Inspection Deployment Models with AWS Network Firewall

1. *Single VPC inspection with AWS Network Firewall (Distributed Inspection)*

2. *Intra-VPC inspection with AWS Network Firewall and VPC routing enhacement*

3. *East-West centralized inspection with AWS Network Firewall and AWS Transit Gateway*

4. *North-South centralized inspection with AWS Network Firewall and AWS Transit Gateway*

5. *Combined inspection with AWS Network Firewall and AWS Transit Gateway*

NEW 6. *Multi-Region centralized inspection with AWS Network Firewall and AWS Transit Gateway*
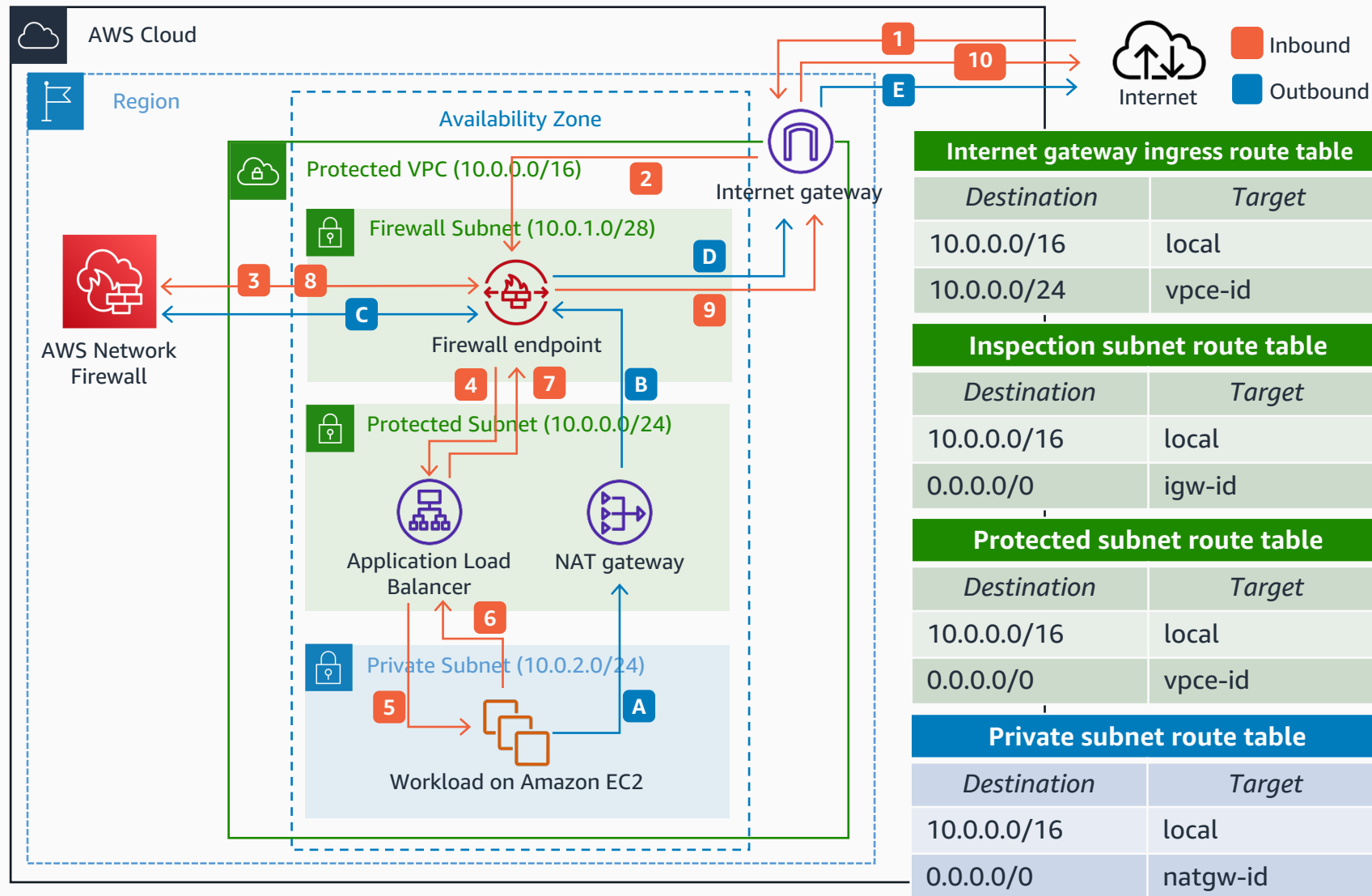
AWS Reference Architecture

Traffic Inspection with AWS Network Firewall

Inspect inbound and outbound traffic using AWS Network Firewall.

