

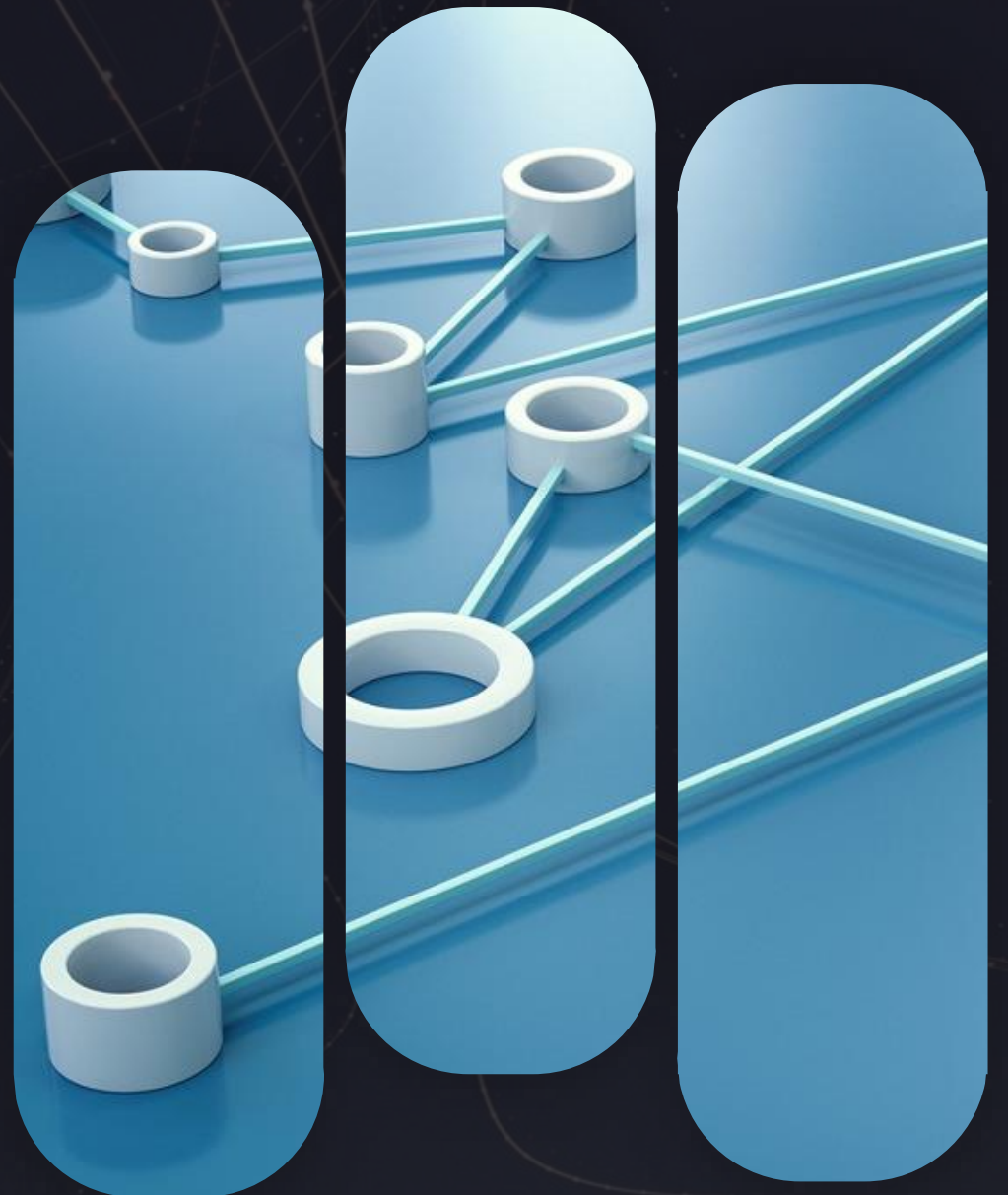


How to Solve Overlapping IP Addresses in AWS

Bayu Wibowo

bwibowo@aviatrix.com

Bayu Wibowo | bwibowo@aviatrix.com
Senior Technical Marketing Engineer
Product Management




Who Am I?



