Transit Network VPC

AWS Reference Deployment Guide

Last updated: May 10, 2017

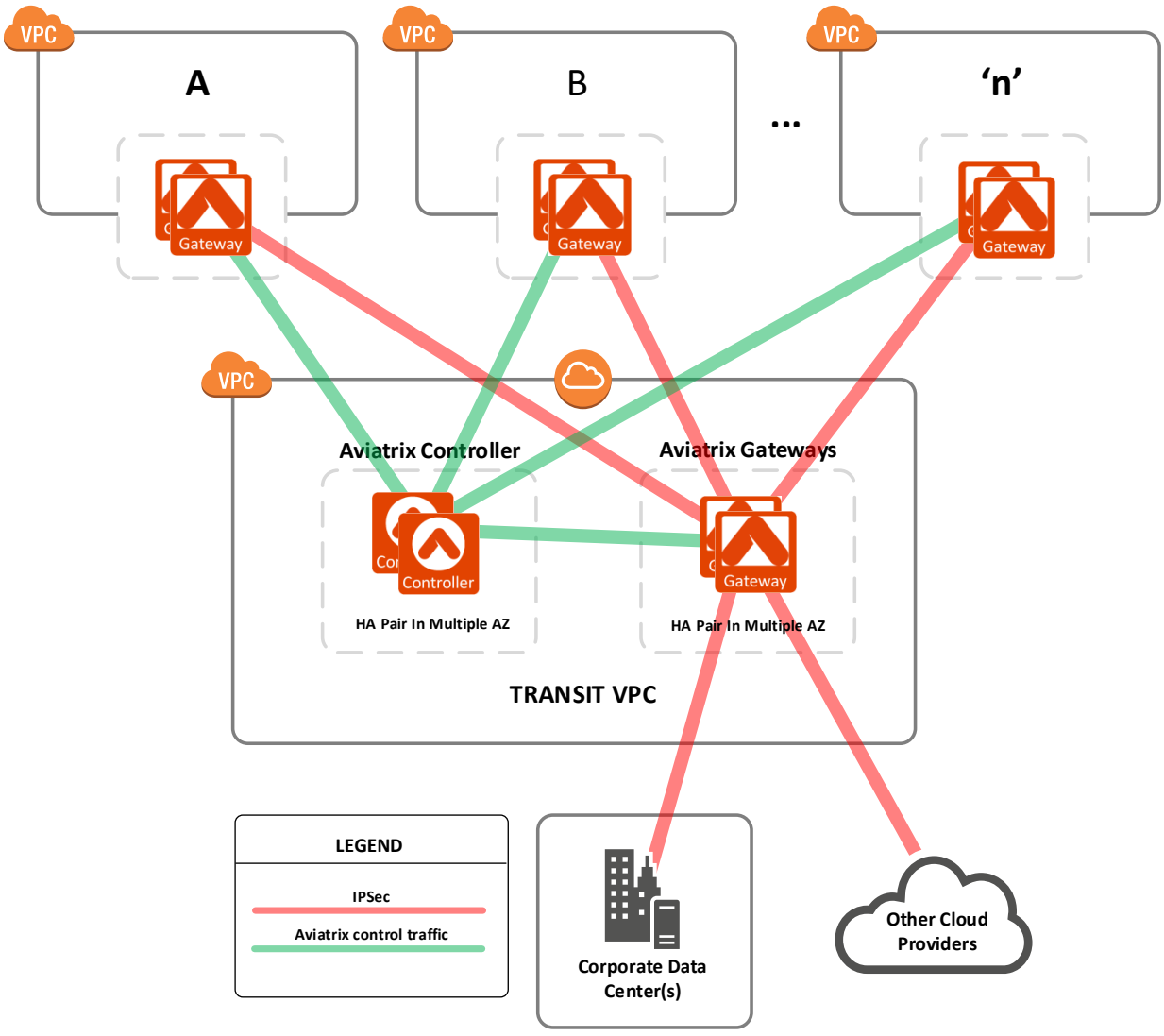
Aviatrix Systems, Inc.
411 High Street
Palo Alto, CA 94301
USA
http://www.aviatrix.com
Tel: +1 844.262.3100

TABLE OF CONTENTS

1 Overview

Aviatrix is a next generation cloud networking solution built from the ground up for the public cloud. It simplifies the way you enable site to cloud, user to cloud and cloud to cloud secure connectivity and access. The Aviatrix solution requires no new hardware and deploys in minutes.

This configuration guide provides step by step instruction on how to build a highly available AWS Transit VPC. Below is an architecture diagram of what a general AWS Transit VPC deployment looks like, where a Hub VPC (or Transit VPC) connects many Spoke VPCs to facilitate communication between Spoke VPC and on-prem network.



