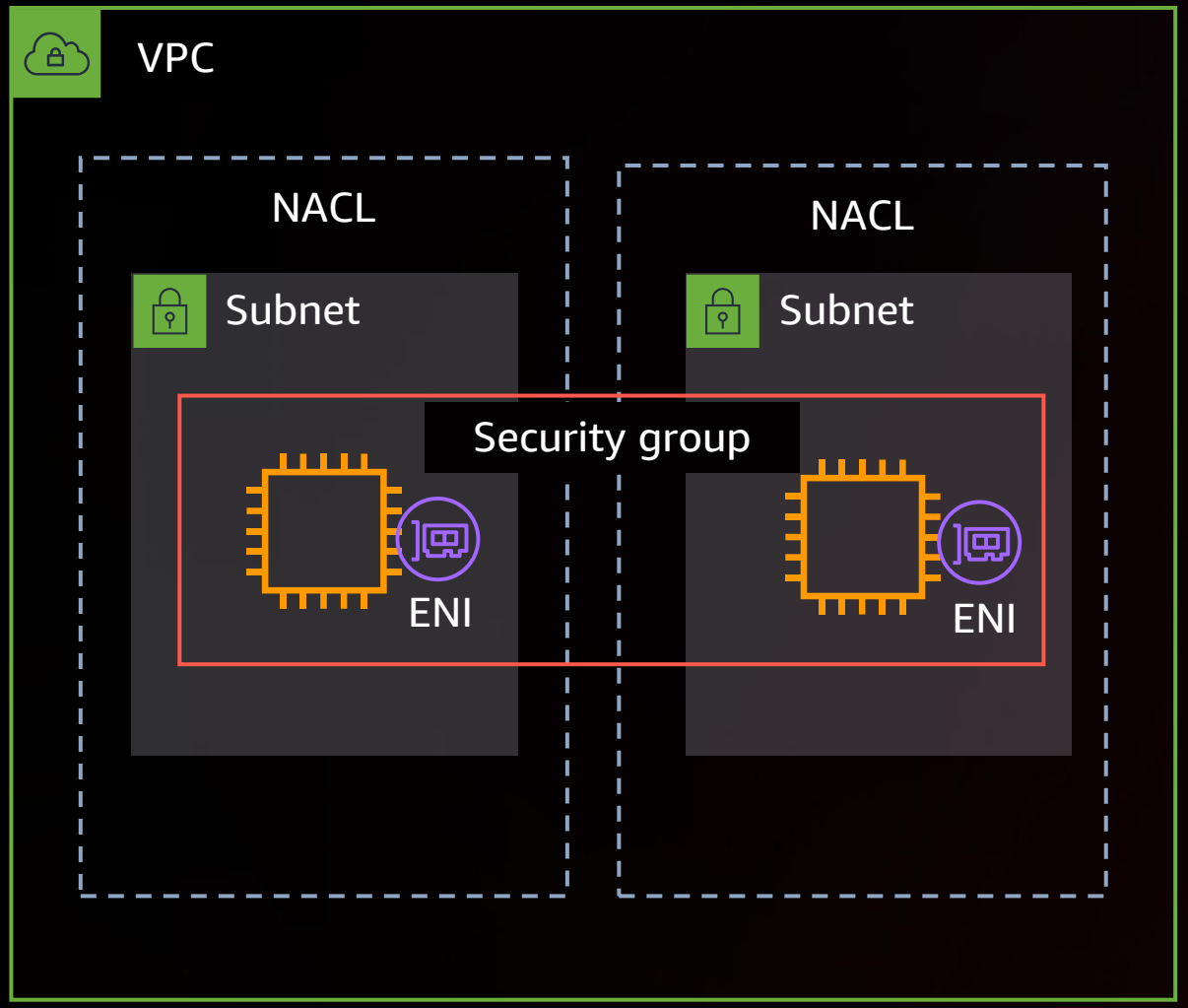
Solutions Architect
Amazon Web Services

Rizwan Mushtaq (he/him)

Principal Solutions Architect
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Basic firewall types – SGs and NACLs



- **Security groups (SGs)**
  - Stateful firewalls
  - TCP/IP layer
  - Applied on an elastic network interface (ENI)
- **Network access control lists (NACLs)**
  - Stateless firewalls
  - TCP/IP layer
  - Applied on a subnet

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Firewall types – Beyond SGs and NACLs

AWS WAF

AWS managed protection for web apps

Cloud-native integration with CloudFront, Application Load Balancer, API Gateway & AWS AppSync

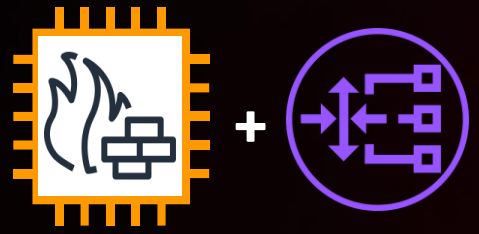
Third-party



Virtual firewall appliance in cloud on EC2

Costly – integration challenges

Third-party & Gateway Load Balancer (GWLB)



