Multicast Reference Architectures with AWS Transit Gateway

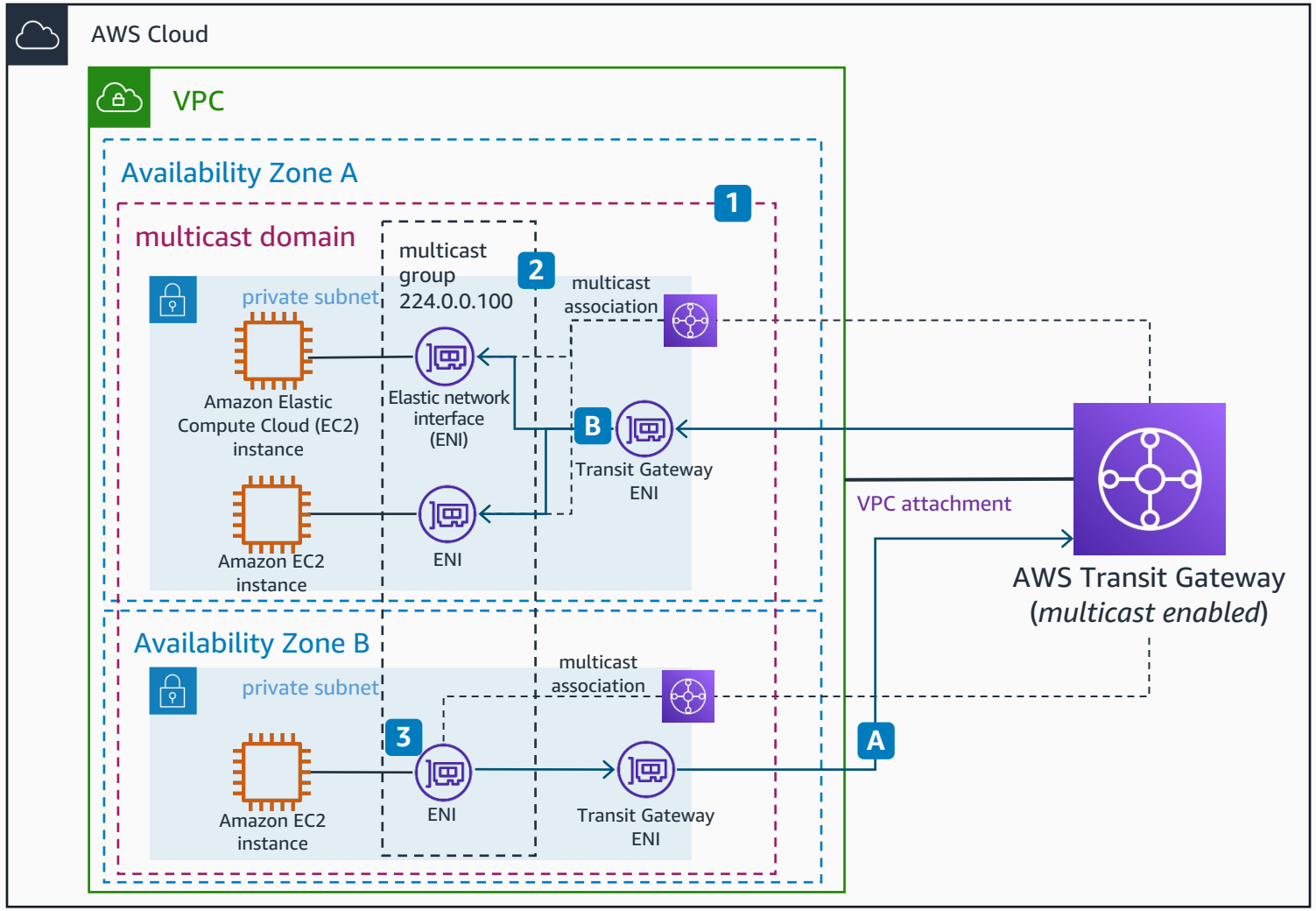
1. *Multicast traffic in a single VPC*
2. *Multicast traffic in multi-account environments*
3. *Integrating external multicast services and AWS*

Reviewed for technical accuracy May 5, 2022

AWS Reference Architecture

Multicast traffic in a single VPC

Use AWS Transit Gateway to build your multicast applications in AWS. This reference architecture series shows how you can do it in a single VPC and in a multi-VPC/multi-account strategy, and also how to integrate external multicast services with AWS. The diagram below shows the configuration for a single VPC.



