AWS re:Invent

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

NET302-R2

Network and security services with AWS Transit Gateway

Kyle Tedeschi
Senior Solutions Architect
AWS

Justin Davies
Principal Product Manager, Amazon EC2
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Overview of AWS network security services

Discussion of use cases

Recent feature updates and new use cases

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS network security services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

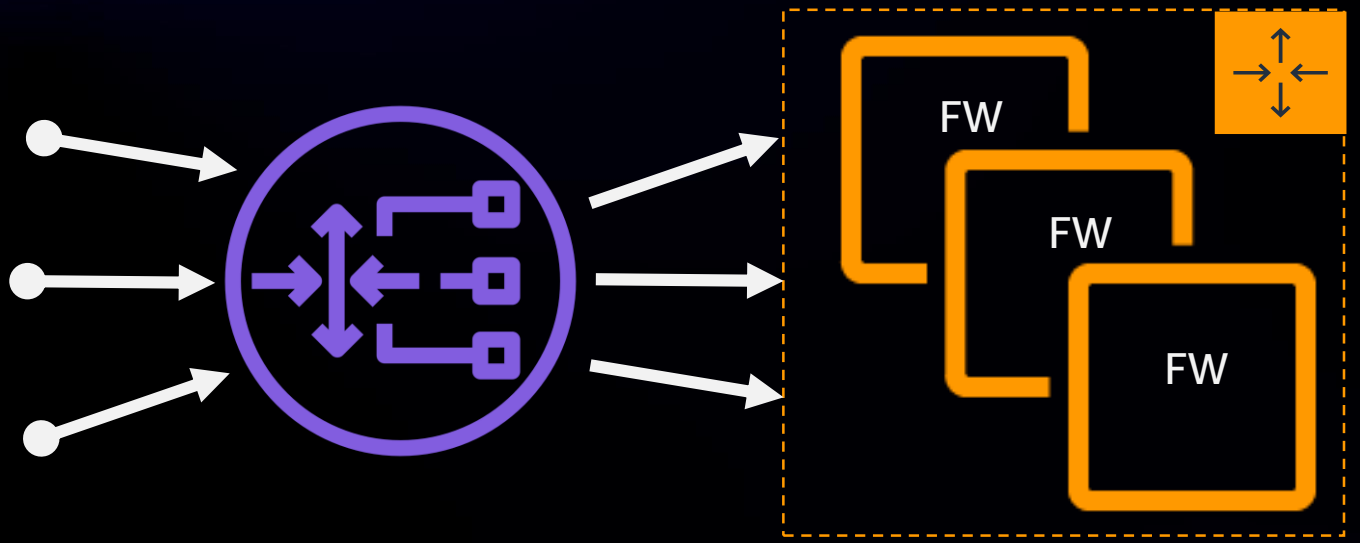
AWS services for securing your Amazon VPC

- AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all of your Amazon VPCs

- AWS Gateway Load Balancer makes it easy to deploy, scale, and manage your third-party virtual appliances on AWS such as firewalls and IPS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Gateway Load Balancer



- 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

appliances

...

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Network Firewall



- 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 Amazon CloudWatch metrics
  - Centralized logging via Amazon S3 and Amazon Kinesis
- Integrated with security services, including
  - **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

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, Amazon CloudFront, Amazon API Gateway

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, Amazon CloudFront, Amazon API Gateway
Firewall type	Stateful and Stateless	Appliance dependent	Stateful	Stateless	Stateless

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, Amazon CloudFront, Amazon API Gateway
Firewall type	Stateful and Stateless	Appliance dependent	Stateful	Stateless	Stateless
OSI layer	L3 – L7	L3 – L7	L3 – L4	L3 – L4	L7

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, Amazon CloudFront, Amazon API Gateway
Firewall type	Stateful and Stateless	Appliance dependent	Stateful	Stateless	Stateless
OSI layer	L3 – L7	L3 – L7	L3 – L4	L3 – L4	L7
Rule types	Allow, Deny, Alert	Appliance dependent	Allow	Allow, Deny	Count, Allow, Block

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, Amazon CloudFront, Amazon API Gateway
Firewall type	Stateful and Stateless	Appliance dependent	Stateful	Stateless	Stateless
OSI layer	L3 – L7	L3 – L7	L3 – L4	L3 – L4	L7
Rule types	Allow, Deny, Alert	Appliance dependent	Allow	Allow, Deny	Count, Allow, Block
AWS Firewall Manager	Yes	No	Yes	No	Yes

