AWS Remote Access VPC Bundle Deployment Guide

Last updated: April 11, 2017

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

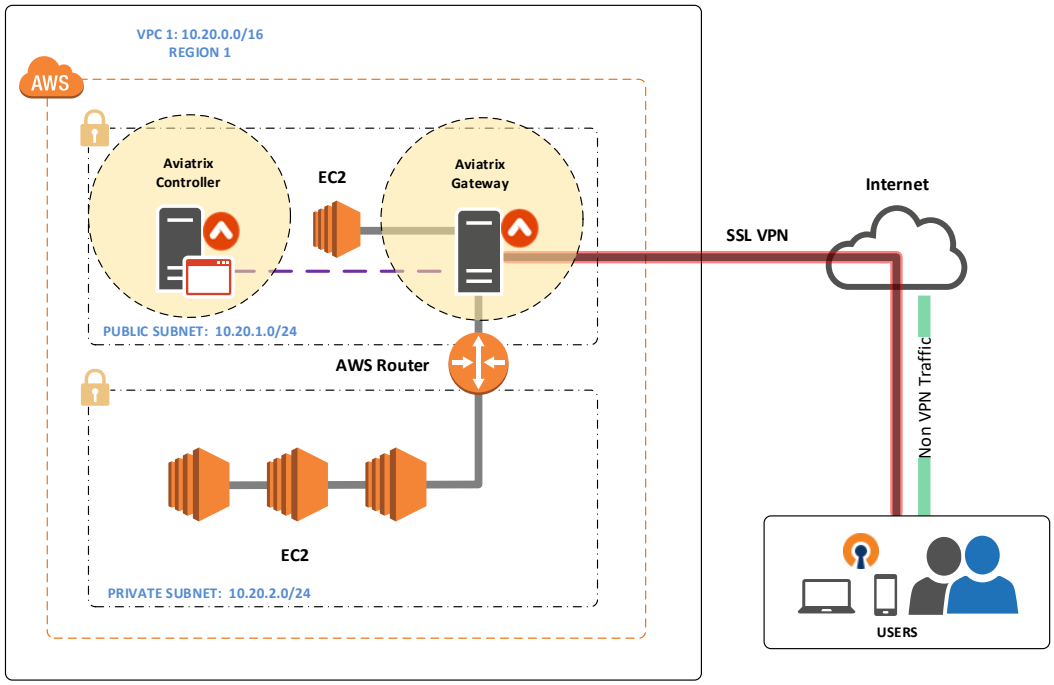
TABLE OF CONTENTS

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 deployment guide provides step by step instruction on how to deploy the Aviatrix remote access VPC bundle in AWS. Once deployed, users will be able to remotely access any resource within the VPC.

Below is a sample architecture of what will be deployed. The bundle will automatically create a new VPC and deploy the Aviatrix controller. After the controller is up, we will use it to deploy the Aviatrix gateway to provide SSL VPN access. The controller will automatically update the routing tables to provide access to both public and private subnets.



1.1 Deployment Objectives

The following features will be enabled after the configuration is complete.

1. Provide user SSL VPN access to the AWS VPC. Uses will be able to access both the public and private subnets.
2. Provide internet access to instances in the private subnet (optional).

2 Pre-Deployment Checklist

Before deployment the remote access VPC bundle, make sure the following is completed.

Pre-Deployment Check List

1. Setup AWS role permissions for Aviatrix.
2. Multi Factor Authentication (MFA) – Optional.
3. Install OpenVPN Client.

These prerequisites are explained in detail below.

2.1 Setup AWS role permissions for Aviatrix

The Aviatrix controller utilizes AWS APIs to manage network resources in AWS. Please follow the instructions in the below document to create the necessary polices and roles for the Aviatrix controller

Setup AWS Permission for Aviatrix

After you done with the permission setup, please fill in the Role ARN for the two roles below. This information will be need for the controller setup later.

