

Aviatrix Multi-Cloud FlightPath – Accelerate Cloud Network Troubleshooting to Minimize Network Downtime

Multi-cloud FlightPath is an integral part of a suite of visibility and operational capabilities of the Multi Cloud Network Architecture that Aviatrix offers. The tool allows CloudOps and Cloud Network Engineering teams to troubleshoot cloud network connectivity issues faster to minimize business disruption.

KEY BENEFITS

Instead of tedious ‘whack-a-mole’ efforts to track down the source of connectivity problems across many screens, the Aviatrix Multi-Cloud FlightPath generates the needed network data quickly and automatically and delivers following benefits:

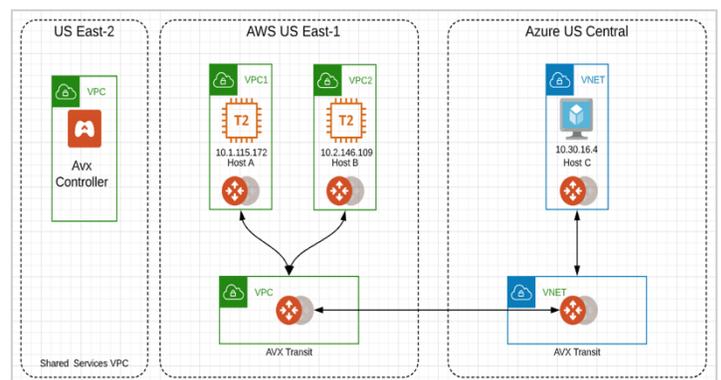
- Automate collection of cloud network data displayed in a single view for faster troubleshooting
- Easily determine and communicate the root problem to other internal groups for quick resolution
- Minimize the impact of cloud network downtime on the business
- Troubleshoot cloud network connectivity problems faster
- Quickly and easily find the source of connectivity issues between cloud network instances/end points

In traditional networking, there are certain tools the operations engineer relies upon for troubleshooting. These include Ping, Traceroute, packet capture, checking route tables, and ACLs along the way to verify connectivity between endpoints. In the cloud network, the native constructs offered by the cloud providers change the rules, and with limited visibility, troubleshooting becomes more complex and time consuming. This is true within a single cloud provider’s environment, but even more so across multiple cloud providers. Cloud Ops and network engineering teams need to take control and make cloud smart operational decisions.

Aviatrix Multi-Cloud Networking Platform enables those teams to save time with daily cloud networking trouble tickets through it’s FlightPath capability. Regardless of which cloud or clouds your deployment is in, Multi-cloud FlightPath can dramatically reduce troubleshooting time with a few simple clicks from the Aviatrix controller.

HOW IT WORKS?

Deployment scenario with AWS and Azure region:



Typically, in order for you to troubleshoot the connectivity between a Host B and Host C, 20+ data points are needed, and it can be a tedious process to do manually.

With FlightPath, the AVX controller already has the awareness of all deployed elements across regions, across clouds, and across accounts, including all the necessary information from native constructs, such as Route Tables, Security Groups, NACLs, transit route tables, etc.

Source to Destination	Return Traffic
1. Source Instance name	1. Source Subnet ID
2. Source IP address	2. Source Route Table ID
3. Source VPC/VNET ID	3. Source outbound NACL rule
4. Source Subnet ID	4. Source Transit Routing or VPC Peering Route
5. Source Route Table ID	5. Destination Instance name
6. Source Outbound Rules in Security Group used	6. Destination IP address
7. Source outbound NACL rule	7. Destination VPC/VNET ID
8. Source Transit Routing or VPC/VNET Peering Route	8. Destination Subnet ID
9. Destination Instance name	9. Destination Route Table ID
10. Destination IP address	10. Destination Route used in Routing table
11. Destination VPC/VNET ID	11. Destination Inbound NACL rule
12. Destination Subnet ID	
13. Destination Route Table ID	
14. Destination Inbound NACL rule	
15. Destination Inbound Rules in Security Group used	

Troubleshooting a real problem in the above scenario:

Ping from host (10.2.146.109) in AWS us-east-1 region VPC2, is not working to host (10.30.16.4) in an Azure Central US region VNET.