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Compare VPC network security controls

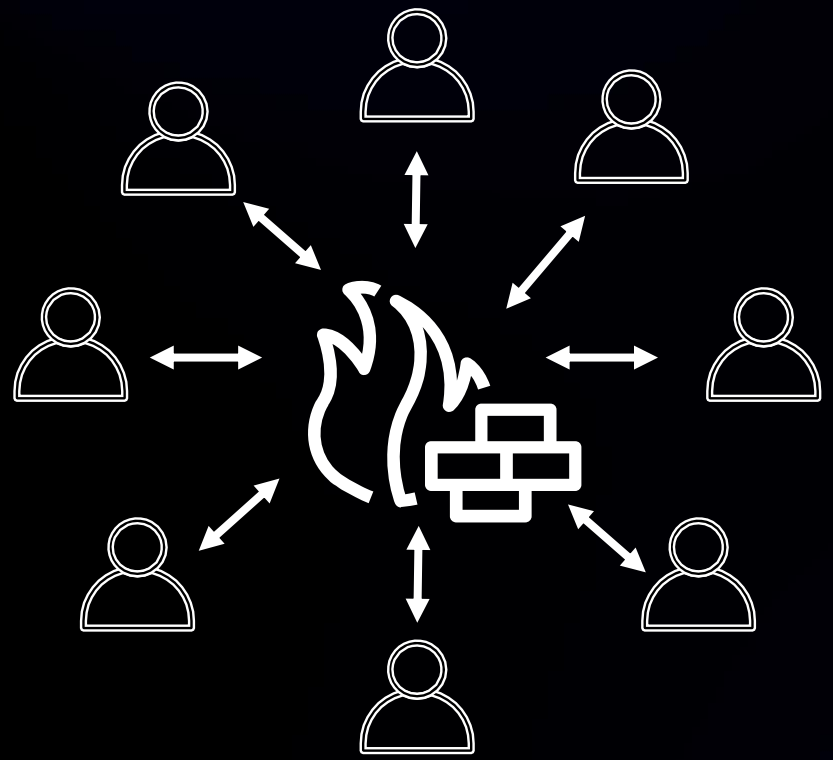
Firewall	AWS Network Firewall	AWS Gateway Load Balancer + Appliance	Security Group	Network ACL	AWS WAF
Key Use Case	Traffic Inspection and filtering; Intrusion Prevention	Traffic Inspection and filtering; Network observability	Access Control	Access Control	Web Apps; Bots; Input validation
Inspection Point	VPC Ingress/Egress	VPC Ingress/Egress	ENI (EC2 instance, Amazon RDS database, etc.)	VPC subnet	ALB, CloudFront, API Gateway
Firewall type	Stateful and Stateless	Appliance dependent	Stateful	Stateless	Stateless
OSI layer	L3 – L7	L3 – L7	L3 – L4	L3 – L4	L7
Rule types	Allow, Deny, Alert	Appliance dependent	Allow	Allow, Deny	Count, Allow, Block
AWS Firewall Manager	Yes	No	Yes	No	Yes
Pricing	Additional cost	Additional cost	No cost	No cost	Additional cost

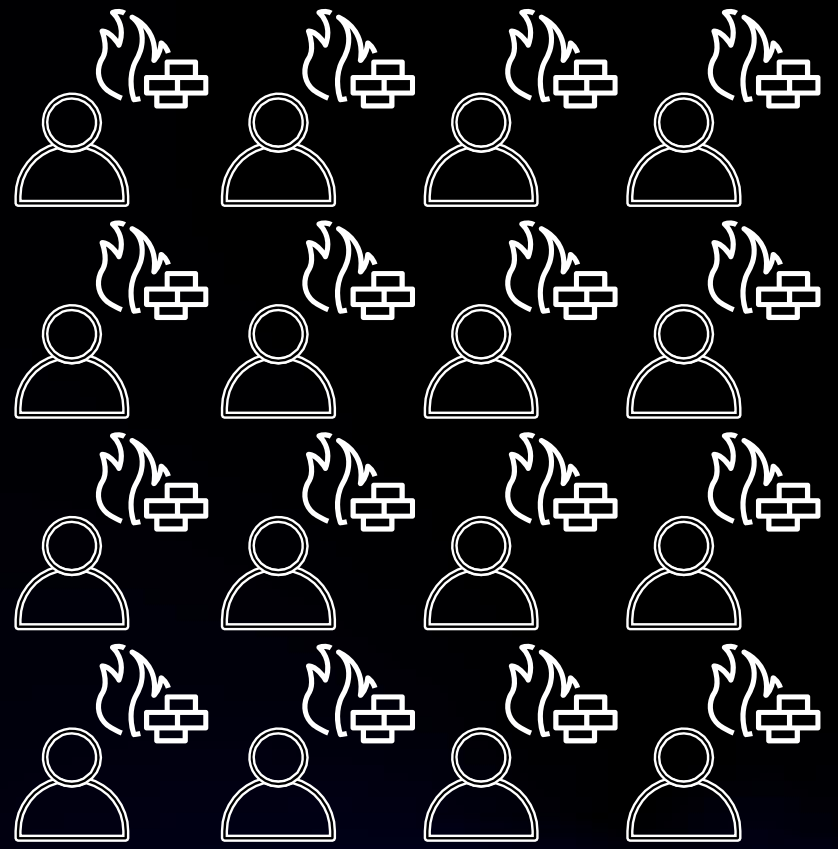
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Discussion of use cases