Bayu Wibowo

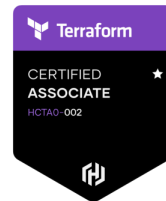
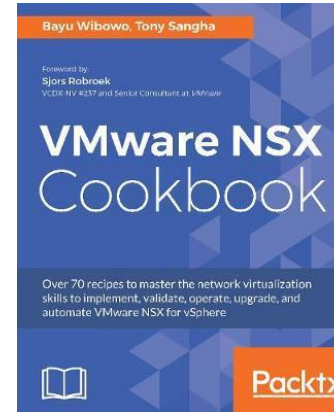
Senior Technical Marketing Engineer

 **Aviatrix | Product Management**

<https://www.linkedin.com/in/bayupw>



DATACOM



Agenda

- Overlapping IP address scenarios
- Solution options:
 1. AWS PrivateLink
 2. AWS NAT Gateway
 3. Aviatrix Secure Cloud Networking Platform
- Summary

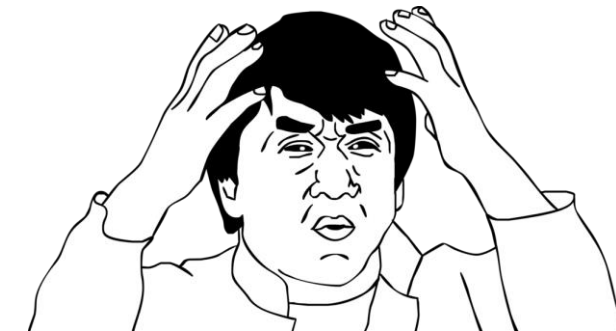
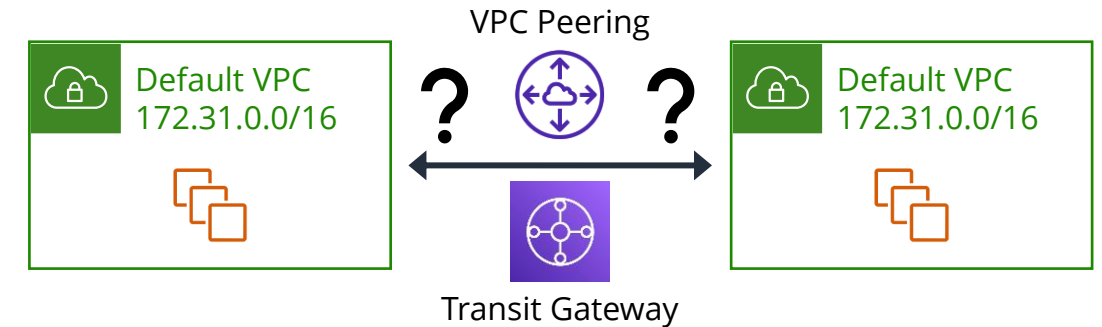
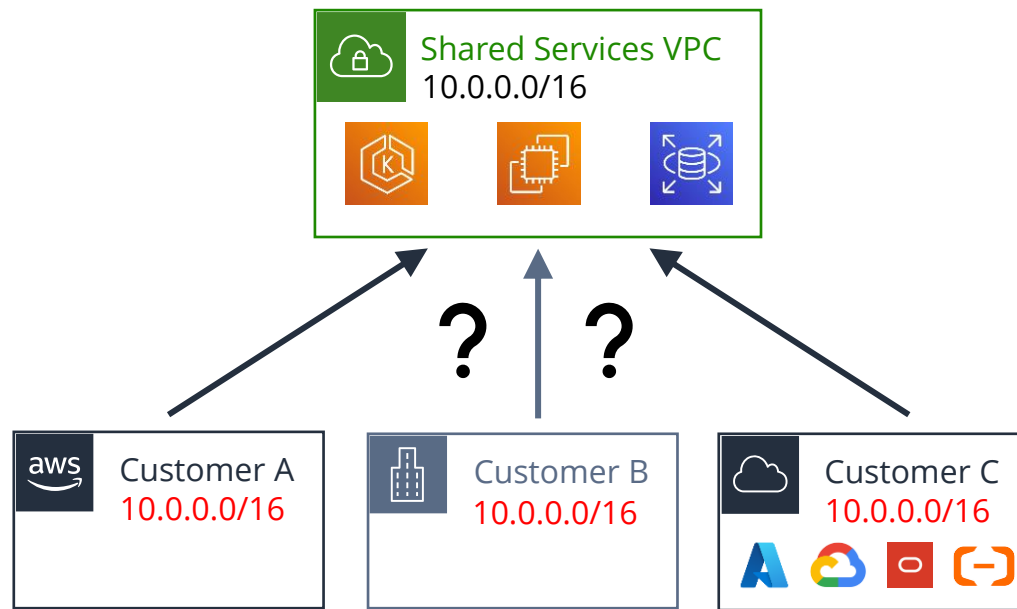