Internet gateway ingress route table

Destination	Target
10.0.0.0/16	local
10.0.0.0/24	vpce-id

Inspection subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Protected subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vpce-id

Private subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	natgw-id

1 Traffic initiated from a client on the internet and destined to the public IP of the Application Load Balancer arrives at the internet gateway.

2 In accordance with the internet gateway ingress table, traffic is sent to the firewall endpoint.

3 Traffic is transparently inspected by **AWS Network Firewall**. Allowed traffic is sent back to the firewall endpoint.

4 According to the inspection subnet route table, traffic is sent to the Application Load Balancer.

5 As per the protected subnet route table, the Application Load Balancer forwards the traffic to the target group (workload on **Amazon EC2**).

6 Response traffic is returned back to the Application Load Balancer according to the private subnet route table.

7 In accordance with the protected subnet route table, traffic is sent to the firewall endpoint.

8 Traffic is sent to **AWS Network Firewall**. Traffic that complies with firewall rules is sent back to the firewall endpoint.

9 As per the Inspection subnet route table, traffic is sent to the internet gateway.

10 Traffic is sent back to the internet.

A Traffic initiated from an instance and directed to the internet is forwarded to the NAT gateway, in accordance with private subnet route table.

B Source IP of traffic is changed to the IP of the NAT gateway, and the traffic is forwarded to the firewall endpoint as per the protected subnet route table.

C Traffic is sent to **AWS Network Firewall** for inspection. Traffic that complies with firewall rules is sent back to the firewall endpoint.

D According to inspection subnet route table, traffic is forwarded to the internet gateway.

E Traffic is sent out to the internet.

AWS Reference Architecture

Intra-VPC Inspection with AWS Network Firewall

Use the VPC routing enhancement to inspect intra-VPC traffic (between subnets of the same VPC)

Region

Protected VPC (10.0.0.0/16)

Availability Zone A

Public subnet route table

Destination	Target
10.0.0.0/16	vpce-id-az-a
0.0.0.0/0	igw-id

Private subnet route table (application)

Destination	Target
10.0.0.0/16	vpce-id-az-a

Private subnet route table (DB)

Destination	Target
10.0.0.0/16	vpce-id-az-a

Public subnet 10.0.0.0/24

NAT gateway

ALB

Private subnet (application) 10.0.1.0/24

Amazon EC2 instance (application)

