
AWS
re:Invent

NET306

Which inspection architecture is right for you?

Justin Davies

Principal Solutions Architect, Network Specialist

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What to expect: First half

Quick review on new services and functionality

- Amazon Route 53 resolver query logs
- AWS Gateway Load Balancer
- AWS Network Firewall



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What to expect: Second half

Top 3 architecture patterns for inspection

How the AWS Network Firewall and AWS Gateway Load Balancer help

New controls on the AWS Transit Gateway to simplify your architecture

”To centralize, or not to centralize, that is the question”

Justin Davies



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Visibility and control



The state of being able to see or be seen



A means of limiting or regulating something

Visibility



AWS Security Hub

Centrally view and manage security alerts and automate compliance checks



Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads



Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS



Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes



AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis



AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational/risk auditing of your AWS account



VPC Flow Logs & Full Traffic Mirroring

Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch logs

Control



AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications



AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS



AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security



AWS Network Firewall (New)

Highly available, scalable, cloud native firewall that allows you to quickly deploy and manage fine-grained inspection and enforcement for your VPCs



Amazon Virtual Private Cloud (Amazon VPC)/AWS Transit Gateway routing tables / Security groups

Logically isolated section of AWS where you can launch resources in a virtual network that you define



AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network



AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems

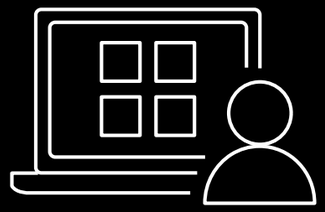
Amazon Route 53 resolver query logs

Client: Where is api.anycompany.com?



Resolver: Here is the answer, and
I logged your request and my response!

Amazon Route 53 resolver query logs



Specify a name for your query logging configuration



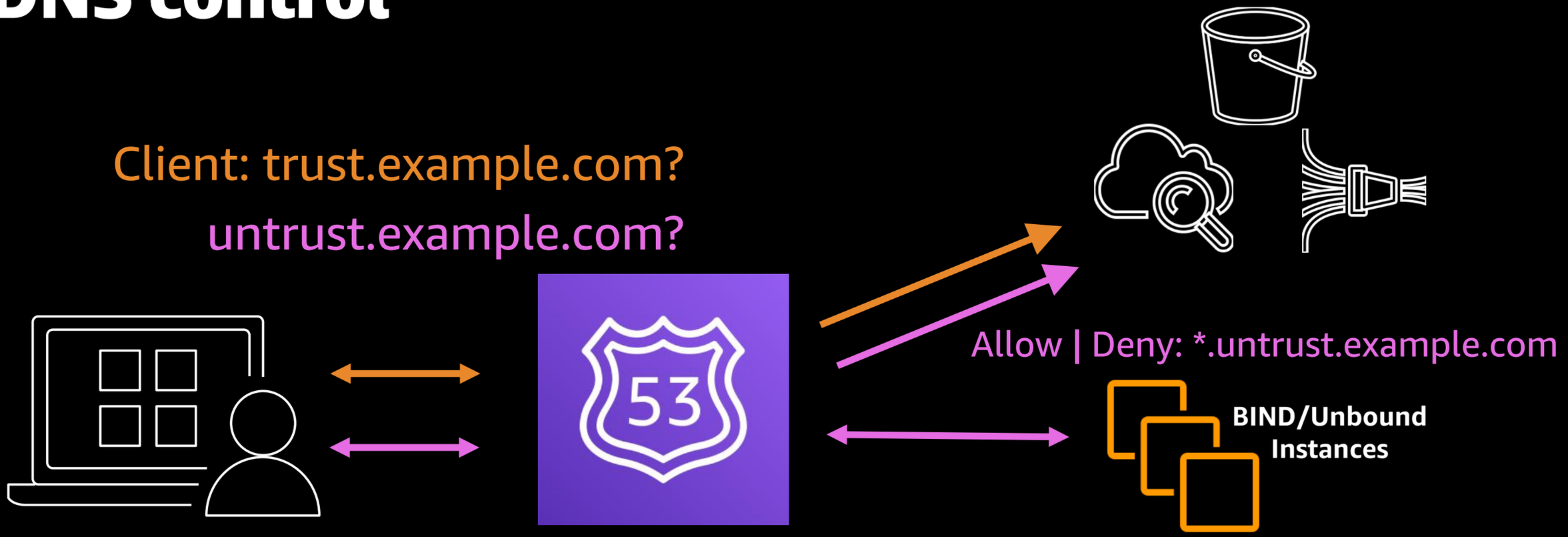
Create a destination target for your logs

- S3 bucket
- Log group
- Kinesis Data Firehose



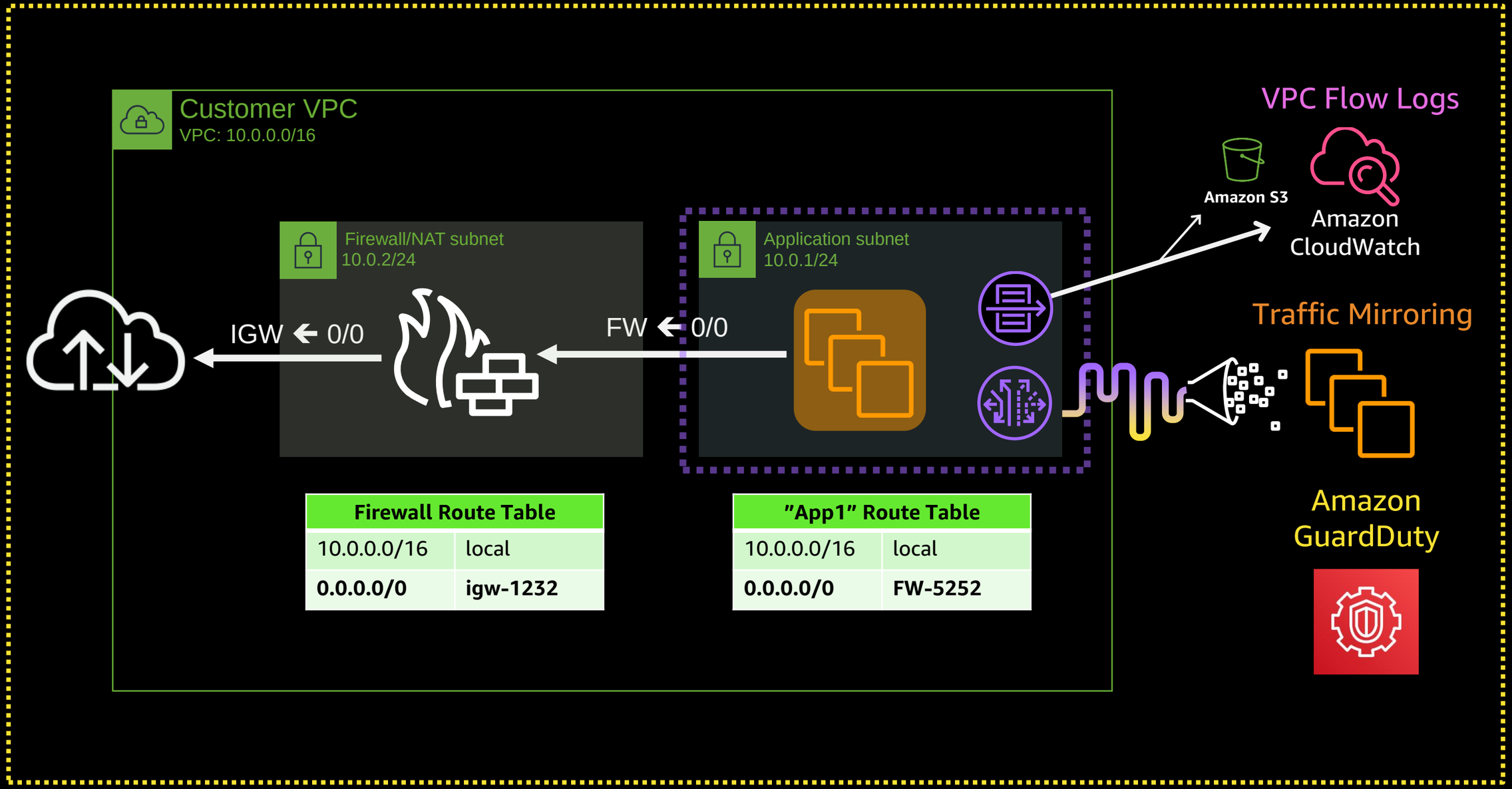
Select the VPCs you wish to log queries for

DNS control

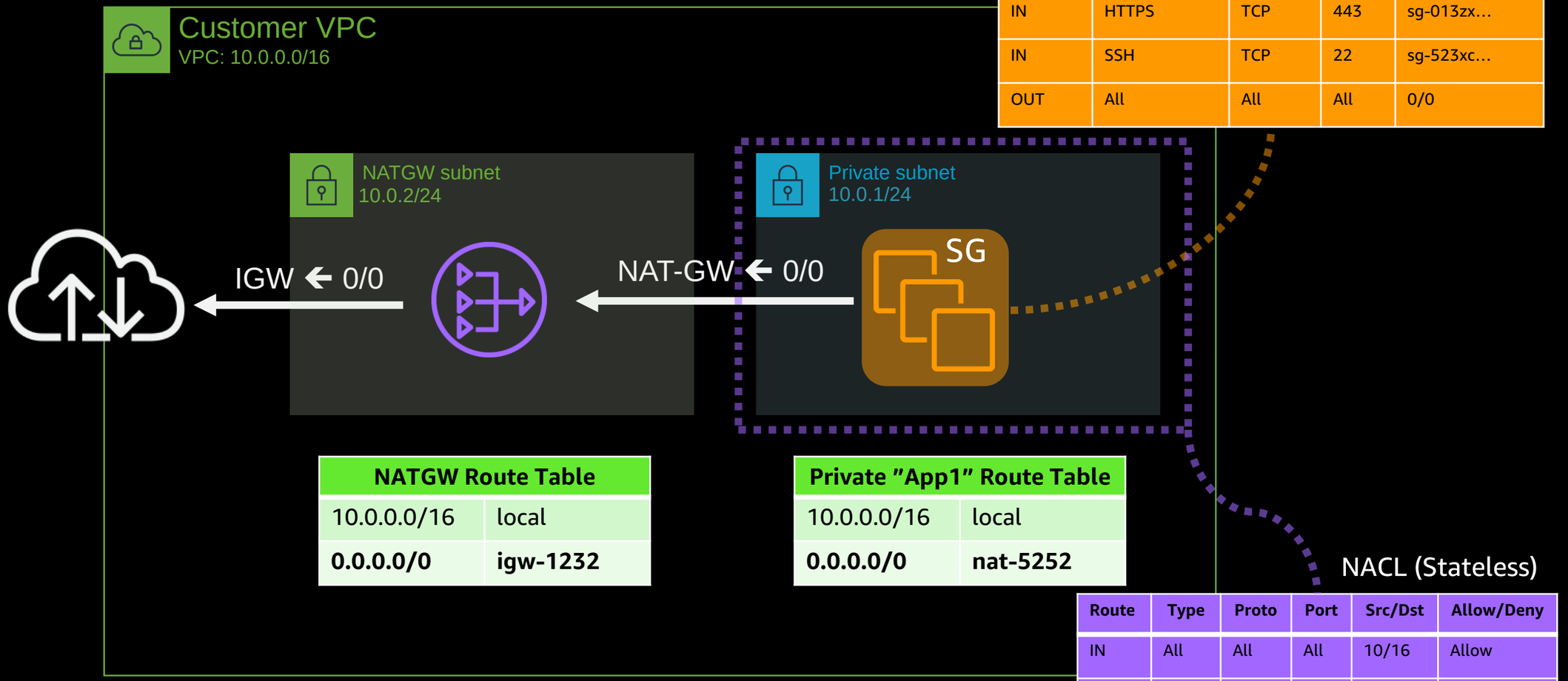


1. Log everything
2. Answer *.trust.example.com directly
3. Forward “untrust” for further inspection

Inline/active vs. out-of-band/passive



I want more



Security Groups (Statefull)