Overlapping IP address scenarios

Problem statement and use cases

Overlapping IP addresses scenarios

- Connecting default VPCs 172.31.0.0/16
- Multi-Cloud inter-connections / different CSP accounts
- M&A, connecting to on-prem, partner/third-party/B2B
- Providing shared services VPC to customers

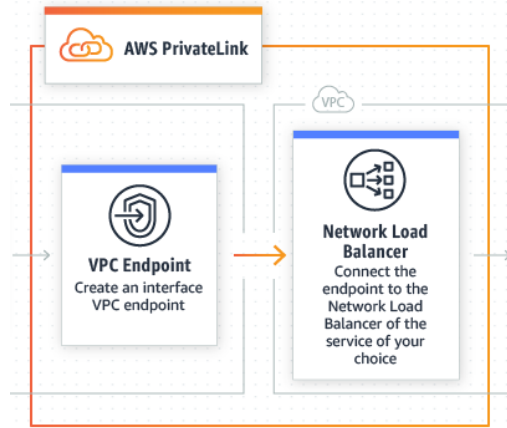




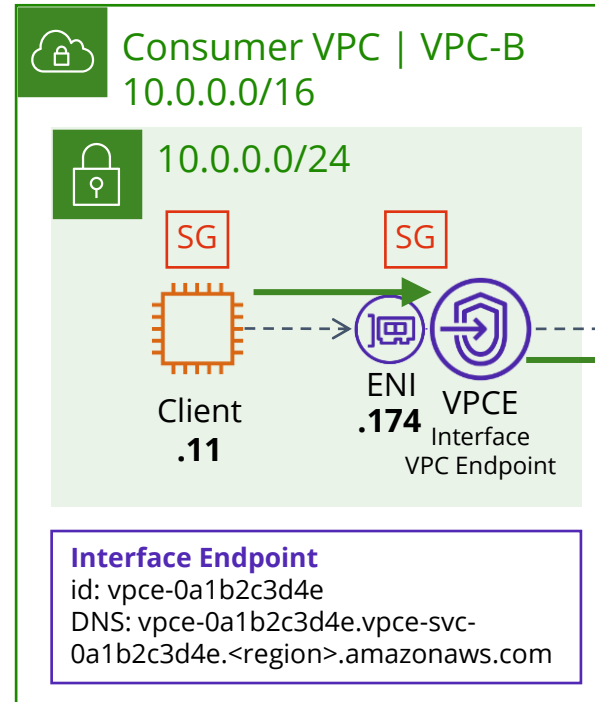
1 | AWS PrivateLink



AWS PrivateLink <https://github.com/bayupw/terraform-aws-overlapping-private-link-demo>

