Introduction to Deploying Transit VPC for Amazon Web Services

This section contains the following topics:

Information About Transit VPC for Amazon Web Services

The Transit VPC design in the Amazon Web Services (AWS) marketplace uses multiple instances of the Cisco CSR 1000v. The Transit VPC design provides secure transit routing between spoke Virtual Private Clouds (VPCs) and the public internet or private data center. A transit VPC acts as a global network transit center, which allows a common strategy to be used to connect multiple, geographically disperse VPCs and remote networks. This can save time and effort and reduce costs, as it is implemented virtually without the traditional expense of establishing a physical presence in a colocation transit hub or deploying physical network gear. The Transit VPC design takes advantage of Cisco routing and security features.

Cisco DMVPN uses a centralized architecture to provide easier implementation and management for deployments that require granular access controls for diverse user communities, including mobile workers, telecommuters, and extranet users. Cisco DMVPN allows branch locations to communicate directly with each other over the public WAN or Internet, such as when using voice over IP (VOIP) between two branch offices. However, it doesn't require a permanent VPN connection between sites. Cisco DMVPN enables the zero-touch deployment of IPsec VPNs and improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization. The Cisco DMVPN solution is widely used to connect data centers and branches. The branches can exist in a public cloud environment such as AWS. The transit VPC design allows for automated DMVPN deployment between the public cloud and the private data center. If you use the Cisco CSR 1000v in the AWS cloud, you can take advantage of the functionality of enterprise-class networking services and VPNs that provide flexibility and security. The transit VPC network is treated as a spoke and is connected to a hub to form part of the DMVPN network. The transit VPC network communicates directly with other spokes, whether the spokes are in physical branch locations, or in private / public clouds.

The decision to use a transit VPC network is determined by your needs to provide connectivity between VPCs in the same account or different accounts and to provide connectivity between the public cloud, private data center and internet. The advantage of using a transit VPC network is that every time a new VPC is deployed, there is no need for manual intervention to provide connectivity—the VPC is automatically connected to the

rest of the network. This document shows how you can deploy a new VPC using an AWS CloudFormation template—see Launching a Transit VPC Hub.

The cost of using a Cisco transit VPC network design depends upon your choice of instance type, type of license and whether the Cisco CSR 1000v spoke VPCs are deployed in High Availability mode. For more information about the cost of instances, refer to the AWS website. You can buy a Bring Your Own License (BYOL) type license directly from Cisco and choose the licensing package that you need. As the transit VPC network requires IPsec, BGP and BFD, you must obtain either a Cisco Security or AX Technology Package License for each Cisco CSR 1000v.

A transit VPC network simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks. Using a transit VPC design with Cisco CSR 1000v routers can save time, effort and money compared to using a network with physical networking gear in a colocation transit hub.

The three main components in the transit VPC design are summarized in the list below. (The processes for launching transit VPC hub, spoke VPC and DMVPN are described later in Deploying Transit VPC for Amazon Web Services.)

1. Transit VPC hub—two Cisco CSR 1000v's are transit routers that connect to "spoke VPC" routers.

   The transit VPC hub controls outward traffic flow; for example, between a spoke VPC and another VPC or remote network. The hub has two Cisco CSR 1000v instances, which allow for VPN termination and routing. Each instance is in a separate Availability Zone.

   For details about launching the transit VPC hub, see Launching a Transit VPC Hub. In the procedure, you use the AWS CloudFormation "transit-vpc-template" to enter values for bootstrapping the AWS infrastructure and automating the deployment of a transit VPC on the AWS Cloud. You can customize the network configuration by adjusting the template parameter values. For example, you can specify any of the available size options for the Cisco CSR 1000v, based on the required network bandwidth.

2. Spoke VPC—a Cisco CSR 1000v that is connects to the transit hub VPC using a dynamically routed VPN connection.

   The VPN connections of spoke VPCs allow the spoke VPCs to use routing and failover capabilities to maintain highly available network connections. IPSec tunnels provide connectivity between spoke VPCs.