Route	Type	Proto	Port	Src/Dst
IN	HTTPS	TCP	443	sg-013zx…
IN	SSH	TCP	22	sg-523xc…
OUT	All	All	All	0/0

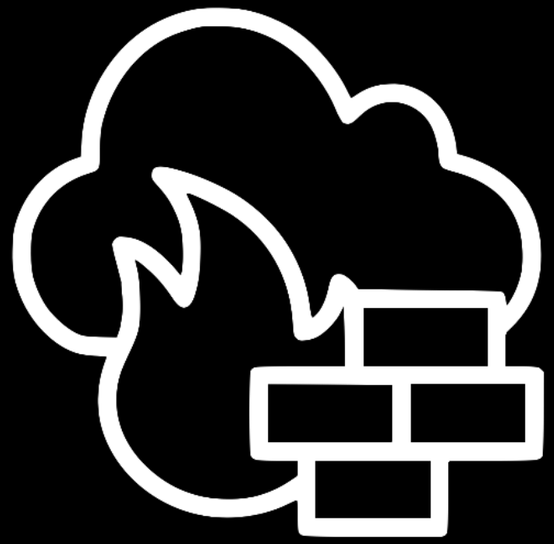
NATGW Route Table	
10.0.0.0/16	local
0.0.0.0/0	**igw-1232**

Private "App1" Route Table	
10.0.0.0/16	local
0.0.0.0/0	**nat-5252**

NACL (Stateless)

Route	Type	Proto	Port	Src/Dst	Allow/Deny
IN	All	All	All	10/16	Allow
IN	All	All	All	0/0	Deny
OUT	All	All	All	0/0	Allow

AWS Network Firewall



Want more?
Check out SEC311

- Highly available and elastically scales
- Centrally managed - simplified deployment
- Fine grained controls –
  - Stateful & Stateless rules
  - FQDN based filtering
  - Regex matching
  - Managed threat lists
- Simplify auditing and visibility
  - Per rule CloudWatch metrics
  - Centralized logging via Amazon S3 and Amazon Kinesis
- Integrated with 14 security services
  - **SIEM –** Splunk, Datadog, Alert Logic, Sumo Logic, IBM Qradar
  - **Threat Intel/Analytics/Governance –** Trend Micro, CrowdStrike, Palo Alto Networks, Check Point, Fortinet
  - **Orchestration/Automation –** HashiCorp/Terraform (support from day 1), Tufin
  - **Managed Services –** Accenture, Rackspace

What if I have a preferred security service?

TREND MICRO

Palo Alto Networks

Check Point SOFTWARE TECHNOLOGIES LTD.

radware

FORTINET

VALTIX



Amazon VPC

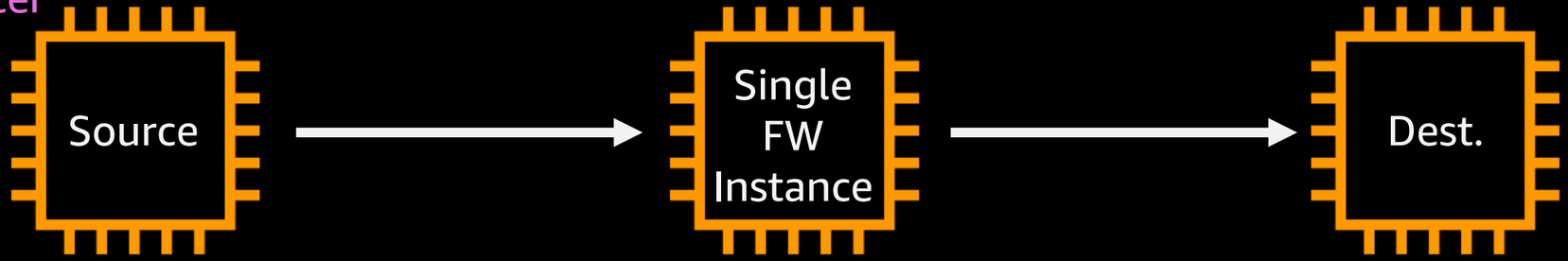
+



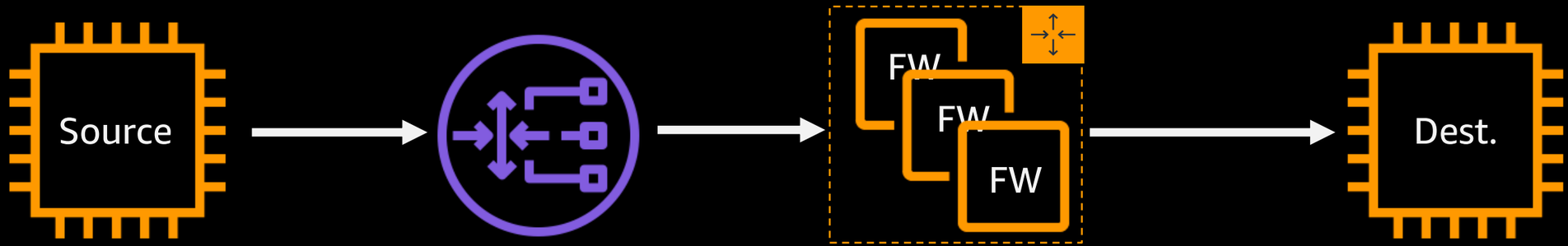
On Premises

What if I have a preferred security service?

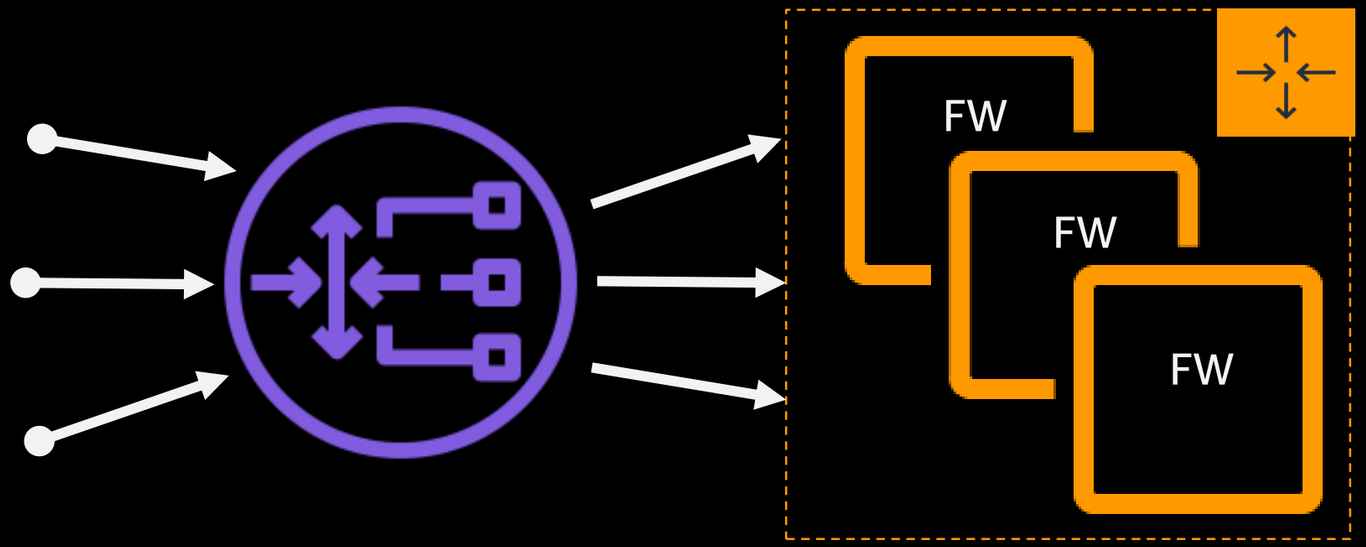
Before AWS Gateway Load Balancer



After AWS Gateway Load Balancer



AWS Gateway Load Balancer



Want more?
Check out NET308

- A new elastic load balancer for any IP traffic
- Can be a next-hop target in a VPC route table
- Supports endpoints in remote VPCs like AWS PrivateLink
- Performs health checking and remediation of failed or saturated targets

TREND MICRO

radware

Check Point SOFTWARE TECHNOLOGIES LTD.