Now supports IPv6

Combine with purpose-built load balancer for firewalls

Easier deployment for scalability and availability

AWS Network Firewall



Use AWS managed firewall instead of third-party

Cloud-native management experience – focused feature set

On-premises



Cloud traffic directed back on-premises to hardware firewall

Lacks scalability – costly

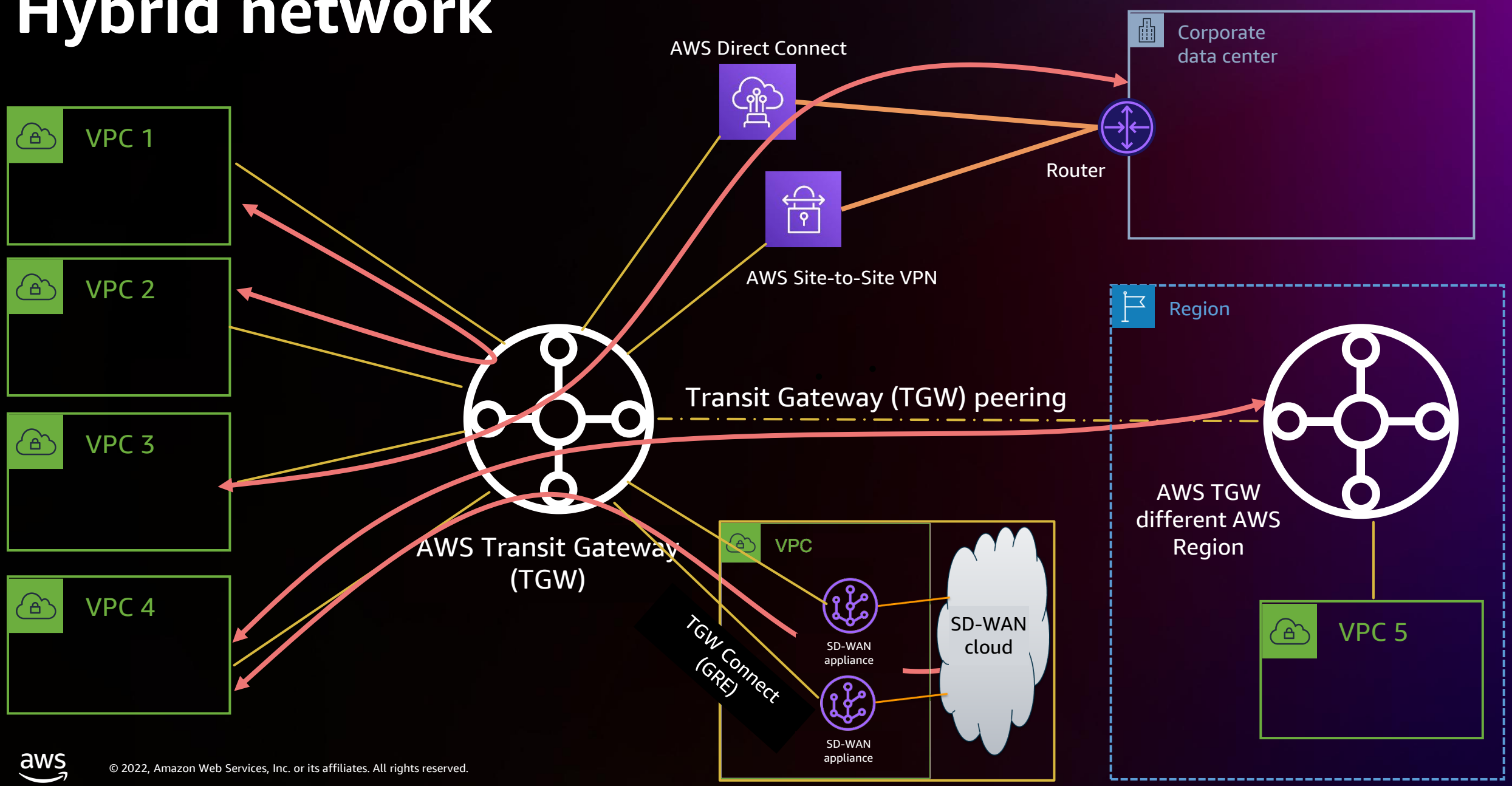
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid connectivity recap

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid network

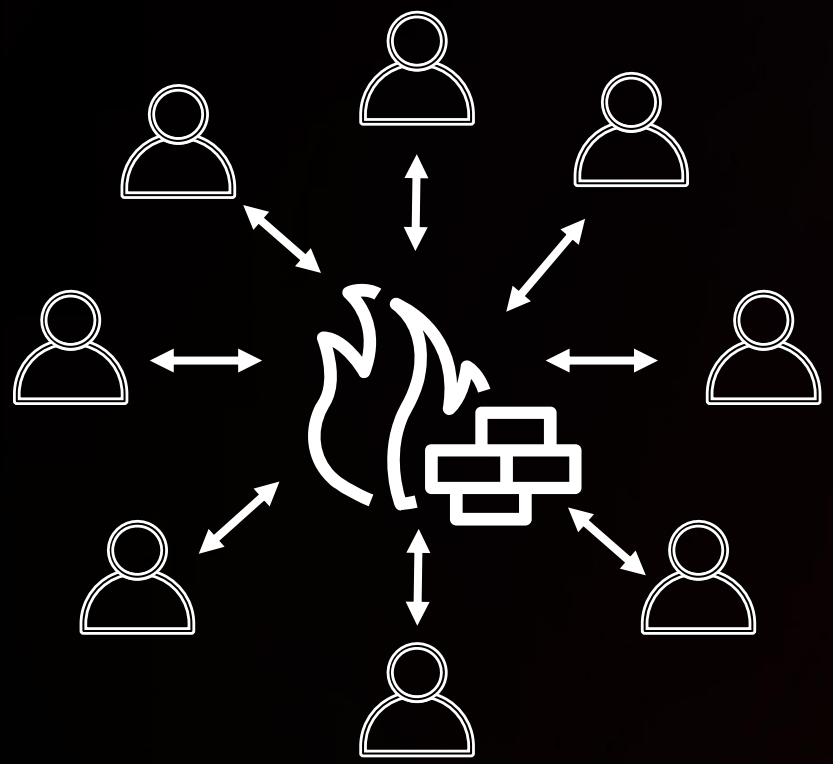


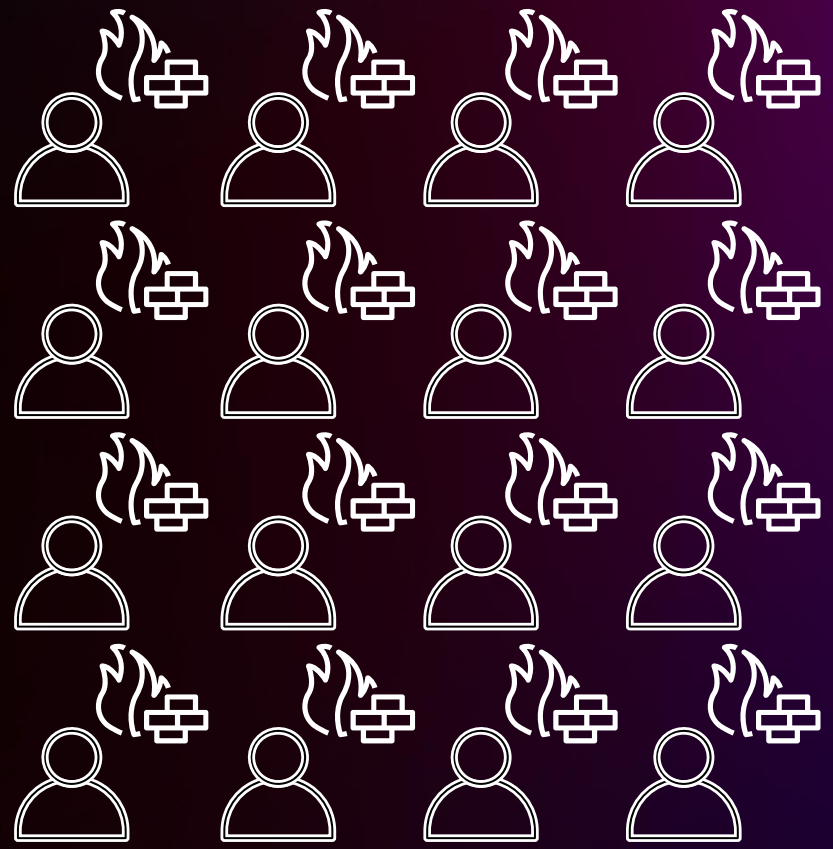
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inspection architectures

