



# **Configuring Aviatrix Encryption**

**For**

**AWS Direct Connect**

**Azure Express Route**

**Google Cloud Interconnect**

Last updated: October 9, 2016

**Aviatrix Systems, Inc.**

4555 Great America Pkwy

Santa Clara CA 95054

USA

<http://www.aviatrix.com>

Tel: +1 844.262.3100

# TABLE OF CONTENTS

---

1	Overview.....	1
1.1	The Problem .....	1
1.2	Aviatrix Encryption .....	1
1.3	Aviatrix Benefits.....	2
2	Configuration Workflow .....	3
2.1	Prerequisites.....	3
2.2	Configuration Procedure .....	3
2.3	Troubleshooting .....	4
3	Appendix –Support.....	5
3.1	Aviatrix Support.....	5

# 1 Overview

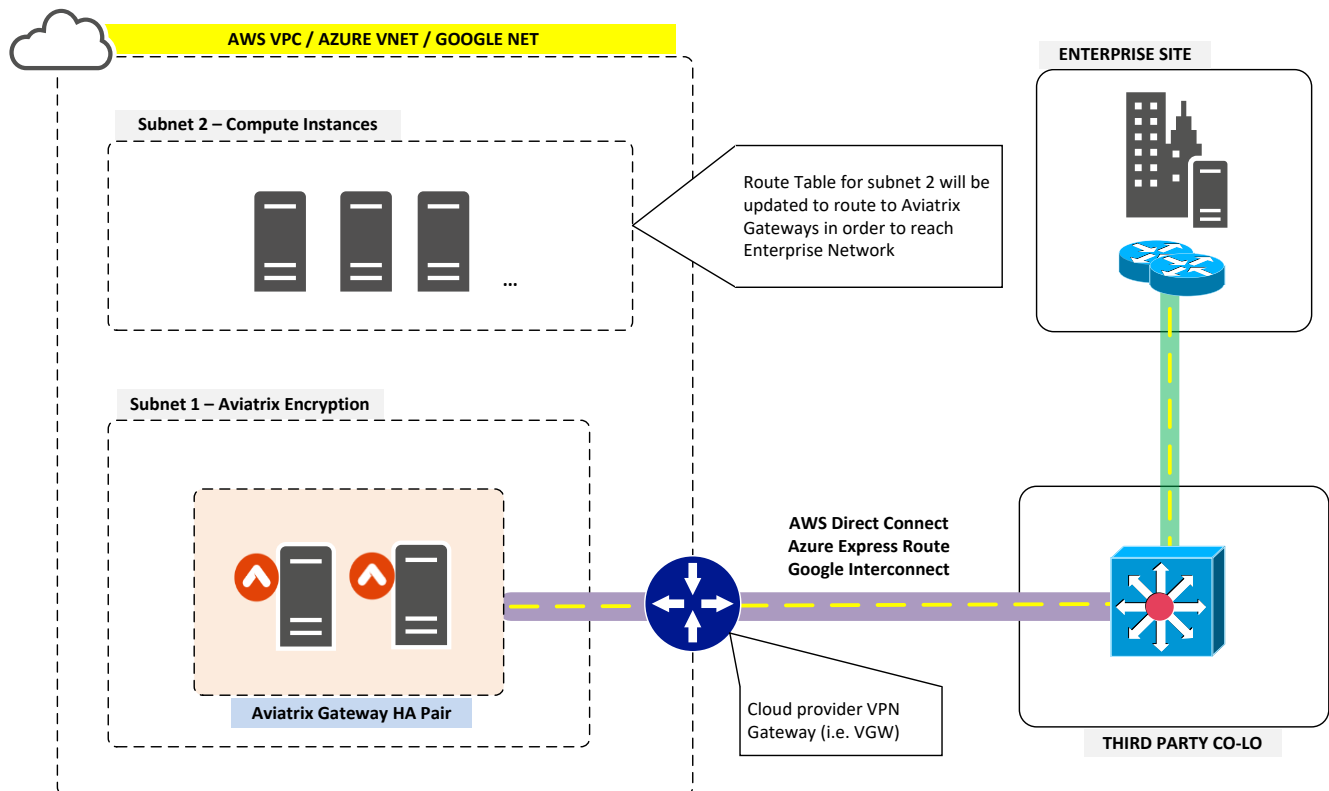
## 1.1 The Problem

Public cloud providers (AWS, Azure, Google) have the ability to provide private routed circuit from an on-premise network to the cloud. The VPN gateway (i.e. VGW) that terminates the private routed circuit (i.e. Direct Connect) connects virtual machines in the cloud with on-prem servers in a traditional routing domain.