Private subnet (DB) 10.0.2.0/24

Amazon RDS

Internet gateway

Firewall subnet 10.0.3.0/28

Firewall endpoint

Firewall subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	natgw-id

AWS Reference Architecture
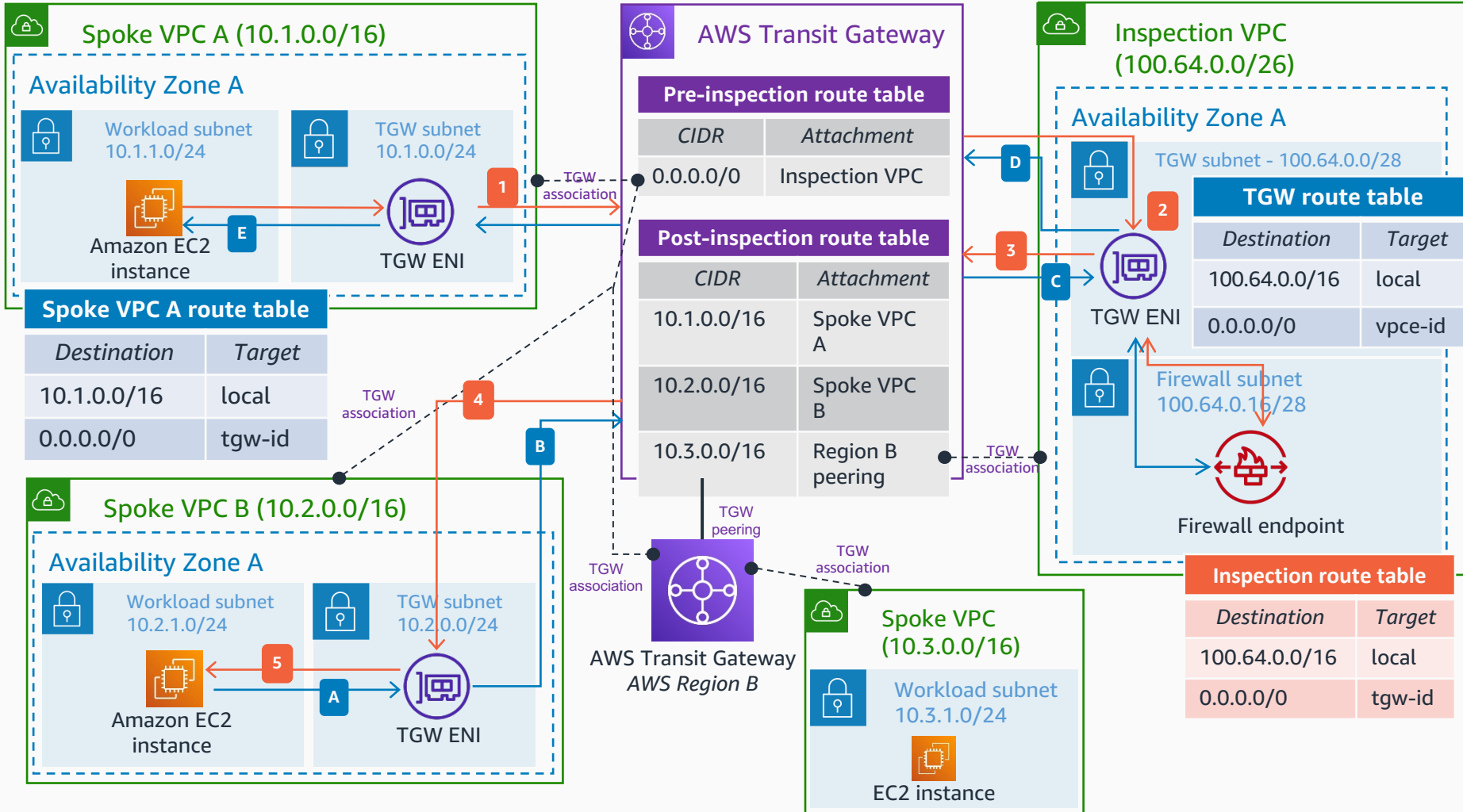
1 Ingress traffic is routed directly to a public workload: web servers or a load balancer.

2 Traffic between the public subnet and the application servers is inspected. It is recommended that you place the firewall endpoint in its own subnet ("Firewall subnet").

3 When the inspection is done, allowed traffic is routed to the application servers.

4
5
6 Outbound traffic to the internet from the application servers: the packets are first sent to the firewall endpoint, and the allowed traffic goes to the load balancer, web servers, or NAT gateway before being sent to the internet.

A
B With VPC routing enhancement, any traffic between private subnets in the VPC can be first sent to the firewall endpoint to inspect the traffic.

C
D You can add a more specific classless inter-domain routing (CIDR) block than the default block in the routing tables to select which inter-VPC traffic is inspected.

For more information about Multi-AZ options or connectivity options using **AWS Transit Gateway**, refer to: Deployment models for AWS Network Firewall with VPC routing enhancements.

East-West Inspection with AWS Network Firewall

Use AWS Transit Gateway to centralize the traffic inspection between several VPCs – both in the same Region, or between Regions.

Spoke VPC A (10.1.0.0/16)

Availability Zone A

Workload subnet 10.1.1.0/24

Amazon EC2 instance

TGW subnet 10.1.0.0/24

TGW ENI

Spoke VPC A route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

AWS Transit Gateway

Pre-inspection route table

CIDR	Attachment
0.0.0.0/0	Inspection VPC

Post-inspection route table

CIDR	Attachment
10.1.0.0/16	Spoke VPC A
10.2.0.0/16	Spoke VPC B
10.3.0.0/16	Region B peering

TGW peering

TGW association

AWS Transit Gateway
AWS Region B

Spoke VPC B (10.2.0.0/16)

Availability Zone A

Workload subnet 10.2.1.0/24

Amazon EC2 instance

TGW subnet 10.2.0.0/24

TGW ENI

Spoke VPC (10.3.0.0/16)

Workload subnet 10.3.1.0/24

EC2 instance

Inspection VPC (100.64.0.0/26)

Availability Zone A

TGW subnet - 100.64.0.0/28

TGW ENI

TGW route table

Destination	Target
100.64.0.0/16	local
0.0.0.0/0	vpce-id

Firewall subnet 100.64.0.16/28

Firewall endpoint

Inspection route table

Destination	Target
100.64.0.0/16	local
0.0.0.0/0	tgw-id

1 Any traffic leaving a spoke VPC is routed to **AWS Transit Gateway (TGW)**. The **Transit Gateway** route table associated with the VPCs and **Transit Gateway** peering forwards the traffic to the Inspection VPC.