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

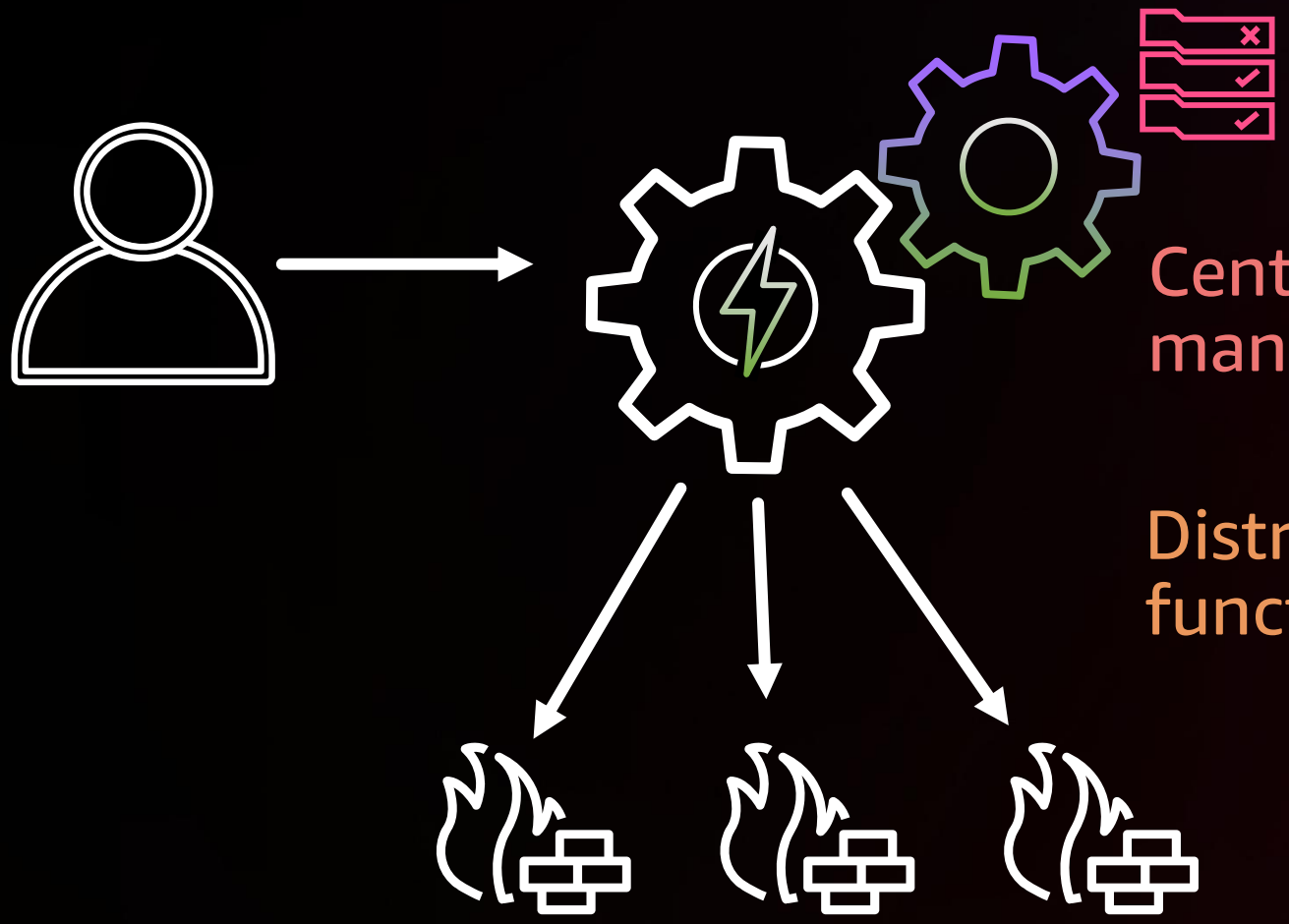
To centralize, or not to centralize?





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Control plane and data plane



Central place to configure and manage = centralized control plane

Distributed processing of rules and functions = distributed data plane

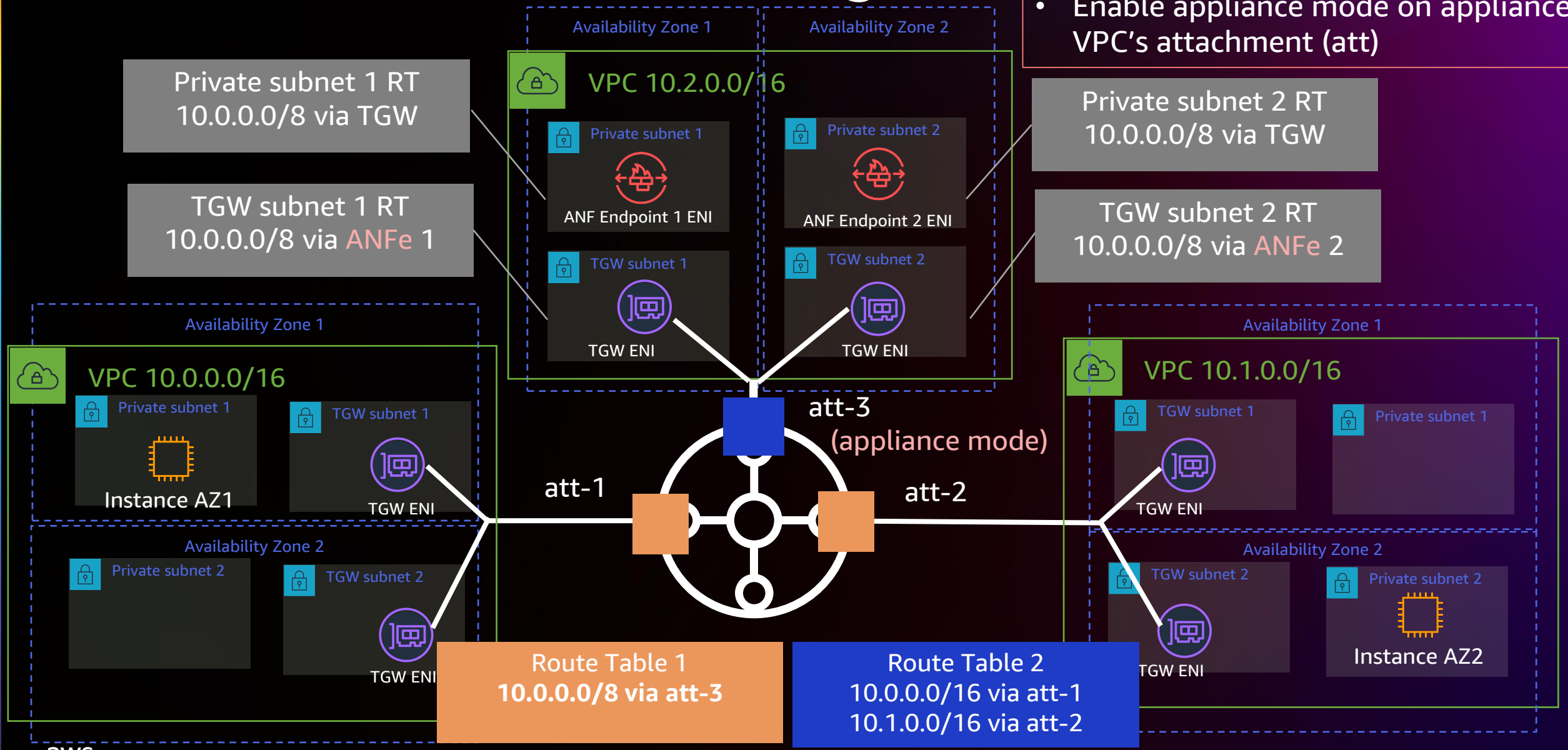
Centralize both?

Distribute both?