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

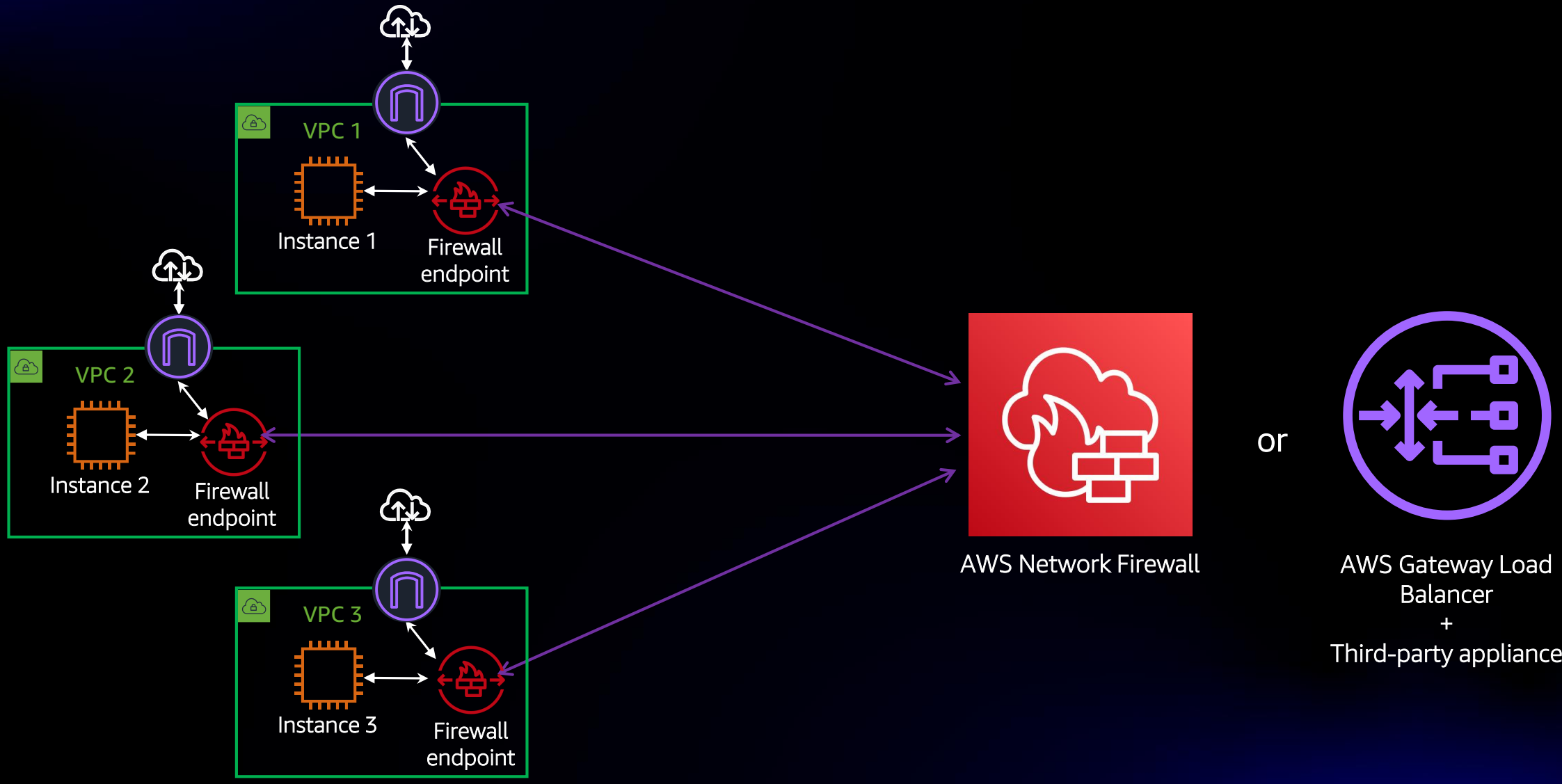
To centralize, or not to centralize?





