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

SEC317-R

Implementing traffic inspection capabilities at scale on AWS

Rohit Aswani (he/him)

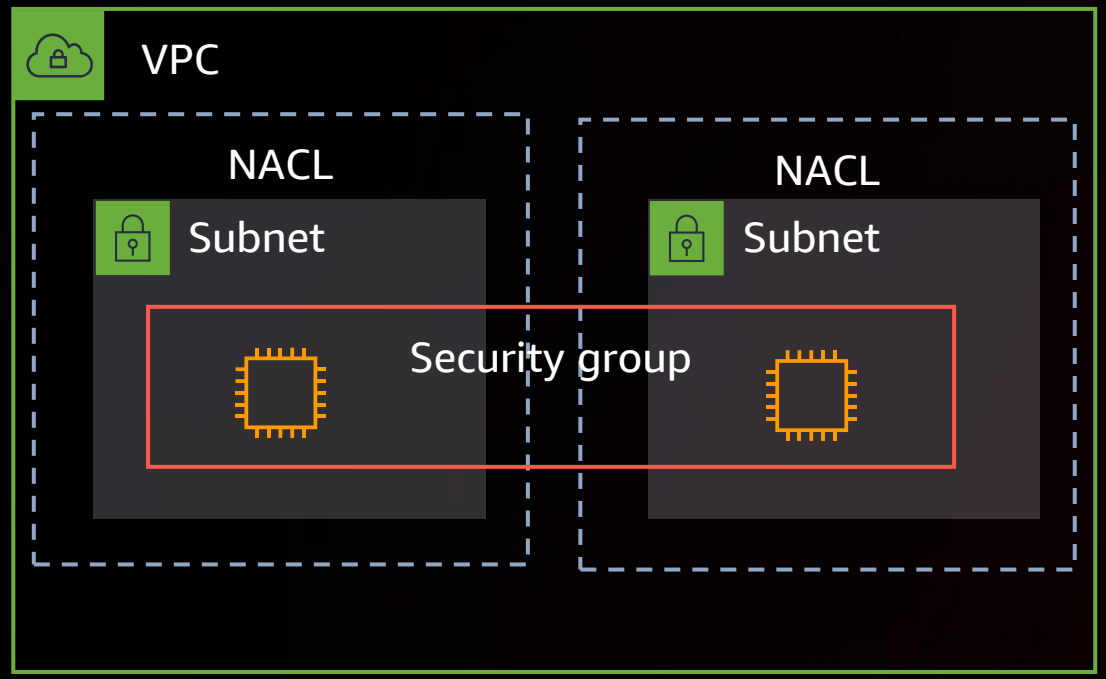
Senior Solutions Architect – Networking Specialist
AWS

Dhanil Parwani (he/him)

Senior Partner Solutions Architect – Networking
AWS

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

Firewall types



- **Security groups (SGs)**
  - Stateful firewalls
  - TCP/IP layer
  - Applied on an 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



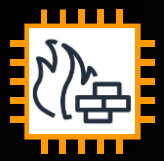
Network Firewall



AWS WAF

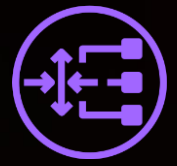


Route 53
Resolver DNS Firewall



Third-party appliance

+



Now supports IPv6

Gateway Load Balancer

- **AWS Network Firewall**
  - AWS-managed firewalling/IPS service
  - Use route tables to transparently apply inspection
- **AWS WAF**
  - Managed AWS WAF service for inbound traffic inspection
  - Protects your web applications from common web issues
  - Integrates with Application Load Balancer, Amazon CloudFront, Amazon API Gateway, and AWS AppSync
- **Amazon Route 53 Resolver DNS Firewall**
  - AWS-managed DNS firewall
  - Block DNS queries for malicious domains and allow queries for trusted domains in your Amazon Virtual Private Cloud (Amazon VPC)
  - Use AWS-managed domain lists or create your own
- **Third-party appliance**
  - A firewall vendor of your choice can run their software on an Amazon EC2 instance
  - Combine with a Gateway Load Balancer from AWS for improved availability and scale
  - Use route tables to transparently apply inspection

aws

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

Network protection use cases

Outbound egress

Trusted internal users or workloads accessing untrusted public internet



East-West

Workload to workload

Internal user to workload



Inbound ingress

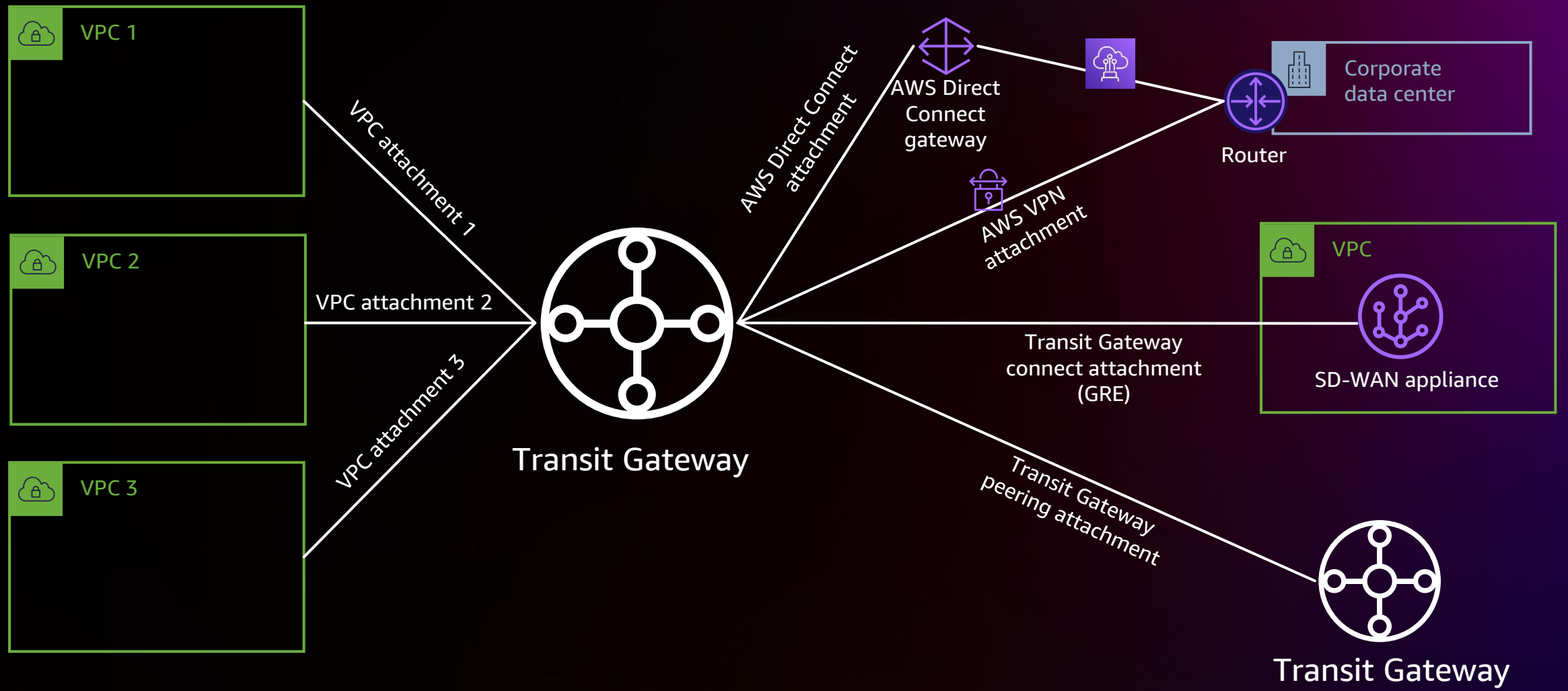
Untrusted external internet users accessing public-facing app