Role Name	Role ARN
aviatrix-role-ec2	
aviatrix-role-app	

2.2 Multi Factor Authentication (optional)

The Aviatrix user VPN solution supports MFA with the following technologies:

1. DUO.
2. Okta.
3. LDAP.

If you plan to use MFA with the Aviatrix VPN solution, please follow the follow instructions to prepare your MFA configuration to integrate it with the Aviatrix.

2.2.1 DUO Configuration

The Aviatrix VPN solution can be integrated with the DUO mobile app for MFA authentication. Please complete the following steps to preconfigure DUO for the Aviatrix integration.

Instructions:

1. Login to DUO with an admin account. From the dashboard click on Applications.
2. Click "+ Protect an Application" on the right.
3. Find the DUO "Auth API" application. Click "Protect this Application".
4. Note the following three pieces of information. This information will be needed during the Aviatrix User VPN configuration.
    a. Integration key.
    b. Secret key.
    c. API hostname.
5. On the left-hand menu, click Users and then "+ New User".
    a. The "username" for the user in DUO must match the "username" that is created in Aviatrix.
    b. Default for everything else is fine.
    c. Send Enrollment Email to user for DUO enrollment.
    d. Repeat this step for additional users as needed.
6. Done – pre-configuration for DUO is complete.

2.2.2 Okta Configuration

The Aviatrix VPN solution can be integrated with Okta for MFA authentication. Please complete the following steps to preconfigure Okta for the Aviatrix integration.

Instructions

1. Login to Okta with an admin account.
2. From the navigation on the top, click Security -> API.
3. Click "Create Token". Give the token a name and then note the Token Value.
4. Get the Okta ULR for your organization. The format of the URL is usually "okta subdomain + okta.com". For example: acme.okta.com or dev-364253.oktapreview.com
5. From the Okta dashboard click on Directory and then "Add Person".
    a. The username for the user must match the username defined in Aviatrix.
    b. Repeat this step for additional users as needed.
6. Done – pre-configuration for Okta is complete.

2.2.3 LDAP Configuration

The Aviatrix VPN solution can be integrated with LDAP for MFA authentication. Please gather the following information from your LDAP system.

Setting	Value
LDAP Server	IP address or FQDN of LDAP server
LDAP Client and CA Certificate	If connection to the LDAP server is via SSL, obtain the client and CA certificate of the LDAP server
Bind DN	DN of a user that has read access on the LDAP server. Ex. CN=admin,DC=mydomain,DC=com

Password	Password for the above user (with read access on the LDAP server)
Base DN for User Entries	Base search DN for users Ex. CN=Users, DC=mydomain, DC=com
Username Attribute	LDAP attribute use to MAP to Aviatrix VPN Users Ex. sAMAccountName
Group Membership DN	DN of group (optional). Used to restrict VPN access to only users in this group

2.3 Install OpenVPN Client

The Aviatrix user VPN solution supports OpenVPN for PCs, MACs, Chromebooks and mobile devices running iOS or Android. To use or test the VPN solution, you must install an OpenVPN client. Instructions on how to download and configure the OpenVPN client can be found here.

Aviatrix User OpenVPN Client Install

3 Deploy the Bundle

The first step is to deploy the bundle from the AWS marketplace. Here is a summary of what will be completed in this step.

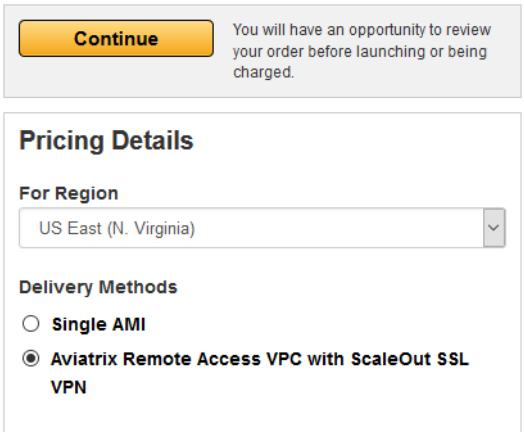
1. Create a new VPC.
2. Deploy the Aviatrix Controller.