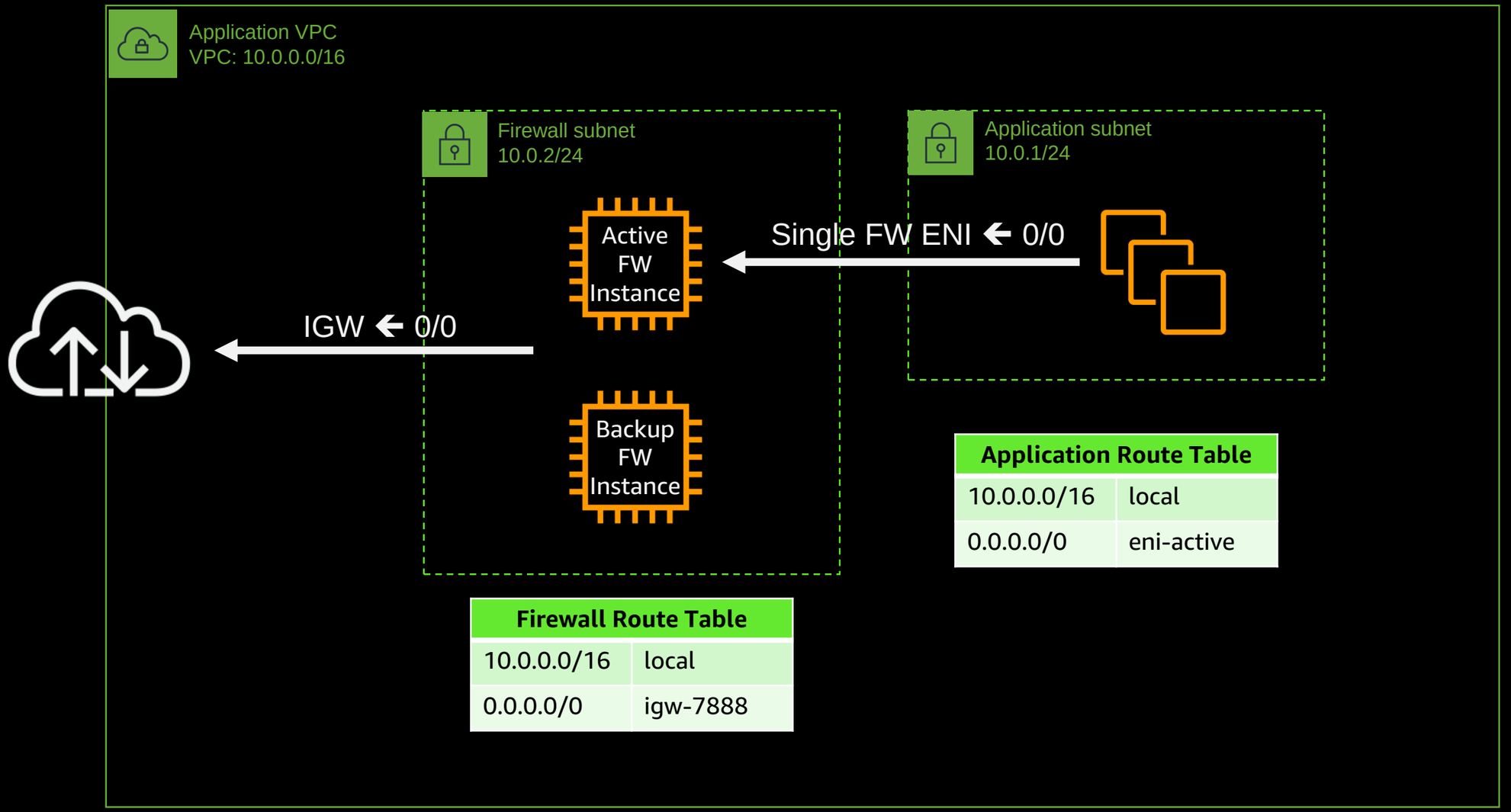
VALTIX

Palo Alto Networks

FORTINET

Custom appliances
…

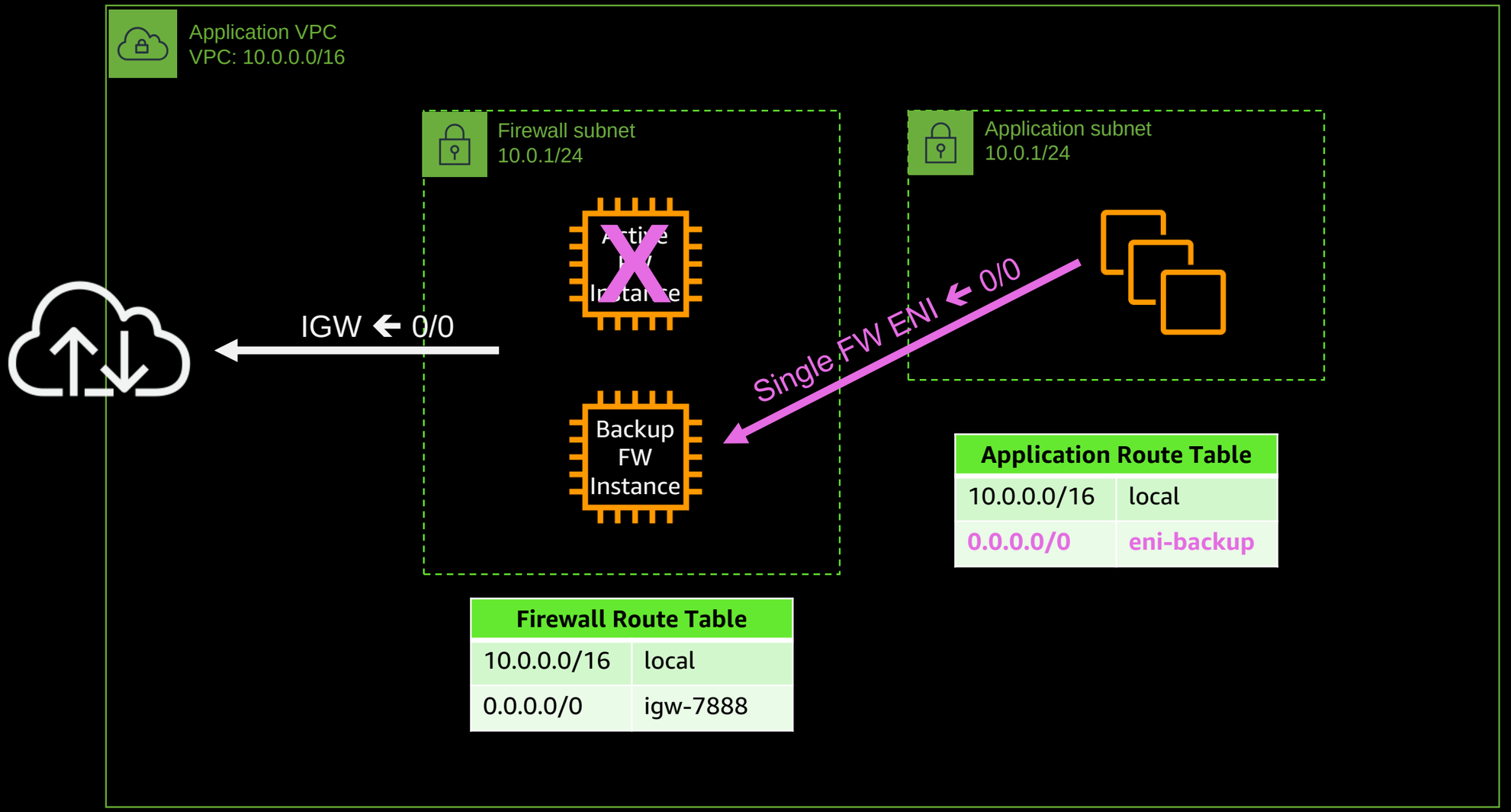
Before AWS Gateway Load Balancer



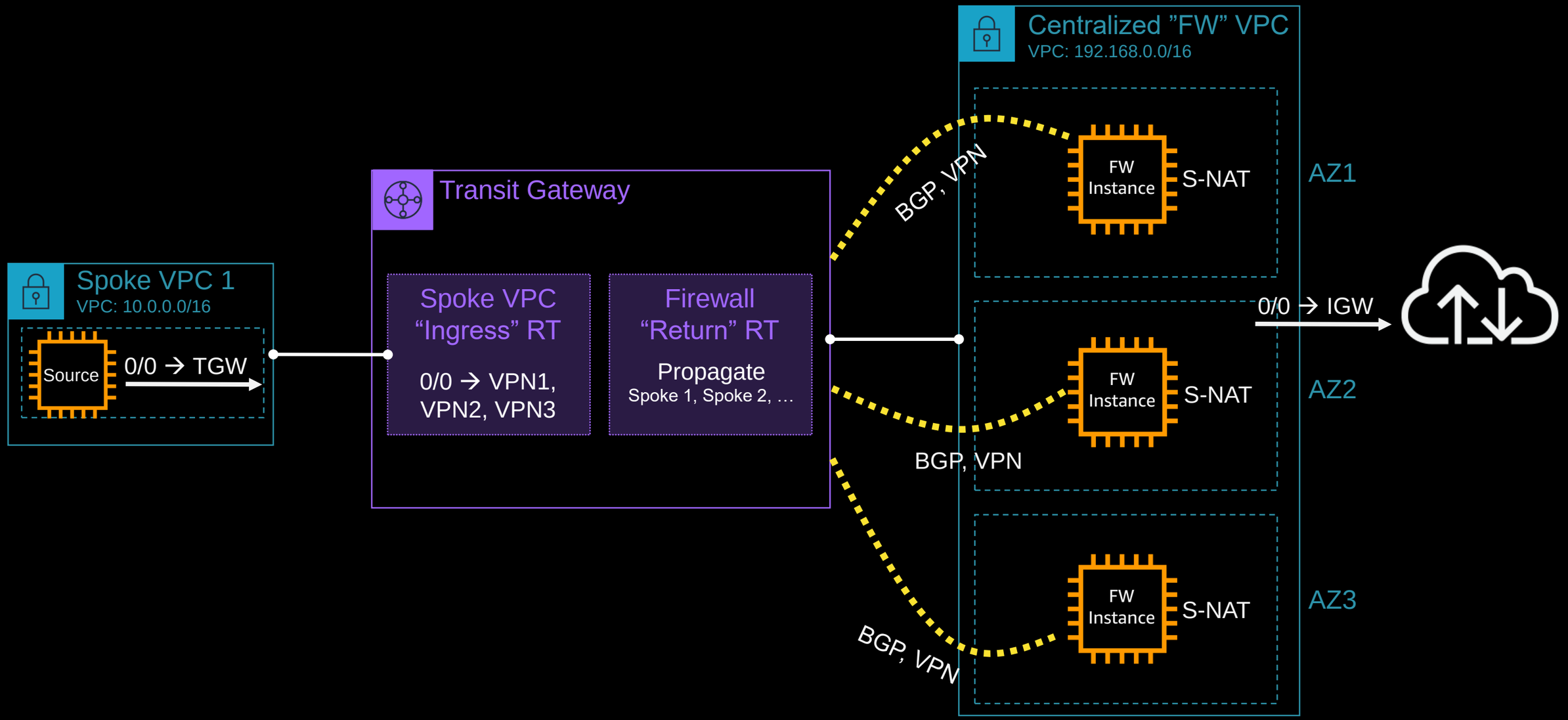
Application Route Table	
10.0.0.0/16	local
0.0.0.0/0	eni-active