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

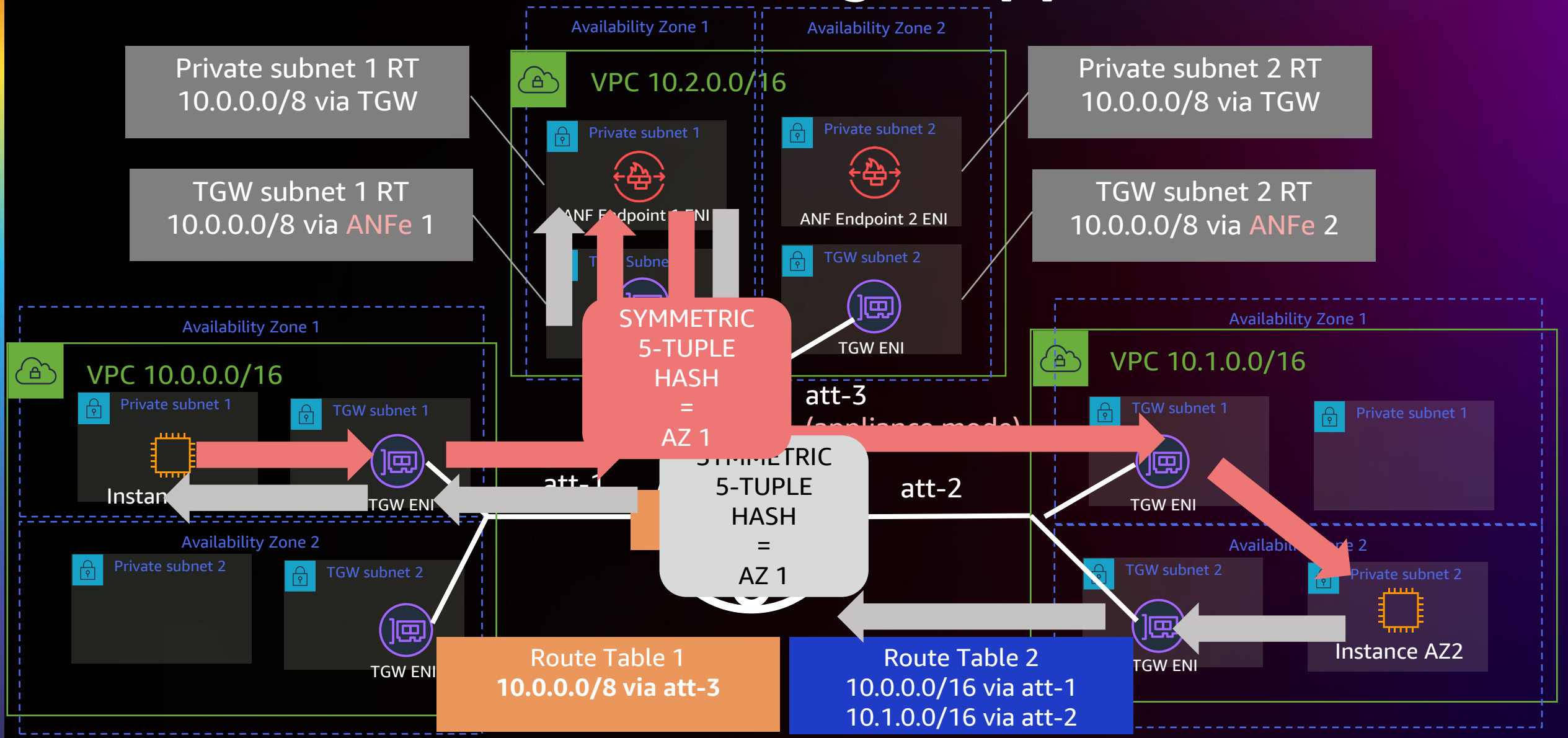
TGW East-West firewalling

Considerations:
- Transit Gateway is a prerequisite
- Enable appliance mode on appliance VPC's attachment (att)



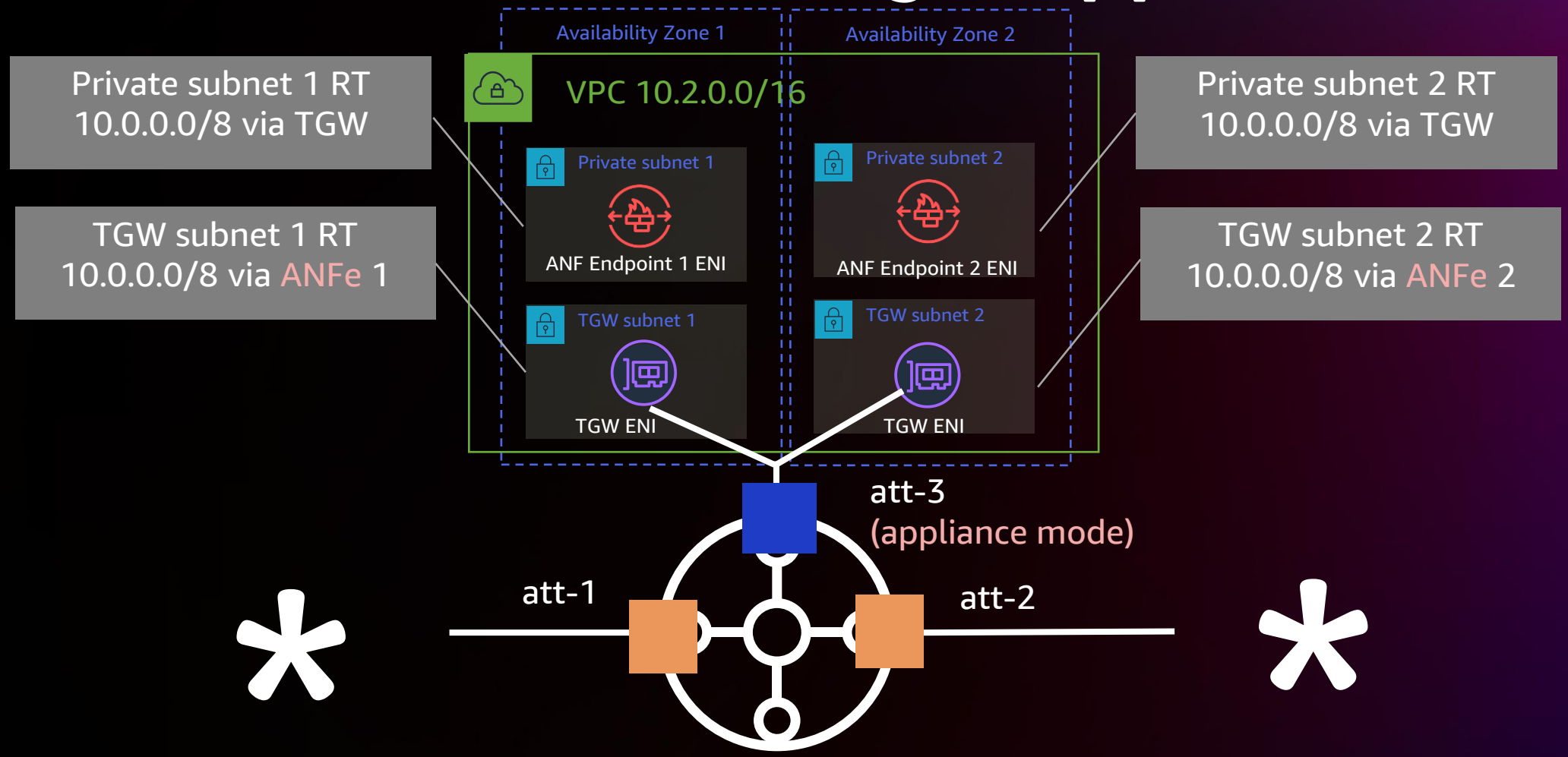
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TGW East-West firewalling & appliance mode



