

AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

N I S 3 4 1

Managing multi-Region & multi-account AWS Network Firewall resources

Pablo Sánchez Carmona

Network Specialist Solutions Architect
AWS

Andy Taylor

Network Specialist Solutions Architect
AWS



Today's agenda

Why are we here? The use case

What are we going to build? The architecture

Let's build!

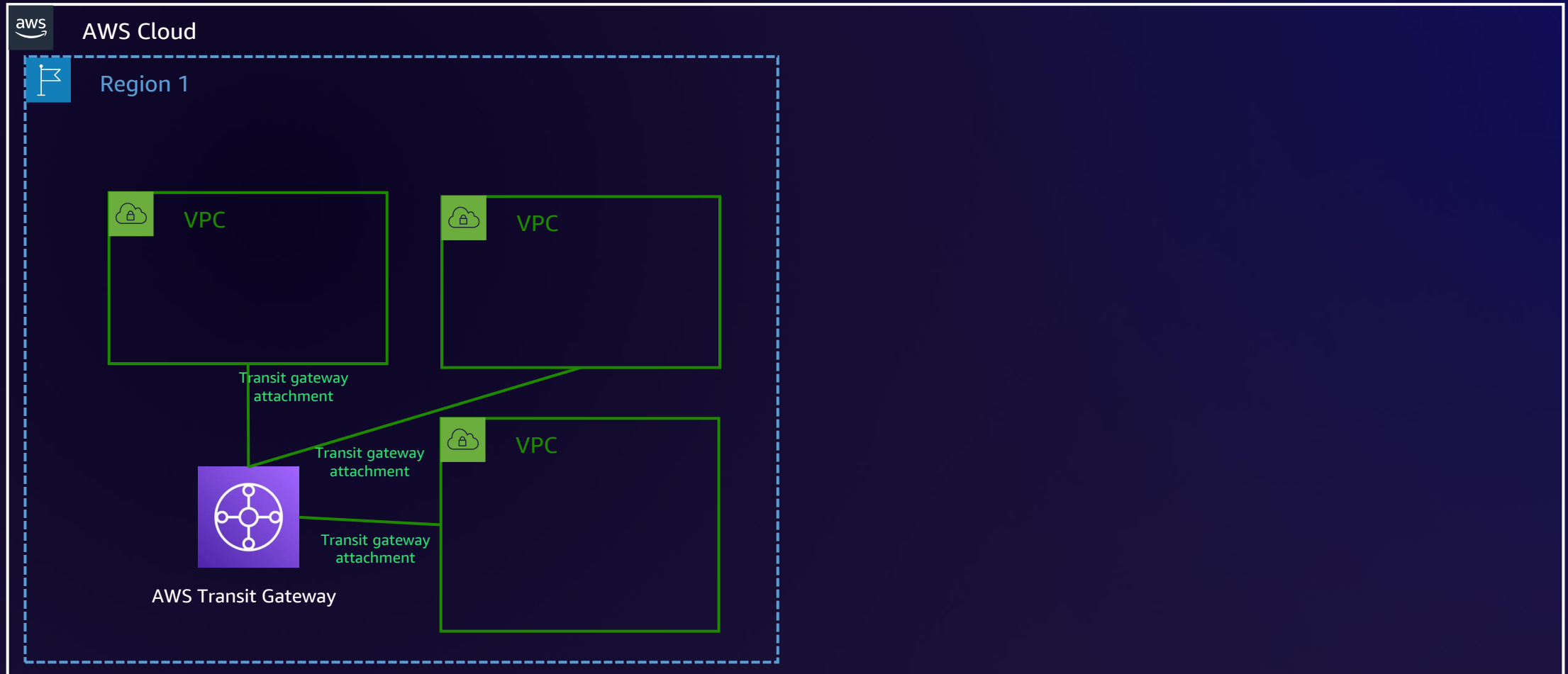
Things to consider and next steps

Today's session

- Networking, level 300
- Infrastructure as code, level 200 – today will show Terraform
- No need for laptops, but we will share the code
- We don't want this to be a demo, we want this session to be an architecture chat . . . while we code it!