Firewall Route Table	
10.0.0.0/16	local
0.0.0.0/0	igw-7888

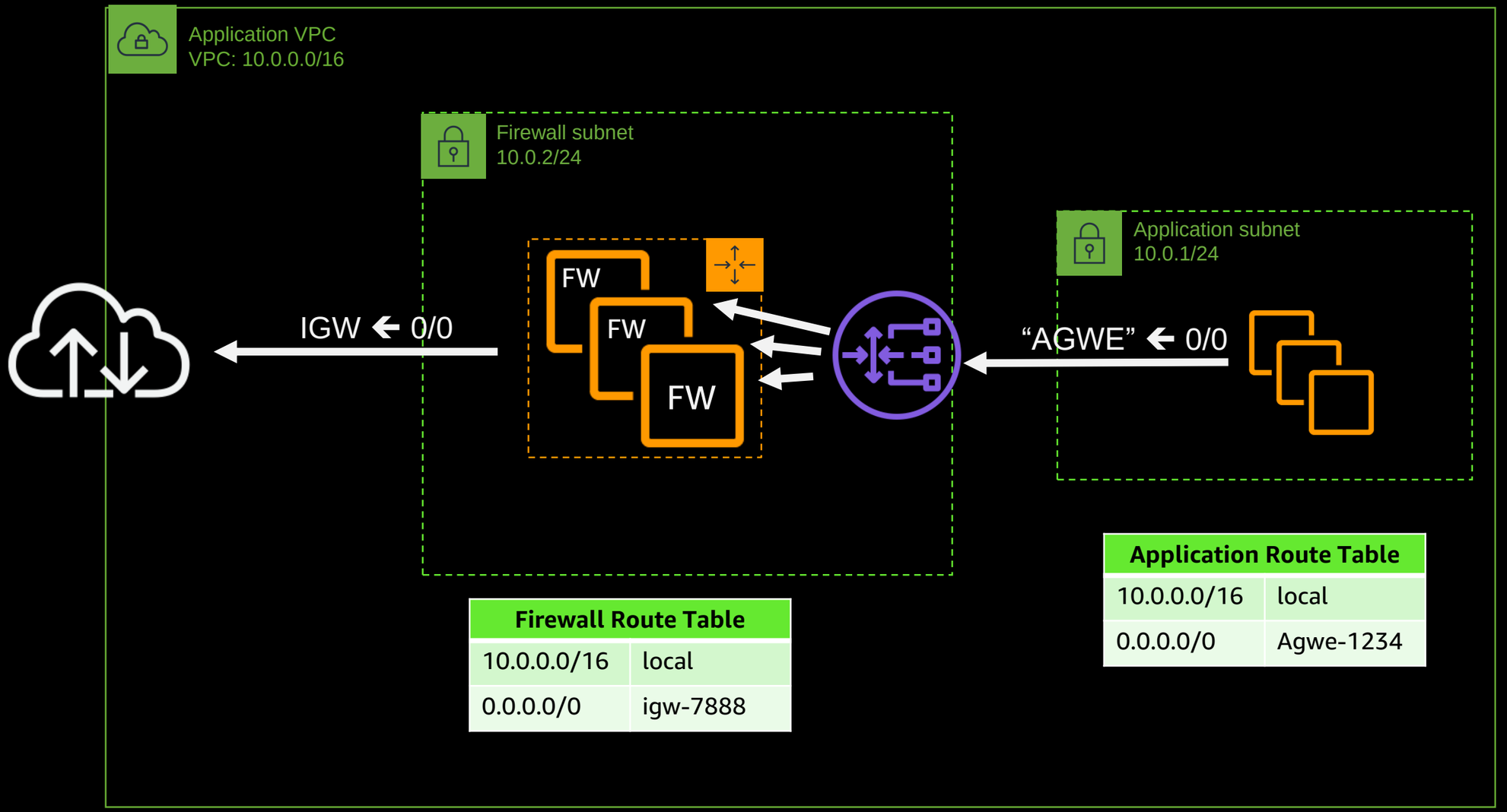
Before AWS Gateway Load Balancer



BGP with VPN overlay and S-NAT



After AWS Gateway Load Balancer

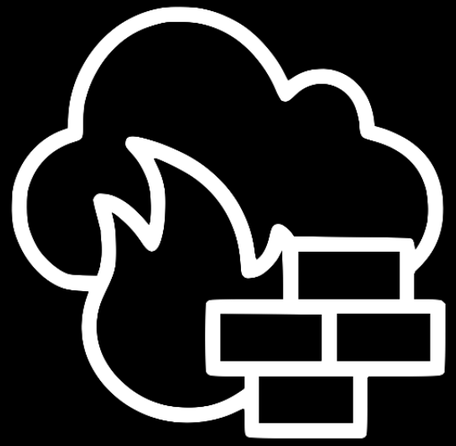


Firewall Route Table	
10.0.0.0/16	local
0.0.0.0/0	igw-7888

Application Route Table	
10.0.0.0/16	local
0.0.0.0/0	Agwe-1234

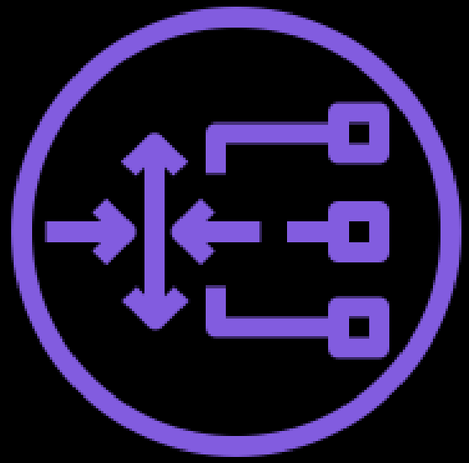
Choose what's right for you

AWS Firewall



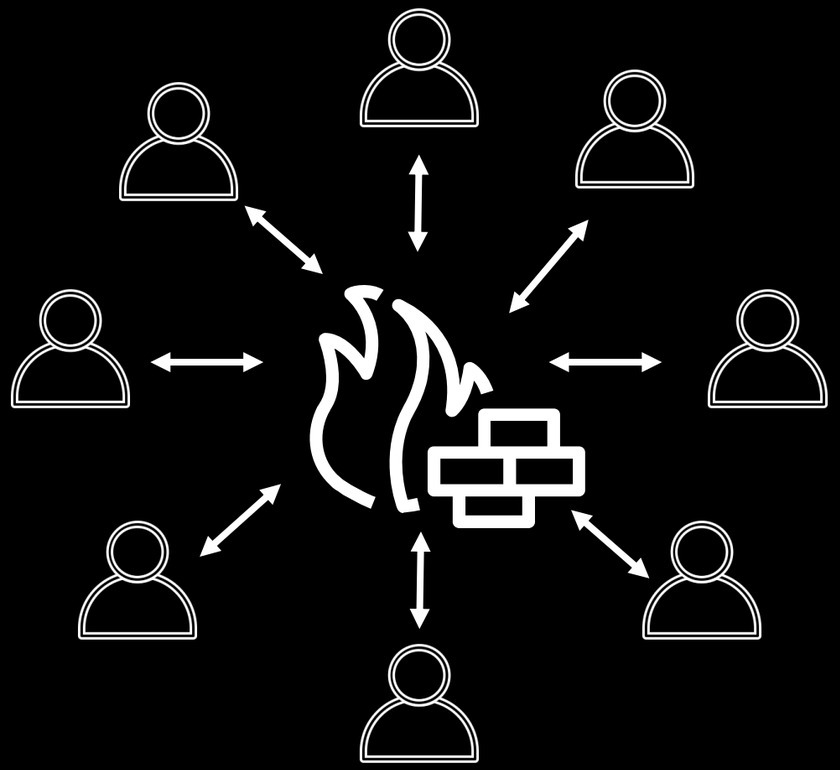
Want more?
Check out SEC311

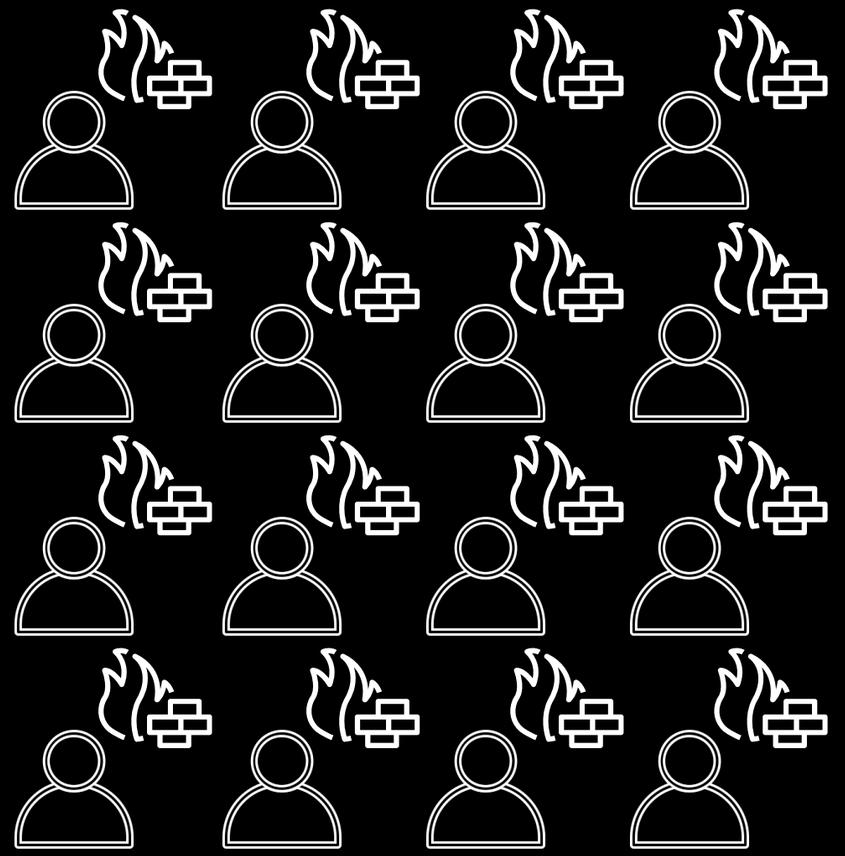
AWS Gateway Load Balancer



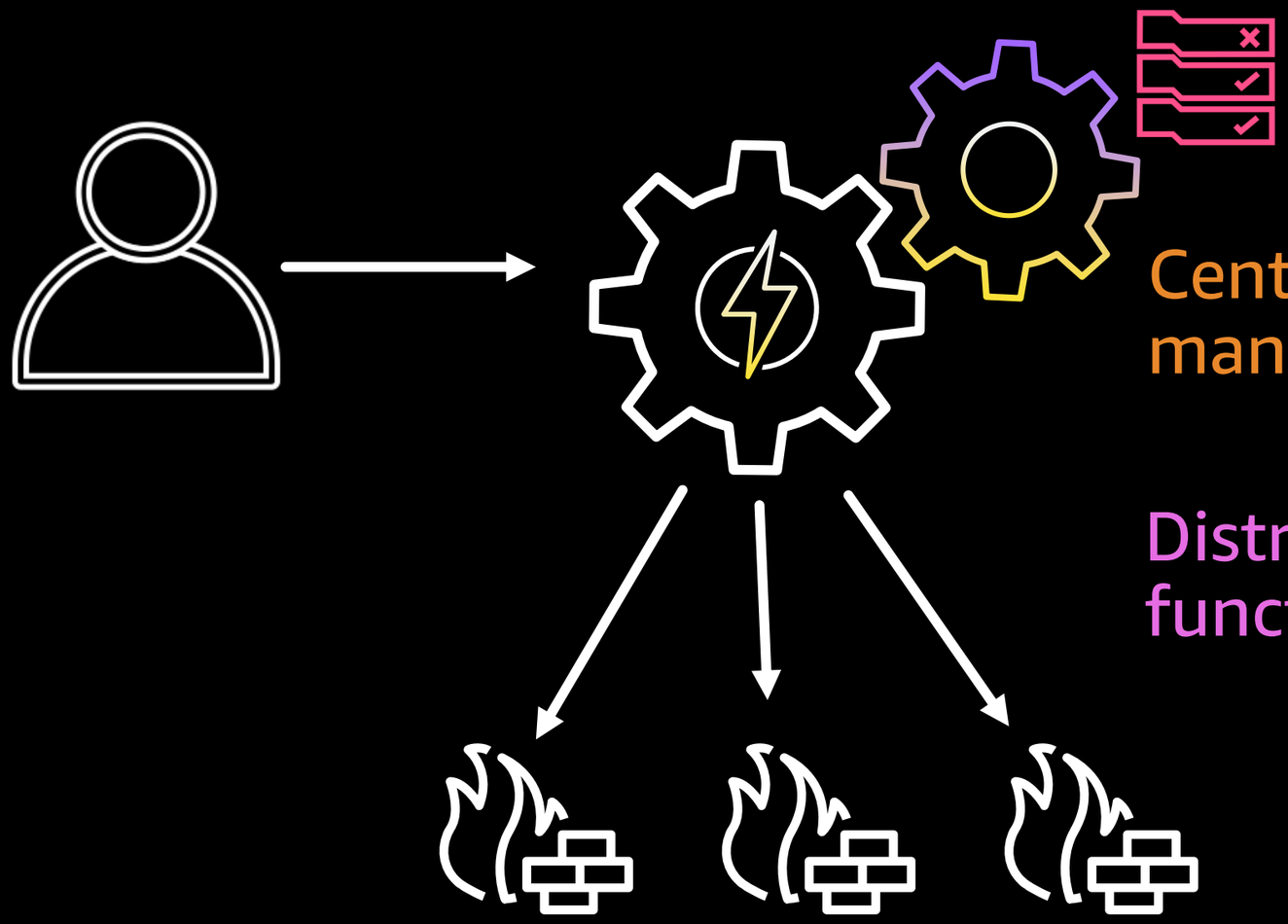
Want more?
Check out NET308

To centralize, or not to centralize?