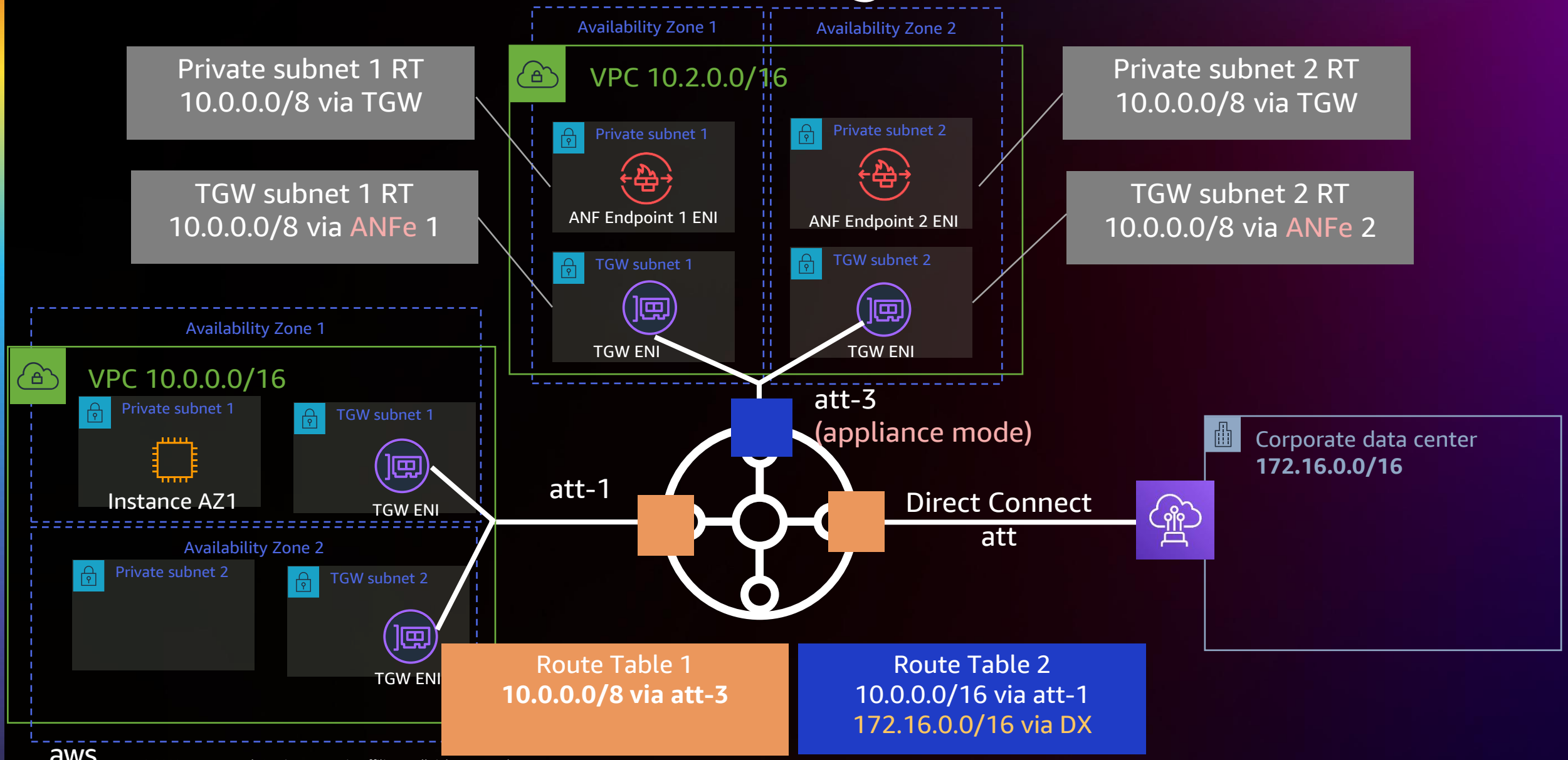
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TGW East-West firewalling & appliance mode



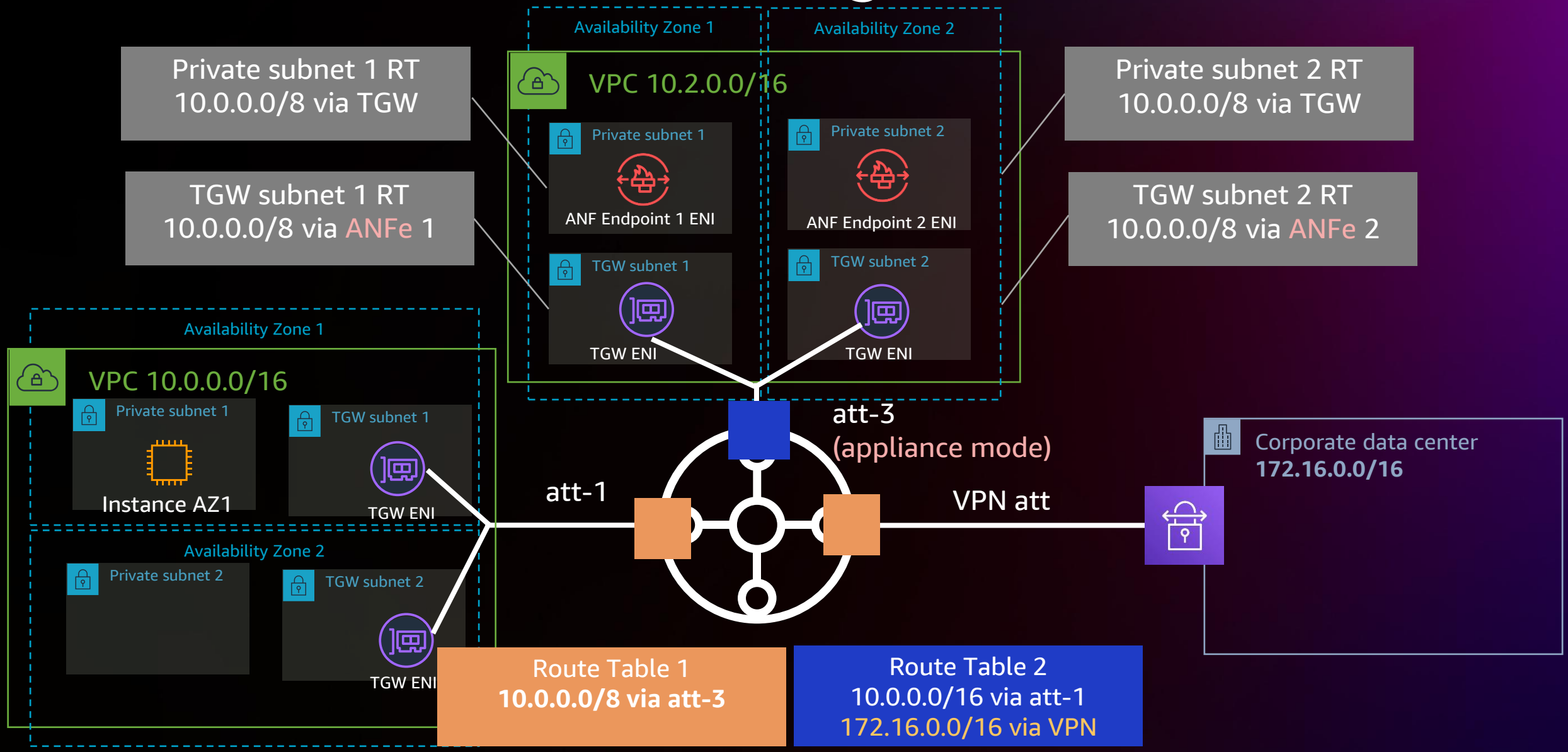
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TGW East-West firewalling (Direct Connect)