The challenge

Enforcing network security without adding complexity to solution development



The challenge

Enforcing network security without adding complexity to solution development



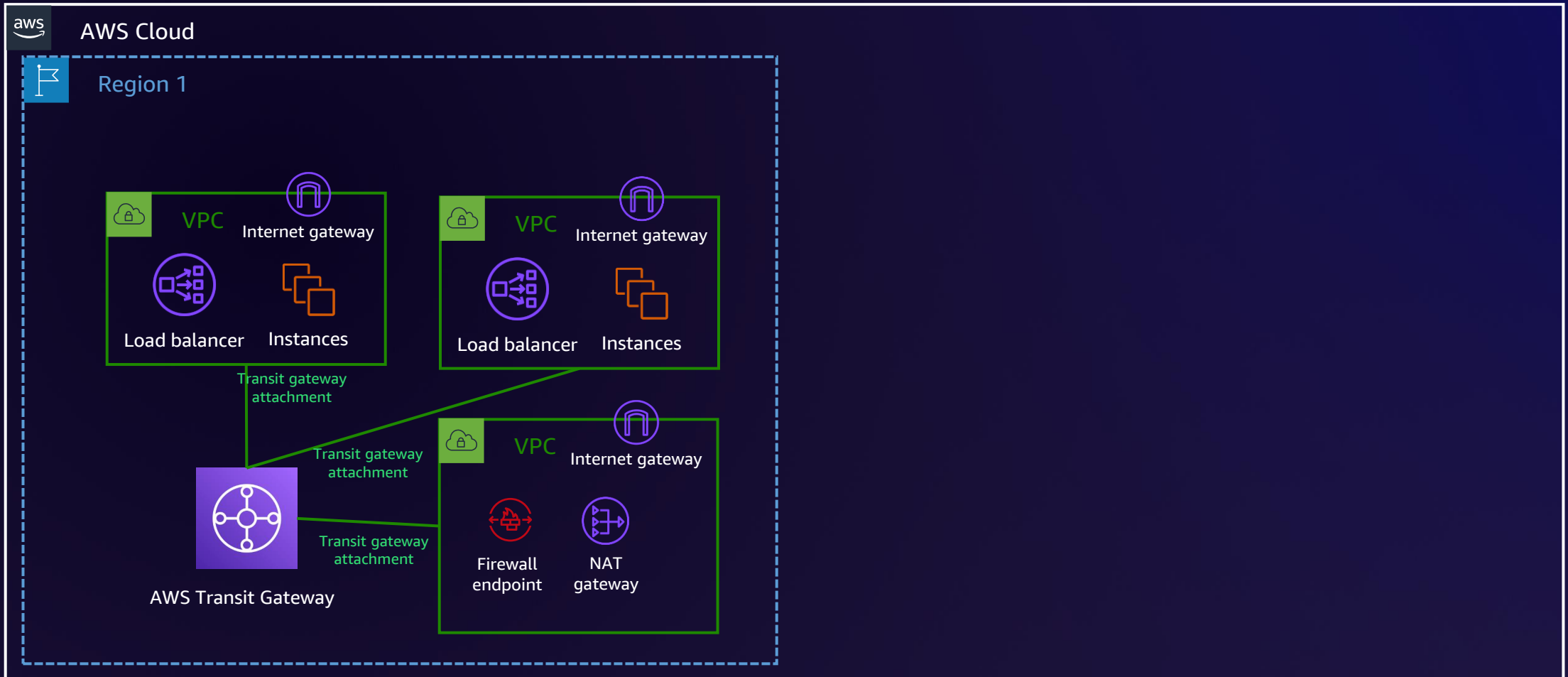
The challenge

Enforcing network security without adding complexity to solution development



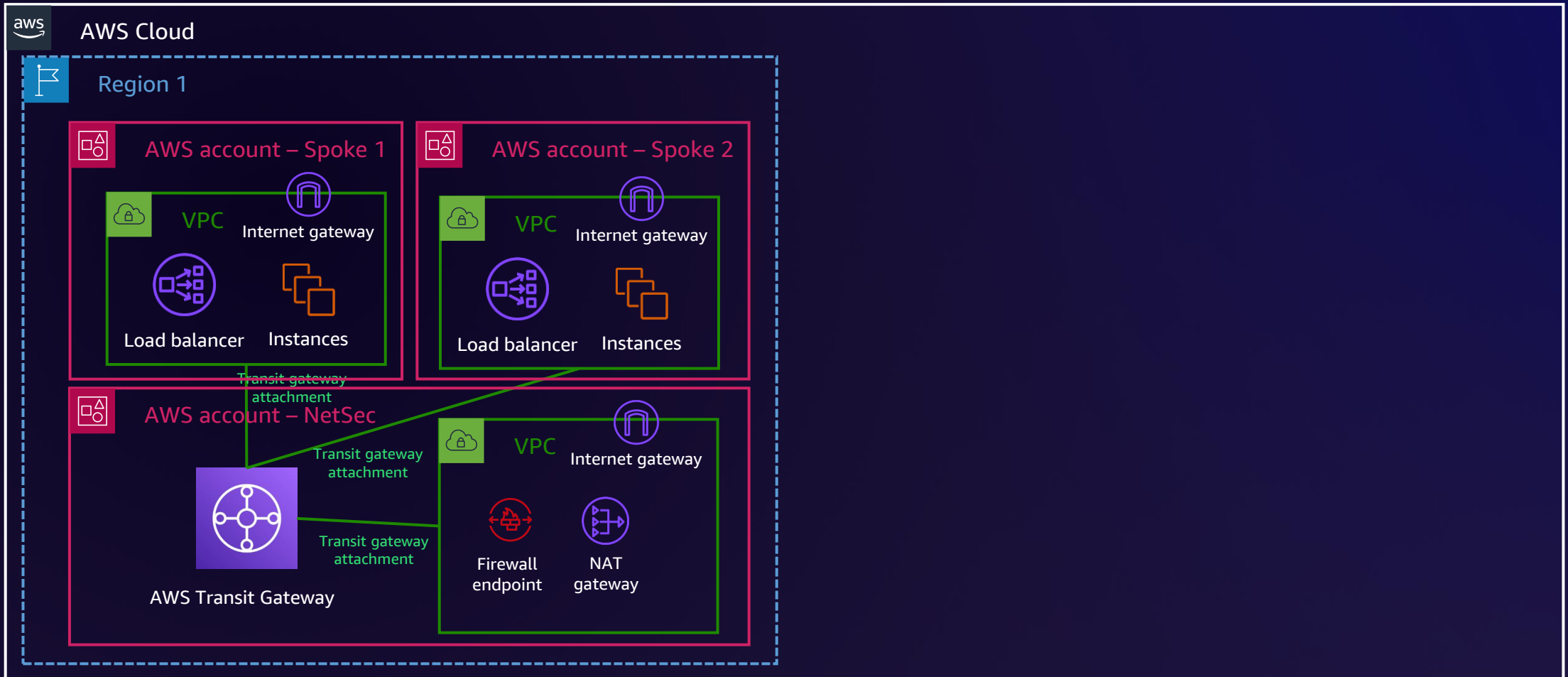
The challenge