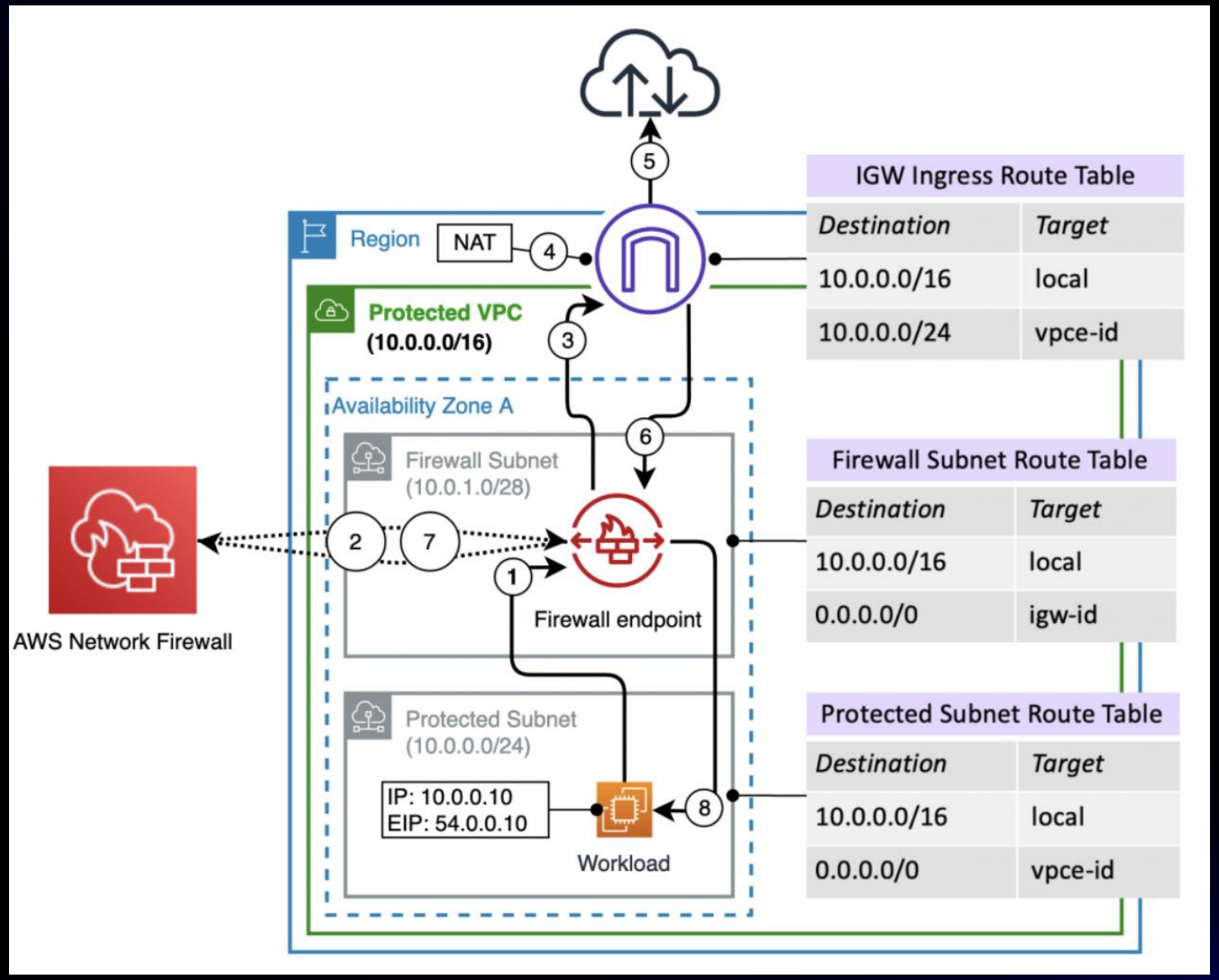
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Distributed security inspection