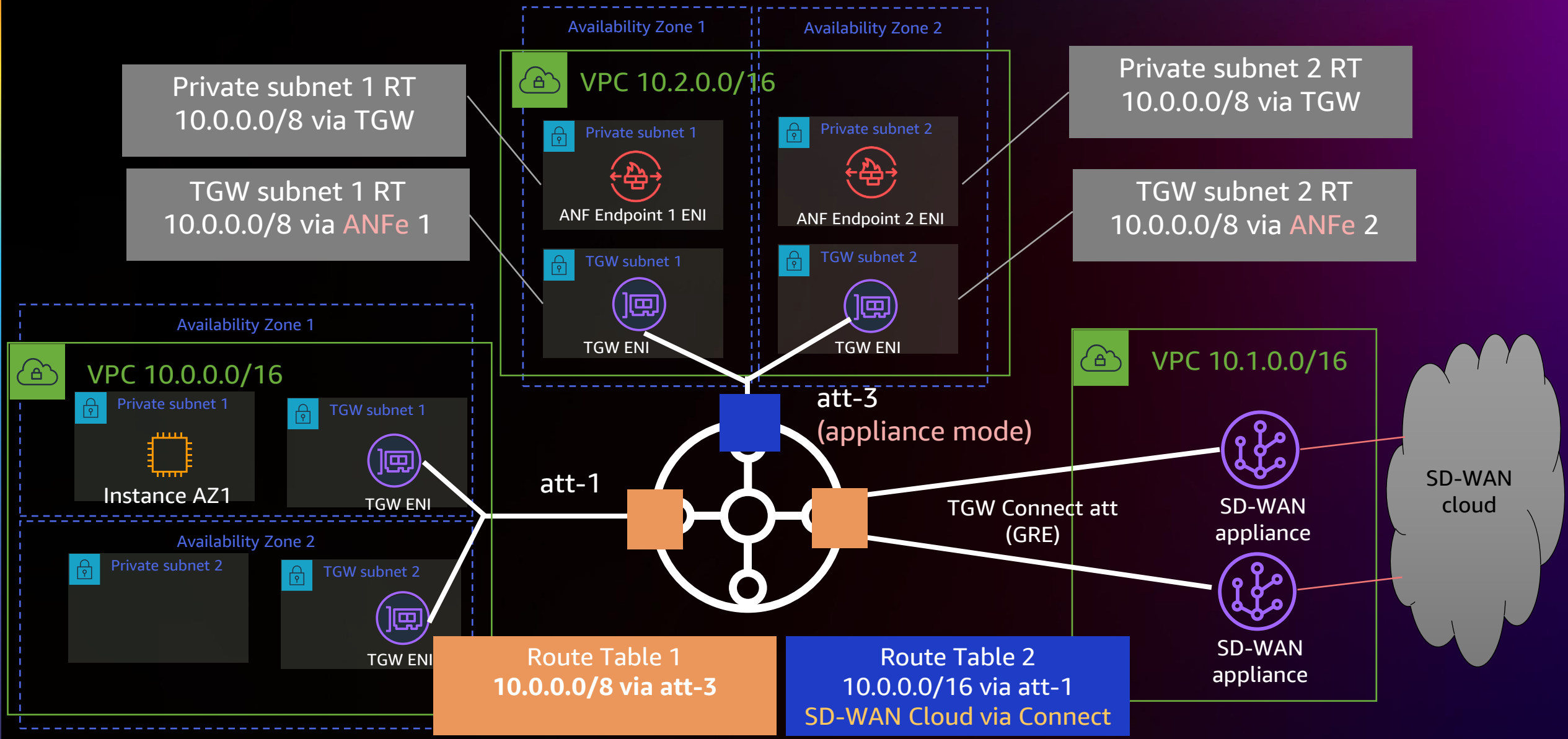
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TGW East-West firewalling (Site-to-Site VPN)



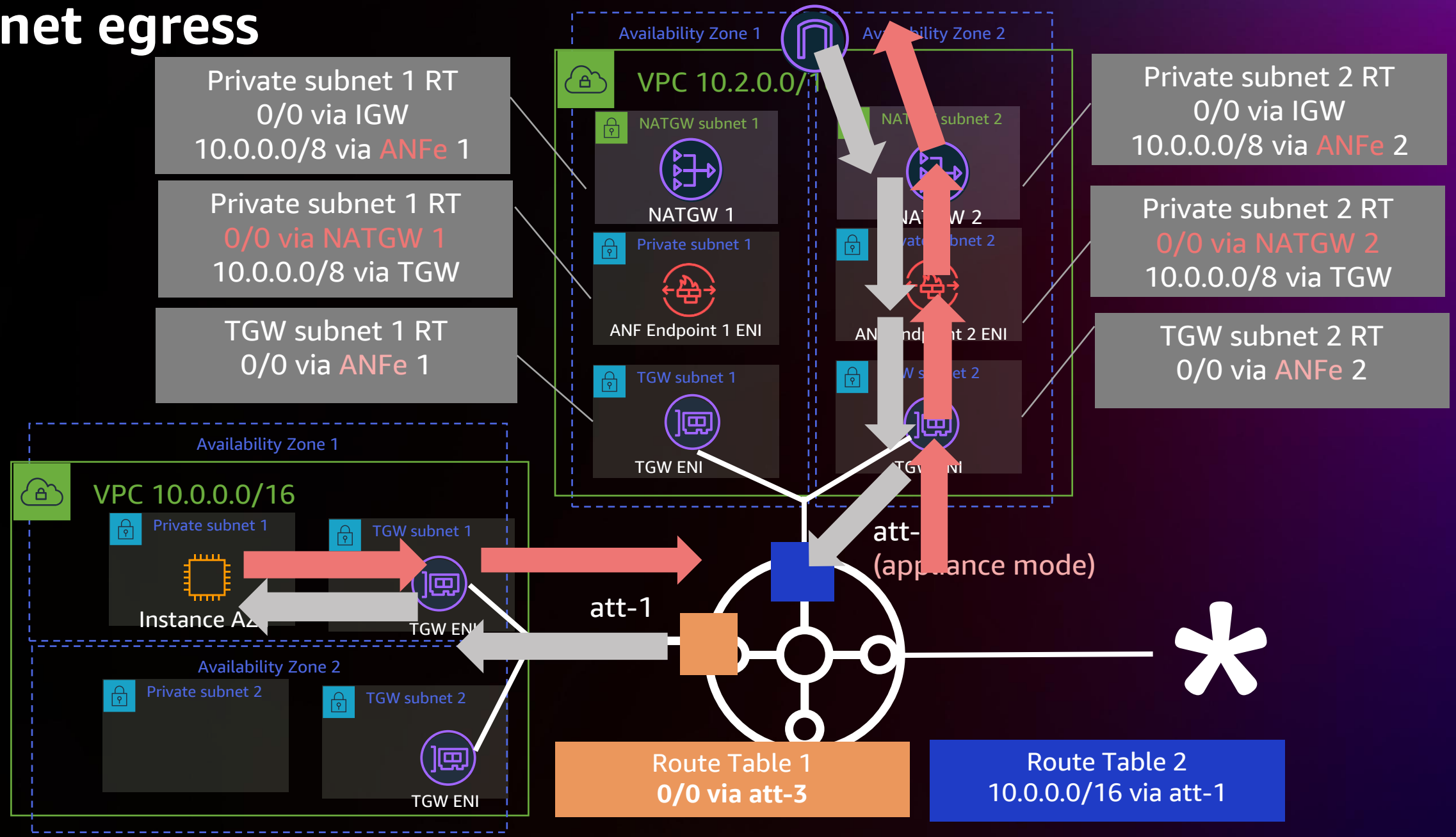
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