2 Aviatrix Solution Key Benefits

Simplicity. Centrally managed, point and click solution deploys in minutes.

Highly Available. Built-in gateway redundancy supports hot standby and fail over in seconds.

Cost Saving. If hub and spoke VPCs are in the same region, encrypted traffic is routed over AWS peering, reducing network bandwidth cost by 10 times (comparing to AWS Transit VPC solution that goes over Internet with VGW for hub and spoke traffic).

Scalable. The solution does not require a unique public IP address on the hub gateway connecting to each spoke gateway. No limits on the number of spoke VPCs can be connected to hub VPC.

Visibility. Central dashboard monitors, displays and alerts link status and link latency.

Additional Benefits. Stateful firewall at the gateway to enforce security policies. OpenVPN based user access allows end to end cloud network solution. For more details, visit www.aviatrix.com.

3 Pre Configuration Checklist

Before configuring user VPC peering, make sure the following is completed.

Pre Configuration Check List

1. Deploy the Aviatrix Controller
2. Check VPC Settings

These prerequisites are explained in detail below.

3.1 Deploy the Aviatrix Controller

The Aviatrix Controller must be deployed and setup prior to configuring VPC and site peering. Please reference the Aviatrix Controller getting started guide for AWS on how to deploy the Aviatrix Controller.

Aviatrix Controller Getting Started Guide

Check and make sure you can access the Aviatrix Controller dashboard and login with an administrator account. The default URL for the Aviatrix Controller is:

