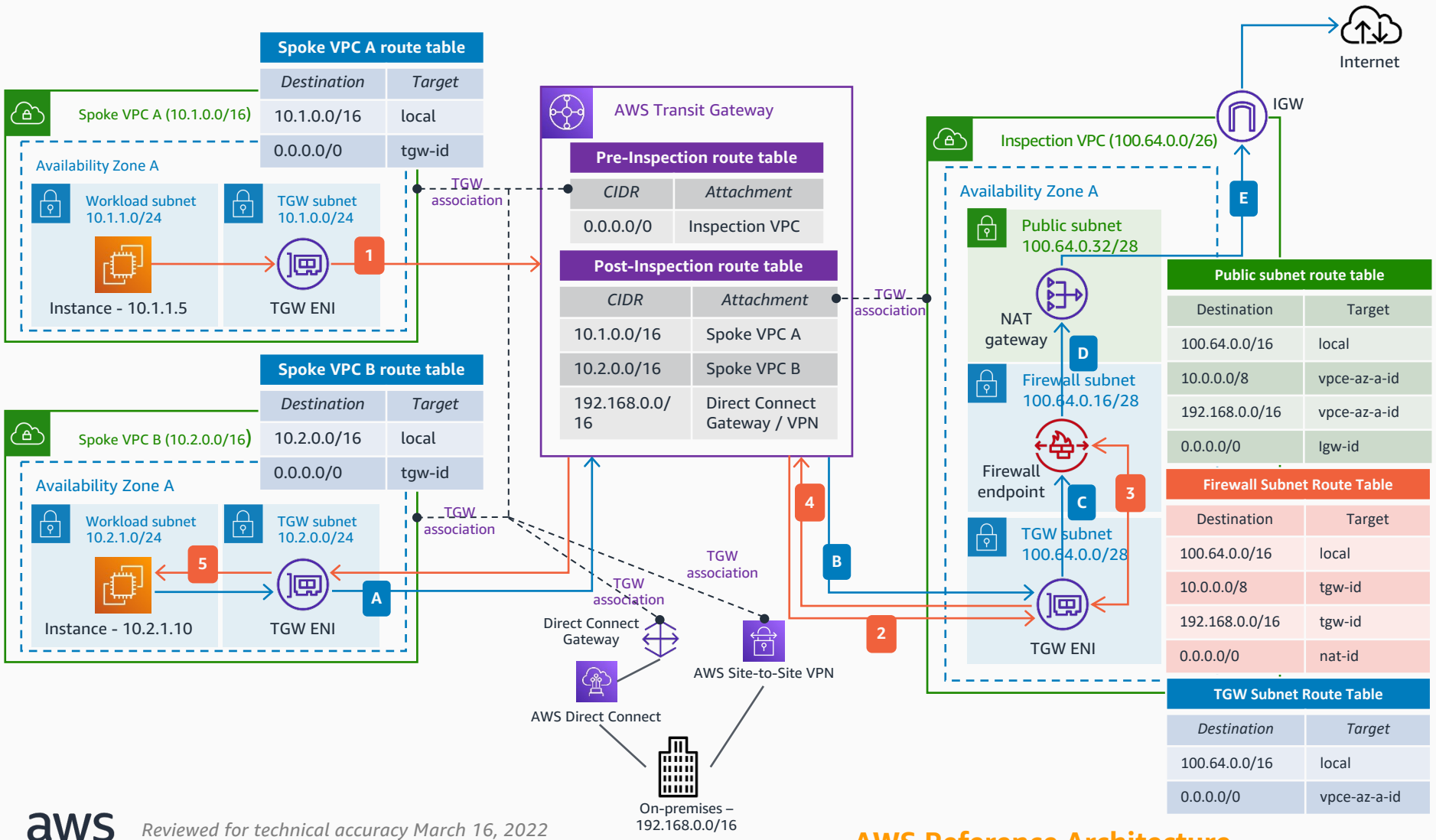
Combined Inspection with AWS Network Firewall

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.



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.

Reviewed for technical accuracy March 16, 2022

AWS Reference Architecture