Enforcing network security without adding complexity to solution development



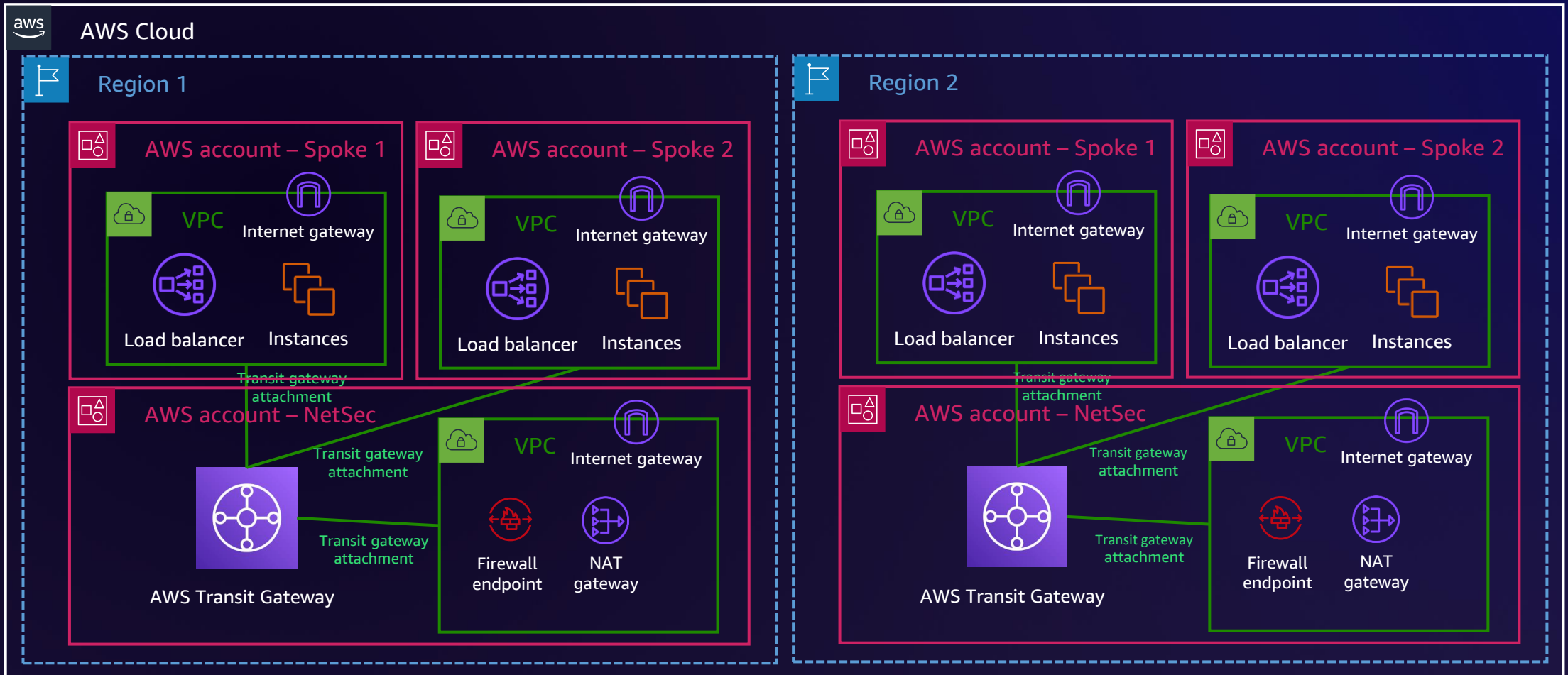
The challenge

Enforcing network security without adding complexity to solution development