https://<public ip of Aviatrix Controller>

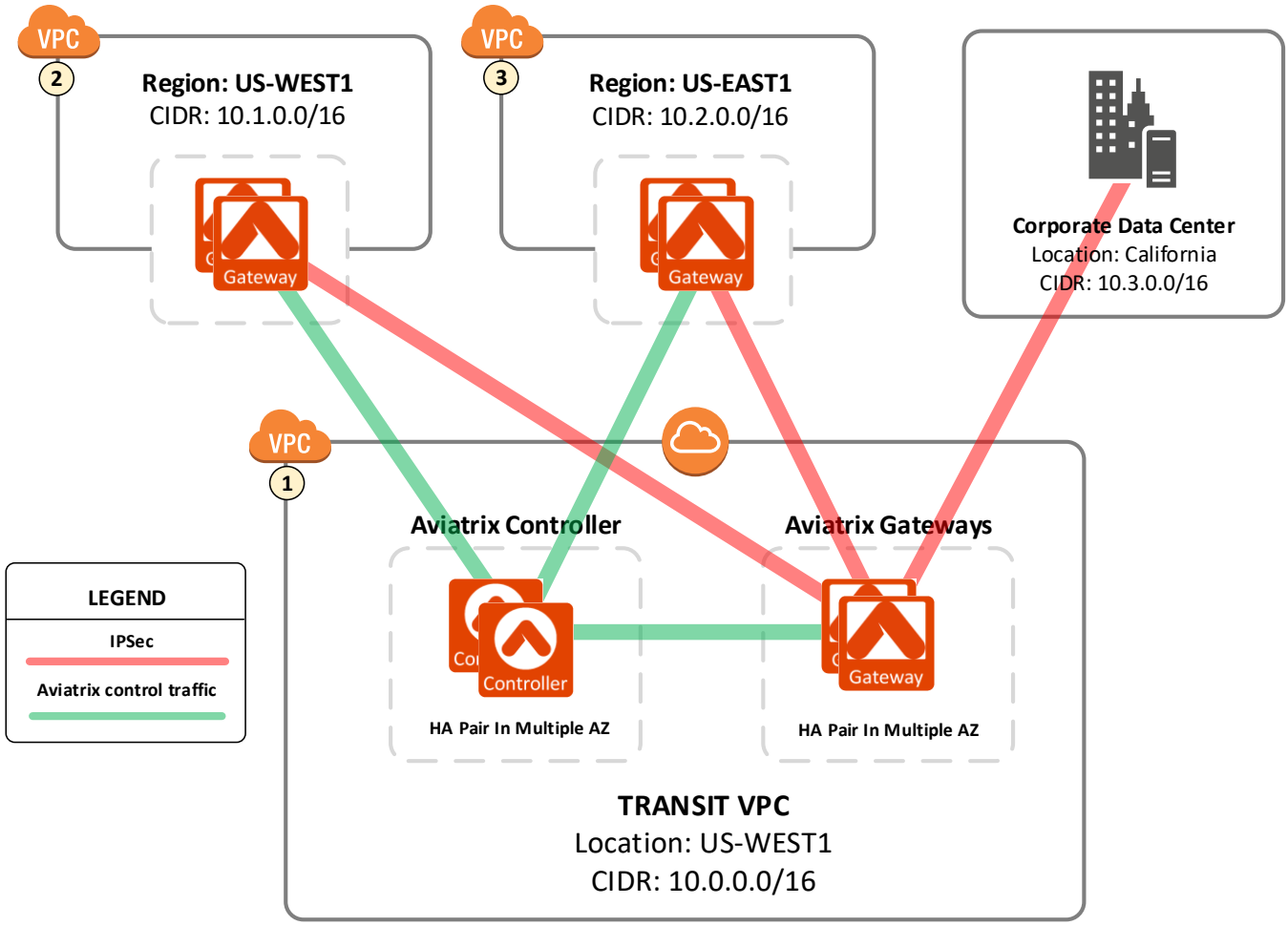
3.2 Check VPC Settings

- The VPC must have at least one public subnet to deploy the gateway. This means one subnet must be associated with a route table that has an IGW as its default route.
- If your hub VPC and spoke VPC are in the same region and you like to route the traffic over AWS peering, go to AWS console and configure the necessary AWS peering between the two VPCs.

4 Configuring VPC Peering

Please make sure the pre-configuration steps in the previous section is completed before proceeding.

The instructions in this section will use the following architecture. The CIDR and subnets may vary depending on your VPC setup; however, the general principals will be the same.



In this example we have three VPCs: Transit VPC, spoke VPC in US-WEST1 and spoke VPC in US-EAST1. The corporate data center is located in California. The system will be configured such that all spoke nodes and sites will be able to communicate with each other via the transit VPC.

4.1 Step 1 – Deploy Gateways

The first step is to deploy Aviatrix gateways in each VPC.

Instructions:

1. Login to the Aviatrix Controller Console
2. Click on Gateway -> Create

Setting	Value
Cloud Type	Choose AWS
Account Name	Choose the account name
Region	Choose the region where your VPC is located
VPC ID	Choose the VPC
Gateway Name	This name is arbitrary (ex. gw01)
Public Subnet	Select a public subnet where the gateway will be deployed
Gateway Size	t2.micro is fine for testing.
Enable NAT	Uncheck this box
VPN Access	Uncheck this box

3. Click "Create". It will take a few minutes for the gateway to deploy. Do not proceed until the gateway is deployed.
4. Repeat steps 2 and 3 for the additional 2 VPCs in this example.
5. Done

4.2 Step 2 – Connect Spoke VPC to Transit VPC

This step explains how to connect a spoke VPC to the transit VPC.

Instructions:

1. From the Aviatrix Controller Console
2. Click VPC/VNet -> Encrypted Peering -> Encrypted Peering.
3. Click Add
4. Select the VPC1 (transit) gateway and VPC2 (spoke 1) gateway for the peering

   Note: If the two VPCs are in the same region, you can check the box "over AWS Peering". This would allow the encrypted peering to route traffic over native AWS peering, resulting in 10 times bandwidth saving.

5. Click Add
6. Select the VPC1 (transit) gateway and VPC3 (spoke 2) gateway for the peering and then click Add
7. Done

4.3 Step 3 – Connect Corporate Data Center to Transit VPC

This step explains how to connect the corporate data center to the transit VPC

Instructions:

1. From the Aviatrix Controller Console
2. Click VPC/VNet -> Site2Cloud - >Add

Setting	Value
VPC ID/VNet Name	Choose Transit VPC ID
Gateway	Choose Transit VPC gateway
Connection Name	This name is arbitrary (ex. corpdatacenter)
Customer Gateway IP Address:	Public IP address of the terminating device at the corp datacenter
Customer Network	10.3.0.0/16 (in this example)
Private Route Encryption	Uncheck
Cloud Subnet	10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16 (in this example)
Null Encryption	Uncheck

3. Click Add
4. Click List, select the Transit VPC ID and then click Run
5. Put a check mark next to your "Connection Name" (from above) and then click download
6. If your terminating device is a Cisco ASA, select ASA, otherwise, select Generic.
7. This template file contains the necessary information to configure the terminating device at the corp data center. Once the terminating device is configured, the tunnel will automatically come up.
8. Done

4.4 Step 4 – Configure Transitive Routing

This step explains how to configure transitive routing so that every spoke and site node can communicate with each other via the transit VPC.