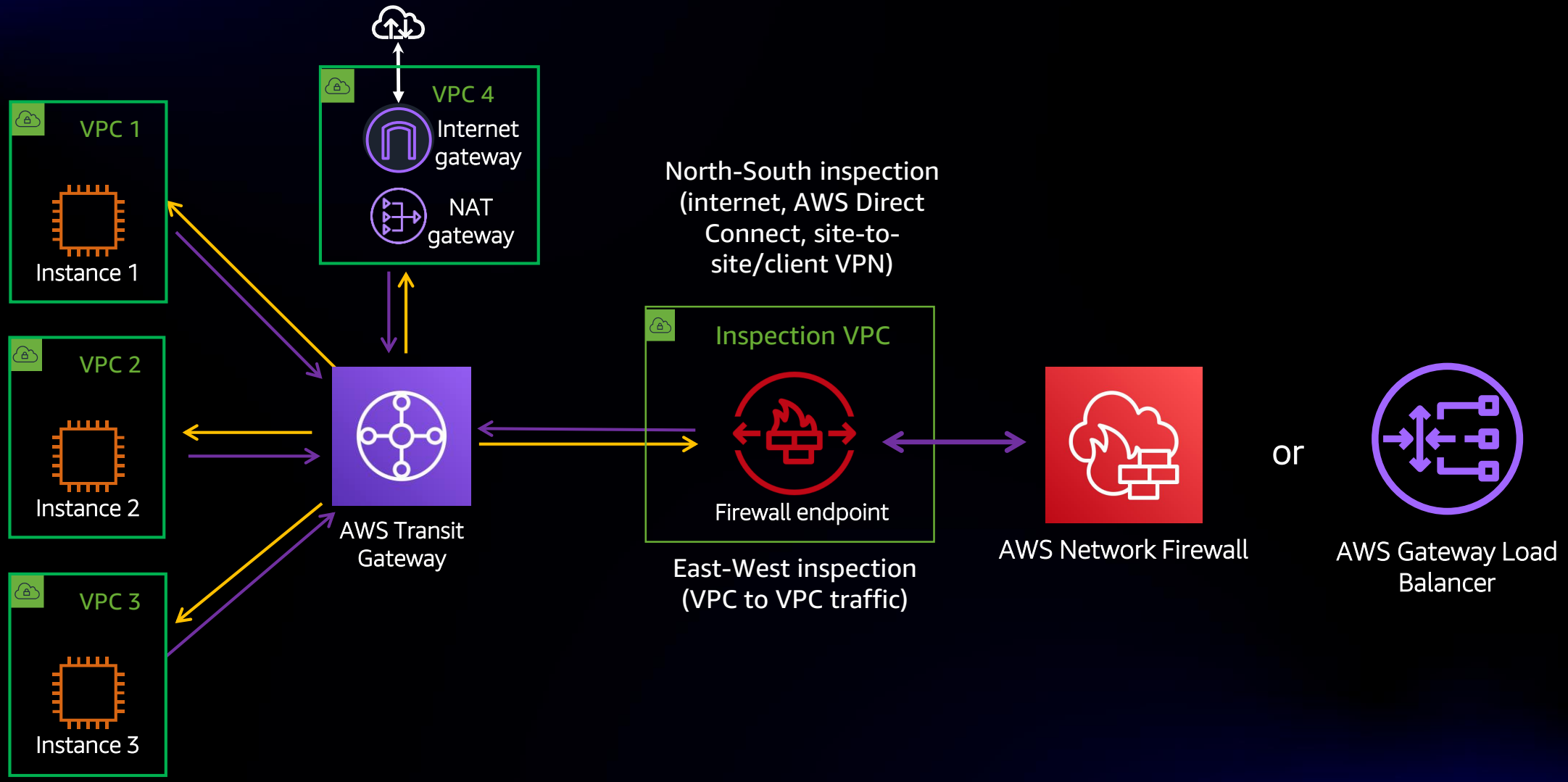
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Distributed security inspection: Details