This step is all automated via an AWS CloudFormation script. Please follow the below instructions to deploy the bundle.

INSTRUCTIONS

1. Go to the Aviatrix Product Page on the AWS Marketplace.
2. Choose "Aviatrix Cloud Networking Remote Access VPC Bundle – 10 Users"

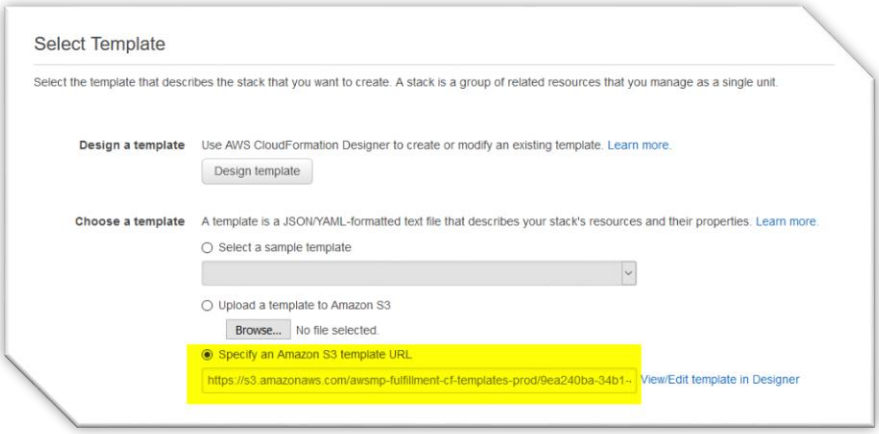
3. On the right-hand side, select the region you want to deploy the bundle in. For Delivery Methods, chose "Aviatrix Remote Access VPC with Scale Out SSL VPN". Click Continue.



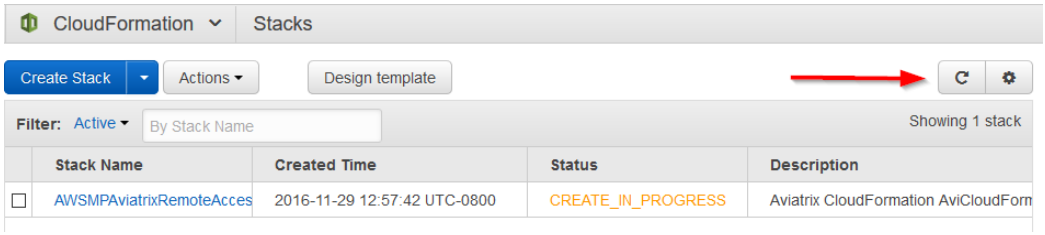
4. If you haven't already done so, you will be prompted to accept license agreement now.
5. From the "Launch on EC2" screen, please note the following:
    a. **Version** – select the latest version available.
    b. **Region** – change the region where the bundle will be deployed if desired.

c. **Deployment Options** – Make sure "Aviatrix Remote Access VPC with Scale Out SSL VPN" is selected.
d. **Launch** – Click the "Launch with CloudFormation Console" when you are ready to proceed.

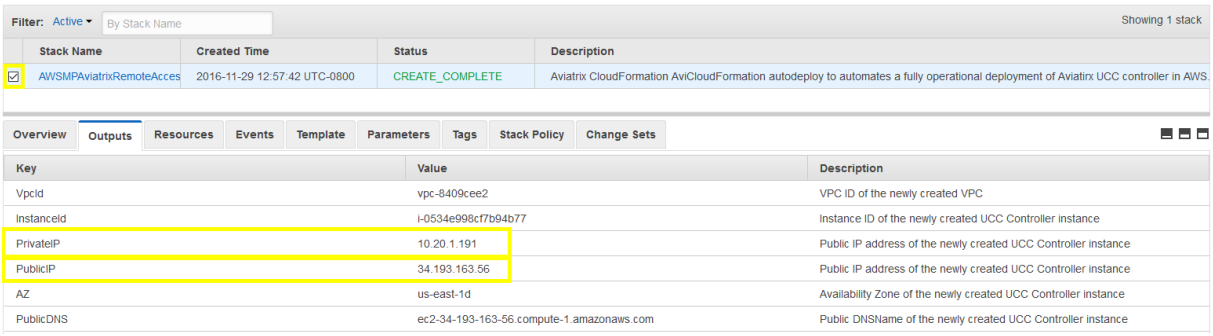
6. You should be redirect to the CloudFormaton Console at this point.
7. For Select Template, use the default one from Amazon S3. Click Next.