TGW East-West firewalling & SD-WAN (TGW Connect)



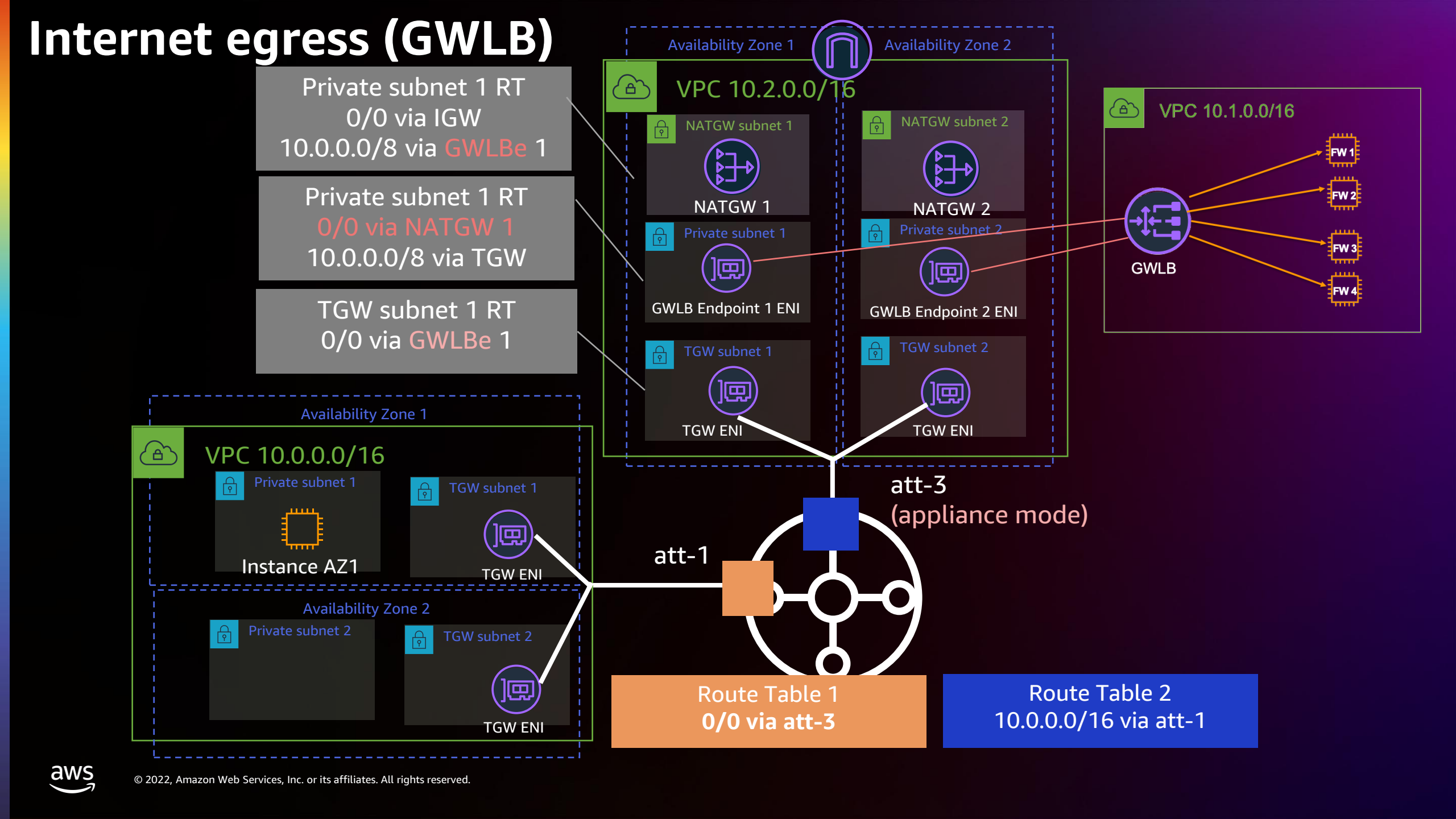
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Internet egress



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Internet egress (GWLB)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inbound centralized VPC security integrations