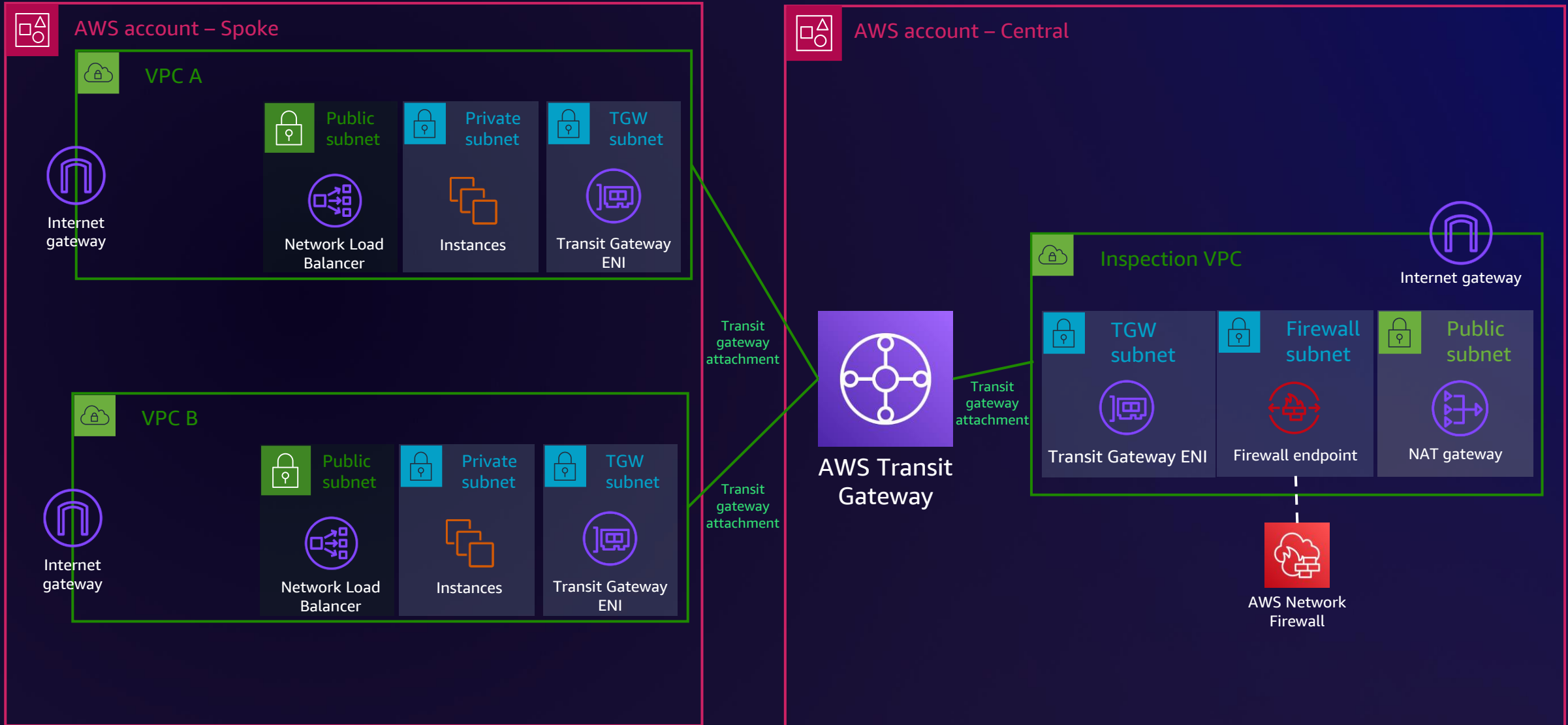


The challenge

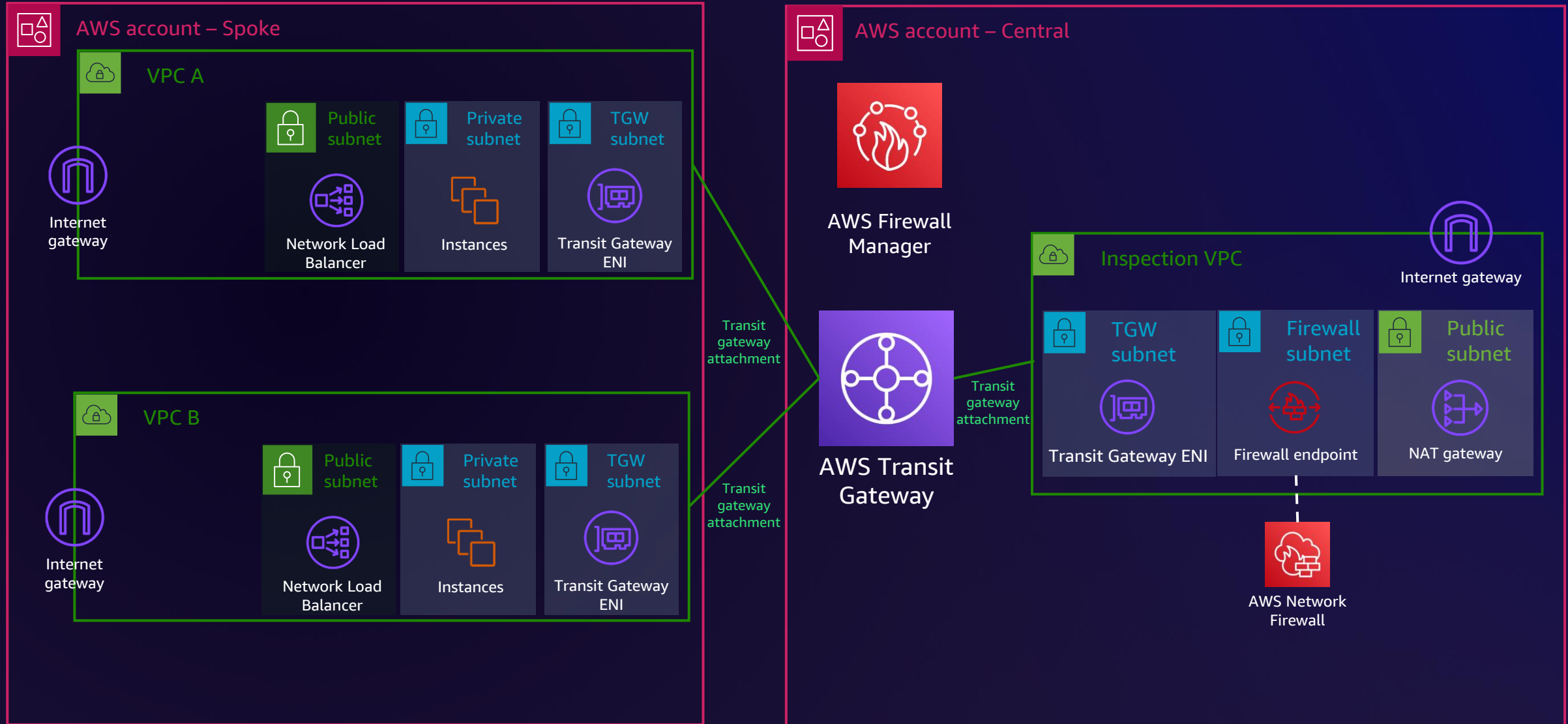
Enforcing network security without adding complexity to solution development