3. DMVPN—dynamically routed VPN connections between private data center, branch networks and spoke VPCs.

   If you already have a DMVPN network with a hub on premise, with spokes for the branches and you would like to expand the branches into the public cloud, you can connect a transit VPC cloud network with your existing DMVPN network.

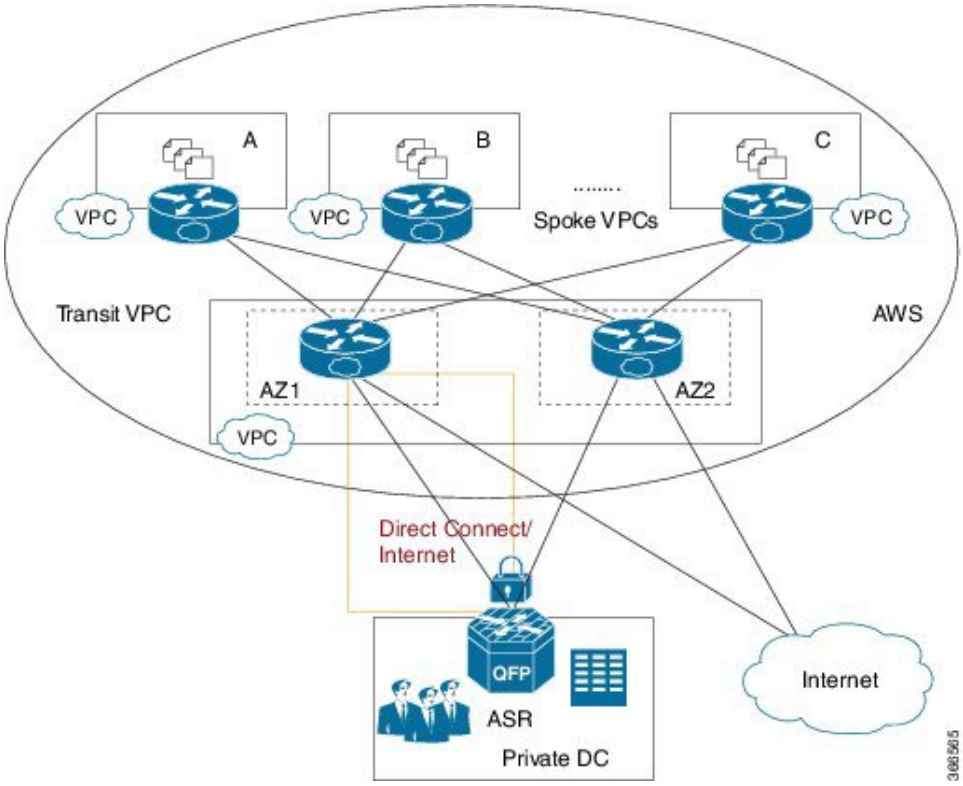
Transit VPC Hub and Spoke VPCs

The transit VPC hub, which uses two Cisco CSR 1000v's as transit routers, connects to spoke VPC's (Cisco CSR 1000v's). An example topology is shown in the figure below. The two transit VPC hub routers are shown in availability zones AZ1 and AZ2.

To deploy transit VPC hub and spoke VPC's, enter values in a template as described in Launching a Transit VPC Hub.

The following figure shows an example transit VPC design in which a transit hub has two Cisco CSR 1000v's (CSR-A and CSR-B).

Figure 1: Transit VPC with Cisco CSR 1000v



DMVPN Transit VPC

In a DMVPN transit VPC design, DMVPN is used to provide dynamically routed VPN connections between the data center, branch networks, transit VPC (hub) and spoke VPCs. Failover capabilities provide highly available network connections to transit VPC instances. Connectivity between the private data center and the public cloud is over the internet; however, it is protected by IPSec.

To deploy DMVPN, enter values in a template as described in Launching DMVPN for Transit VPC.

The following figure shows an example DMVPN Transit VPC design, with a private data center hub, two branch networks (DMVPN hubs) and transit VPC/spoke VPCs.

Figure 2: DMVPN with Transit VPC