AWS WAF

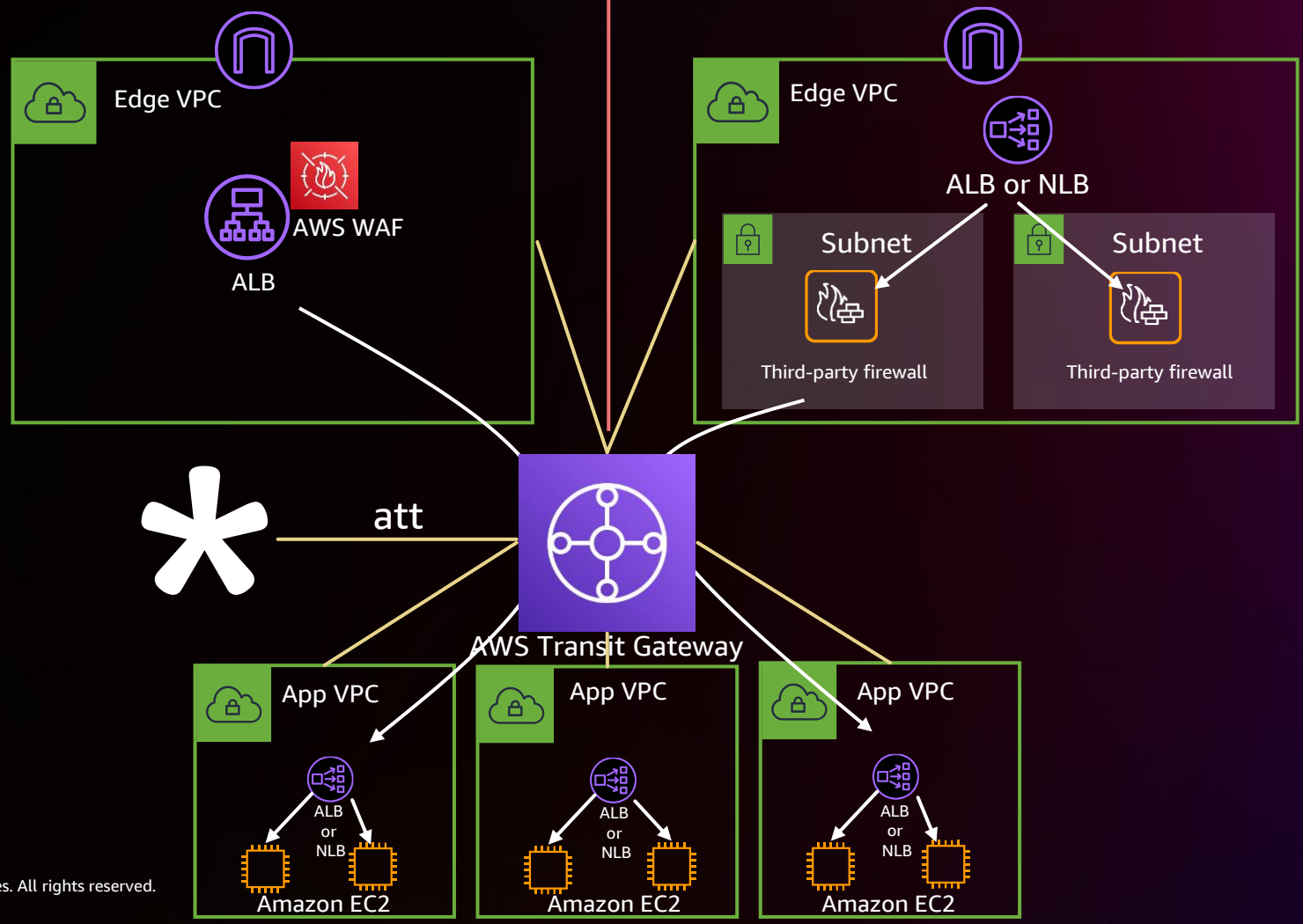
Considerations

- Edge VPC ALB can only target IPs, not hostnames
- App VPC ELB must use Network Load Balancer (NLB) to provide a static IP to edge VPC ALB

ELB sandwich

Considerations

- Third-party firewall should support targeting hostnames to allow both NLB and ALB in app VPCs



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inbound centralized VPC security integrations

AWS Network Firewall

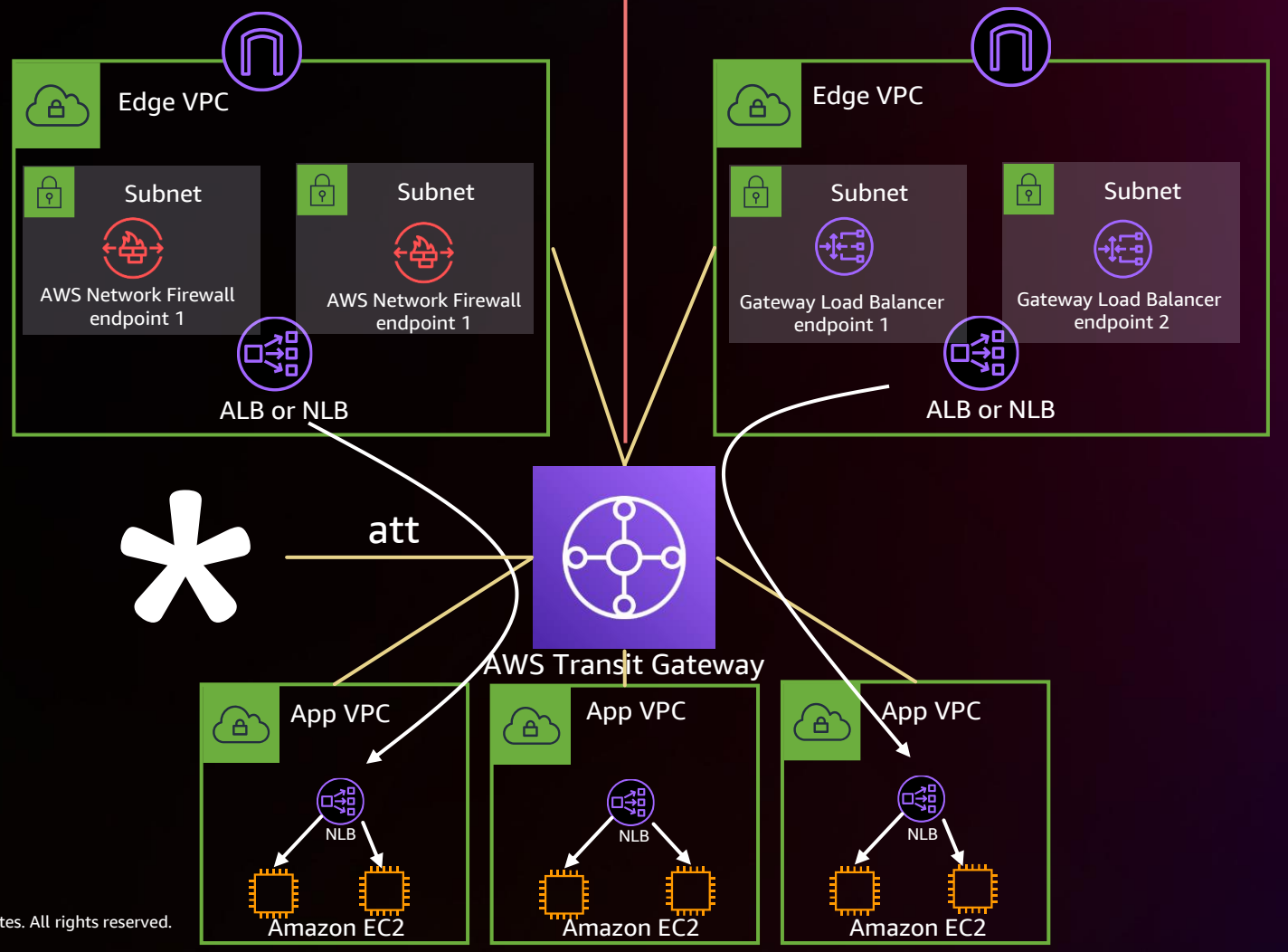
Considerations

- Edge VPC ELB can only target IPs, not hostnames
- App VPC ELB must use NLB to provide a static IP to edge VPC ELB
- ELB can terminate TLS, but Network Firewall cannot inspect encrypted traffic

Gateway Load Balancer

Considerations

- Edge VPC ELB can only target IPs, not hostnames
- App VPC ELB must use NLB to provide a static IP as the target for the Edge VPC ELB
- For TLS decryption, the firewalls behind the Gateway Load Balancer need a valid certificate, which can only be created outside of AWS Certificate Manager (ACM)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Nolan Chen
https://www.linkedin.com/in/nolan-chen-91a7b2/

Rizwan Mushtaq
https://www.linkedin.com/in/rmushtaq/



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.