Implemented separately or combined

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

AWS Transit Gateway



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

Outbound egress inspection

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

AWS Network Firewall top use cases

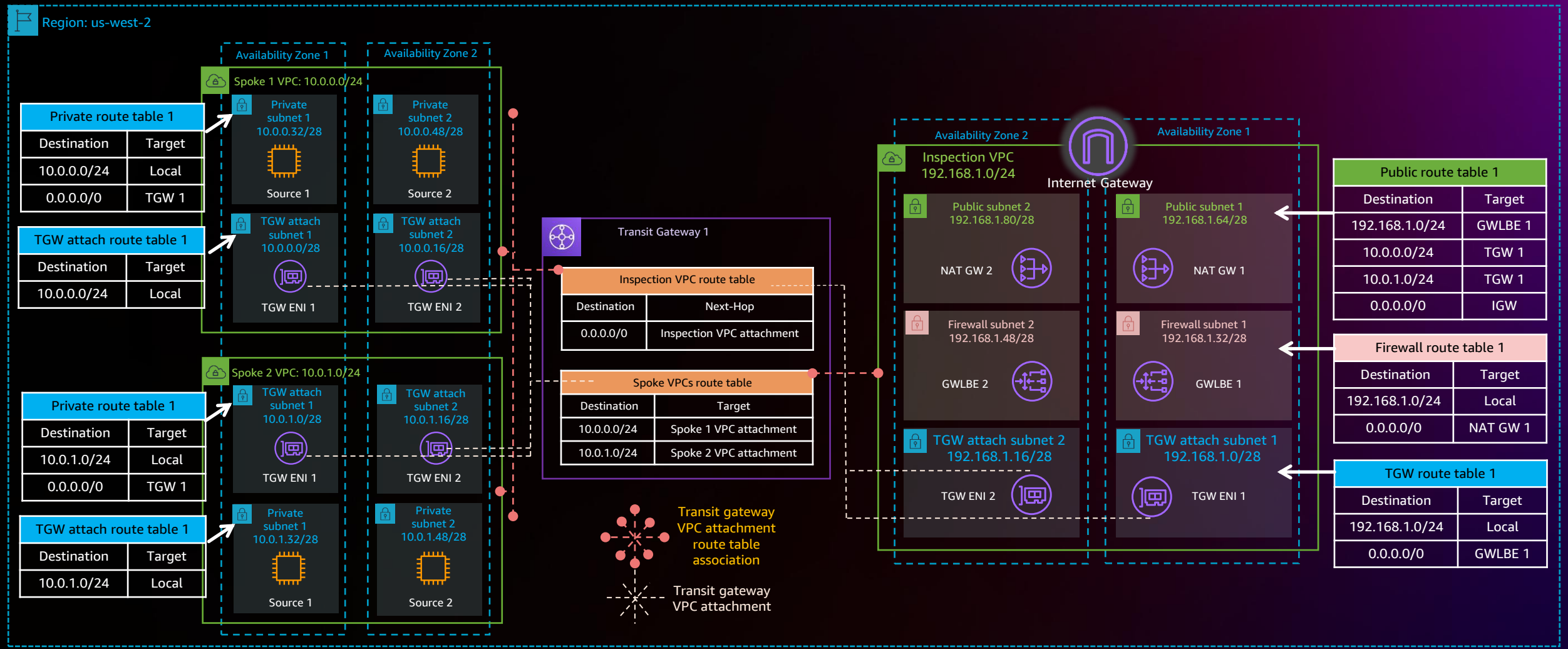
- Domain/FQDN filtering
- DenyListing of known-bad and AllowListing of known-good
- Ensure ports are only used by their legitimate protocol
- Block vulnerable versions of transport layer security (TLS)
- Block direct-to-IP communications
- Threat hunting/reverse stack ranking

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

Centralized egress

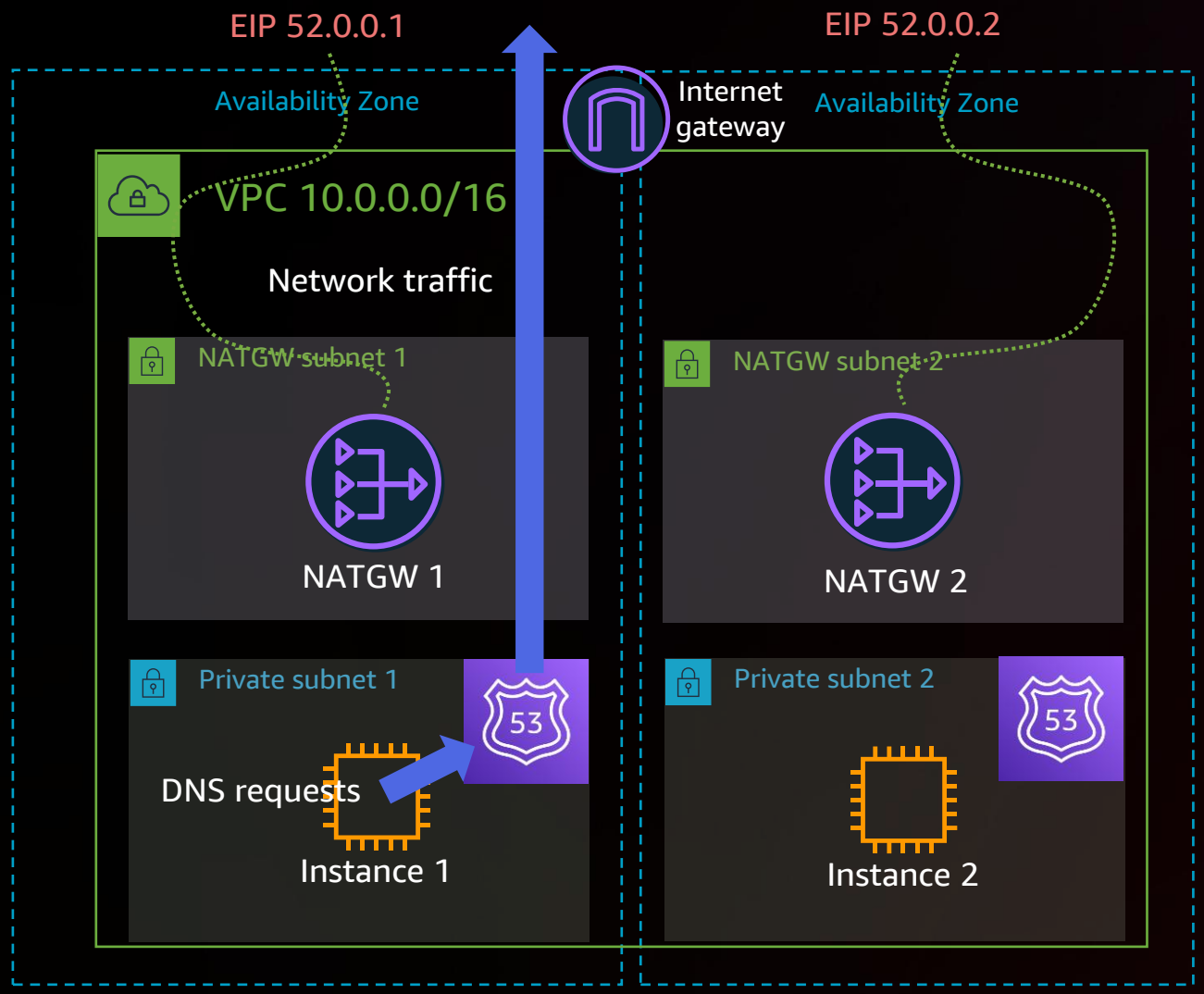
VPC TO INTERNET (NORTH-SOUTH)

