AWS re:Invent

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

NET311-R2

Network architectures for ingress traffic inspection

Alexandra Huides
Senior Solutions Architect – Networking
AWS

Tom Adamski
Principal Solutions Architect – Networking
AWS

Design considerations

INBOUND INSPECTION CHECKLIST

Application type

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

Control plane & data plane

- Centralized
- Distributed

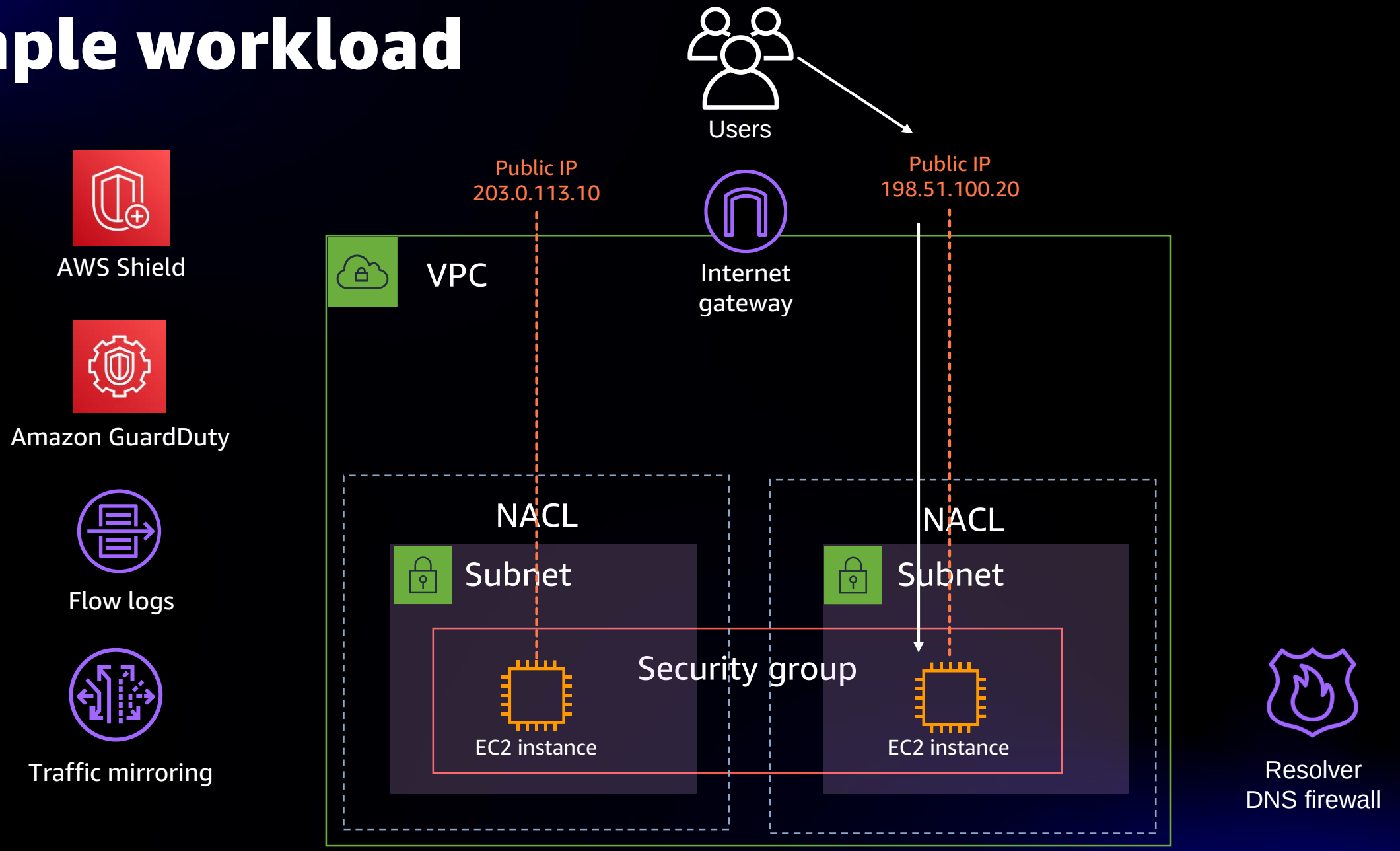
Inspection depth

- TCP/IP filtering
- Application-aware

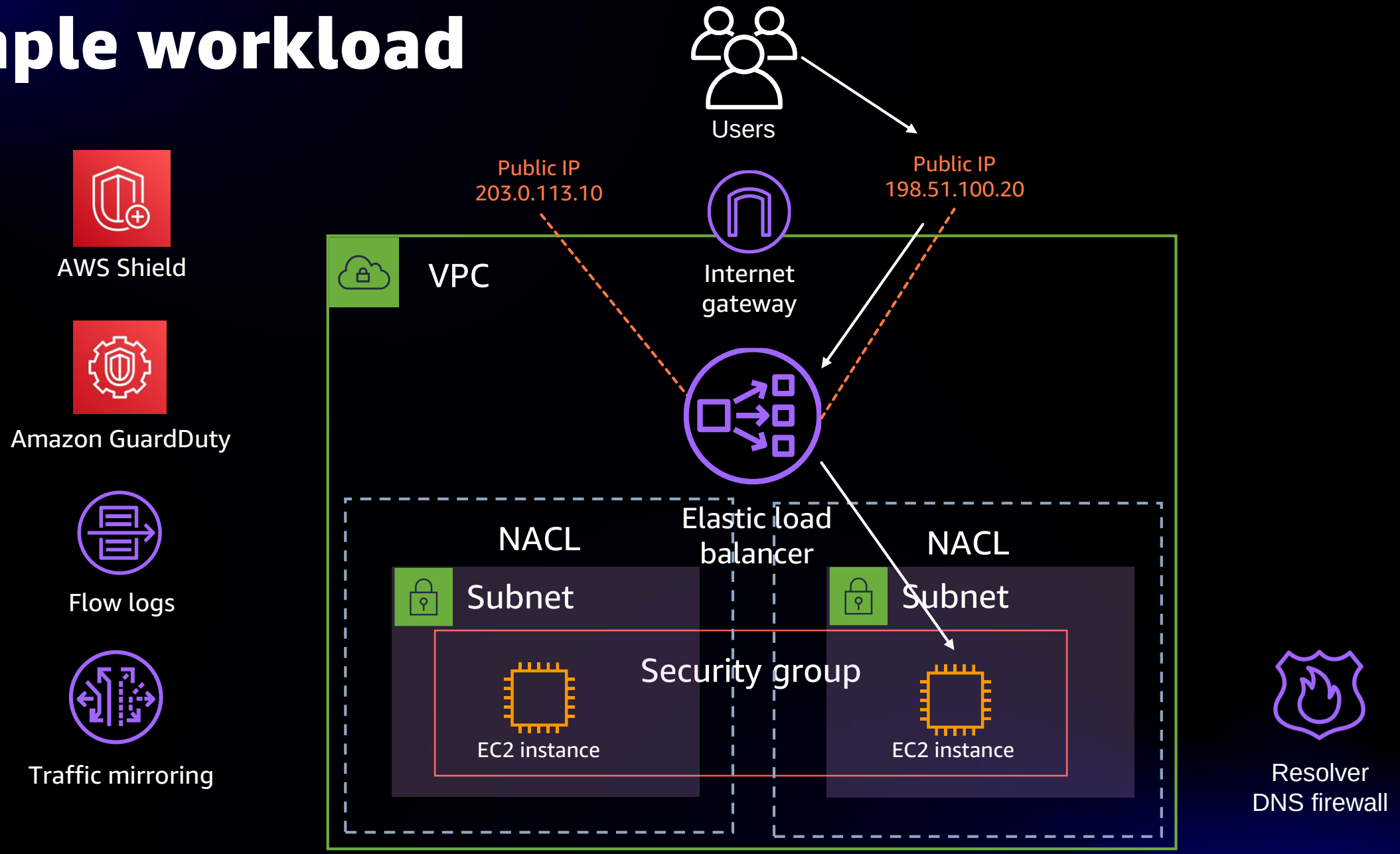
Scale

- One VPC
- Many VPCs

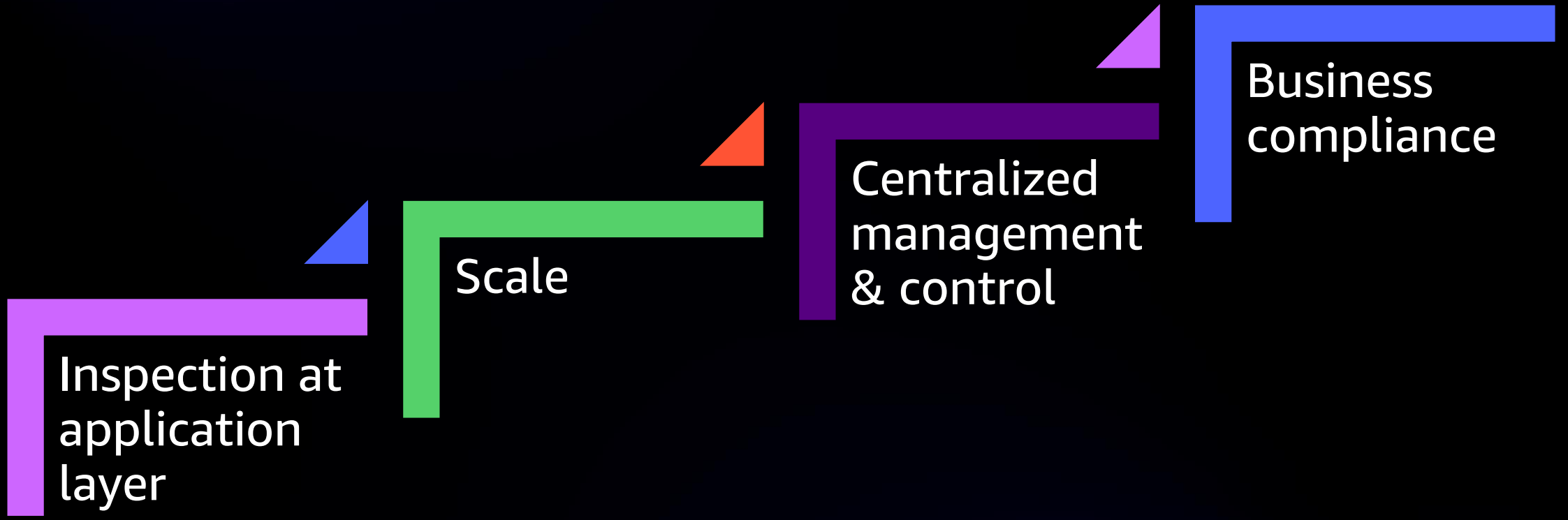
Sample workload



Sample workload



Why go beyond SG & NACLs for ingress?