1 You can achieve segmentation of the multicast traffic by creating a multicast domain, which defines the subnet(s) that participates in the multicast communication. Multicast association (domain membership) is defined at the subnet level, and a single subnet can only be associated with one multicast domain.

2 A multicast group defines the number of hosts that will send and/or receive the same multicast traffic. You can define several multicast groups within the same multicast domain. It is identified by a group IP address, and its membership is defined by individual ENIs.

3 An ENI associated with a supported **Amazon EC2** instance receives multicast traffic by being a multicast group member. Nitro instances* can receive and/or send traffic in a static source group membership configuration. With IGMPv2** enabled, any Nitro instance can send traffic without static configuration. Non-Nitro instances can only receive traffic via static configuration.

A An **EC2** instance in Availability Zone B sends a multicast packet using the multicast group IP address 224.0.0.100.

B The packet will arrive at the **AWS Transit Gateway**, which will redirect it to the other instances in the same group (the two located in Availability Zone A).

** For more information about Nitro instances, refer to Instances built on the Nitro System.*

*** For more information about the IGMPv2 protocol, refer to the RFC 2236.*

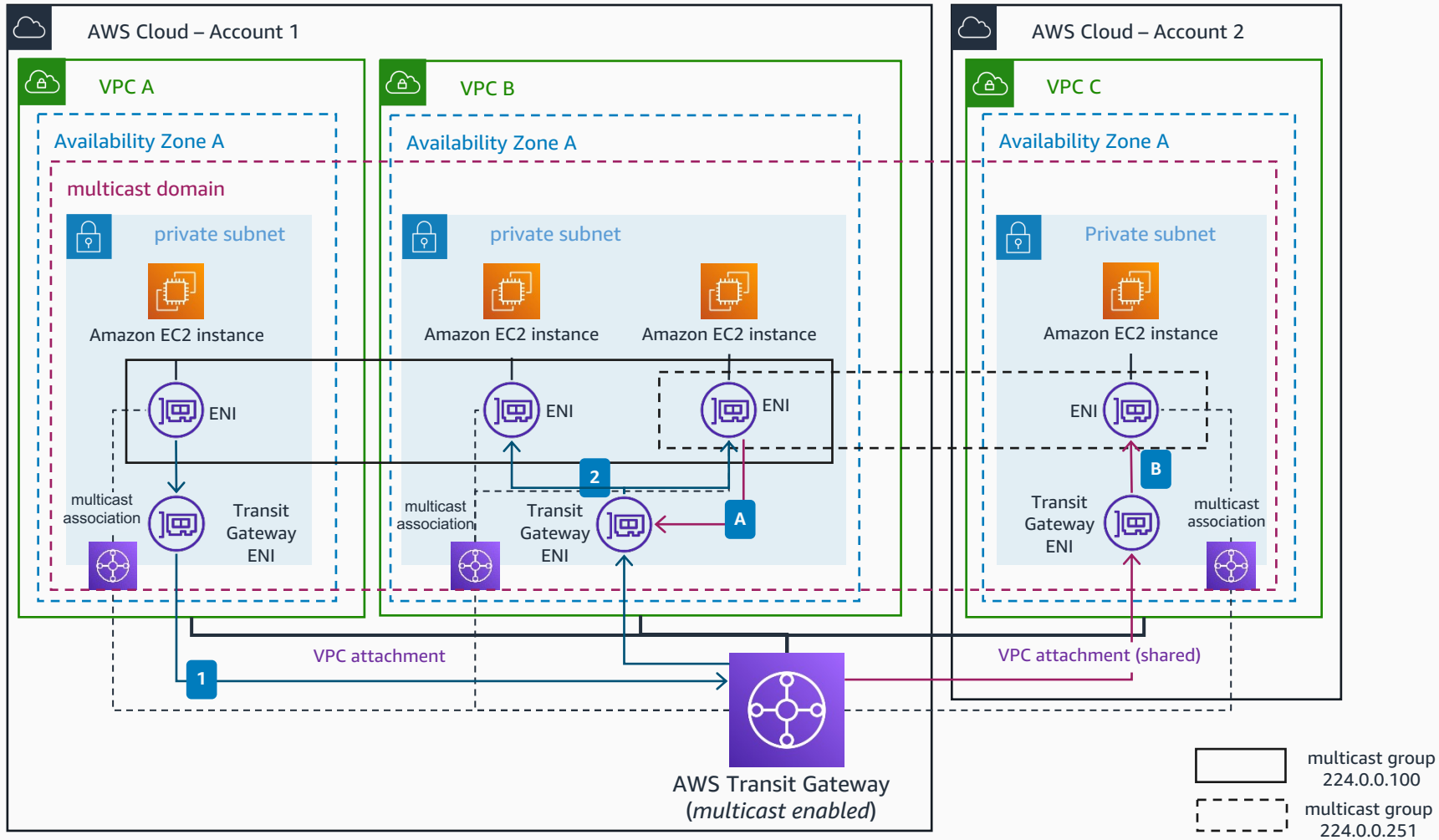
For more information about multicast on AWS Transit Gateway, refer to Multicast on transit gateways.