Consideration
Enable appliance mode
on appliance VPCs attachment



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

DNS is an additional egress path in default VPC config

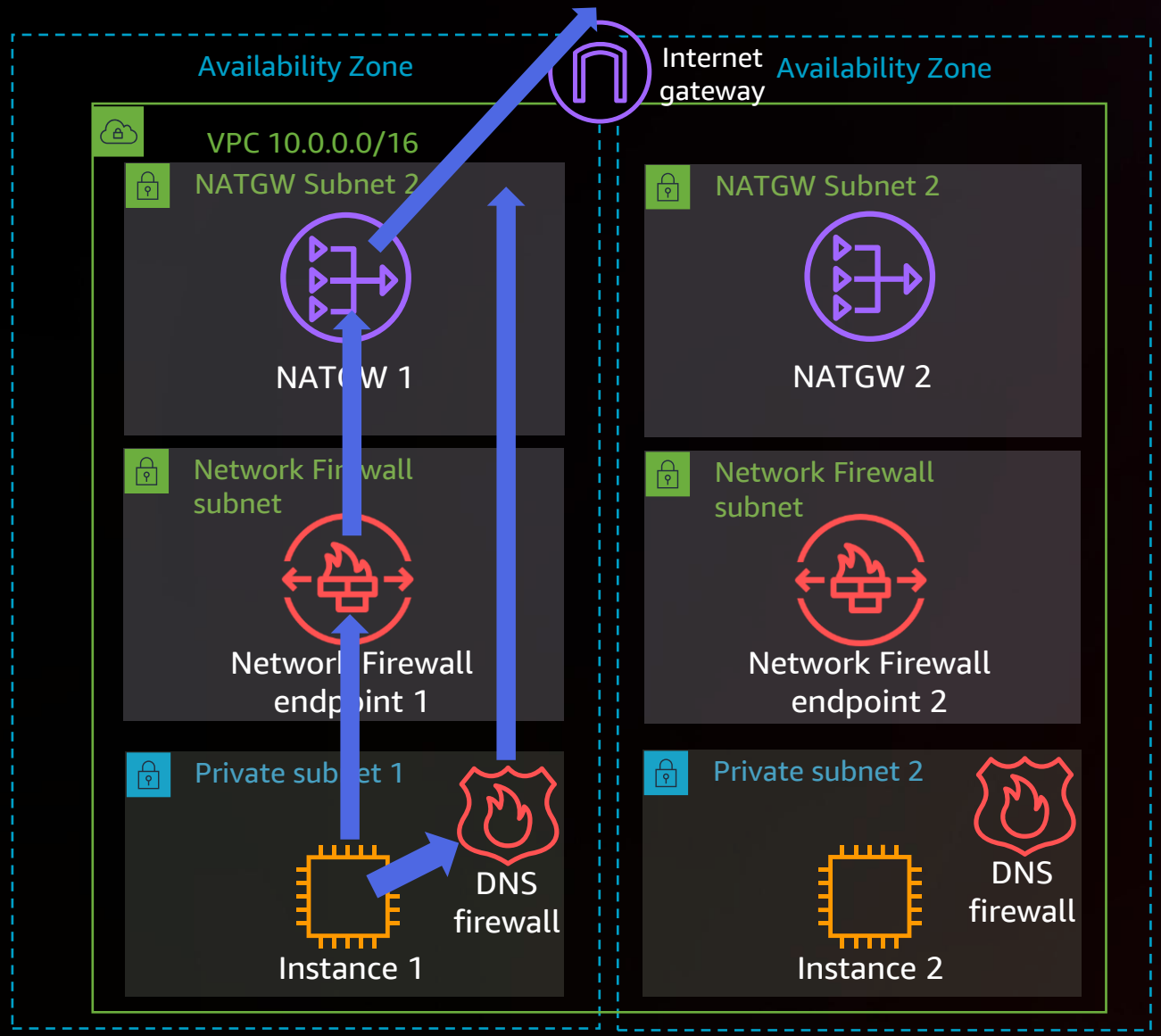


Considerations

- Amazon-provided DNS (.2 resolver) is on by default, but can be disabled in VPC settings
- If enabled, it cannot be blocked by security groups or NACLs
- Defaults to no filtering of DNS queries
- DNS tunneling is an alternate egress path out of the VPC

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

AWS Network Firewall and DNS firewall deployment



Deployment considerations

- DNS firewall rule group applied on a per-VPC basis
- AWS Network Firewall requires an additional subnet containing only the firewall endpoint(s)
- Egress traffic is routed first to AWS Network Firewall endpoint and then NAT gateway

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

Egress security best practices

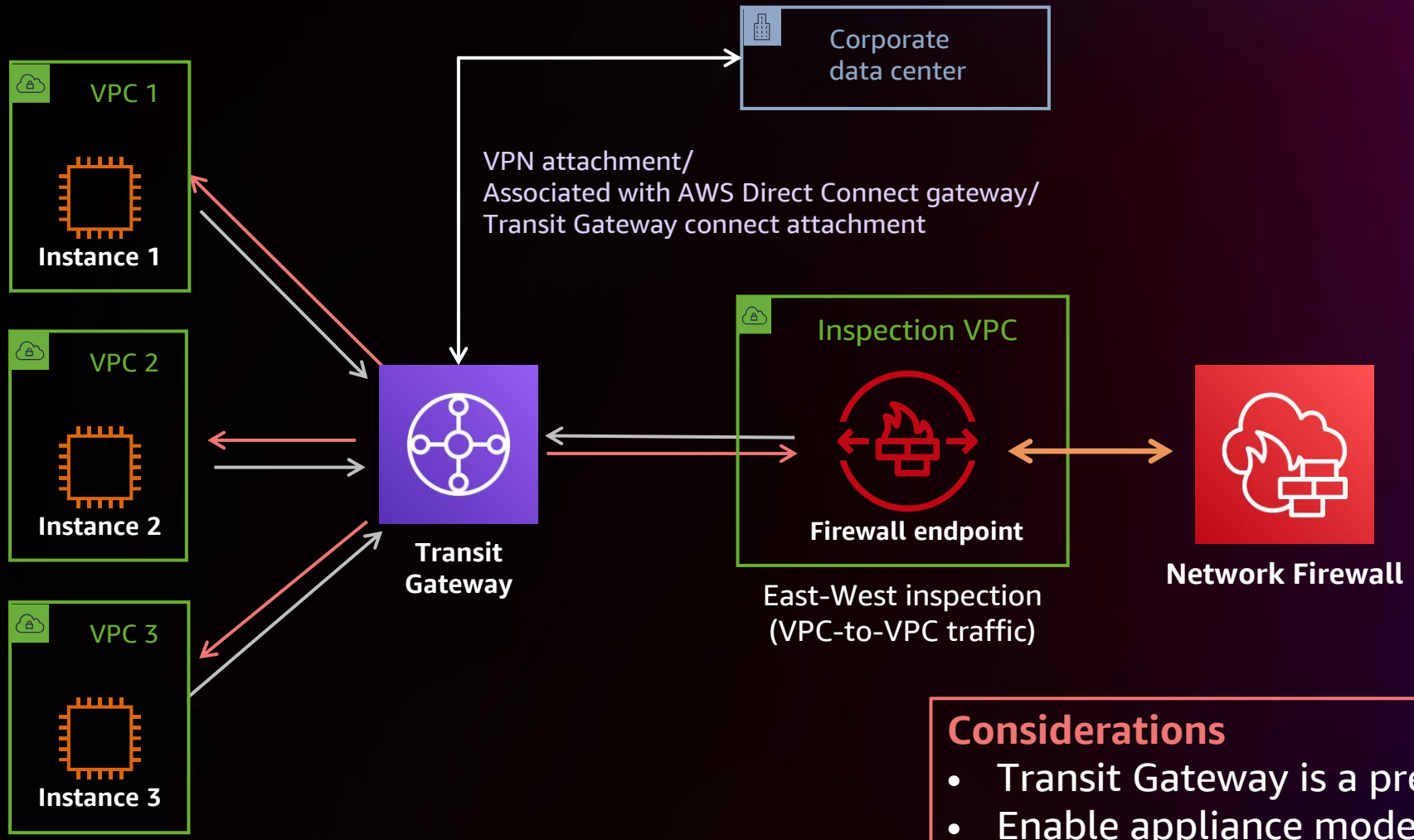
- Only allow ports outbound that need to be allowed, and block all others
- AllowList model for known IPs/TLDs
- Block known high-risk FQDNs with AWS-managed rules
- Use protocol/port enforcement rules (HTTP can only use 80)
- Block direct-to-IP communications (traffic that doesn’t originate with a DNS request)
    - HTTP HOST header and TLS SNI should include FQDN, not IP
- Block known high-risk CIDRs
- Block embargoed country ccTLDs in HTTP/TLS/DNS
- Block well-known DNS over HTTPS (DoH), DNS over TLS (DoT), and DNSCrypt servers