Centralized versus distributed – Data plane models

Centralized

Internet access to multiple VPCs via a single VPC

Higher data processing costs, lower per-hour costs

Distributed

Each VPC has its own internet access

Lower data processing costs, higher per-hour costs

* Management / control plane can be centralized in both scenarios

Distributed VPC security integrations

AWS WAF

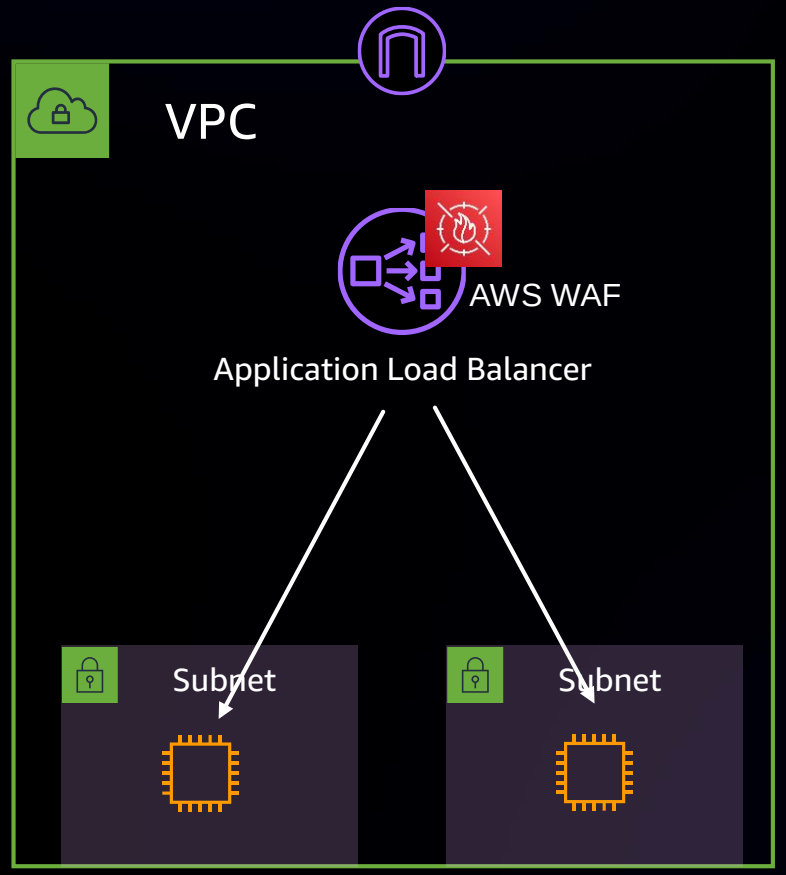