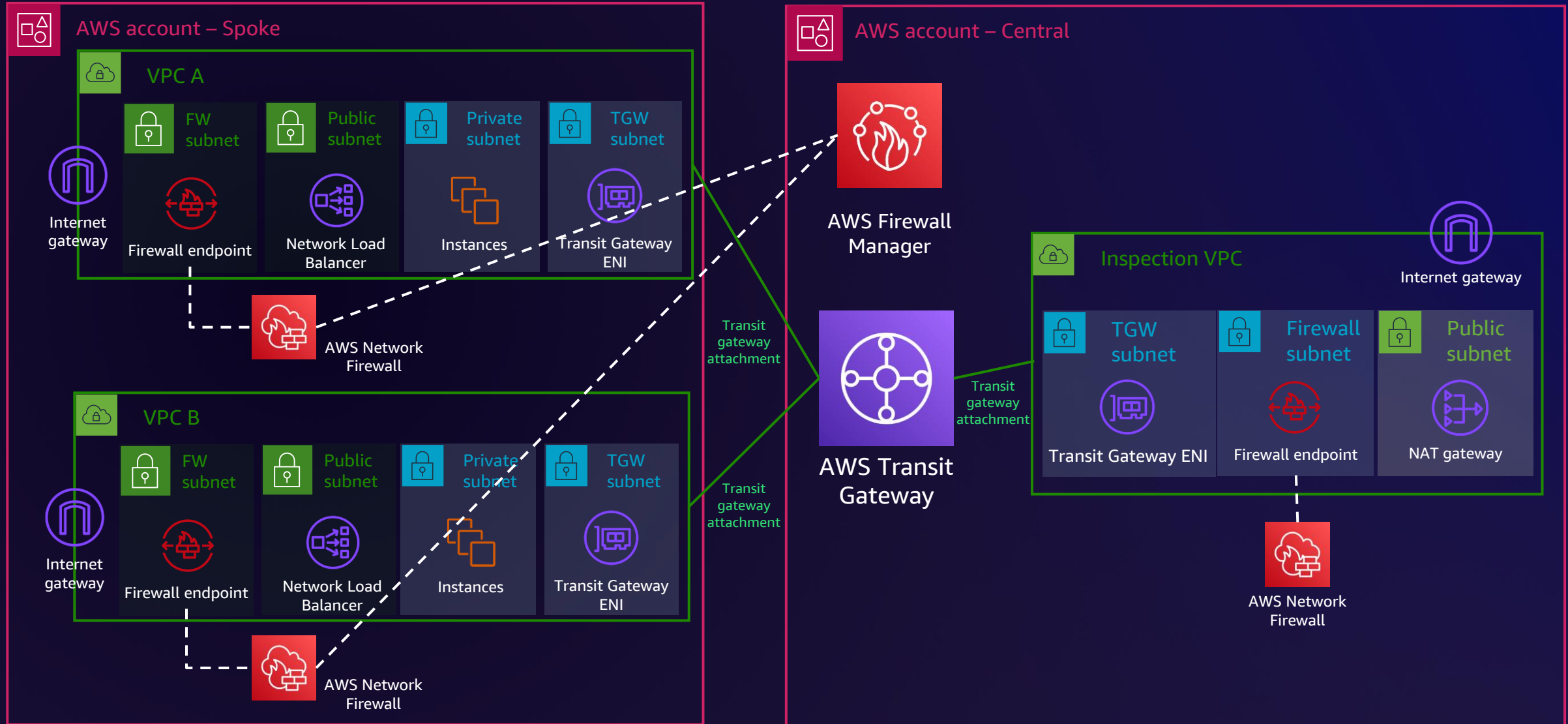
The architecture



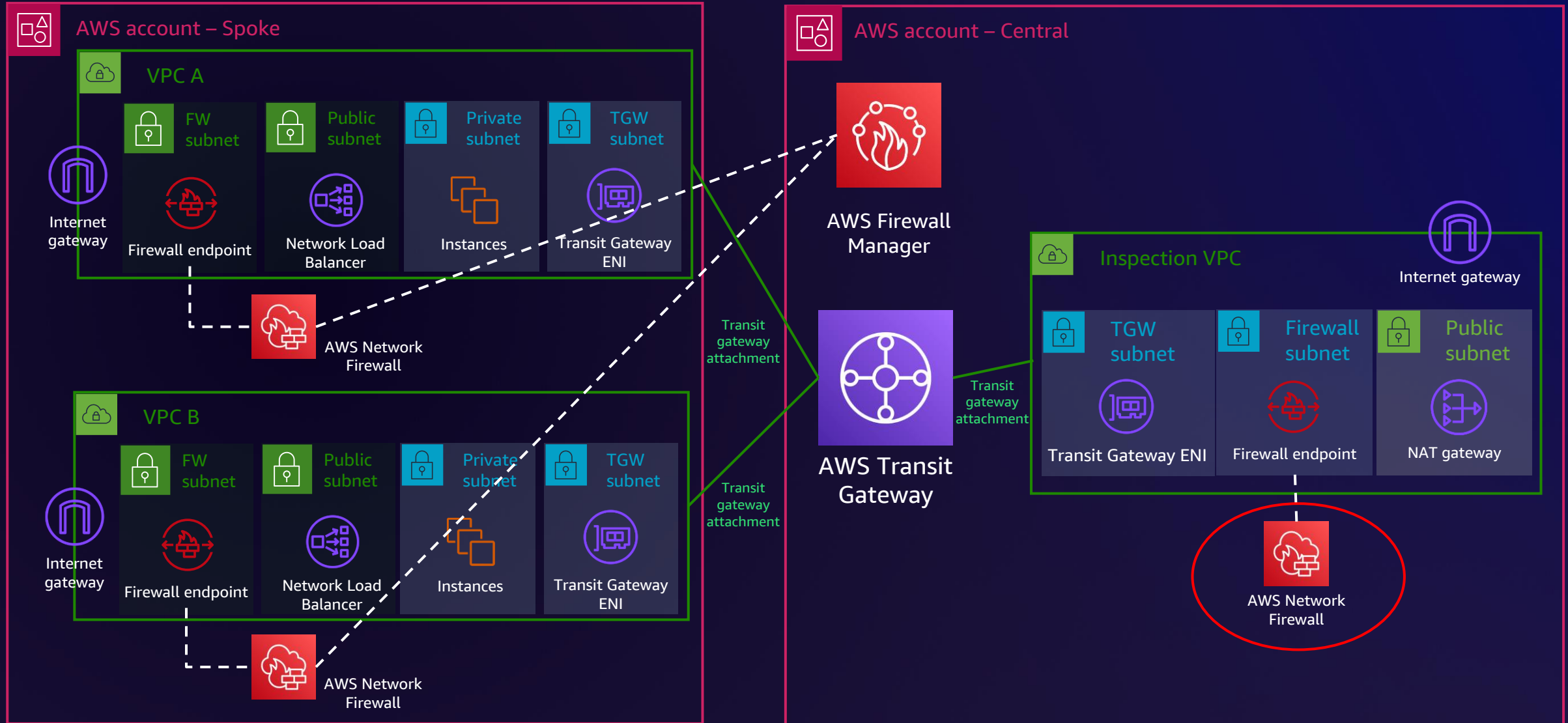
The architecture



The architecture



The architecture



Code time!