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

East-West inspection

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

Centralized: East-West



Considerations

- Transit Gateway is a prerequisite
- Enable appliance mode on appliance VPC's attachment

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

Inbound ingress inspection

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

Inbound inspection checklist



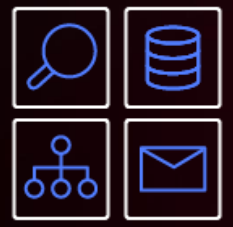
Application type

- HTTP(S)
- Non-HTTP(S)



Control plane and data plane

- Centralized
- Distributed



Inspection depth

- Port/IP filtering
- Application aware



Scale

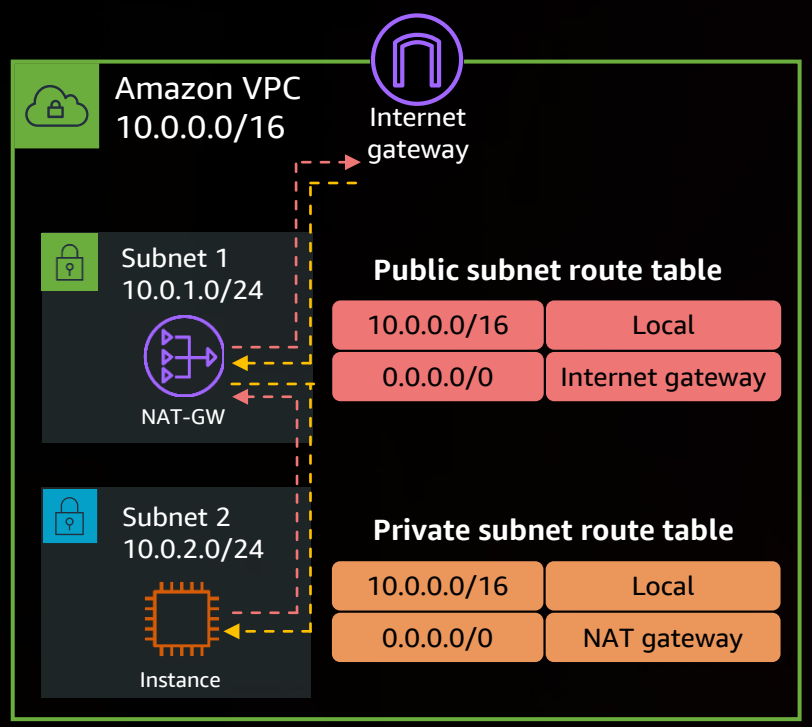
- One VPC
- Many VPCs

aws

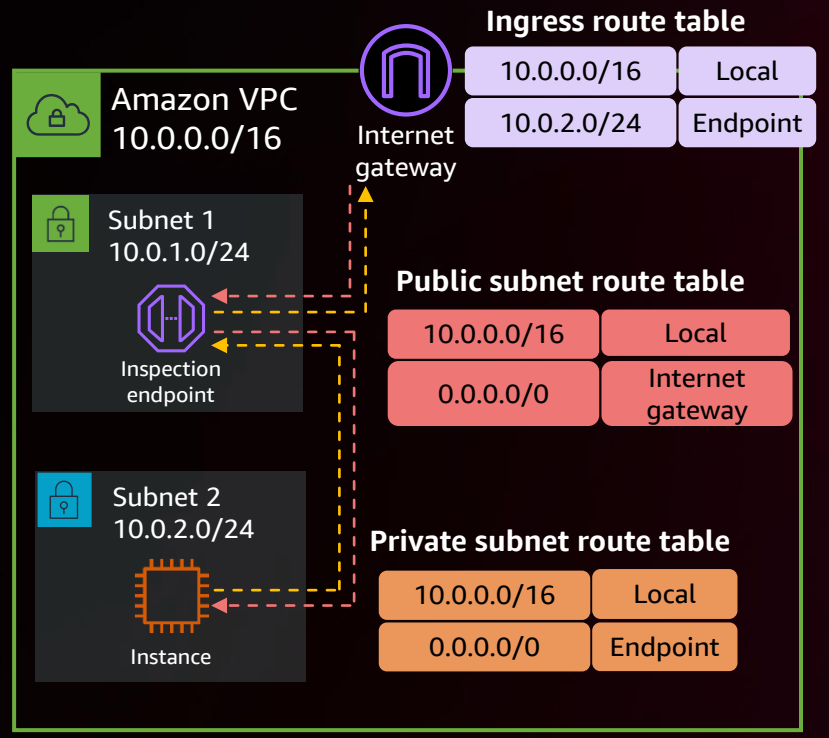
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architectural constructs: Amazon VPC routing