2 The Inspection VPC route table forwards all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the **Transit Gateway**.

3 The **Transit Gateway** route table associated with the Inspection VPC attachment has all the routes within the network.

4 In this particular example, the traffic is destined to Spoke VPC B.

5 In Spoke VPC B, the **TGW** subnet route table is routing the traffic to the destination instance.

A Traffic from an instance in Spoke VPC B to Spoke VPC A first reaches the **Transit Gateway** endpoint in the **TGW** subnet. The traffic is routed to the **Transit Gateway**.

B The **Transit Gateway** route table sends the traffic to the Inspection VPC, where it is routed to the firewall endpoint for inspection.

C

D Allowed traffic comes back to the **Transit Gateway**. The route table associated with the Inspection VPC forwards the traffic to the Spoke VPC A.

E

** It is recommended to use Transit Gateway appliance mode in the Inspection VPC **Transit Gateway** attachment to maintain flow symmetry.*
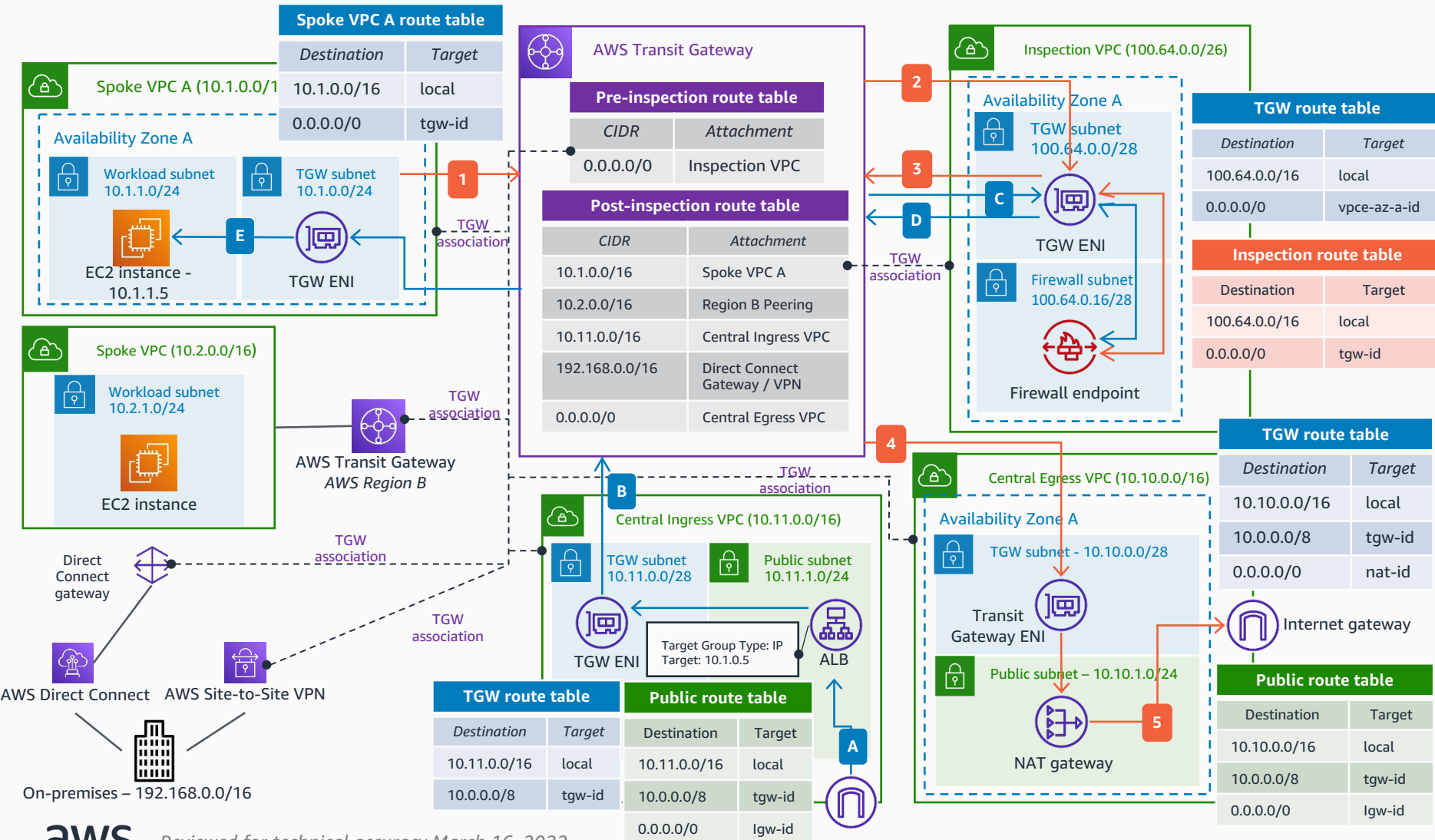
For more information about deployment models with **AWS Network Firewall** and **AWS Transit Gateway**, refer to: Deployment Models for AWS Network Firewall.