Instructions:

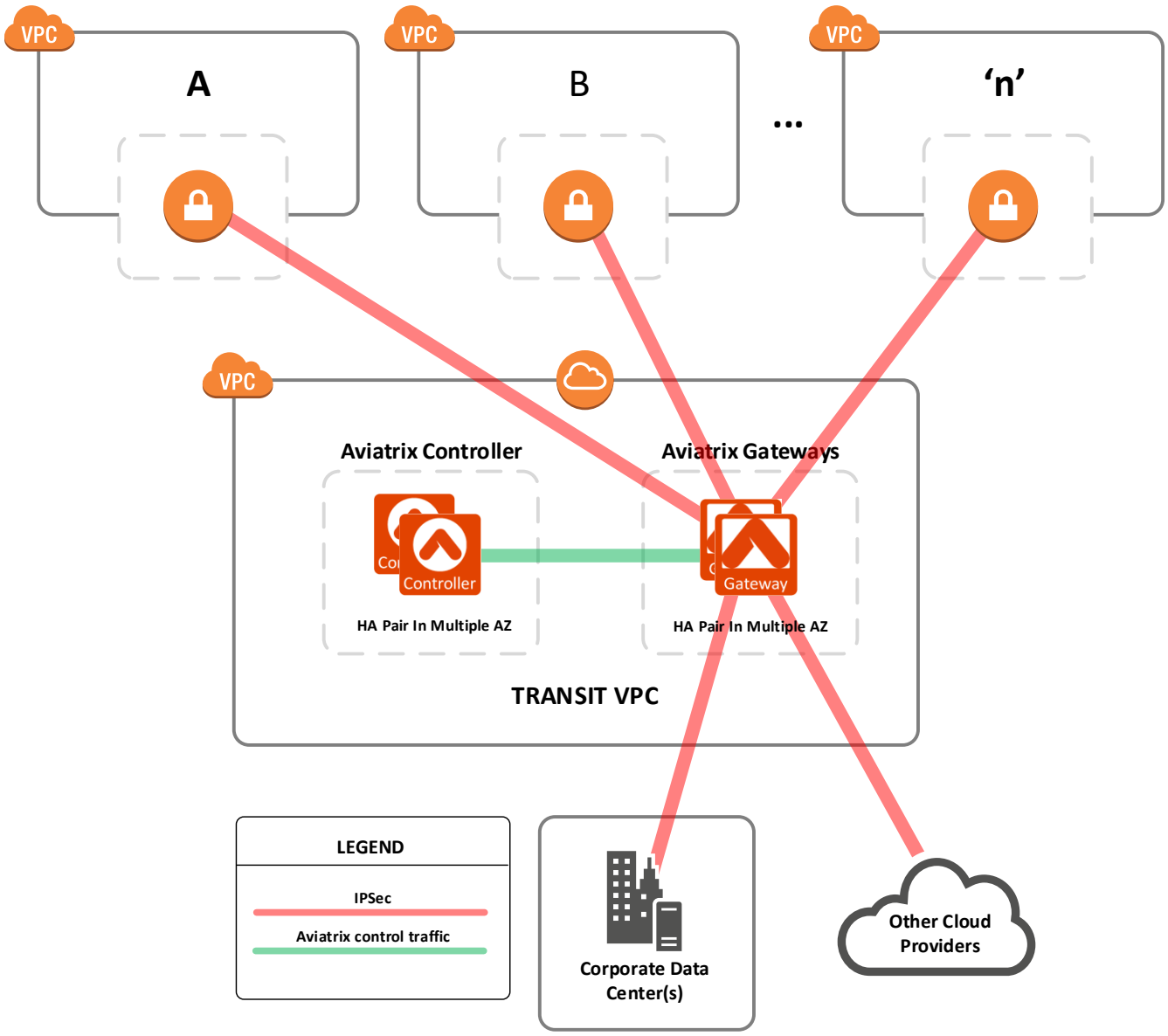
1. From the Aviatrix Controller Console
2. Click VPC/VNet -> Encrypted Peering -> Transitive Peering
    a. For VPC2 (spoke 1) select:
        i. Click Add
        ii. Source VPC: VPC2, Next Hop VPC: VPC1 (transit), Destination CIDR: 10.2.0.0/16
        iii. Click Add and then Add again
        iv. Source VPC: VPC2, Next Hop VPC: VPC1 (transit), Destination CIDR: 10.3.0.0/16
        v. Click Add
    b. For VPC3 (spoke 2) select:
        i. Click Add
        ii. Source VPC: VPC3, Next Hop VPC: VPC1 (transit), Destination CIDR: 10.1.0.0/16

iii. Click Add and then Add again
iv. Source VPC: VPC3, Next Hop VPC: VPC1 (transit), Destination CIDR: 10.3.0.0/16
v. Click Add

3. Done

5 Appendix – Terminating on VGW

The Aviatrix transit VPC solution also supports terminating on AWS VGWs in the spoke VPC. In this case, the AWS VGWs must be manually setup in each spoke VPC.



6 Appendix –Support

6.1 Aviatrix Support

Standard: 8x5 Enterprise Phone Support, email support, product-specific knowledge-base and user forum is included. For Additional levels of support and support offers please visit:

www.aviatrix.com/support

6.2 AWS Support

AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers. The service helps customers of all sizes and technical abilities to successfully utilize the products and features provided by Amazon Web Services. Learn more