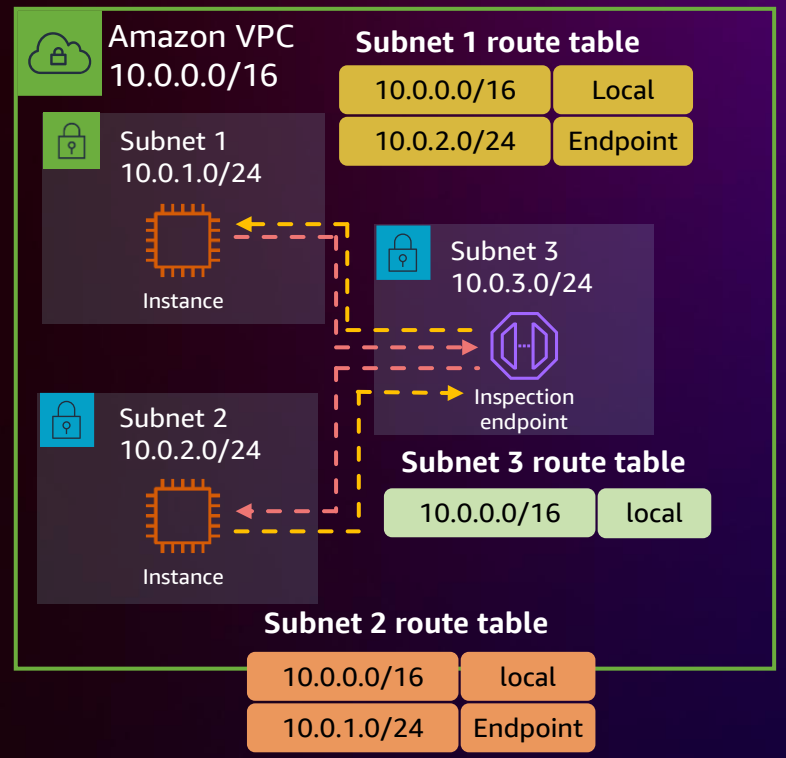
Subnet routing



Ingress routing



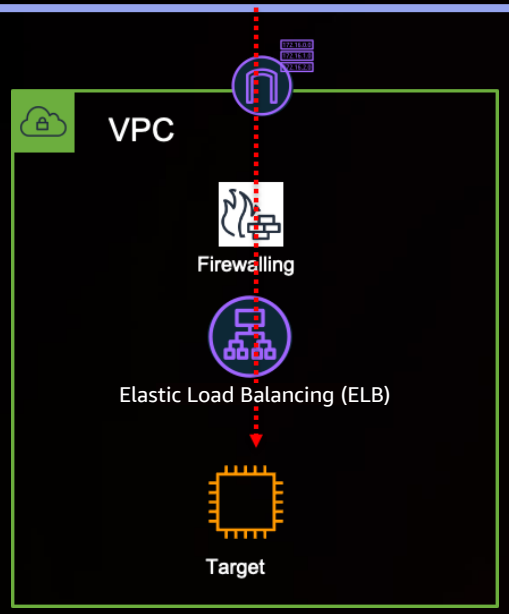
More specific routing



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

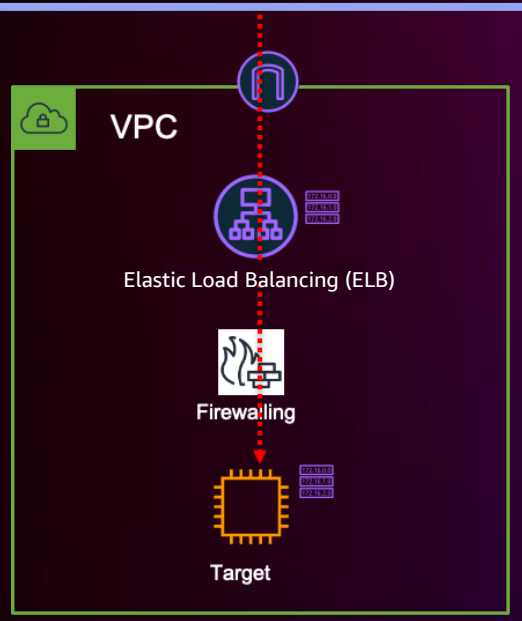
Ingress routing vs. More specific routing

Ingress routing



- Firewall will see all inbound traffic
- Firewall will see client IP address in packet
- Firewall needs public certificate to decrypt TLS

More specific routing



- Firewall will see only traffic already accepted by ELB
- Firewall doesn't see the client IP address in packet
- Firewall can use private certificate to decrypt TLS

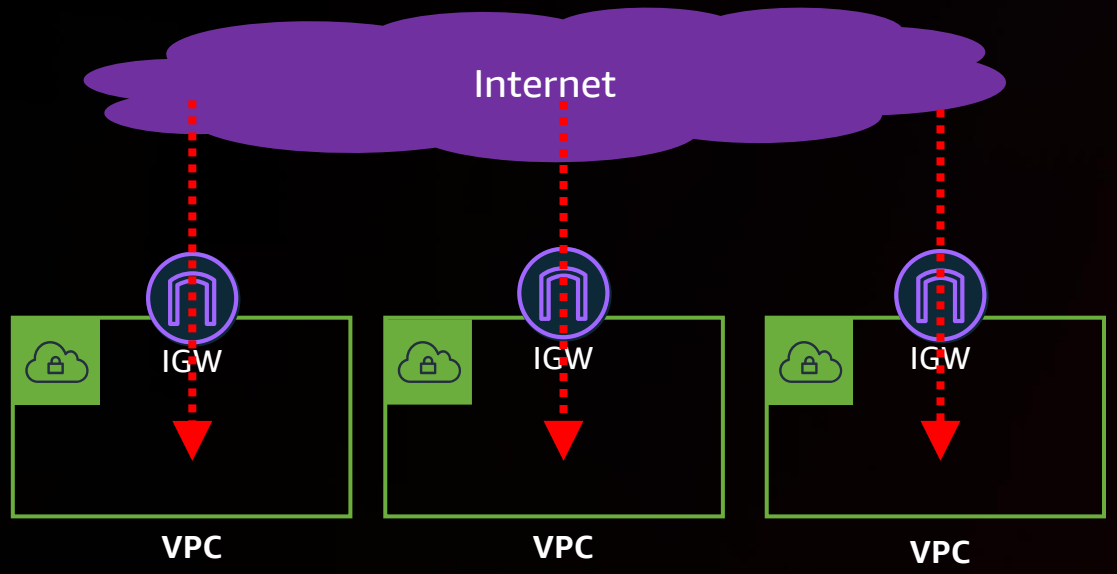
More specific routing is not supported with:

- Network Load Balancer with client IP address preservation and IP-type targets
- Instance target types

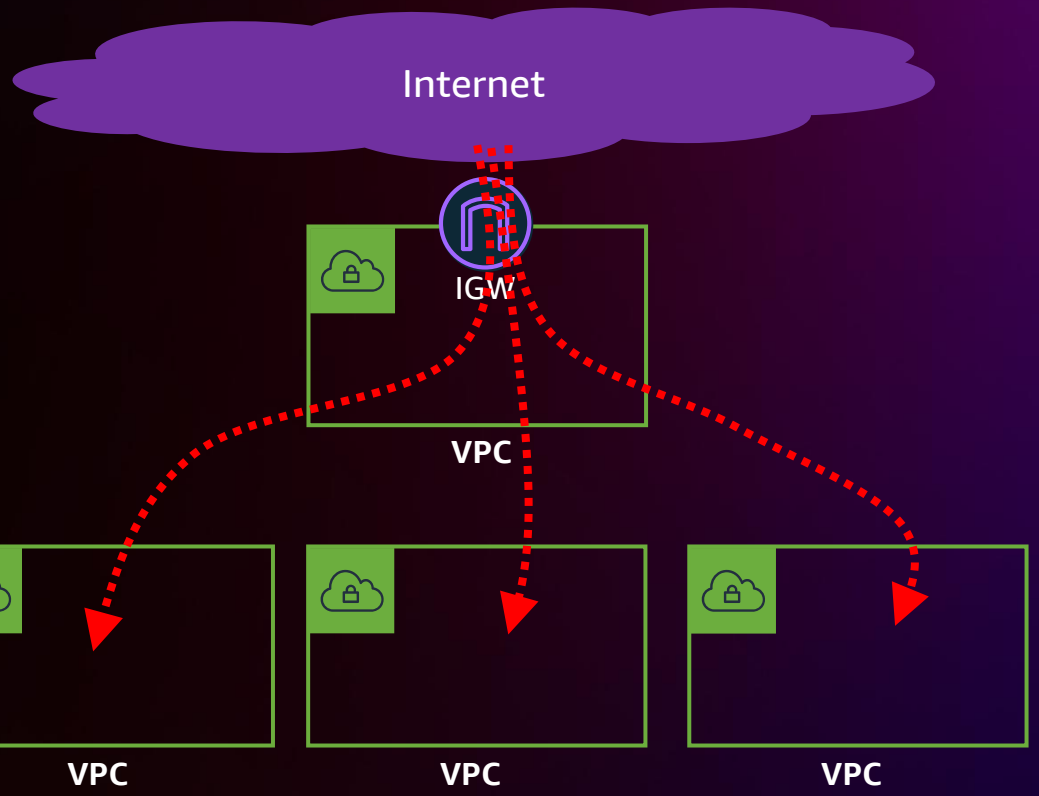
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Distributed vs. centralized deployments