AWS Reference Architecture

North-South Inspection with AWS Network Firewall

Use AWS Transit Gateway to centralize the traffic inspection from/to the Internet, or from/to on-prem facilities connected via AWS Direct Connect or AWS Site-to-Site VPN.

Spoke VPC A route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

AWS Transit Gateway

Pre-inspection route table

CIDR	Attachment
0.0.0.0/0	Inspection VPC

Post-inspection route table

CIDR	Attachment
10.1.0.0/16	Spoke VPC A
10.2.0.0/16	Region B Peering
10.11.0.0/16	Central Ingress VPC
192.168.0.0/16	Direct Connect Gateway / VPN
0.0.0.0/0	Central Egress VPC

TGW route table (Inspection VPC)

Destination	Target
100.64.0.0/16	local
0.0.0.0/0	vpce-az-a-id

Inspection route table

Destination	Target
100.64.0.0/16	local
0.0.0.0/0	tgw-id

TGW route table (Central Egress VPC)

Destination	Target
10.10.0.0/16	local
10.0.0.0/8	tgw-id
0.0.0.0/0	nat-id

Public route table (Central Egress VPC)

Destination	Target
10.10.0.0/16	local
10.0.0.0/8	tgw-id
0.0.0.0/0	igw-id

TGW route table (Central Ingress VPC)

Destination	Target
10.11.0.0/16	local
10.0.0.0/8	tgw-id

Public route table (Central Ingress VPC)

Destination	Target
10.11.0.0/16	local
10.0.0.0/8	tgw-id
0.0.0.0/0	igw-id

Target Group Type: IP
Target: 10.1.0.5

AWS Reference Architecture

1. Traffic from the instance in Spoke VPC A destined to the internet is routed to the **Transit Gateway**. The **Transit Gateway** route table associated with the attachment sends all the traffic (0.0.0.0/0) to the Inspection VPC.

2. The Inspection VPC **TGW** subnet route table sends all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the **Transit Gateway**.

3. The **Transit Gateway** route table associated with the Inspection VPC attachment has all the routes within the network.

4. In this particular use case, as the traffic needs to be routed to the internet, the **Transit Gateway** will forward the traffic to the Central Egress VPC.

5. The **TGW** subnet route table of the Central Egress VPC sends the traffic to the NAT gateway, so the private IP of the client can be translated to the private IP of the NAT gateway, and in turn, translated to the public IP by the internet gateway.

A. Traffic coming from the internet reaches the Central Ingress VPC. In this example, an Application Load Balancer sends the request to the target group of configured IP addresses through the **Transit Gateway**.

B. The traffic is forwarded to the Inspection VPC in accordance to the Pre-inspection route table in **Transit Gateway**.