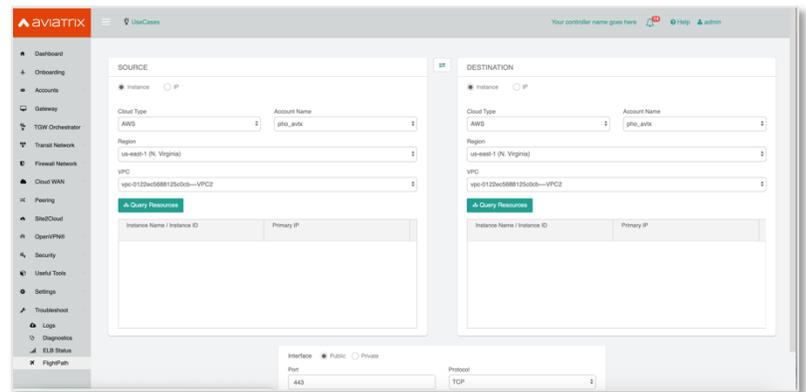
```

ec2-user@ip-10-2-146-109:~$ ping 10.30.16.4
PING 10.30.16.4 (10.30.16.4) 56(84) bytes of data:
^C
--- 10.30.16.4 ping statistics ---
56 packets transmitted, 0 received, 100% packet loss, time 4102ms

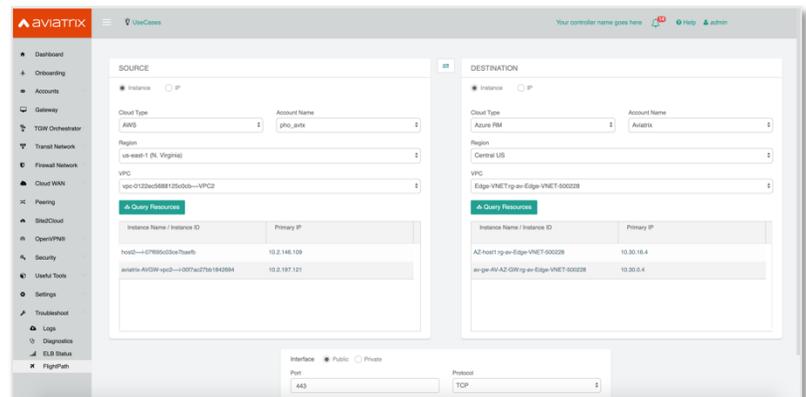
ec2-user@ip-10-2-146-109:~$ ping 10.30.16.4
PING 10.30.16.4 (10.30.16.4) 56(84) bytes of data:
^C
--- 10.30.16.4 ping statistics ---
56 packets transmitted, 0 received, 100% packet loss, time 56327ms

ec2-user@ip-10-2-146-109:~$ ping 10.30.16.4
PING 10.30.16.4 (10.30.16.4) 56(84) bytes of data:
^C
--- 10.30.16.4 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8188ms
    
```

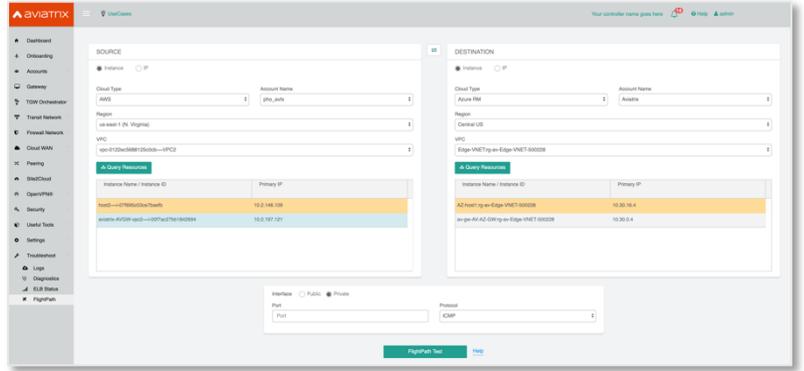
Step 1: Log into the Aviatrix controller and select the “Troubleshoot” node from the left menu. Then select “FlightPath”.



Step 2: Select the cloud (AWS, AWS Gov, GCP or Azure) for both Source and Destination; Choose the Account Names; Select the Regions; Choose the VPC or VNETs; Then click on “Query Resources”. Query Resources will bring up all of the resources in the VPN/VNET including their IP addresses.

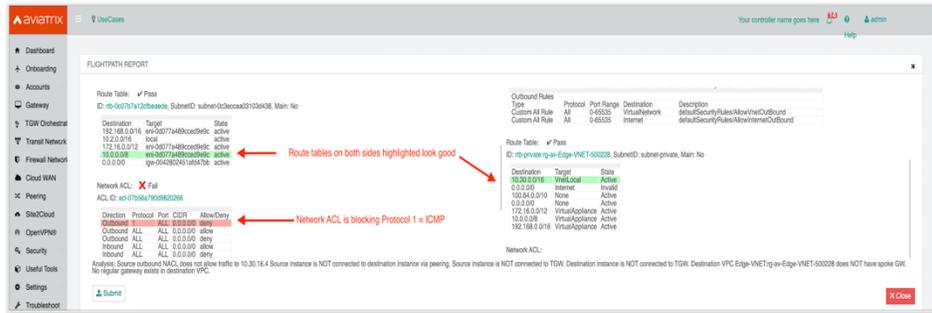
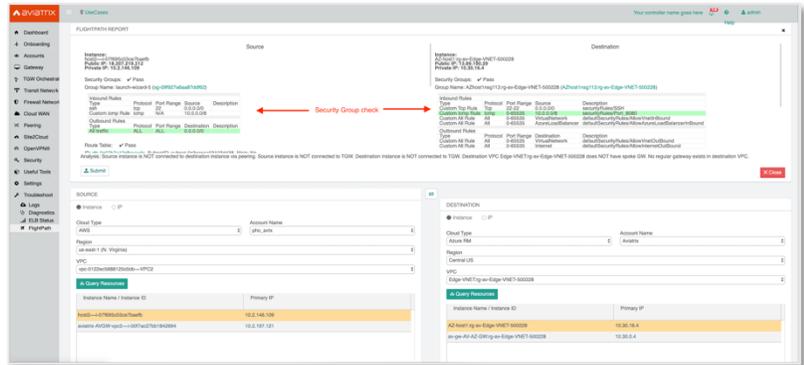