Distributed ingress traffic



Centralized ingress traffic



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

Distributed VPC security integrations

AWS WAF

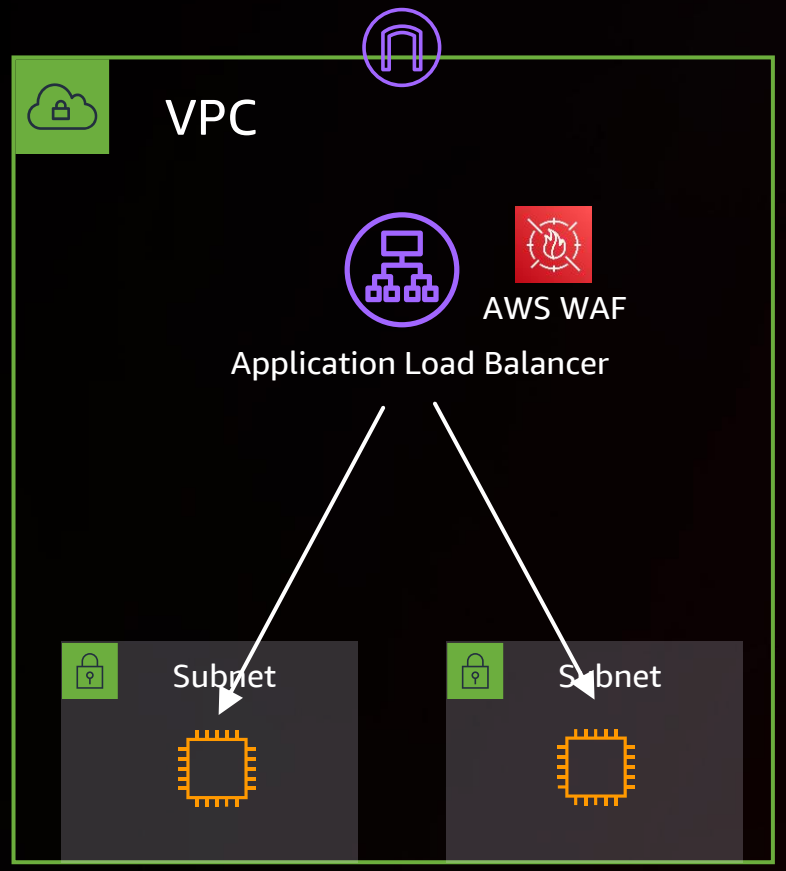
Supported app
HTTP(S) only

TLS decryption
True

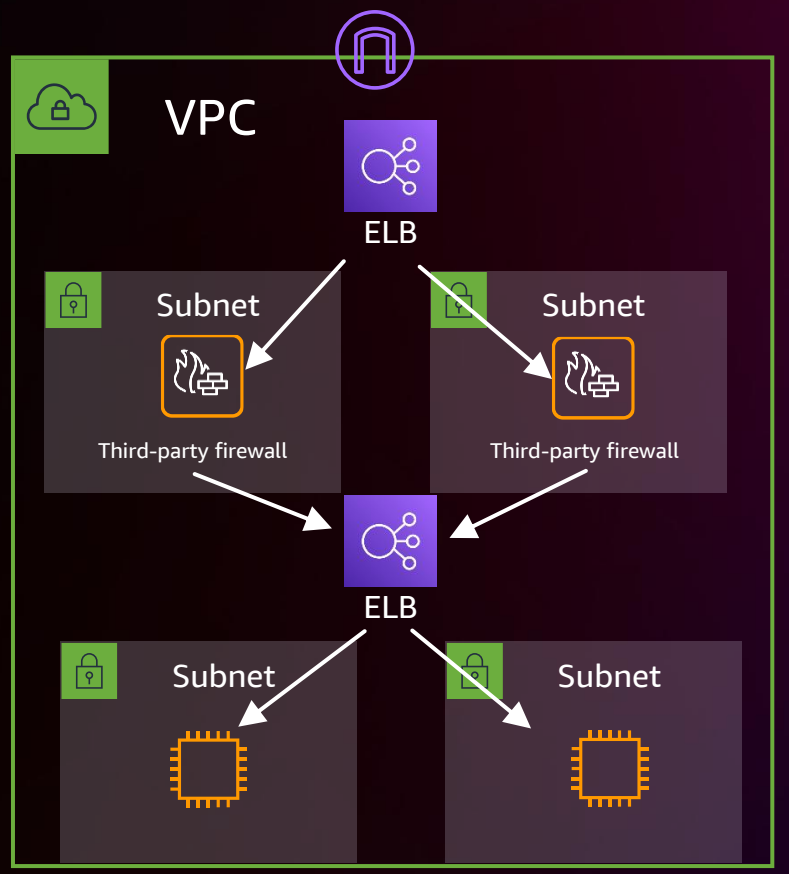
Inspection depth
Application layer

Data plane
Distributed

Management
Centralized via FMS



ELB sandwich



Supported app
Any

TLS decryption
True

Inspection depth
Application layer

Data plane
Distributed – new firewalls required for each VPC

Management
Centralized using firewall vendor tools

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

Distributed VPC security integrations

Network Firewall

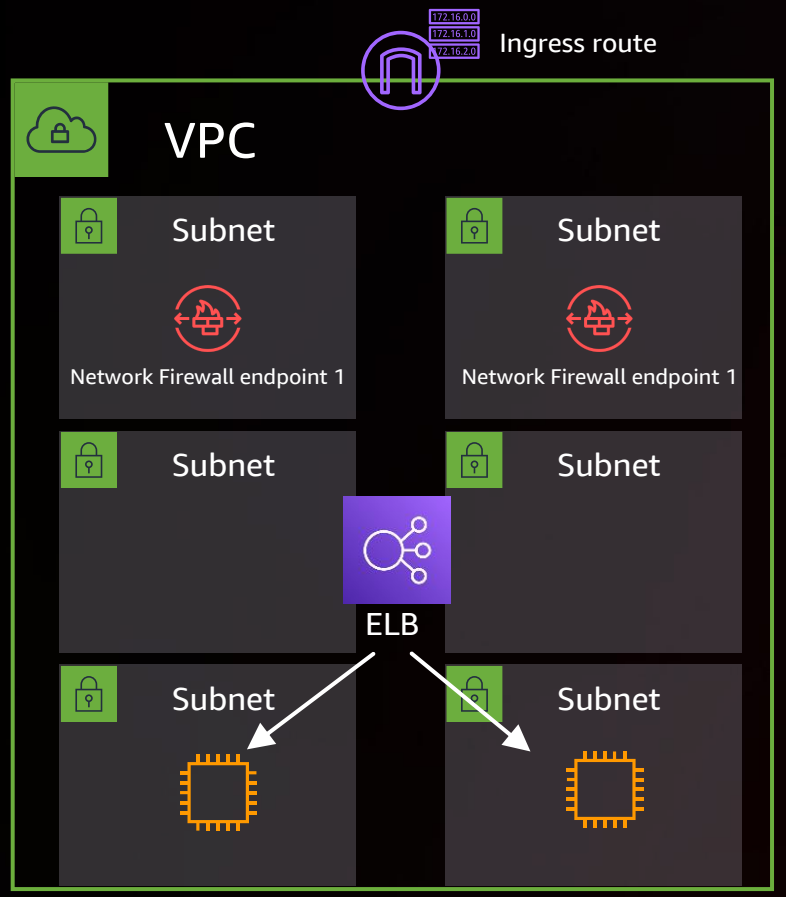
Supported app
Any

TLS decryption
False