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?

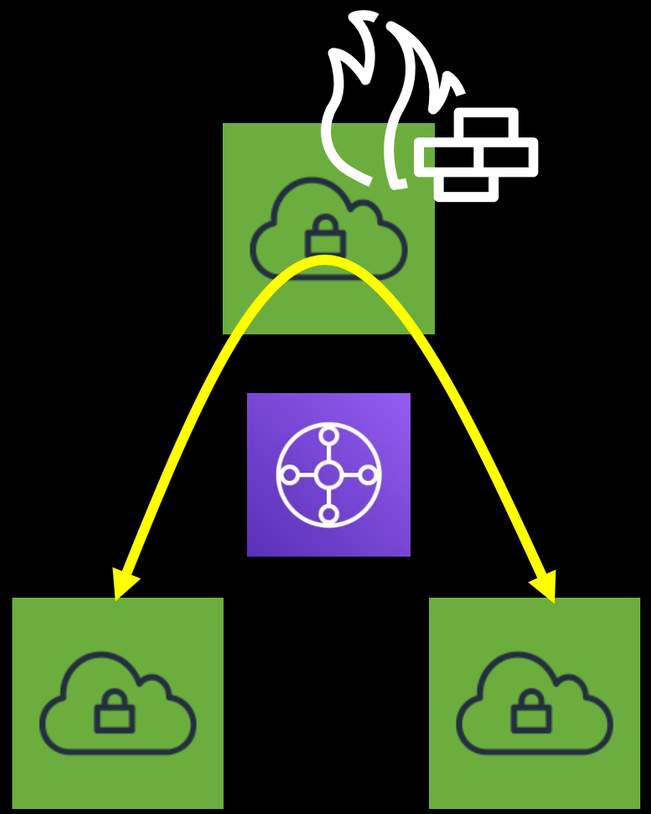
Top 3 architecture patterns for inspection



Distributed
North/South

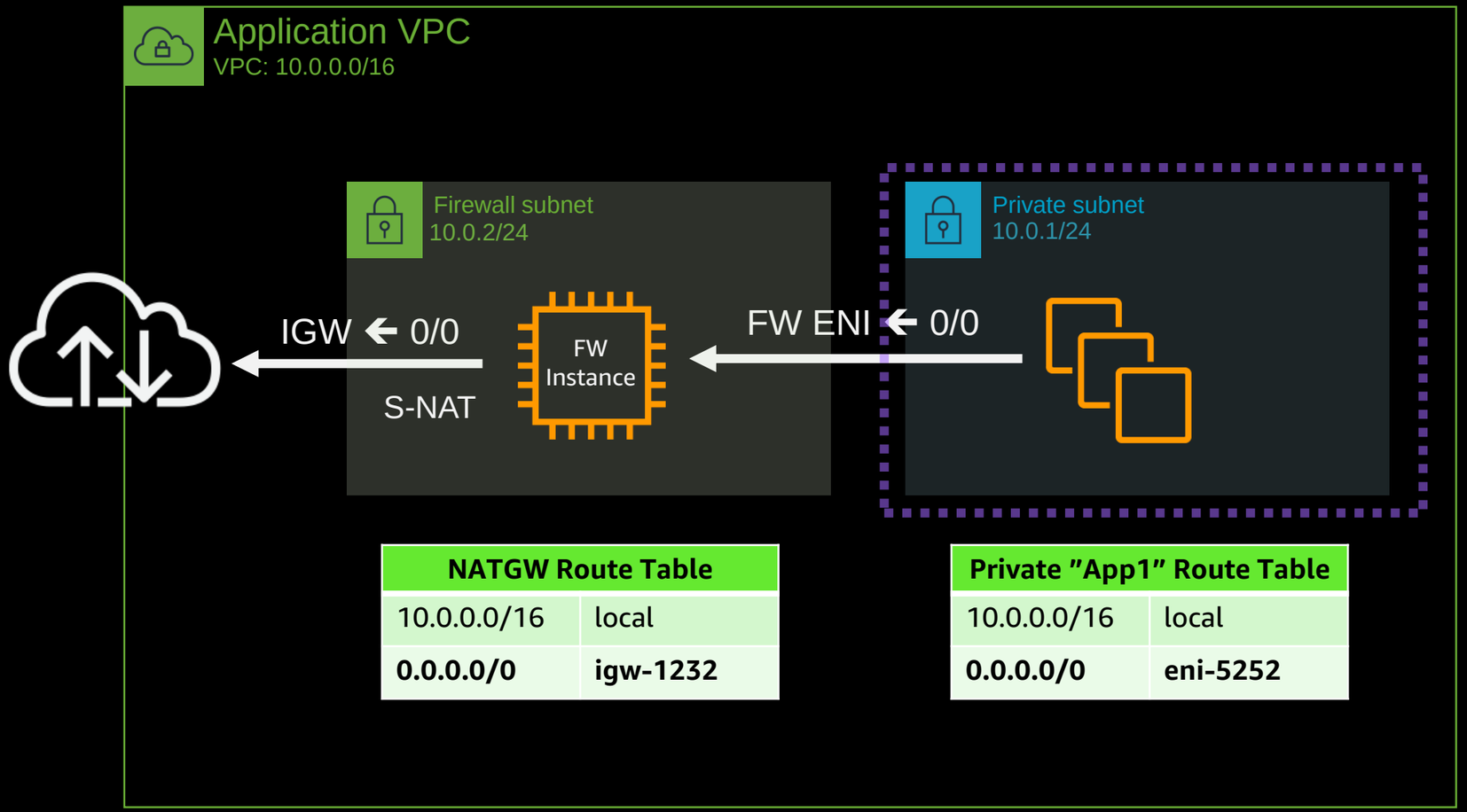


Centralized
North/South



Centralized
East/West

1/ Distributed North/South



NATGW Route Table	
10.0.0.0/16	local
0.0.0.0/0	**igw-1232**

Private "App1" Route Table	
10.0.0.0/16	local
0.0.0.0/0	**eni-5252**

1/ Distributed North/South: Side note

NO!



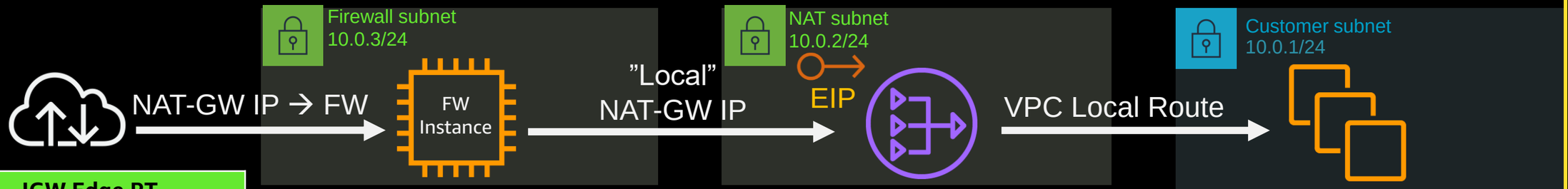
IGW Edge RT	
10.0.0.0/16	local

NAT-GW Route Table	
10.0.0.0/16	local
~~10.0.1/24~~	~~eni-1234~~
0.0.0.0/0	Igw-7888

FW Route Table	
10.0.0.0/16	local
0.0.0.0/0	Nat-4234

Application Route Table	
10.0.0.0/16	local
0.0.0.0/0	eni-1234

YES!



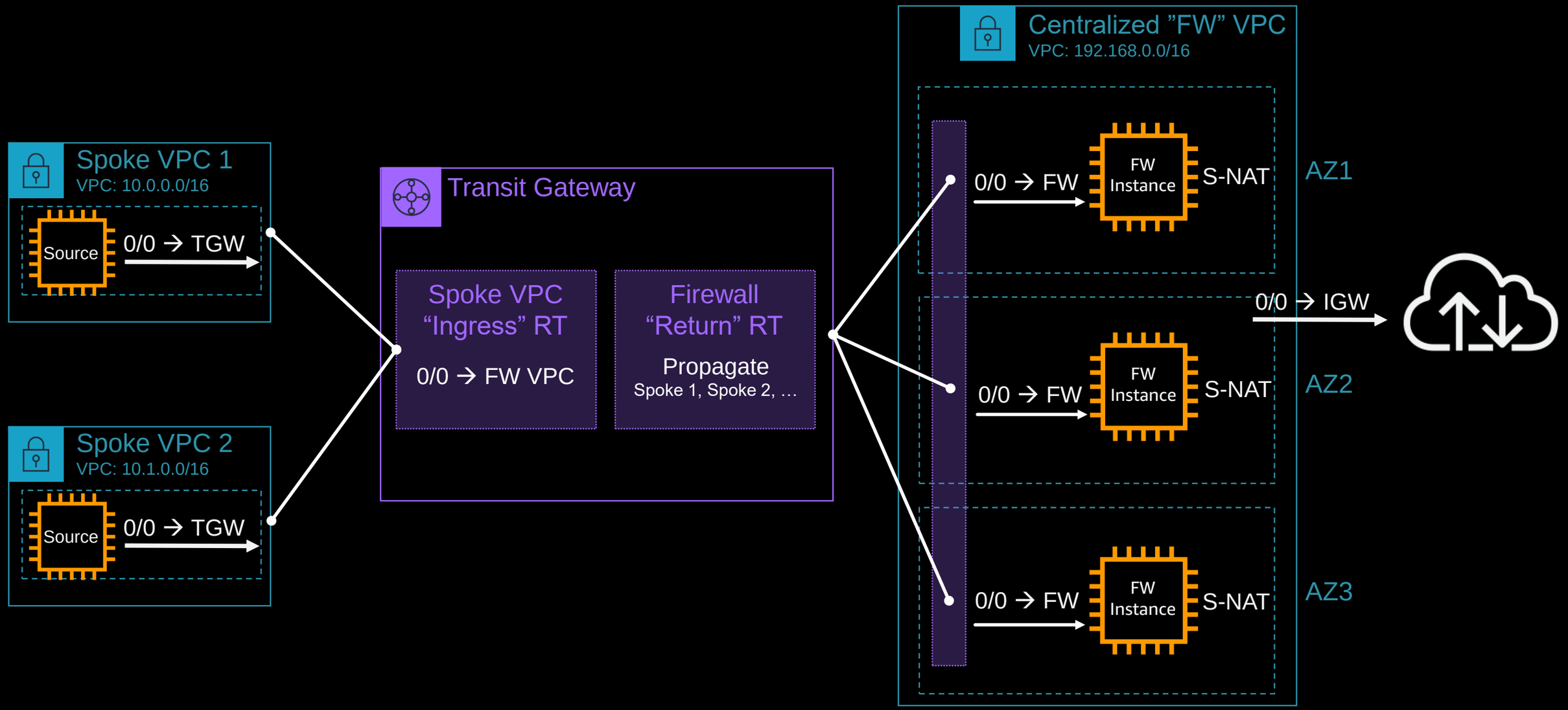
IGW Edge RT	
10.0.0.0/16	Local
10.0.1/24	eni-1234