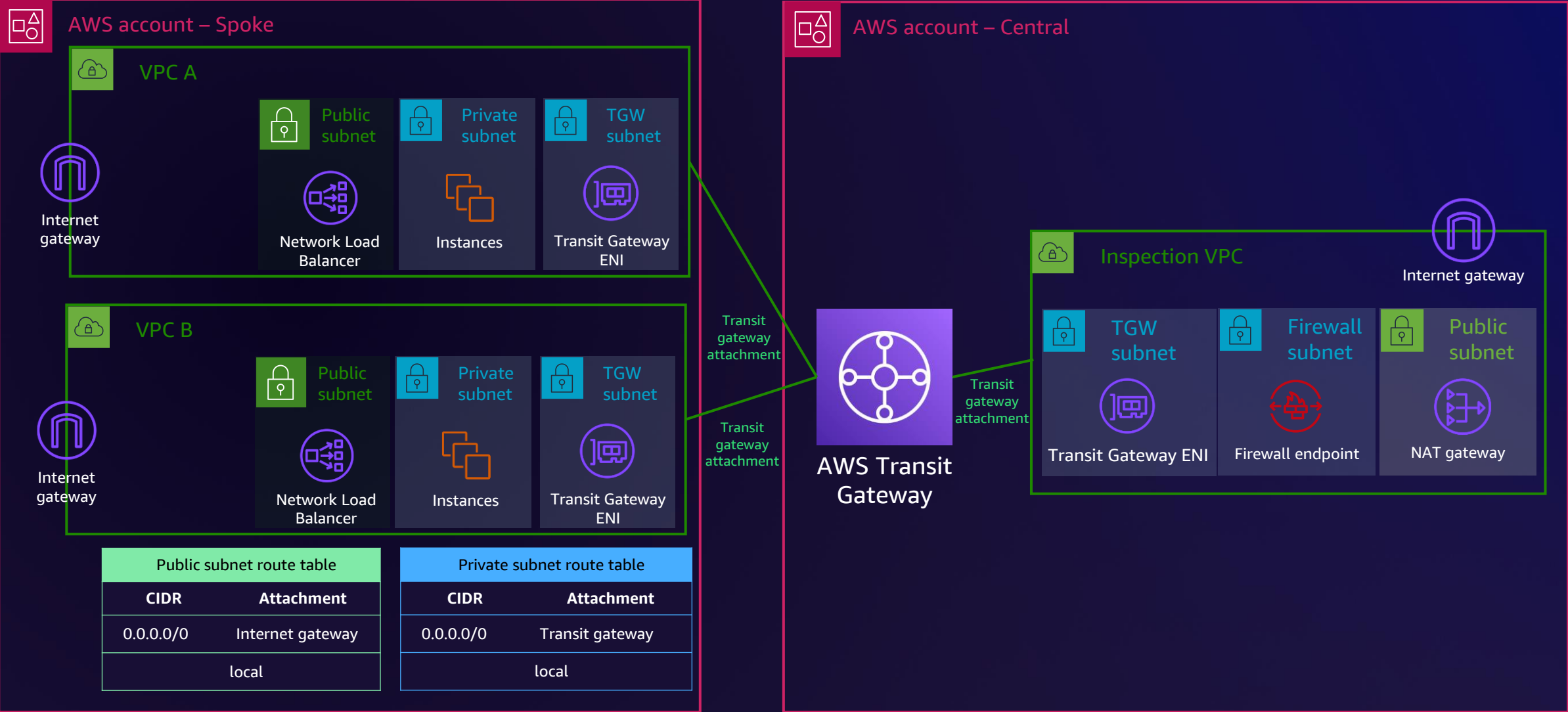


Today's code

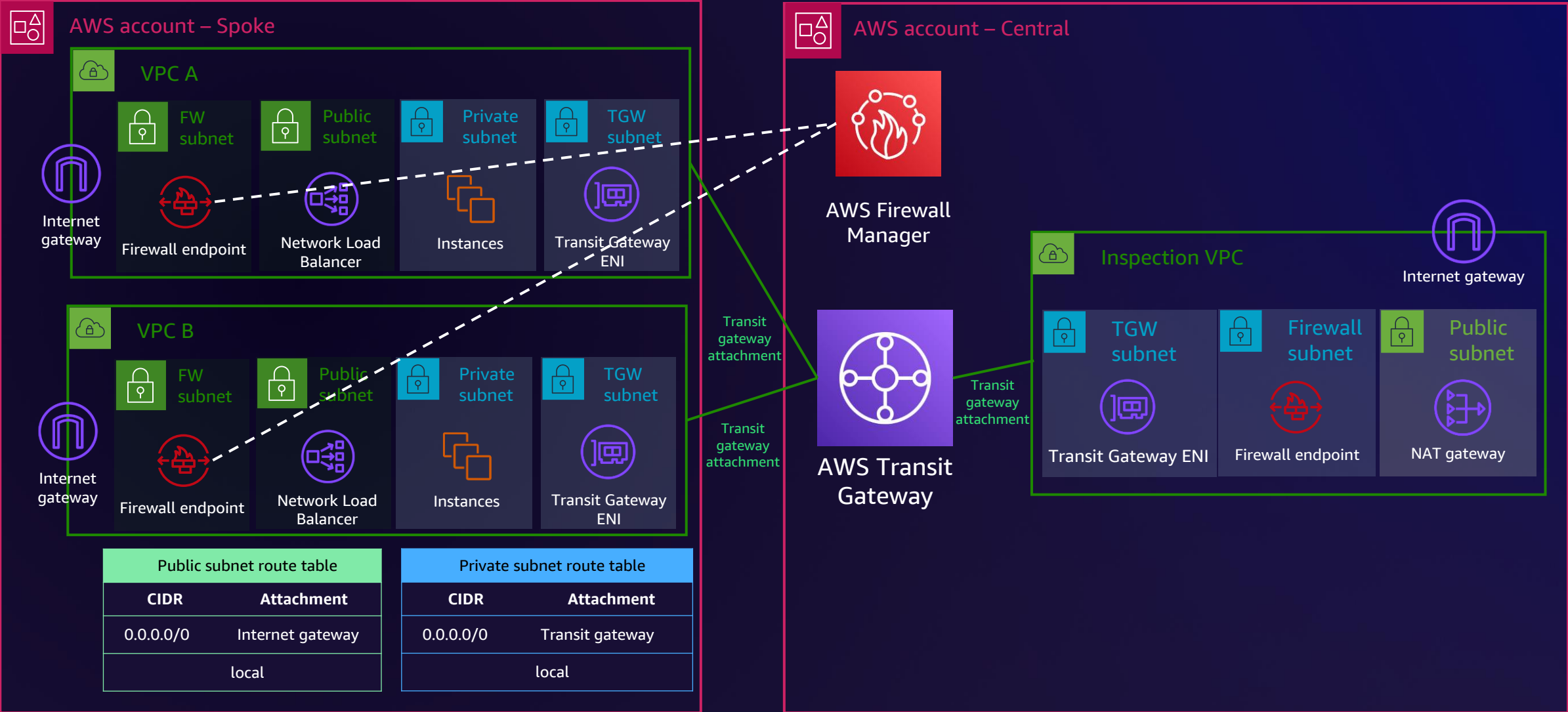


<https://shorturl.at/fsQU1>

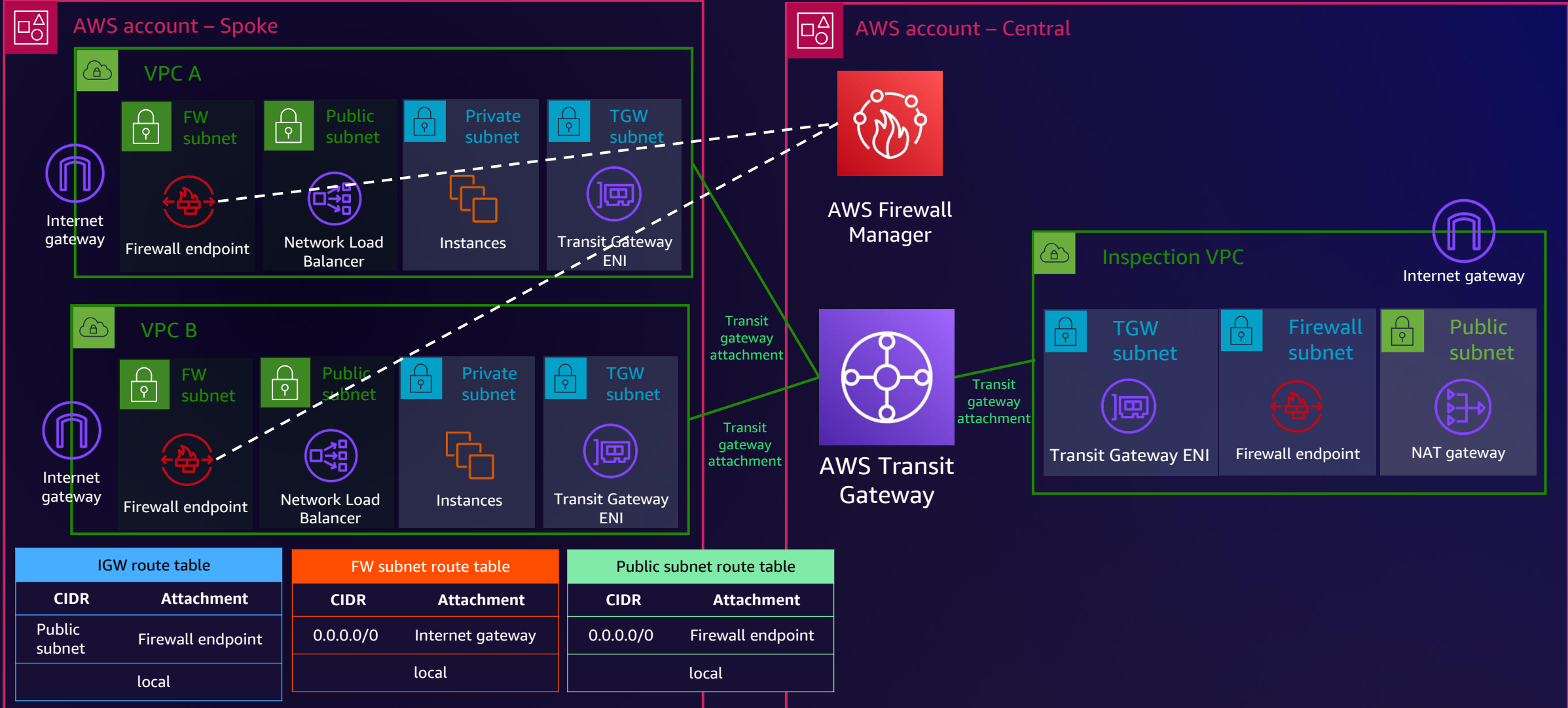
Initial state



Step 1 – Creating the AWS Firewall Manager policy



Step 2 – Creating VPC routes in spoke accounts



Things to consider and next steps

- What about multiple AWS Regions?
- Inbound traffic and Application Load Balancer – why not AWS WAF?
- AWS Firewall Manager also manages security groups
- Who manages the VPC route configuration?
- And the Network Firewall resource that was not created with Firewall Manager?

Additional resources



Amazon VPC Terraform module

<https://registry.terraform.io/modules/aws-ia/vpc/aws/latest>



Hub and Spoke Terraform module

<https://registry.terraform.io/modules/aws-ia/network-hubandspoke/aws/latest>



AWS Network Firewall workshop

<https://catalog.workshops.aws/networkfirewall/en-US>



AWS Firewall Manager workshop

<https://catalog.workshops.aws/firewall-manager/en-US>



<https://shorturl.at/fsQU1>

Thank you!



Please complete
the session survey
in the mobile app