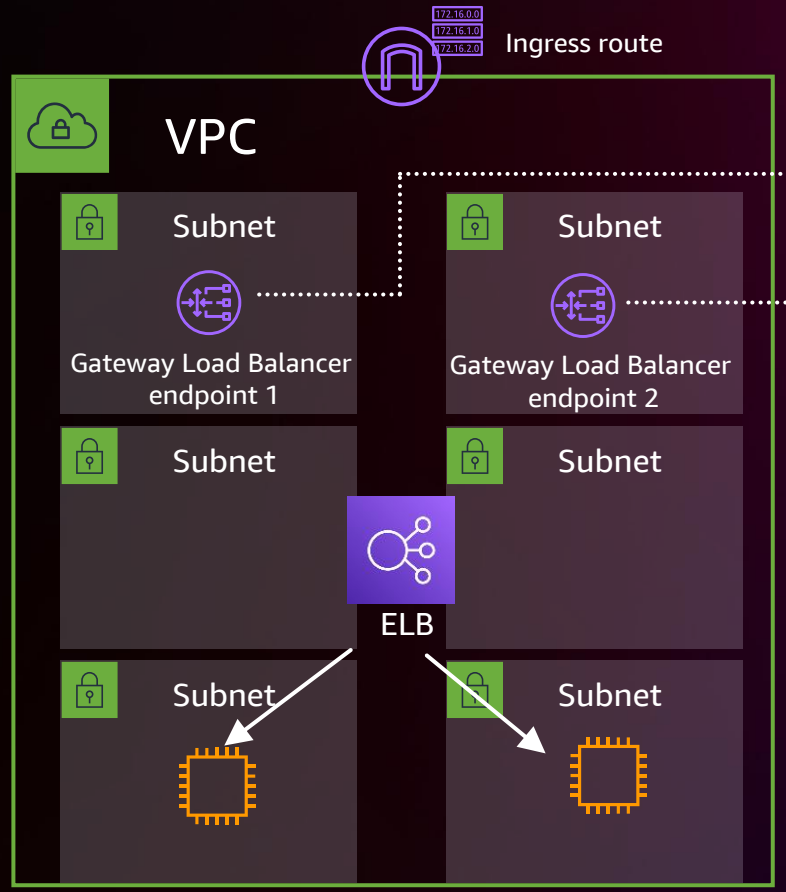
Inspection depth
Application layer if not encrypted

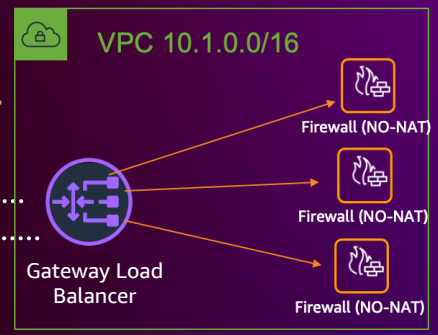
Data plane
Distributed

Management
Centralized via AWS Firewall Manager



Gateway Load Balancer





Supported app
Any

TLS decryption
Depends on firewall vendor

Inspection depth
Application layer if decryption is supported

Data plane
Distributed

Management
Centralized via firewall vendor tools

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

Centralized VPC security integrations

AWS WAF

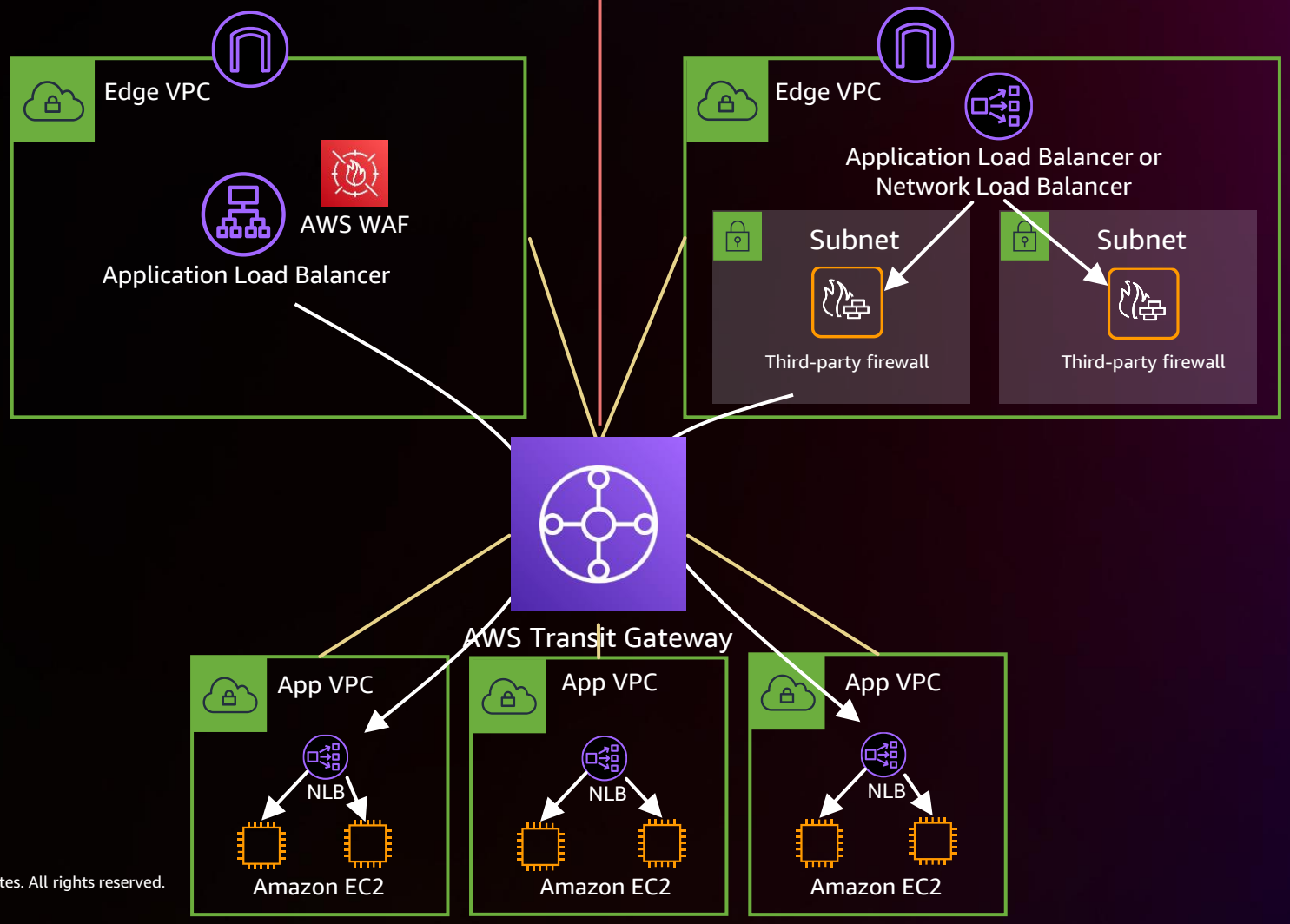
Considerations

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

ELB sandwich

Consideration

Third-party firewall should support targeting hostnames to allow both Network Load Balancer and Application Load Balancer in app VPCs