FW Route Table	
10.0.0.0/16	local
0.0.0.0/0	**Igw-7888**

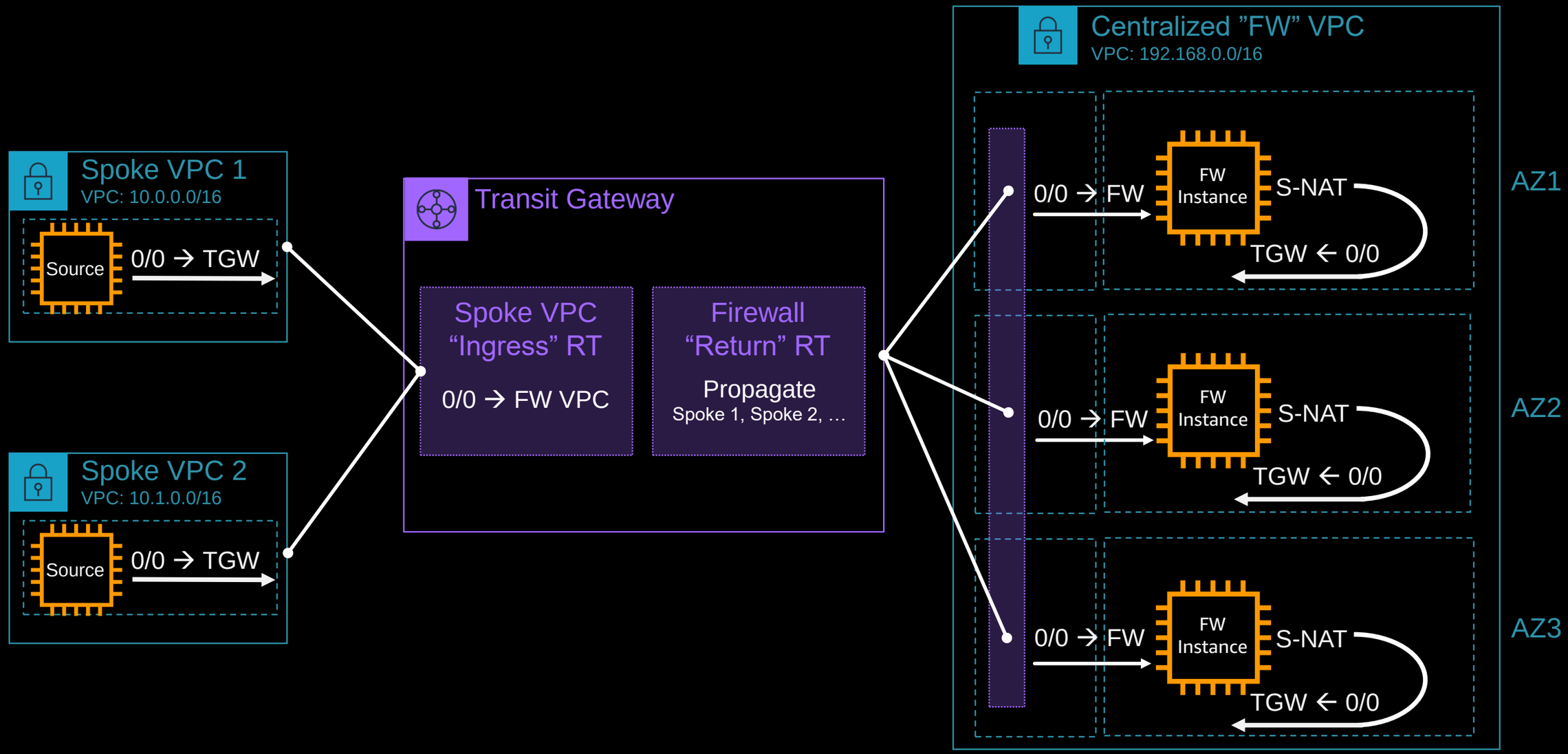
NAT-GW Route Table	
10.0.0.0/16	local
0.0.0.0/0	eni-1234