Supported app:
HTTP(S) only

TLS decryption:
True

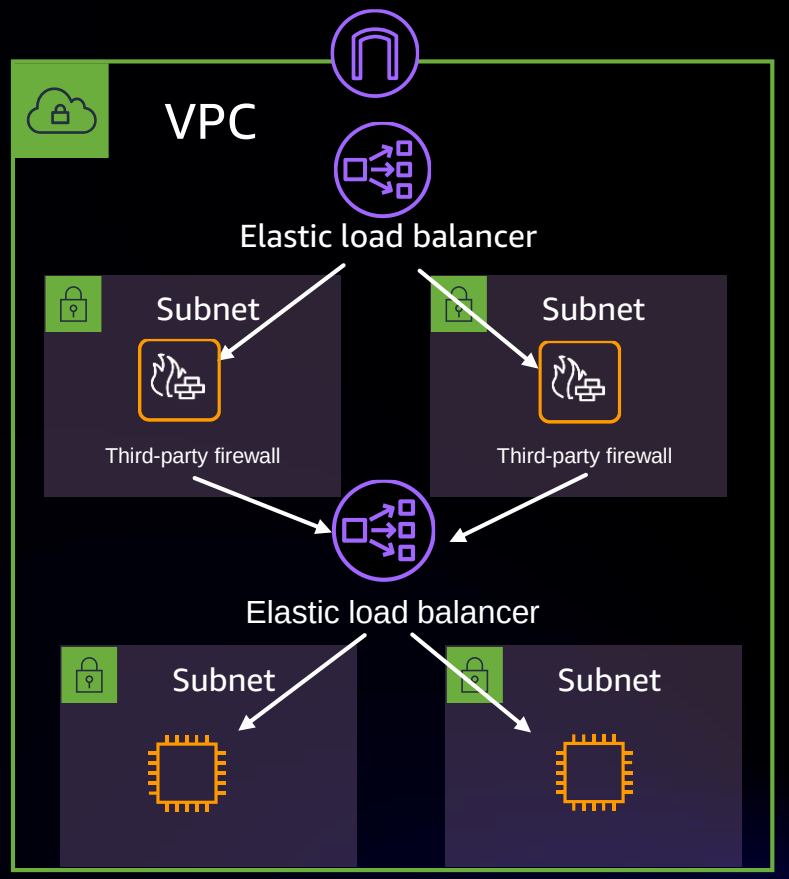
Inspection depth:
Application layer

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

Distributed VPC security integrations

AWS Network Firewall

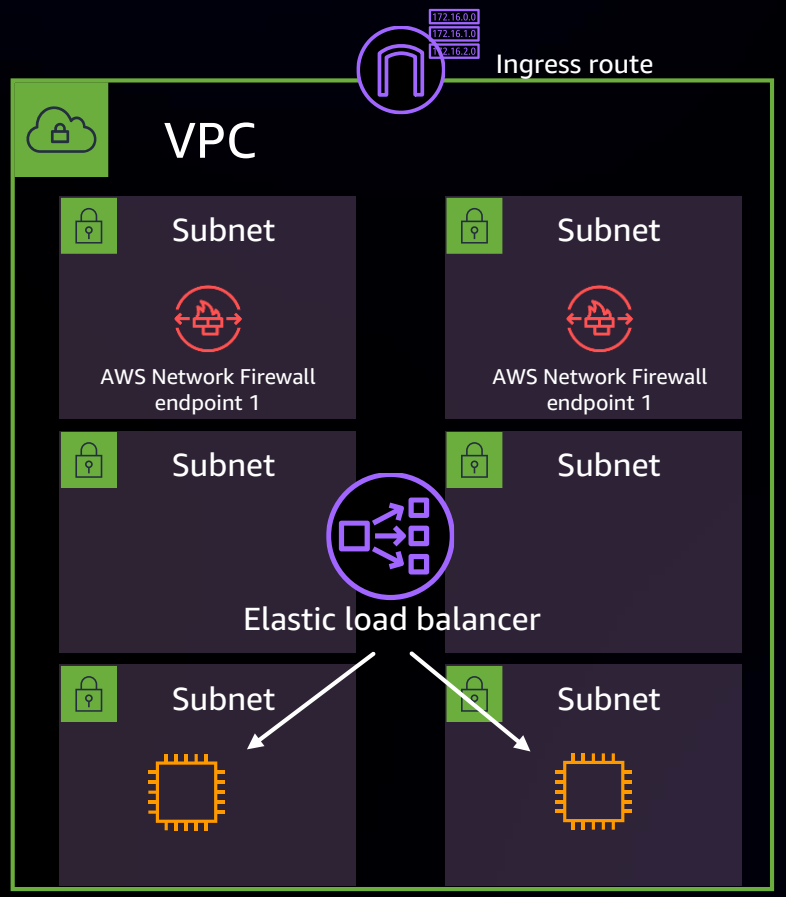
Supported app:
Any

TLS decryption:
False

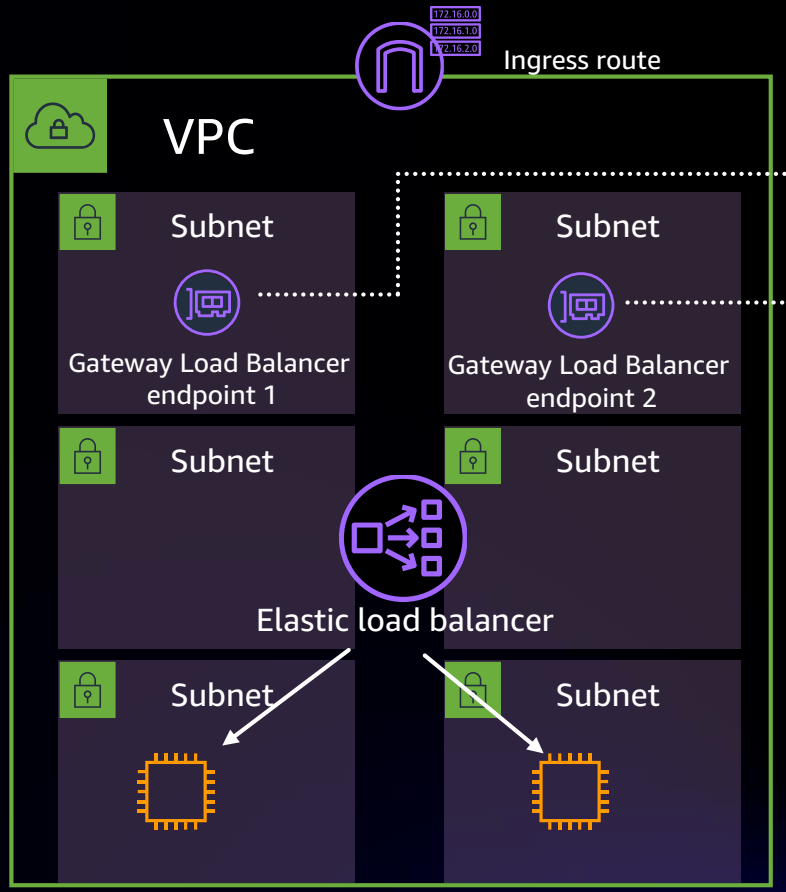
Inspection depth:
Application layer if not encrypted