8. Specify Details.
   a. **Stack Name** – use the default or enter in a name for the stack.
9. Parameters.
   a. **VpcCidrBlock** – Enter a CIDR block for the VPC. In this example, we'll use (10.20.0.0/16).
   b. **InstanceType** – t2.medium is the minimum requirement for the Aviatrix Controller.
   c. **KeyName** – Select the keyname that will be used for the controller. If you don't see an option here, it means you have not created a key pair in the AWS region where you want to deploy the bundle. In this case, please go to the AWS EC2 console and create a key pair.
   d. **SubnetCidrBlock** – Enter a subnet block. In this example, we'll use (10.20.1.0/24).
   e. **SshAccessIpRange** – Enter 0.0.0.0/0.
   f. **WEBLocaiton** – use the default (0.0.0.0/0).
10. Tags (optional) – this allows you to associate tags to the Aviatrix controller.
    a. Key =Name, Value = Aviatrix Controller.
    b. Add more if desired.
11. Permissions – leave this blank and use the default settings. The CloudFormation script will automatically assign the Aviatrix controller the proper roles (i.e. the ones you created in the pre-requisites section).
12. Advanced –use default settings.
13. Click Next.
14. Review your settings, check the "Acknowledge" check box at the bottom and then click "Create".
15. You can check the progress of the CloudFormation script by clicking on the "Refresh" button on the right.



16. The CloudFormation script will take roughly 2-3 minutes to complete. After the CloudFormation script is complete, check the checkbox next to the script and then click on the Outputs tab.



Please make note of the public and private IP of the Aviatrix Controller.

17. From a browser, login to the Aviatrix controller. The default access URL is:

    https://public_ip_of_aviatrix_controller
    Login: admin
    Default Password: private IP of the Aviatrix controller (in this example it is 10.20.1.191)

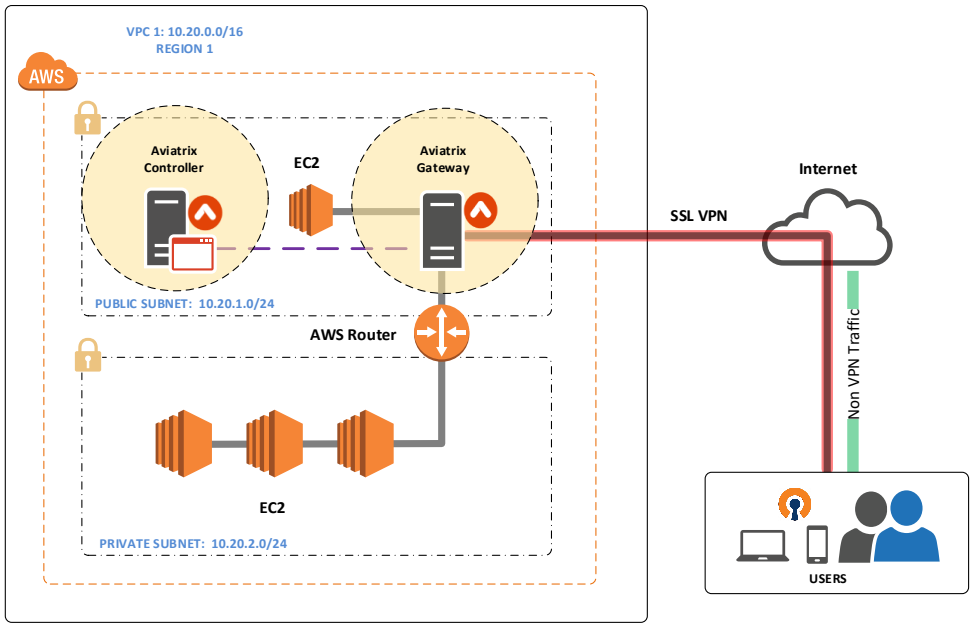
    After the first login, the system will prompt you to set a recovery email, change the default password and perform an update of the system. This process will take 2-3 minutes.