C. As with the egress traffic, the Inspection VPC **TGW** subnet route table sends all the traffic to the firewall endpoint. Allowed traffic is

D. forwarded back to the **Transit Gateway** and subsequently to the destination VPC (Spoke VPC A).

E. The Spoke VPC A route table sends the traffic to the desired instance - 10.1.1.5.

It is recommended to use Transit Gateway appliance mode in the Inspection VPC Transit Gateway attachment to maintain flow symmetry.
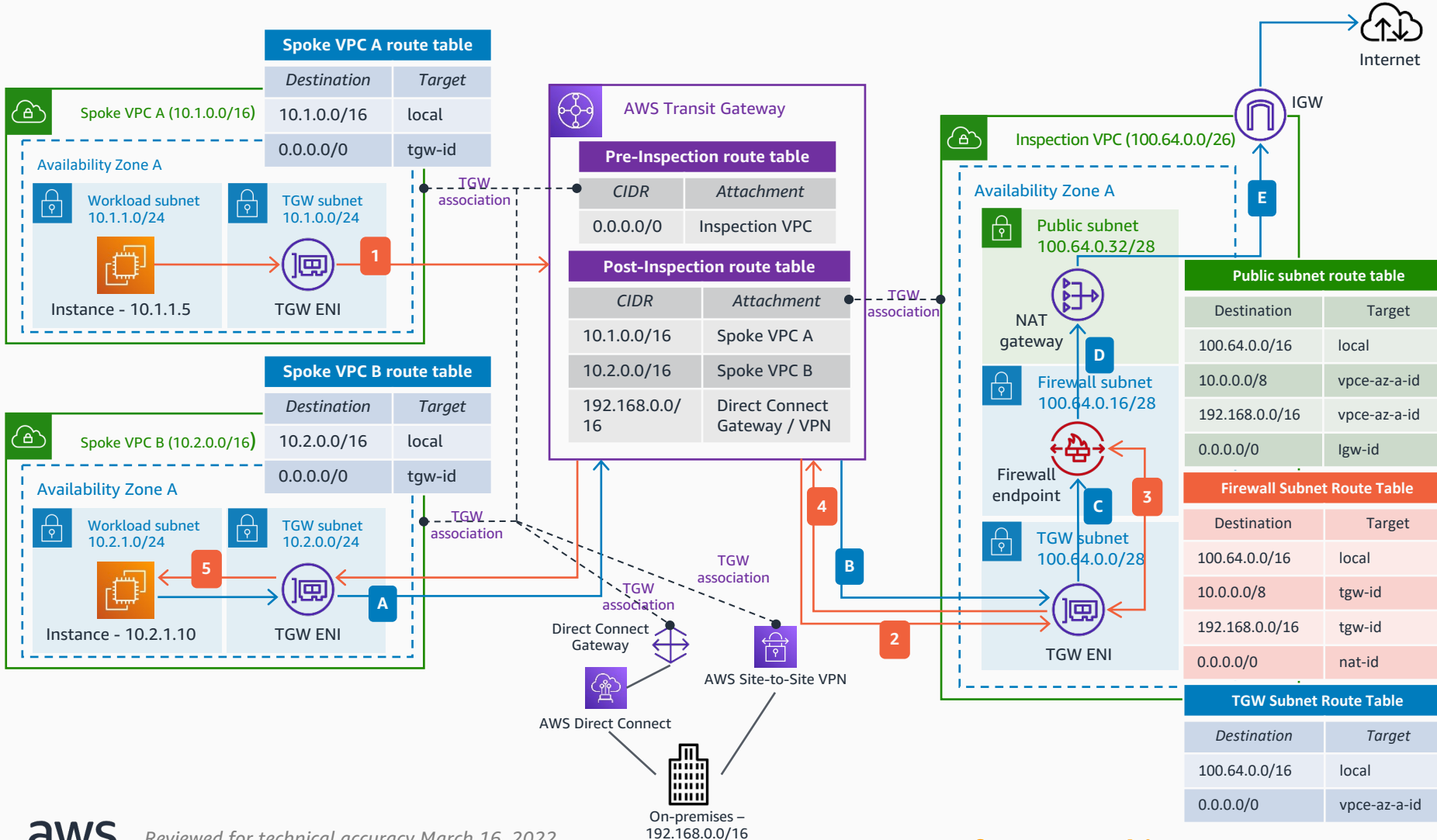
Combined Inspection with AWS Network Firewall

Use AWS Transit Gateway to centralize the East/West inspection between VPCs, while you have a NAT gateway in the Inspection VPC for centralized egress and the North/South inspection.