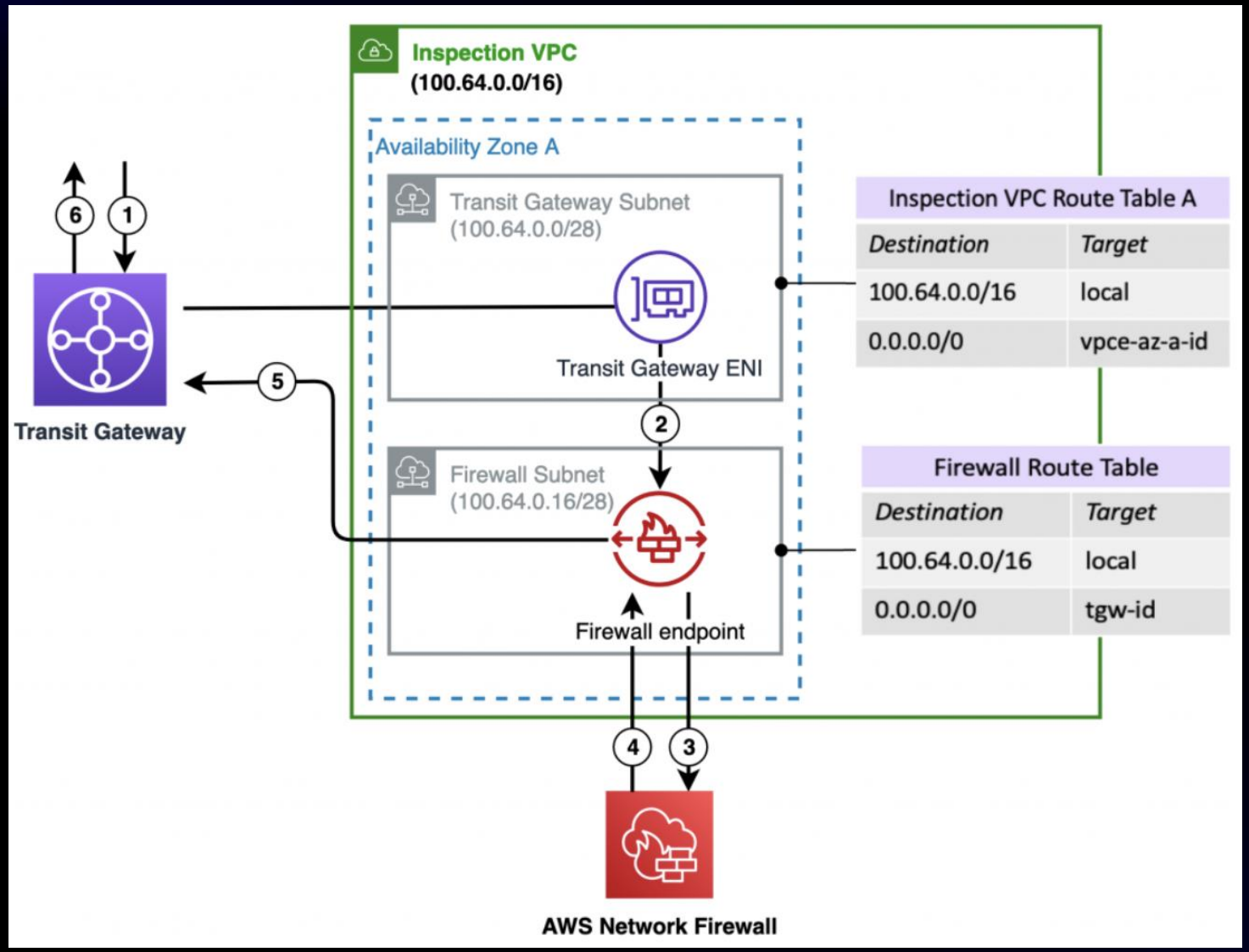
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Centralized security inspection



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Centralized security inspection: Details