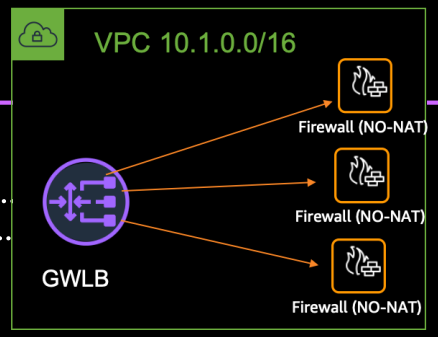
Data plane:
Distributed

Management:
Centralized via FMS



Gateway Load Balancer





Supported app:
Any

TLS decryption:
Depends on firewall vendor

Inspection depth:
Application layer if decryption supported

Data plane:
Distributed

Management:
Centralized via firewall vendor tools

aws

Centralized VPC security integrations

AWS WAF

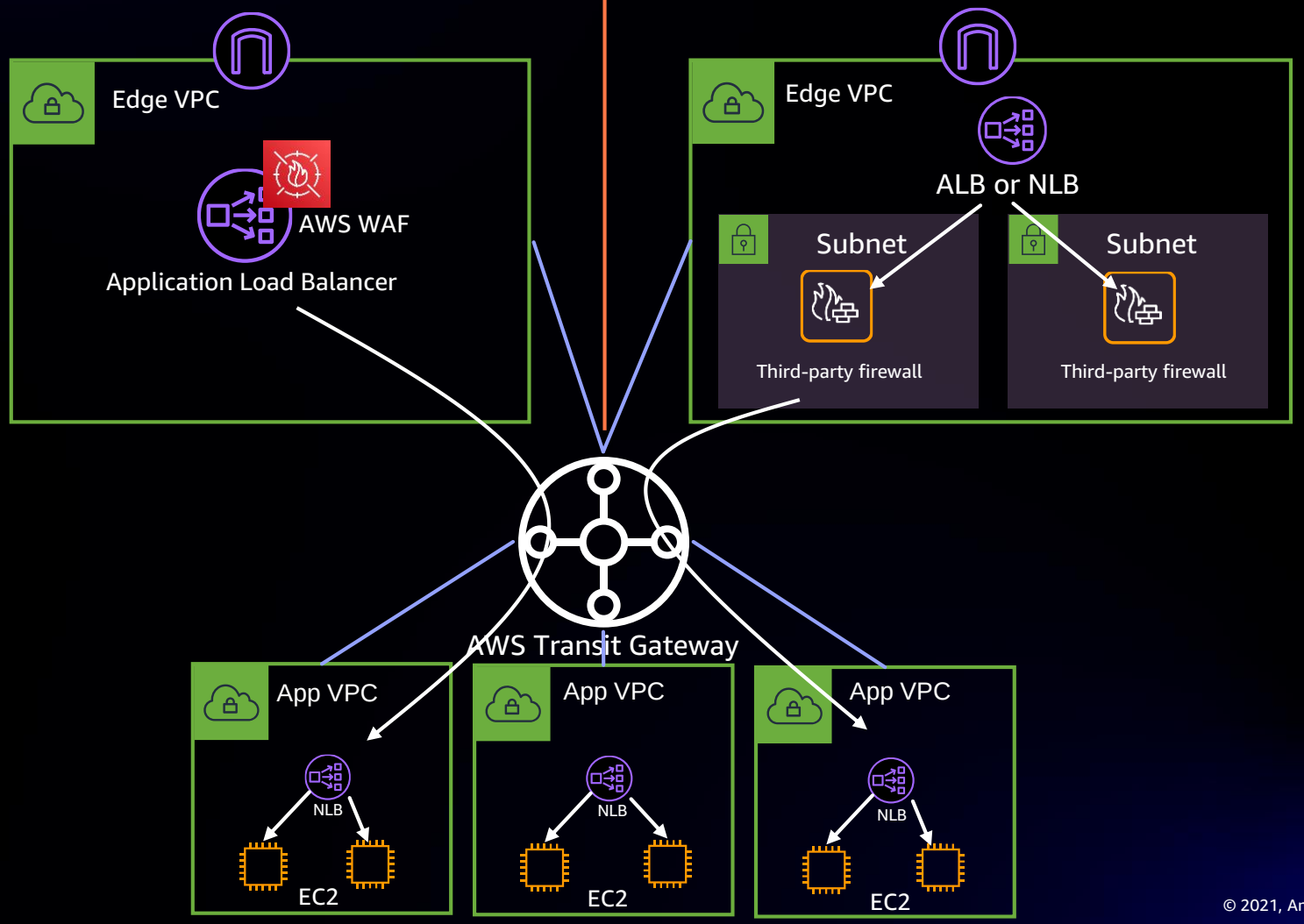
Considerations:

- Edge VPC ALB can only target IPs, not hostnames
- App VPC ELB must use 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



Centralized VPC security integrations

AWS Network Firewall

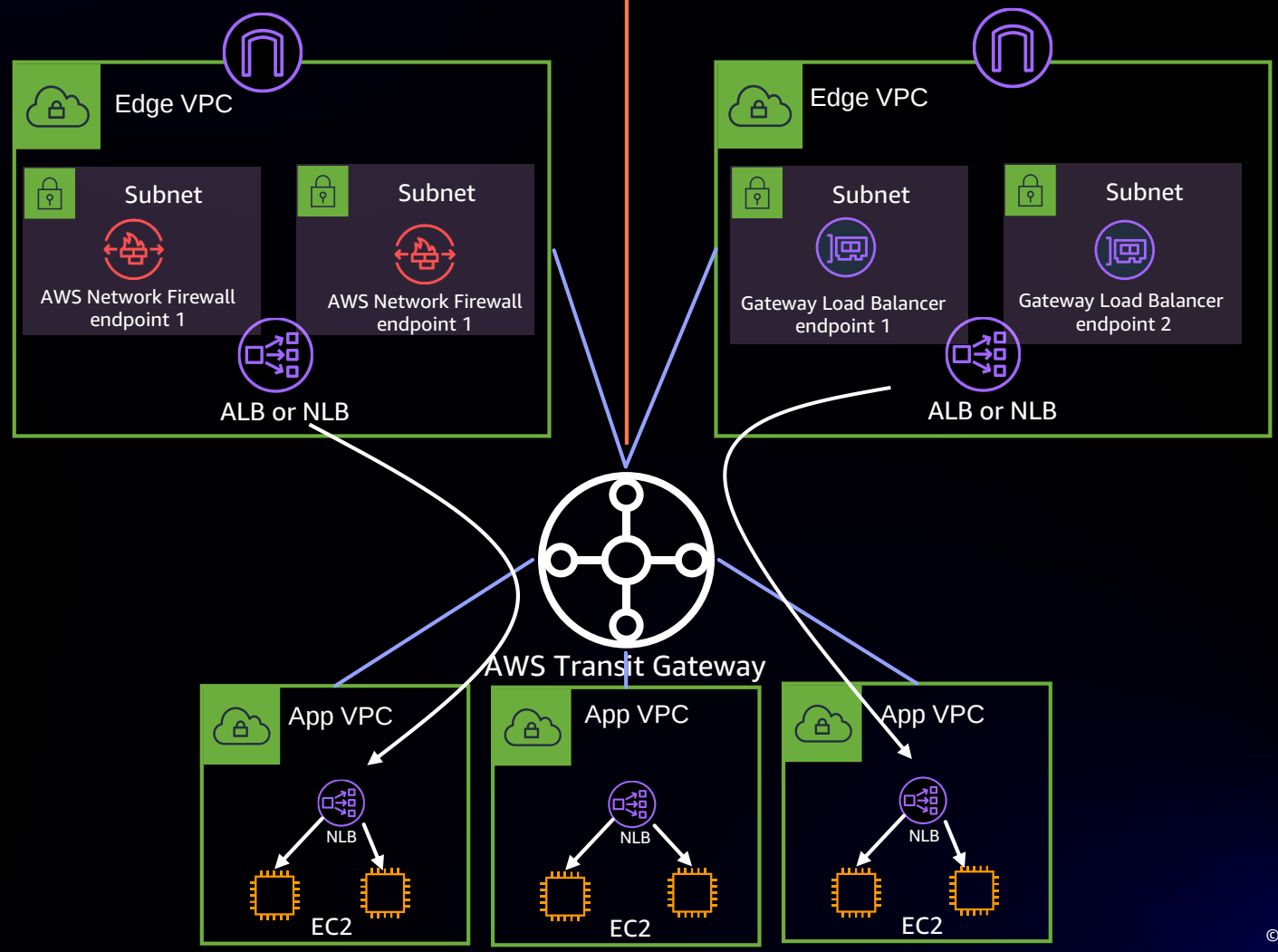
Considerations:

- 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 ANF can not

Gateway Load Balancer

Considerations:

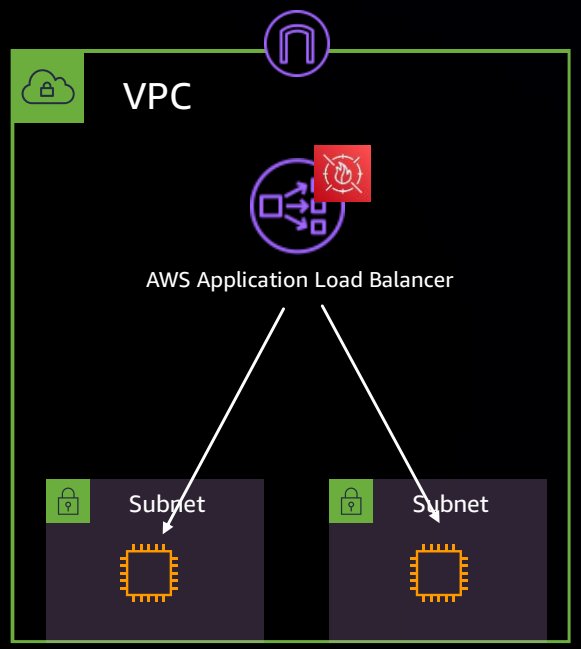
- Edge VPC ELB can only target IPs, not hostnames
- App VPC ELB must use NLB to provide a static IP as target for the Edge VPC ELB
- For TLS decryption, the firewalls behind the Gateway Load Balancer need a valid certificate, which can only be created outside of ACM



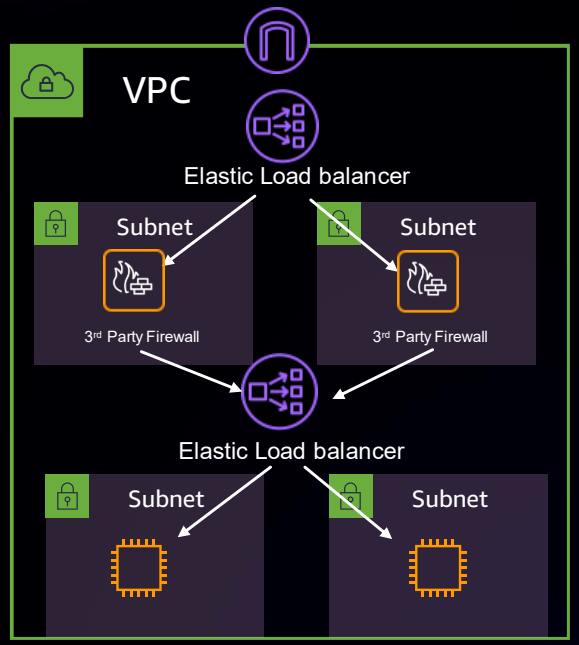
Use case example 1

Application type	Control plane & data plane	Inspection depth
HTTPS	Distributed	Application-aware