Reviewed for technical accuracy May 9, 2022

AWS Reference Architecture

Multicast traffic in multi-account environments

You can use AWS Resource Access Manager (RAM) to share multicast domains to other AWS accounts. The consumers can associate/disassociate subnets to the multicast domain, and register/deregister group members or group sources. If you are sharing multicast domains within AWS Organizations, remember that you need to enable sharing.



1 All the subnets in Amazon Virtual Private Clouds (VPCs) from both accounts are associated to the multicast domain. In the first example, instances in VPCs from Account 1 use the 224.0.0.100 multicast group for their multicast communication. Those instances use the IGMP protocol to dynamically join, leave, and send messages within the group, so the group members can be senders and receivers at the same time.

2 Any multicast message sent by any instance in the group will be received by the others, using **AWS Transit Gateway** as the multicast router.

A The **EC2** instance located in the VPC from Account 2 joined the multicast group 224.0.0.251 using a static source group membership configuration, meaning that it can only receive traffic.

B One of the instances in VPC B sends multicast traffic to the 224.0.0.251 multicast group using the **Transit Gateway** as multicast router. If IGMPv2 is enabled for the domain, any instance (if Nitro) will also be able to send traffic.

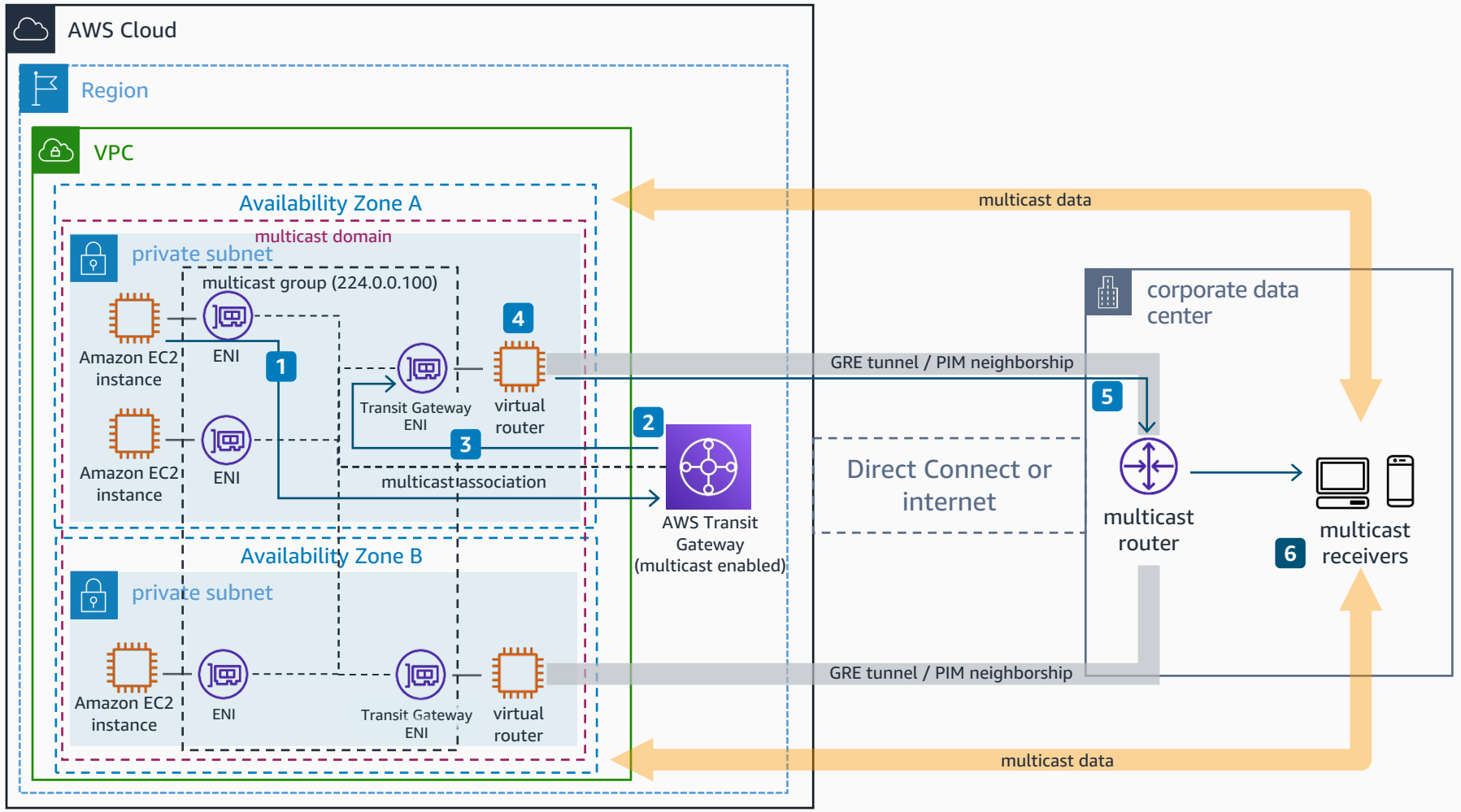
For more information about how you can use IGMP to join multicast groups in AWS, refer to Automating service discovery using AWS Transit Gateway Multicast with IGMP.

Reviewed for technical accuracy May 9, 2022

AWS Reference Architecture

Integrating external multicast services and AWS

Integrating external multicast services and AWS by leveraging third party, multicast-routing-capable appliances within a VPC.



1. The multicast source sends traffic to a multicast group – or physical/virtual network interface controller (NIC) outside AWS – through its ENI.
2. An **AWS Transit Gateway** with the multicast domain configuration and registered source and members forwards the packet to the virtual router.
3. The virtual router deployed in an **Amazon VPC** receives the multicast packets.
4. The virtual routers are responsible for delivering the multicast packets between different network segments, Protocol Independent Multicast (PIM*) being a popular choice. In this example, the multicast packets are forwarded via a Generic Routing Encapsulation (GRE**) tunnel established between the virtual routers in AWS and the multicast router in the corporate data center.
5. The on-premises router receives packets via the tunnel and decapsulates them.
6. Decapsulated packets are sent over the downstream multicast interface to the receivers.

** To know more about PIM, refer to the RFC 7761.*

*** To know more about GRE, check the RFC 2784.*

For more information about integrating external multicast services with AWS using AWS Transit Gateway, refer to Integrating external multicast services with AWS.

Reviewed for technical accuracy May 9, 2022

AWS Reference Architecture