Spoke VPC A route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC A (10.1.0.0/16)

Availability Zone A

Workload subnet 10.1.1.0/24

TGW subnet 10.1.0.0/24

Instance - 10.1.1.5

TGW ENI

1

TGW association

AWS Transit Gateway

Pre-Inspection route table

CIDR	Attachment
0.0.0.0/0	Inspection VPC

Post-Inspection route table

CIDR	Attachment
10.1.0.0/16	Spoke VPC A
10.2.0.0/16	Spoke VPC B
192.168.0.0/16	Direct Connect Gateway / VPN

Spoke VPC B route table

Destination	Target
10.2.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC B (10.2.0.0/16)

Availability Zone A

Workload subnet 10.2.1.0/24

TGW subnet 10.2.0.0/24

Instance - 10.2.1.10

TGW ENI

5 **A**

TGW association

TGW association

TGW association

Direct Connect Gateway

AWS Direct Connect

AWS Site-to-Site VPN

On-premises – 192.168.0.0/16

AWS Reference Architecture

Inspection VPC (100.64.0.0/26)

Availability Zone A

Public subnet 100.64.0.32/28

NAT gateway **D**

Firewall subnet 100.64.0.16/28

Firewall endpoint **C** **3**

TGW subnet 100.64.0.0/28

TGW ENI

2 **B**

4

IGW **E**

Internet

Public subnet route table

Destination	Target
100.64.0.0/16	local
10.0.0.0/8	vpce-az-a-id
192.168.0.0/16	vpce-az-a-id
0.0.0.0/0	Igw-id

Firewall Subnet Route Table

Destination	Target
100.64.0.0/16	local
10.0.0.0/8	tgw-id
192.168.0.0/16	tgw-id
0.0.0.0/0	nat-id

TGW Subnet Route Table

Destination	Target
100.64.0.0/16	local
0.0.0.0/0	vpce-az-a-id

---

1 Traffic from an instance in Spoke VPC A destined to another instance in Spoke VPC B (East/West traffic) is routed to the **Transit Gateway**.

2 The **Transit Gateway** route table associated with the attachment sends all the traffic (0.0.0.0/0) to the Inspection VPC.

3 The Inspection VPC TGW subnet route table sends all the traffic to the firewall endpoint. The allowed traffic is forwarded back to the TGW ENI.

4 As per the **Transit Gateway** route table associated with the Inspection VPC, the traffic is sent to Spoke VPC B.

5 Finally, in the TGW subnet route table of the Spoke VPC B, the traffic is sent to the destination – 10.2.1.10.

A Traffic from an instance in Spoke VPC B destined to the internet (North/South traffic) is routed to the **Transit Gateway**.

B The **Transit Gateway** route table associated with the attachment sends all the traffic (0.0.0.0/0) to the Inspection VPC – same as in the previous example.

C The Inspection VPC **TGW** subnet route table sends all the traffic to the firewall endpoint, where it is transparently analyzed.

D Allowed traffic is sent to the NAT gateway as per the Firewall subnet route table.

E The private IP of the client is translated to the private IP of the NAT gateway, and in turn, translated to the public IP by the internet gateway.

** It is recommended to use Transit Gateway appliance mode in the Inspection VPC **Transit Gateway** attachment to maintain flow symmetry.*