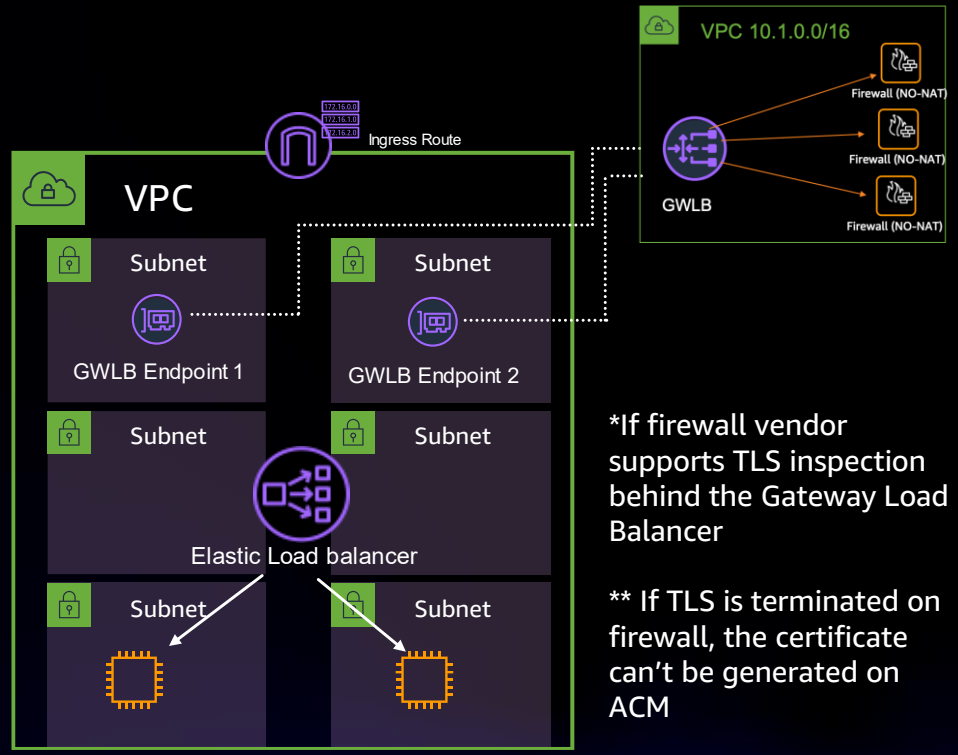
AWS WAF



ELB SANDWICH



Gateway Load Balancer

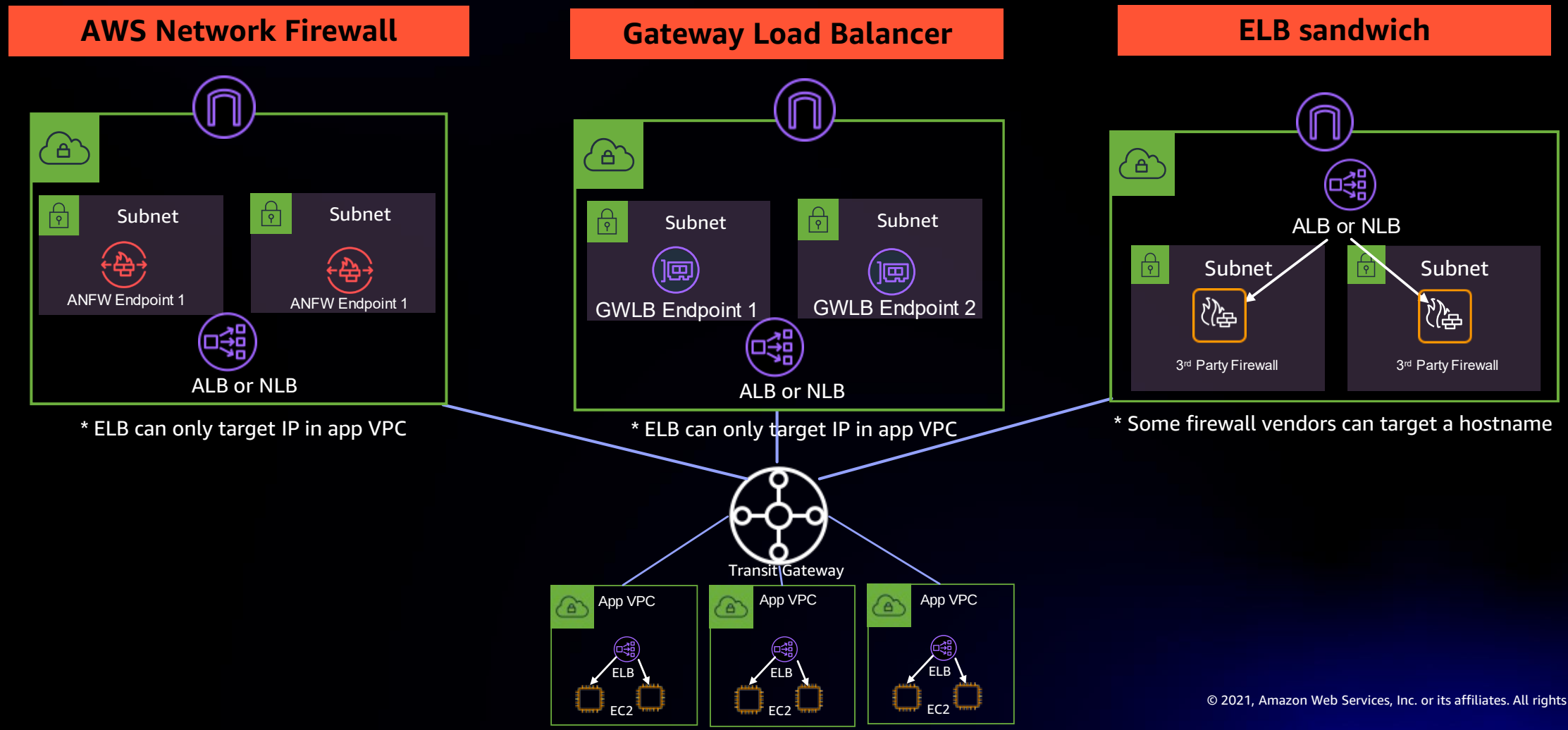


*If firewall vendor supports TLS inspection behind the Gateway Load Balancer

** If TLS is terminated on firewall, the certificate can't be generated on ACM

Use case example 2

Application type	Control plane & data plane	Inspection depth
TCP [non-HTTP(S)]	Centralized	Network



Thank you!

Alexandra Huides
linkedin.com/in/rodicaalexandrahuides

Tom Adamski
linkedin.com/in/tomadamski83