Step 3: Select the hosts to test to/from. In this case, Host B = 10.2.146.109; Host C = 10.30.16.4. Choose whether this is going over the public or private interface, and port and protocol.

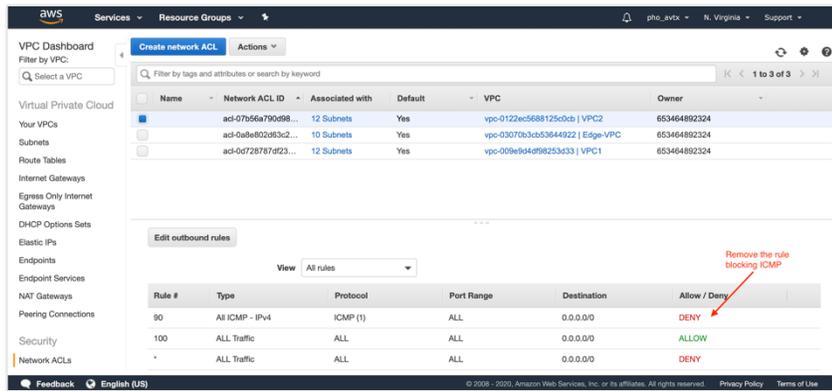


Step 4: Click on FlightPath Test!

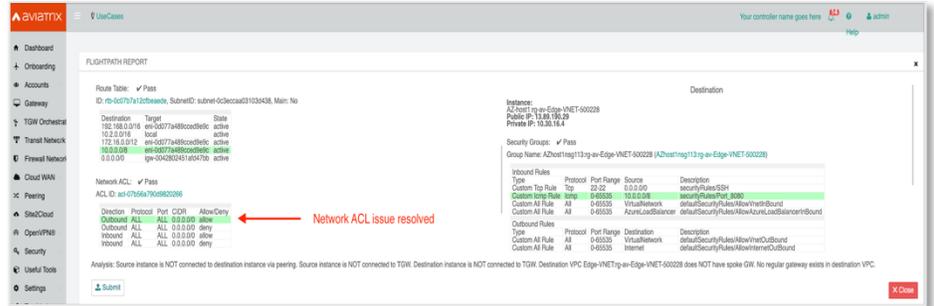
Within seconds, a full analysis report is generated based on this IP/protocol/port between source and destination. It checks on both inbound and outbound Security Groups, Native VPC/VNET Route Tables, gateway route tables and Network ACLs.



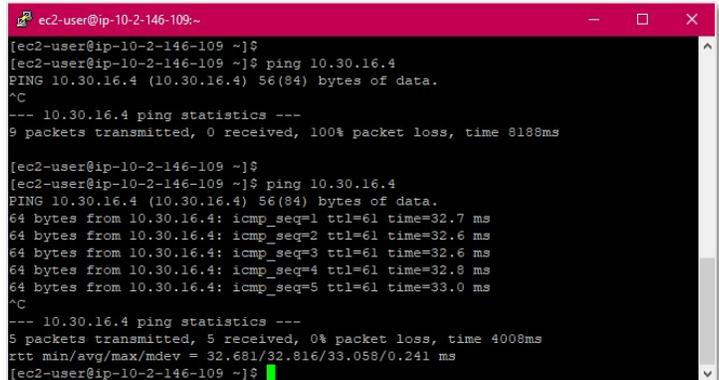
Step 5: Now, in just a couple of clicks, the problem has already been pin-pointed. All we need to do is fix the rule in the NACL in AWS:



Step 6: Check FlightPath again after fixing the outbound Network ACL.



Check Ping again.



CONCLUSION

Troubleshooting in a multi-cloud network can be complex and there are many data points to consider with native cloud constructs. Cloud infrastructure is dynamic, and every new instance involves security groups, access lists, and route tables. This can lead to a lengthy troubleshooting through a manual and tedious process, even for a cloud veteran.

With Aviatrix Multi-Cloud FlightPath, all the guesswork and manual steps are eliminated with a simple automated GUI workflow. By automating the collection of cloud network troubleshooting data and displaying it in a single view, FlightPath eliminates the time, frustration and human errors required to find the source of connectivity issues that are reported as problems. It also makes it easy to communicate the source of the problem, and the required fix, to other internal groups so they can take appropriate actions.

For more details, check out docs.aviatrix.com or connect with our technical solution engineer through aviatrix.com online chat.