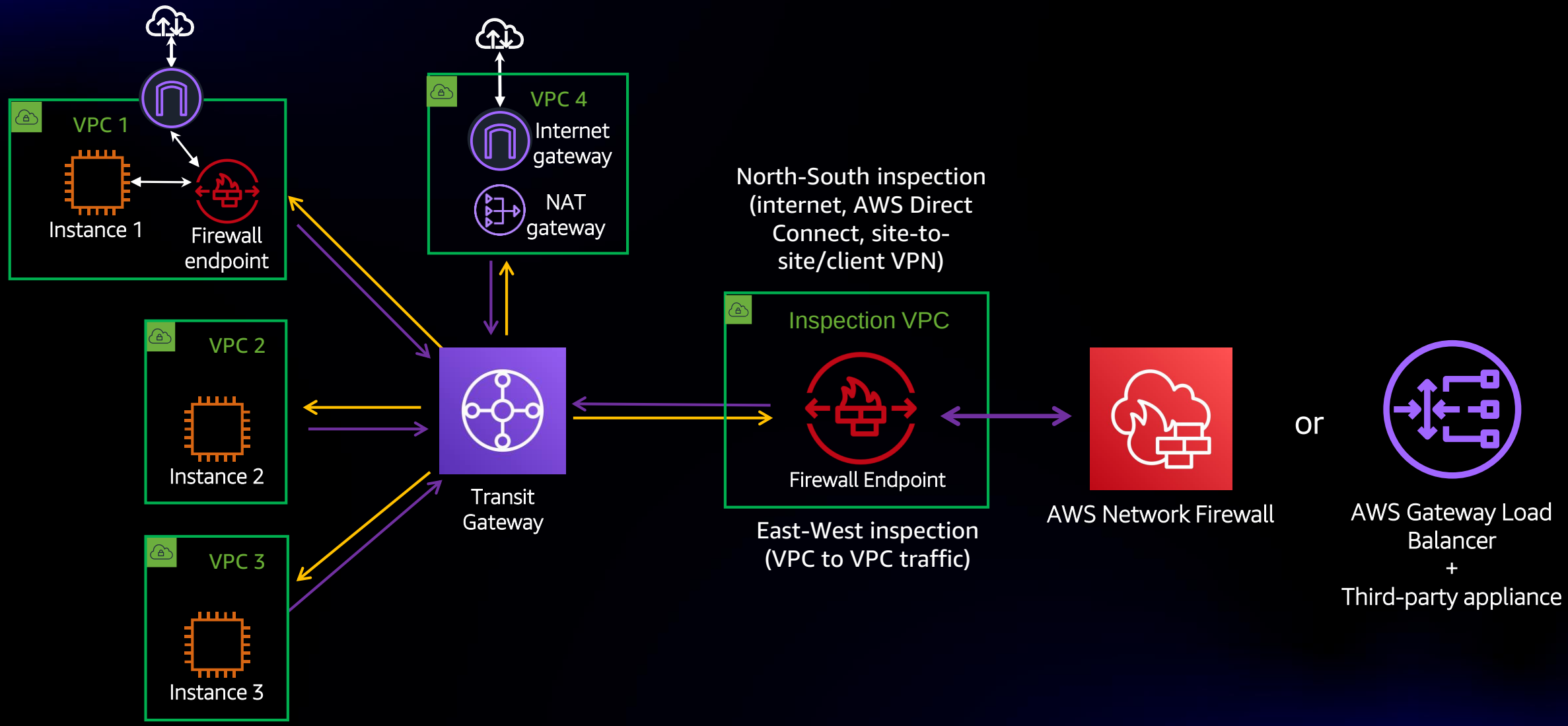


Traffic flowing symmetrically with [TGW appliance mode]

This new TGW feature ensures that return traffic is processed by the same AZ

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Hybrid (mix of both) security inspection



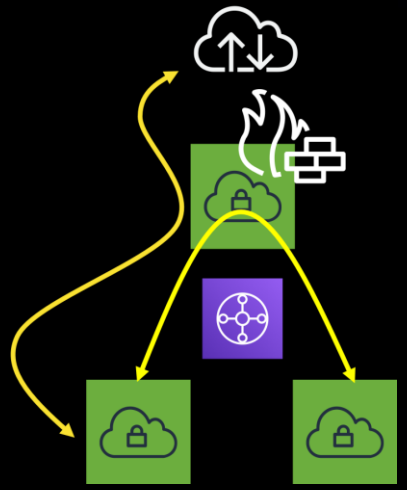
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service updates: New features and use cases

Gateway Load Balancer (and AWS Network Firewall)

- Support for subnet-subnet inspection
- Support for AWS PrivateLink traffic

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Service updates: New features and use cases

AWS Network Firewall

- Supports PCI compliance
- Supports HIPAA eligibility
- Strict-order rule execution
- Optional default drop

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q: How can we improve in terms of overall service gaps, feature gaps with existing services, or areas like technical content?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Kyle Tedeschi
ktedesc@amazon.com

Justin Davies
daviesju@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.