



Configuring User VPN For AWS

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

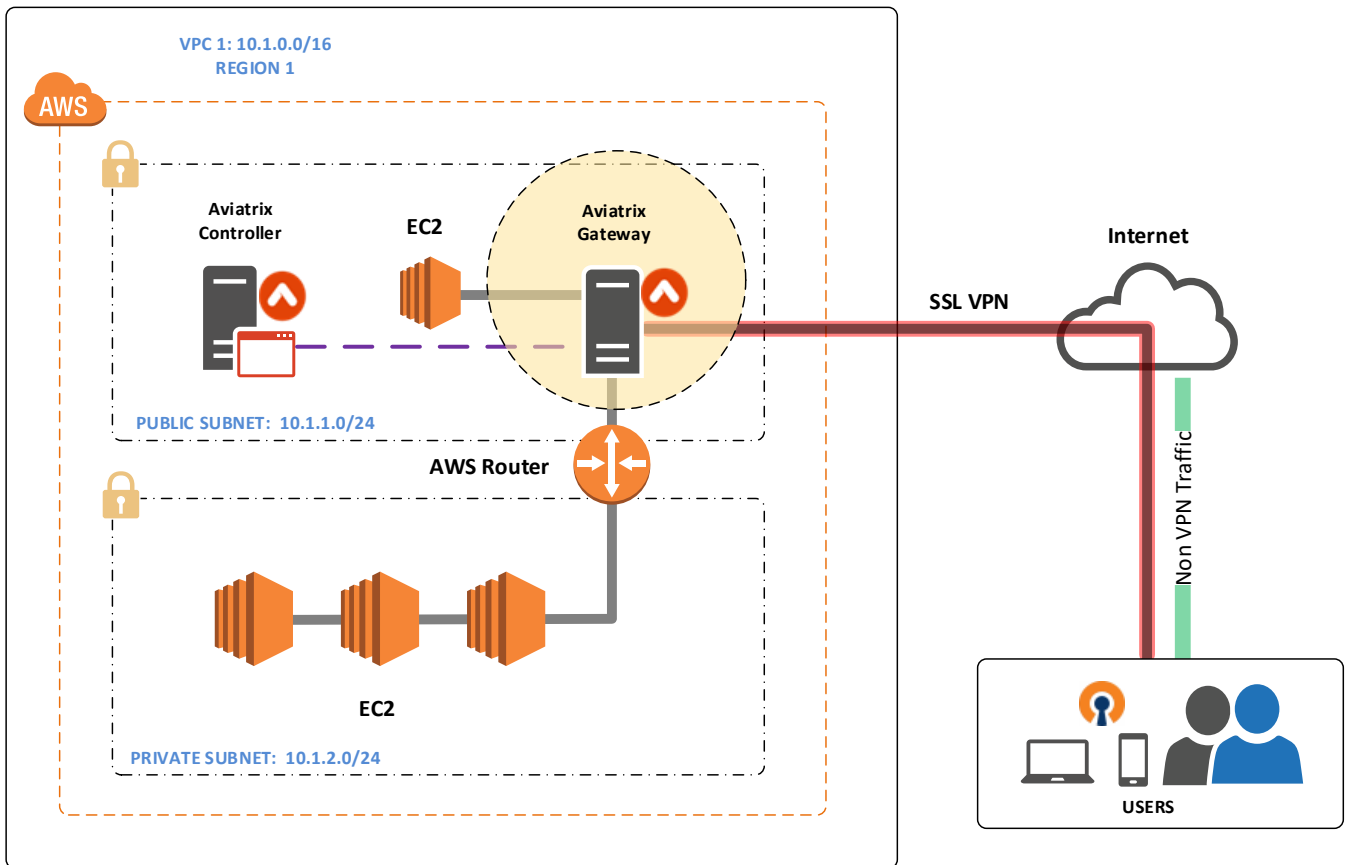
TABLE OF CONTENTS

1	Overview.....	3
1.1	Configuration Objectives.....	3
2	Pre Configuration Checklist.....	4
2.1	Deploy the Aviatrix Controller.....	4
2.2	Multi Factor Authentication.....	4
2.2.1	DUO Configuration.....	4
2.2.2	Okta Configuration.....	5
2.2.3	LDAP Configuration.....	5
2.3	Install OpenVPN Client.....	6
3	Configuring User VPN.....	7
4	Appendix –Support.....	9
4.1	Aviatrix Support.....	9

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 configure user VPN access. The following example will be used in this guide.



1.1 Configuration Objectives

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

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

2 Pre Configuration Checklist

Before configuring user VPN access, make sure the following is completed.

Pre Configuration Check List

1. Deploy the Aviatrix Controller
2. Multi Factor Authentication (MFA) - Optional
3. Install OpenVPN Client

These prerequisites are explained in detail below.

2.1 Deploy the Aviatrix Controller

The Aviatrix Controller must be deployed and setup prior to configuring user VPN access. 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>`

2.2 Multi Factor Authentication

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

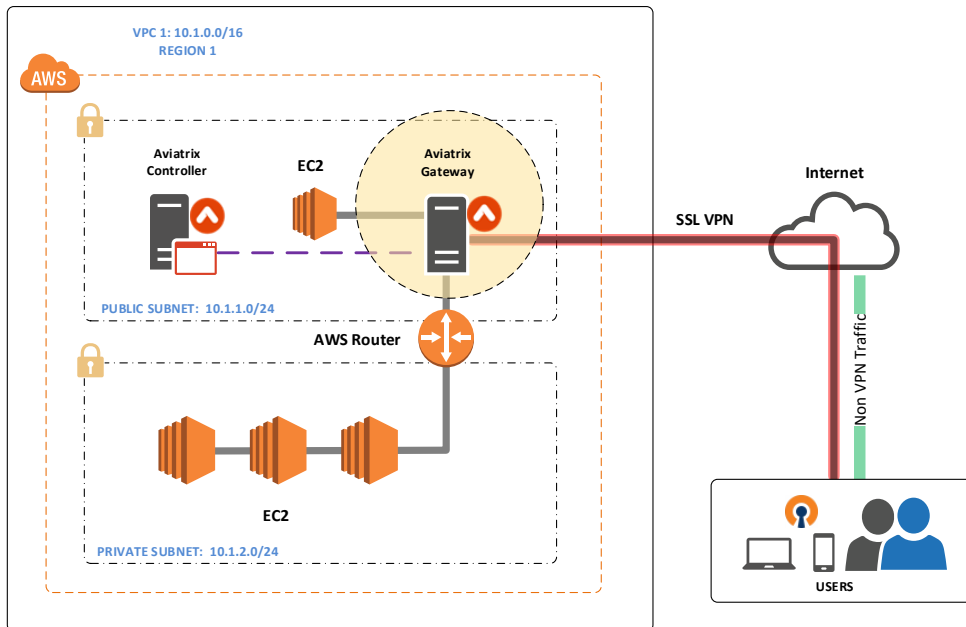
The Aviatrix user VPN solution supports OpenVPN for PCs, MACs, Chromebooks, and mobile devices running iOS or Android. In order to use or test the VPN solution, you must install an OpenVPN client. Instructions on how to download and configure the OpenVPN client can be found [here](#).

[Aviatrix User OpenVPN Client Install](#)

3 Configuring User VPN

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 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 required 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.
 - 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.

4 Appendix –Support

4.1 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