If you want to check an example of this architecture in Terraform, check: AWS Hub and Spoke Architecture with an Inspection VPC.
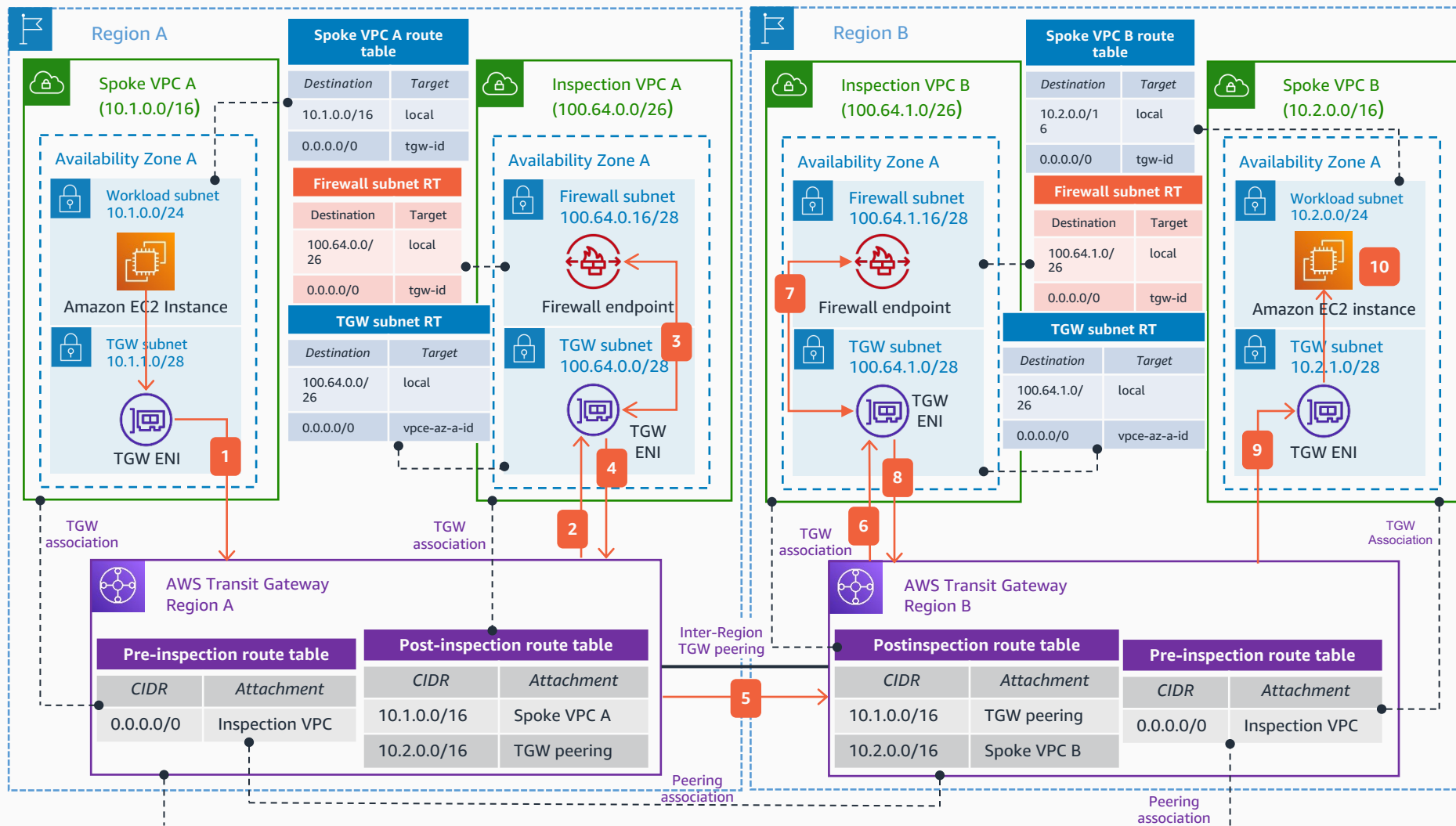
Multi-Region Inspection with AWS Network Firewall

When using AWS Transit Gateway to centralize your inspection and inter-Region peering between two AWS Regions, it is a best practice to inspect the traffic in each AWS Region to avoid asymmetric traffic.

1 Traffic from an instance in Spoke VPC A destined to another instance in Spoke VPC B is routed to the **Transit Gateway** in Region A as per the Spoke VPC A route table.

2 The **Transit Gateway** (Region A) route table associated with the attachment (Pre-inspection route table) sends all the traffic (0.0.0.0/0) to the inspection VPC A.

3 The inspection VPC A **TGW** subnet route table sends all the traffic to the firewall endpoint for transparent inspection.

4 The allowed traffic is forwarded back to the **TGW** ENI.

5 As per the **Transit Gateway** (Region A) route table associated with the Inspection VPC A (Post-inspection route table), the traffic is sent to Region B via the **Transit Gateway** peering.

6 As per the **Transit Gateway** (Region B) route table associated with the **Transit Gateway** peering (Pre-inspection route table), the traffic is sent to the inspection VPC B for inspection.

7 The inspection VPC B TGW subnet route table sends all the traffic to the firewall endpoint for transparent inspection.

8 The allowed traffic is forwarded back to the TGW ENI.

9 As per the **Transit Gateway** (Region B) route table associated with the inspection VPC A (Post-inspection route table), the traffic is sent to Spoke VPC B.

10 Traffic is forwarded to the destination – the **Amazon EC2** instance in Spoke VPC B.

AWS Reference Architecture

** It is recommended to use Transit Gateway appliance mode in the Inspection VPC **Transit Gateway** attachments to maintain flow symmetry.*