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

Centralized VPC security integrations

Network Firewall

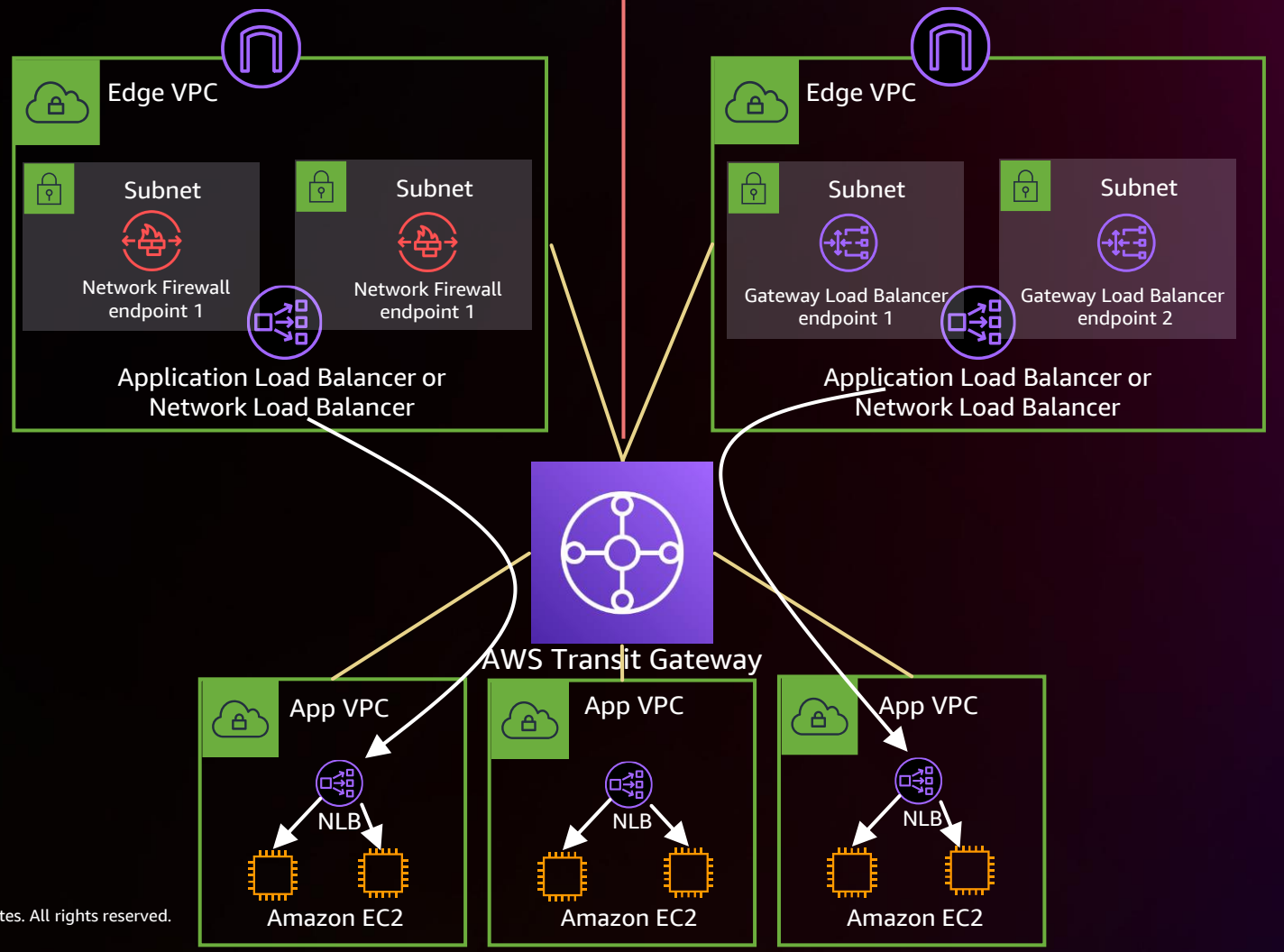
Considerations

- Edge VPC ELB can only target IPs, not hostnames
- App VPC ELB must use Network Load Balancer to provide a static IP to edge VPC ELB
- ELB can stop TLS, but Network Firewall cannot

Gateway Load Balancer

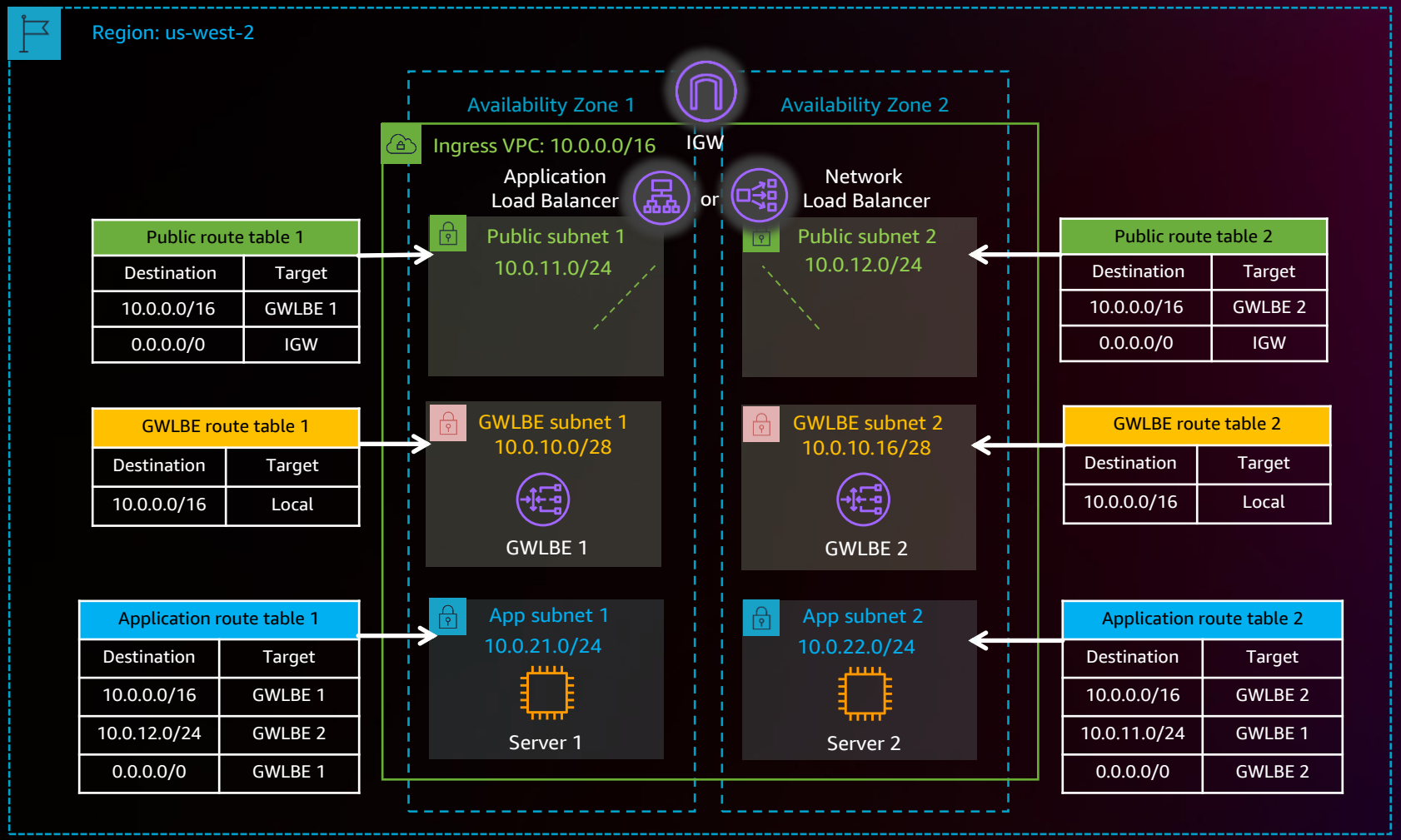
Considerations

- Edge VPC ELB can only target IPs, not hostnames
- App VPC ELB must use Network Load Balancer 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.

Distributed ELB to target: More specific routing



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

Thank you!

Rohit Aswani
linkedin.com/in/aswanirohit

Dhanil Parwani
linkedin.com/in/dhanil-parwani



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

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