While these private routed circuits provide a private link between a customer's on-prem network and the cloud without going through the Internet, packets between the on-prem edge and cloud network travel through exchange points and third party provider networks and are not encrypted. If encryption is a requirement for security and compliance reasons, this is a problem.

## 1.2 Aviatrix Encryption

The Aviatrix Site2Cloud solution can be applied to encrypted traffic over a private routed connection (i.e Direct Connect, Express Route, Interconnect) as show below.



In the diagram above, an encrypted IPSec tunnel is established between the Aviatrix gateway and the customer's edge router.

The Aviatrix gateway is deployed in a separate subnet from the subnets where user virtual machines are launched. (For simplicity, the Aviatrix controller is not drawn.) This is necessary as the Aviatrix gateway is the router for user subnets to reach the Enterprise site.

Aviatrix gateways can be deployed in a 1:1 redundancy fashion where a backup gateway is ready to take over should the primary IPSec tunnel goes down due to gateway VM hardware/software failure.

### 1.3 Aviatrix Benefits

Aviatrix gateways are deployed and managed by an Aviatrix Cloud Connect Controller (not shown in the diagram) which itself is a cloud instance or VM. Some of the benefits are highlighted below:

- The gateway interoperates with third party routing and firewall devices.
- The gateway is launched from the controller web console with a few clicks.
- Aviatrix gateways support 1:1 redundancy for high availability without any additional helper instance or VM. The controller monitors all IPSec tunnel status and automatically re-program the cloud infrastructure routing table and switch to a standby gateway instance when the tunnel goes down.
- The controller provides diagnostic capabilities for troubleshooting the gateway and IPSec tunnel status.
- Cloud VPN capability is integrated with the gateway, which enables individual users at remote sites to connect to VPC/VNet/NET securely and directly without having to hair pinning back to headquarter datacenter.
- Extensive logging allows administrators to have complete visibility of network event and user browsing history.

## 2 Configuration Workflow

---

### 2.1 Prerequisites

Before configuring Aviatrix Encryption for private routes, you must deploy an Aviatrix Controller. For information on how to deploy Aviatrix Controller, please reference the following documentation:

<http://aviatrix.com/documentation/>


If you already have an Aviatrix Controller deployed, make sure it is running the latest software. Check the upper right hand corner from the controller GUI. If there is an “NEW” alert message, please click upgrade to download and install the latest release.

The Aviatrix gateway requires its only public subnet.

### 2.2 Configuration Procedure

The configuration workflow is as follows.

From the Aviatrix Controller GUI:

1. Create a gateway in the VPC/VNet/NET where you like to connect to enterprise datacenter
  - a. Go to Gateway -> Create, make sure:
    - The gateway is launched in a different subnet from the user subnets. In this example, the gateway is deployed in Subnet 1.
    - Disable VPN access if user SSL VPN is not needed
2. (Optional) If HA is enabled, create a backup gateway in the same VPC/VNet/NET.
  - a. Go to Gateway -> Create, make sure:
    - The gateway is launched in a different subnet from the user subnets. In this example, the gateway is deployed in Subnet 1.
    - Disable VPN access if user SSL VPN is not needed
3. Create a connection to the Enterprise site
  - a. Go to Site2Cloud -> Add New
    - Select the VPC/VNet Name where Aviatrix gateway for encryption is launched.
    - Connection Type = Unmapped
    - Connection Name = (Name is arbitrary. E.g. datacenter1)
    - Remote Gateway IP Address = IP address of terminating device
    - Enable HA = Checked this if HA is desired
    -  **• Private Route Encryption = Check**
    - Primary Gateway = Chose the gateway that was created in step 1
    - Backup Gateway = Chose the gateway that was created in step 2 (optional)
    - Remote Subnet = Subnet on the remote side (use comma to separate if more than one)

- Local Subnet = Subnet on the AWS site (use comma to separate if more than one)
  - Pre-share key = Leave blank.
  - Click OK.
4. After the Site2Cloud connection is created, click on the connection and then download the configuration template for your terminating device. If your device model is not in the “Vendor” dropdown list, select “Generic” for vendor.

## 2.3 Troubleshooting

Tunnel status can be checked from the Controller. From the Controller GUI:

1. Click Site2Cloud -> Diagnostics
2. Select the following:
  - a. VPC ID / VNet / NET = Select the network that your gateway is in
  - b. Connection = Select the connection you want to troubleshoot
  - c. Gateway = Select the gateway that is terminating the tunnel
  - d. Action = Select the diagnostics that you want to see
3. Click OK.

## 3 Appendix –Support

---

### 3.1 Aviatrix Support

Aviatrix Cloud Gateway (Scale Out VPC Peering and VPN)

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](http://www.aviatrix.com/support)