**VPC to VPC connectivity**

Customers can use two different VPC flow patterns to set up multi-VPC environments: many-to-many, or hub-and-spoke. In the many-to-many approach, the traffic between each VPC is managed individually between each VPC. In the hub-and-spoke model, all inter-VPC traffic flows through a central resource, which routes traffic based on established rules.

**VPC peering**

The simplest way to connect two VPCs is to use VPC Peering. In this setup, a connection enables full bidirectional connectivity between the VPCs. This peering connection is used to route traffic between the VPCs. VPCs across accounts and AWS Regions can also be peered together. VPC peering incurs costs only for traffic traveling over the connection (there is no hourly infrastructure fee). VPC peering is point-to-point connectivity, and it does not support transitive routing. For example, if you have a VPC peering connection between VPC A and VPC B and between VPC A and VPC C, an instance in VPC B cannot transit through VPC A to reach VPC C. To route packets between VPC B and VPC C, you are required to create a direct VPC peering connection.

There is a maximum limit of up to 125 active peering connections per VPC.

[n(n-1)/2] where n=total number of VPCs

**AWS Transit Gateway**

AWS Transit Gateway provides a hub and spoke design for connecting VPCs and on-premises networks as a fully managed service without requiring you to provision virtual appliances like the Cisco CSRs. No VPN overlay is required, and AWS manages high availability and scalability. Transit Gateway enables customers to connect thousands of VPCs. You can attach all your hybrid connectivity (VPN and Direct Connect connections) to a single Transit Gateway instance, consolidating and controlling your organization's entire AWS routing configuration in one place (refer to the figure under Transit VPC Solution). Transit Gateway controls how traffic is routed among all the connected spoke networks using route tables. This hub-and-spoke model simplifies management and reduces operational costs because VPCs only connect to the Transit Gateway instance to gain access to the connected networks.

**Transit VPC solution**

Transit VPCs can solve some of the shortcomings of VPC peering by introducing a hub and spoke design for inter-VPC connectivity. In a transit VPC network, one central VPC (the hub VPC) connects with every other VPC (spoke VPC) through a VPN connection typically leveraging BGP over IPsec. The central VPC contains Amazon Elastic Compute Cloud (Amazon EC2) instances running software appliances that route incoming traffic to their destinations using the VPN overlay. Transit VPC peering has the following advantages:

• Transitive routing is enabled using the overlay VPN network — allowing for a simpler hub and spoke design.

• When using third-party vendor software on the EC2 instance in the hub transit VPC, vendor functionality around advanced security (layer 7 firewall/Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) ) can be used. If customers are using the same software on-premises, they benefit from a unified operational/monitoring experience.

• The Transit VPC architecture enable connectivity that may be desired in some use-cases. For example, you can connect an AWS GovCloud instance and Commercial Region VPC or a Transit Gateway instance to a Transit VPC and enable inter-VPC connectivity between the two Regions. Evaluate your security and compliance requirements when considering this option. For additional security, you may deploy a centralized inspection model using design patterns described later in this whitepaper.