Application Route Table	
10.0.0.0/16	local
0.0.0.0/0	Nat-4234

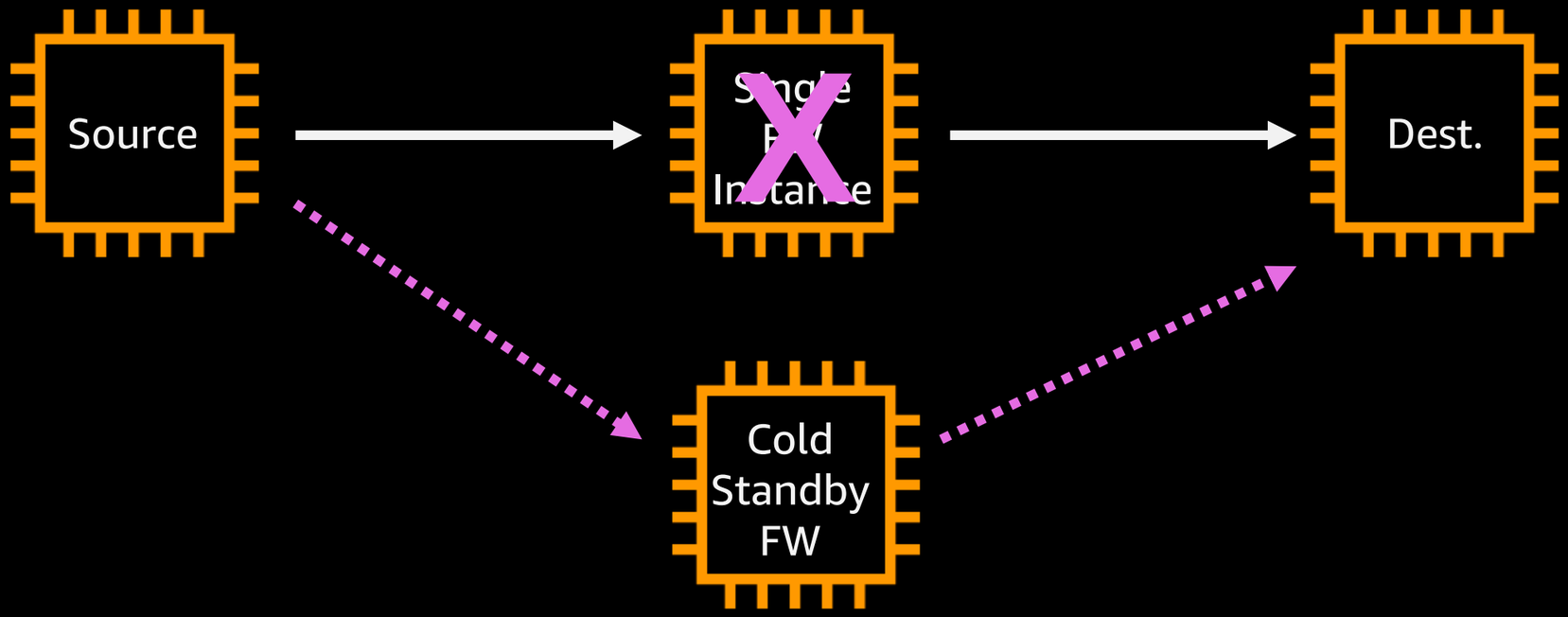
2/ Centralized North/South



3/ Centralized East/West

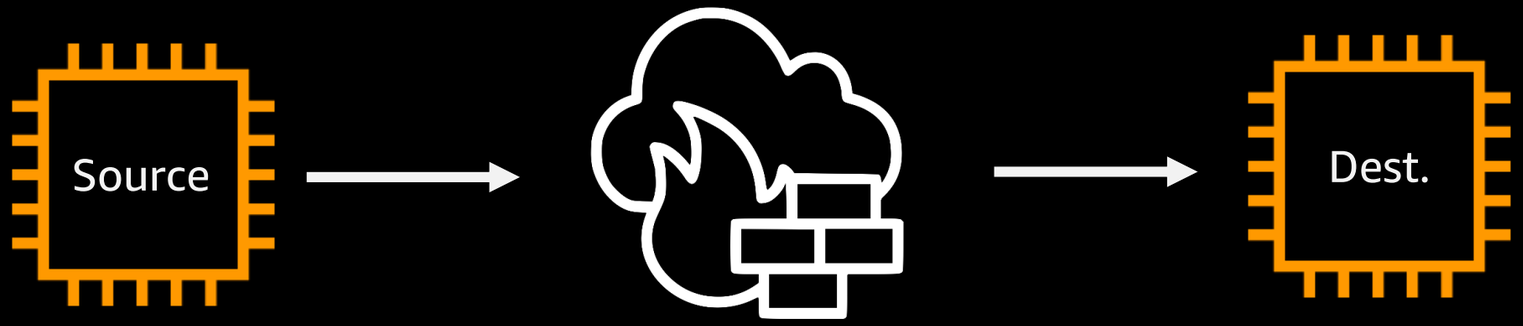


Availability and scalability: Before

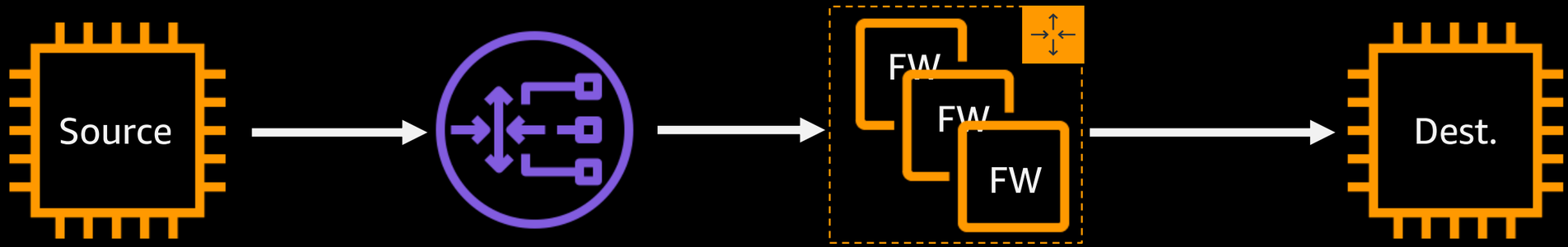


Availability and scalability: After

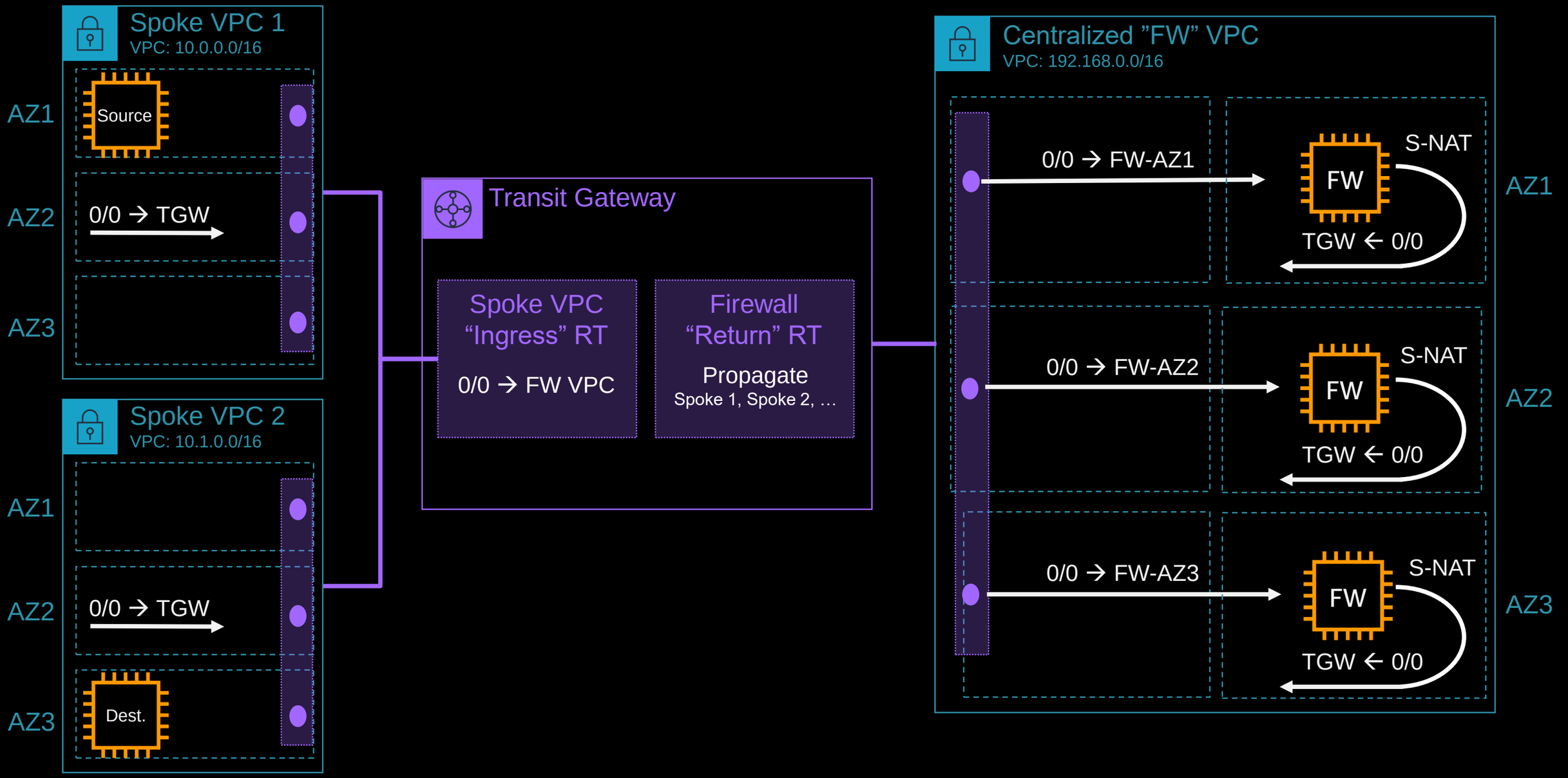
AWS Network Firewall



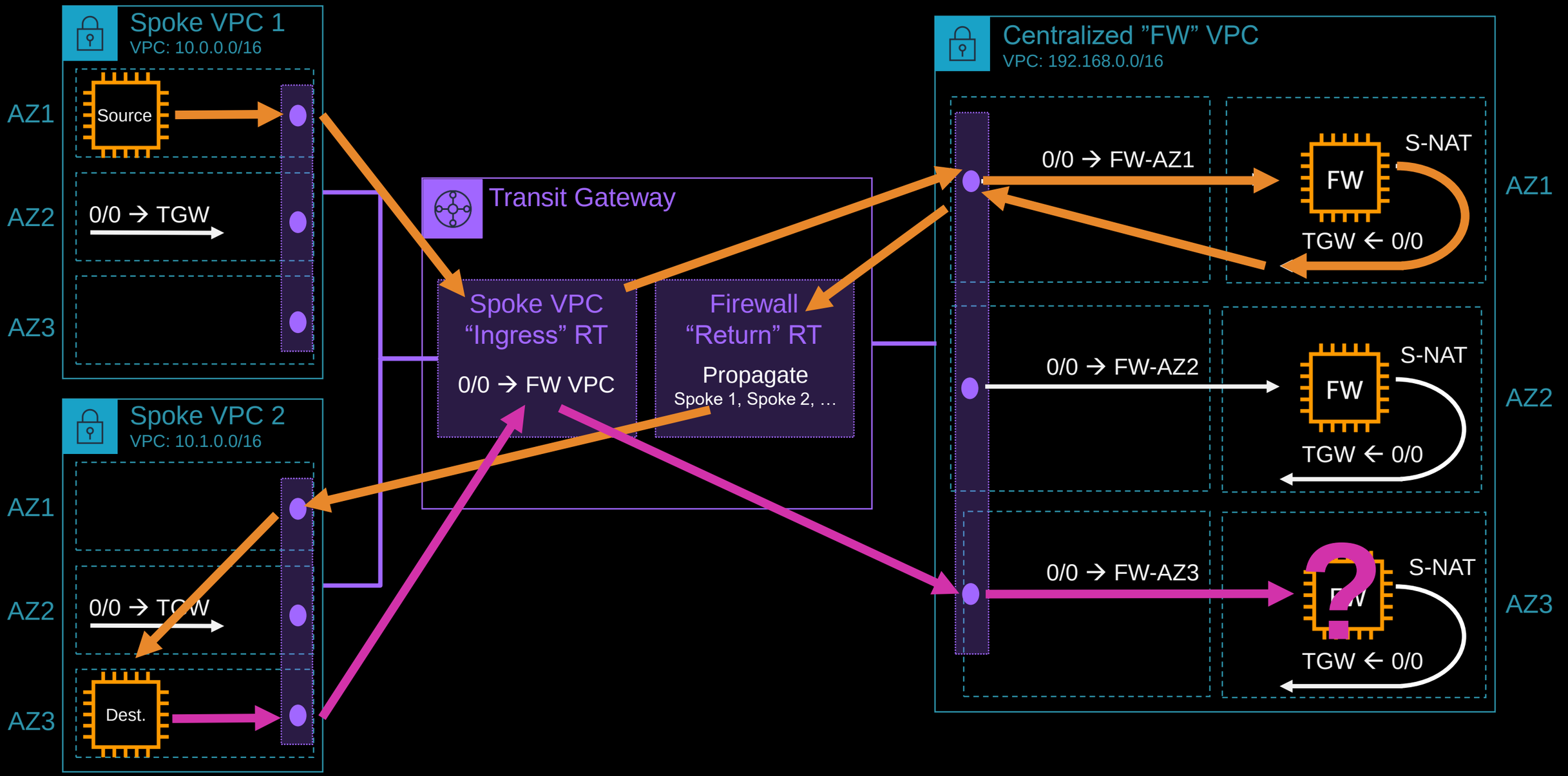
AWS Gateway Load Balancer



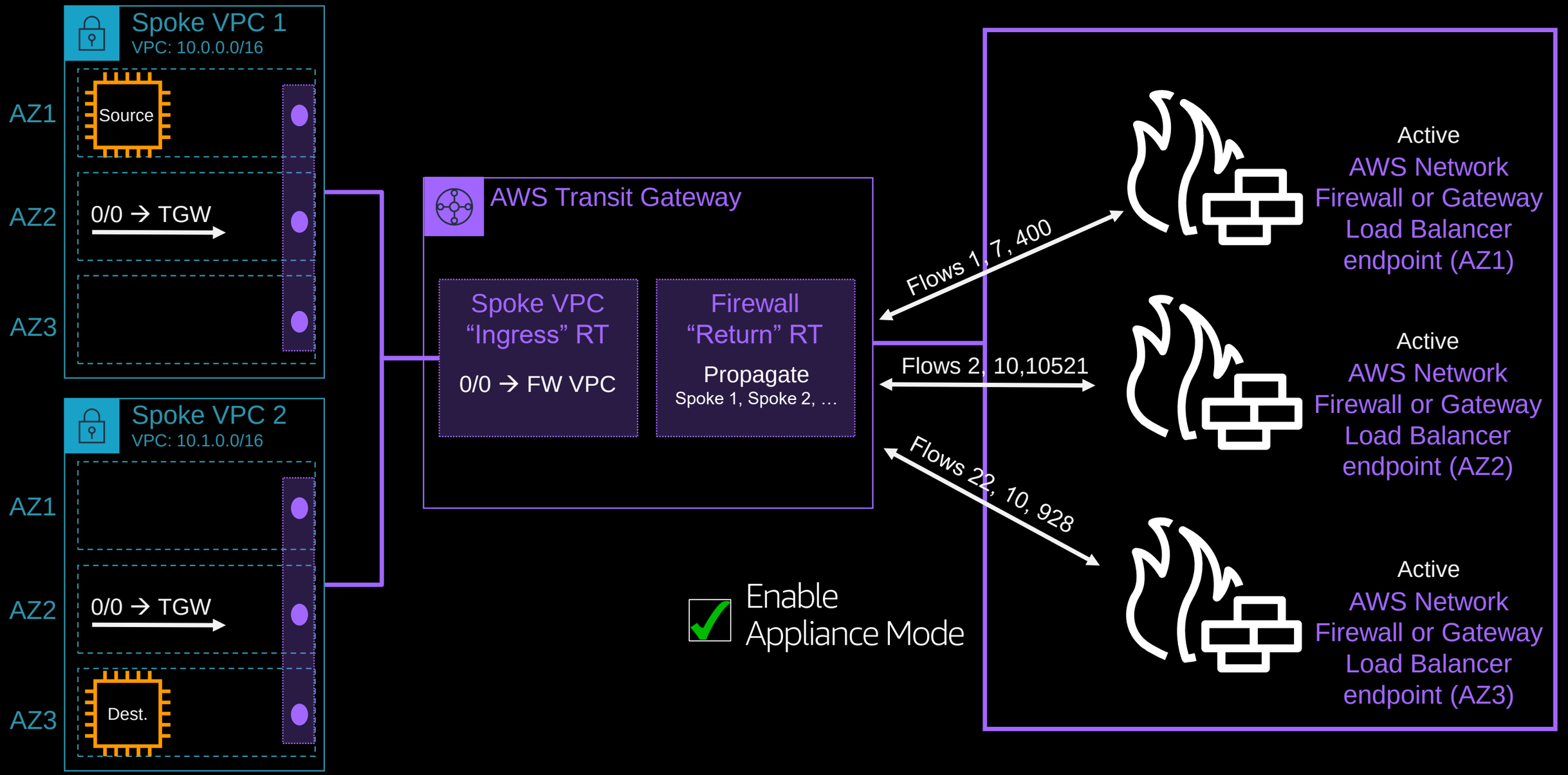
Stateful firewalls require state: Before