18. After the system update, login to the controller.
19. Click Onboarding -> AWS.
20. Under Create Account.
    a. Account Name (this is an arbitrary value, ex. Devops).
    b. Email: (set an email for the admin account).
    c. Password (choose a password for the account).
    d. AWS Account Number: (enter your 12 digit AWS account number).
    e. Check “IAM role-based”.
        i. AWS Role ARN (this is the aviatrix-role-app ARN).
        ii. AWS Role EC2 (this is the aviatrix-role-ec2 ARN).
    f. Click “Save”.
21. Done – the controller is now ready for User VPN configuration.

4 Configuring User VPN

Please make sure the pre-deployment steps in the previous section are completed before proceeding.

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



INSTRUCTIONS:

1. Login to the Aviatrix Controller.
2. Click on Gateway > +New Gateway.
   Please reference the following table when choosing the settings for the Gateway:

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 that you want to provide user VPN access
Gateway Name	This name is arbitrary (ex. vpn-gw01)
Public Subnet	Select a public subnet where the gateway will be deployed
Gateway Size	t2.micro is fine for testing. m3.medium or higher is recommend for production
Enable NAT	Check this box if you want to provide internet access for private subnets within your VPC
VPN Access	Check this box

VPN CIDR Block	The default is 192.168.43.0/24. The value is fine as long as it does not overlap with your existing subnets.
Two-step Authentication	If you plan to use multi-factor authentication, select one of the supported vendors; otherwise, select disable
DUO	
Integration Key	This is the integration key for the protected app
Secret Key	This is the secret key for the protected app
API Hostname	This is the API hostname for the protect app
Push Mode	Default (Auto)
Okta	
URL	URL to Okta sign-on page (ex. acme.okta.com)
Token	API Token
Username Suffix	This is typically the email suffix for your users. If you are uncertain, leave this field blank
Max Connections	Default (100)
Split Tunnel Mode	Set this to Yes, if you only want to route VPC traffic through the VPN (i.e. regular internet traffic will be routed locally).
Additional CIDRs	Enter in additional CIDRs that will be allowed through the tunnel (optional)
Nameservers	Enter in DNS servers for VPN users (optional)
Search Domains	Enter in search domain for VPN users (optional)
Enable ELB	Default (Yes)
Enable Client Certificate	Default (Yes)
Enable Client Certificate Sharing	Default (No)
Enable Policy Based Routing	Default (not check)
Enable LDAP	Default (not check) – Check this box and fill in the requited information to use LDAP for MFA (optional)

3. Click “OK”. It will take a few minutes for the gateway to deploy. Do not proceed until the gateway is deployed.
4. Create VPN User.
    a. Click OpenVPN > VPN Users.
    b. Click + Add New.
    c. Select the VPC ID where the gateway is deployed.
    d. Select the LB Name (if one was used).
    e. Set the User Name. If you are using MFA, this username must match the username that was created in the MFA platform (i.e DUO, Okta).
    f. Set User Email.
    g. Check Profile if you want to assign a security profile to the user (optional).
    h. Click OK – This will trigger an email to the end user with the appropriate configuration file and instructions to connect to the VPN.
    i. Repeat the “Create VPN User” step for additional users as needed.
5. Done.

5 Appendix –Support

5.1 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