Symmetric routing (Double-click to view)

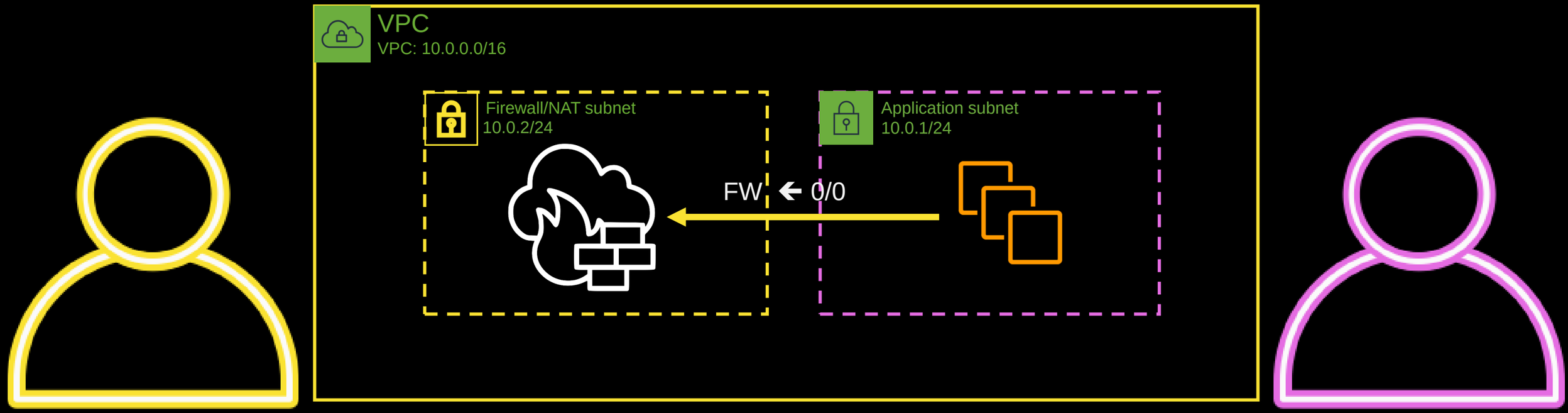


Stateful firewalls require state: After



Separation of duties

Want more info on VPC sharing?
Check out NET303

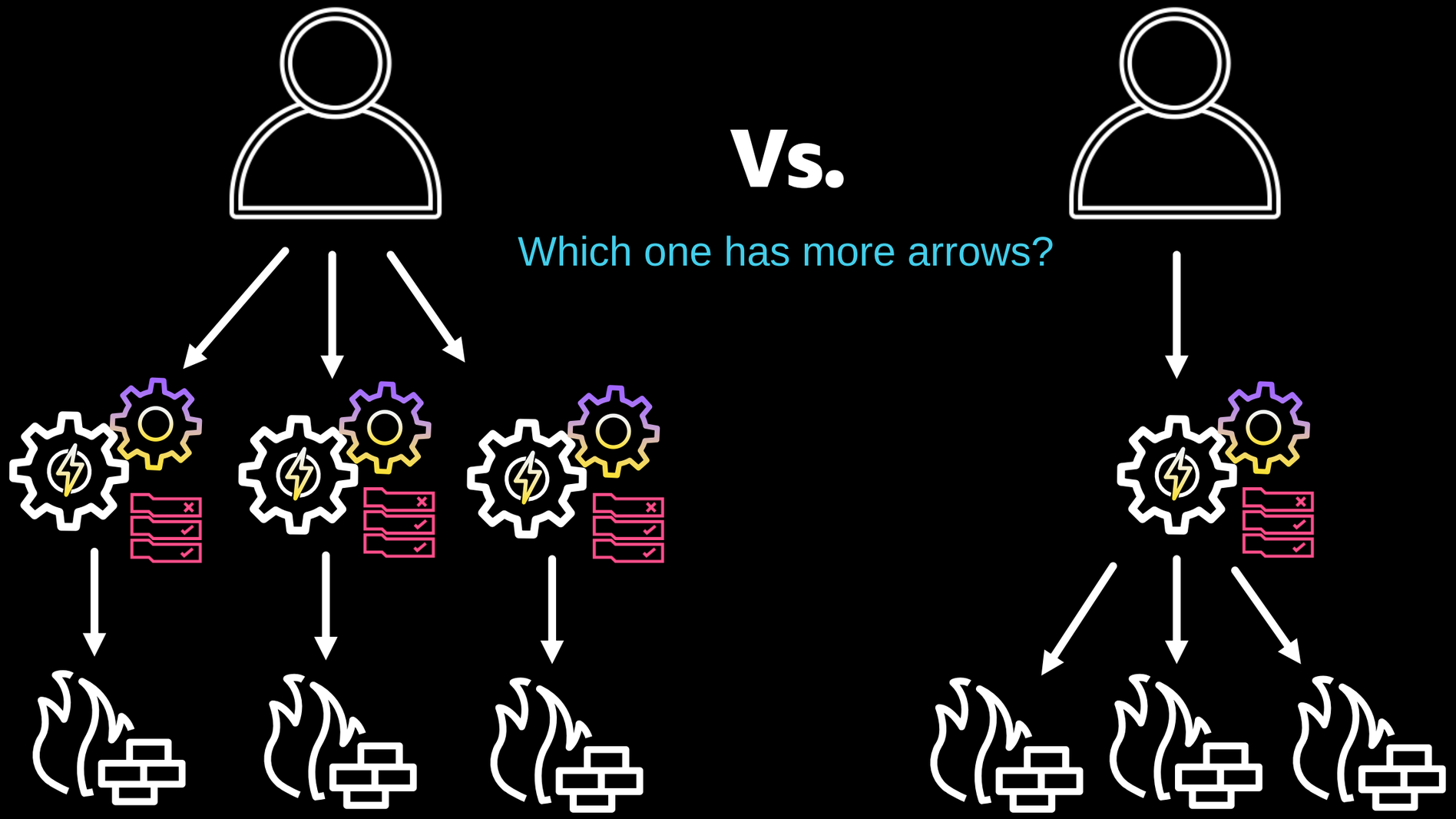


Infrastructure InfoSec team owns VPC

Share subnet 10.0.1/24 with team pink

Application team deploys resources in defined subnet

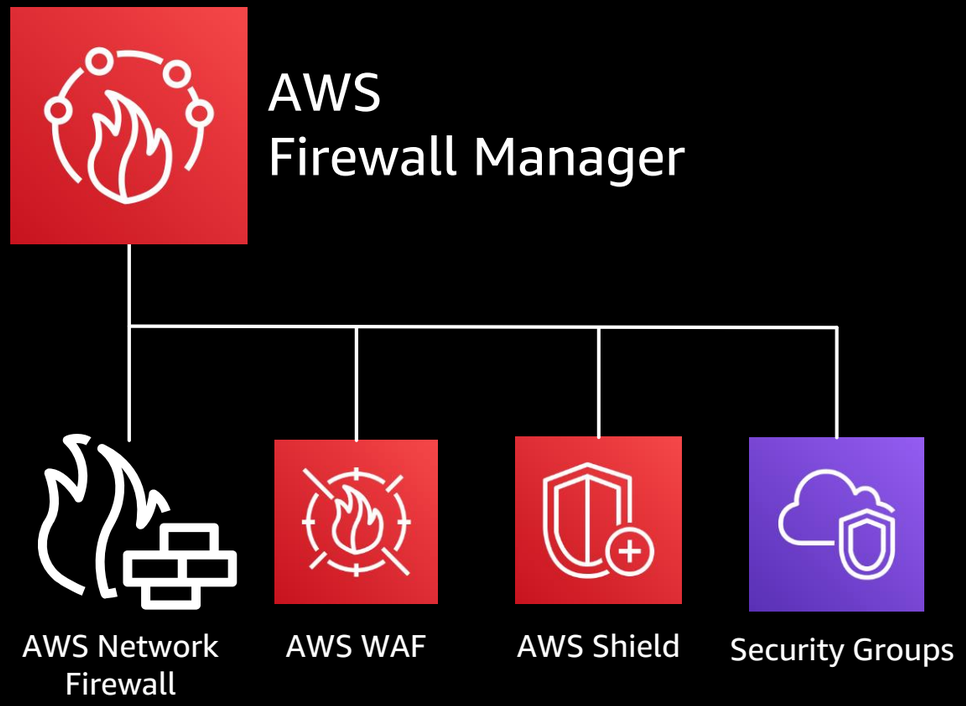
Centralize management of security controls



Centralize management of security controls



Centralize control plane further with AWS Firewall Manager

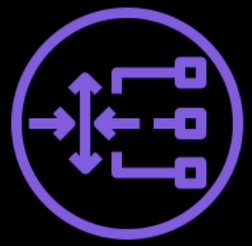


- One place to manage all firewall controls on AWS: AWS Network Firewall, AWS WAF, Shield, and Security Groups
- Centrally manage and deploy baseline security for AWS Network Firewall, AWS WAF, VPC security groups and DDoS protections across thousands of accounts
- Continuously manage and audit security Groups to prevent overly permissive rules
- Enforce protections, even as new applications are created
- View compliance posture centrally across AWS accounts

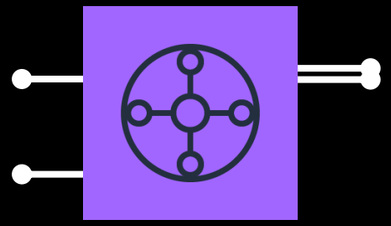
Recap



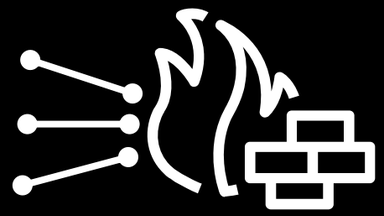
AWS Network Firewall



AWS
Gateway Load Balancer



AWS Transit Gateway
appliance mode



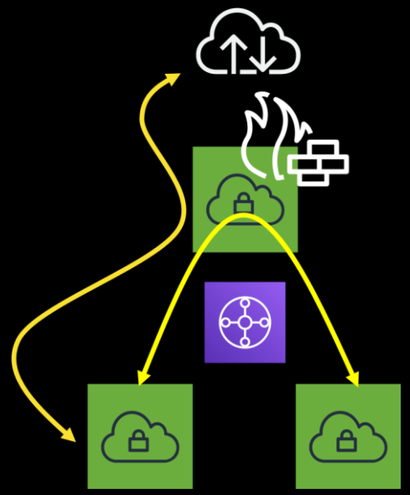
AWS Gateway Load
Balancer
and AWS Firewall
endpoints

Which inspection architecture is right for you?



Distribute

- As much data-plane / processing as you can
- High bandwidth use-cases to avoid adding redundant data processing



Centralize

- As much control-plane / configuration as you can
- Operations, log aggregation visualization
- Low bandwidth, many VPCs

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.