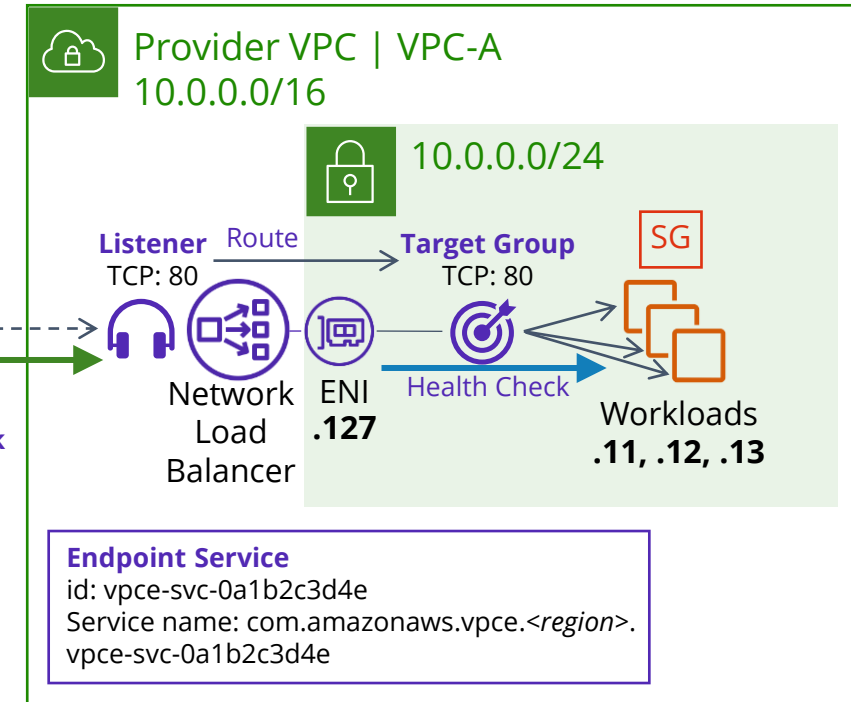


- AWS NLB & VPC Endpoint
- Simple routing
- Source IP is NLB (SNAT)
- Uni-directional traffic
- TCP only, UDP listener is not supported
- Enable PPv2 (Proxy Protocol version 2) to get source IP
- No TGW / security inspection VPC between VPCE & NLB



Route Table

Destination	Next Hop
10.0.0.0/16	local




Route Table

Destination	Next Hop
10.0.0.0/16	local



2 | AWS NAT Gateway

AWS Overlapping NAT Gateway Blog



Contact Us

Support

My Account

Sign In

Create an AWS Account

Products

Solutions

Pricing

Documentation

Learn

Partner Network

AWS Marketplace

Customer Enablement

>

Search

Blog Home

Category

Edition

Follow

Search Blogs

Networking & Content Delivery

How to solve Private IP exhaustion with Private NAT Solution

by SaiJeevan Devireddy and Chandini Penmetsta | on 01 SEP 2021 | in Networking & Content Delivery | Permalink | Share

Introduction:

As our computing needs evolve, one of the most common questions we hear from customers is, "how do I manage my private IP space? I'm almost out of it."

It's difficult to assign separate Private IP ranges (RFC 1918) to different business units in an organization because the available IPv4 address range is restricted. With the growing popularity of micro-service based architecture, where each task needs its own IP address, organizational need for IP addresses is ever increasing. Moreover, when an organization grows, they will eventually run out of Private IP ranges and are forced to use overlapping Private IP ranges across business units. It becomes even more challenging to establish connectivity between business units with overlapping CIDR ranges.

To overcome overlapping IP address limitations, customers can use solutions like AWS PrivateLink, IPv6 or use self managed NAT'ing appliances to translate IPv4 addresses and enable communication between networks with overlapping CIDR ranges. In the last approach, managing NAT rules and the IP address assignment will induce operational overhead.

We now have a Cloud Native Solution to provide IPv4 address translation functionality between private environments, thanks to the launch of the new Private NAT Gateway. In this blog post, we'll illustrate how to use a managed service like Private NAT Gateway to maximize private IPv4

Resources

Networking Products

Getting Started

What's New

Amazon CloudFront

Follow

Twitter

Facebook

LinkedIn

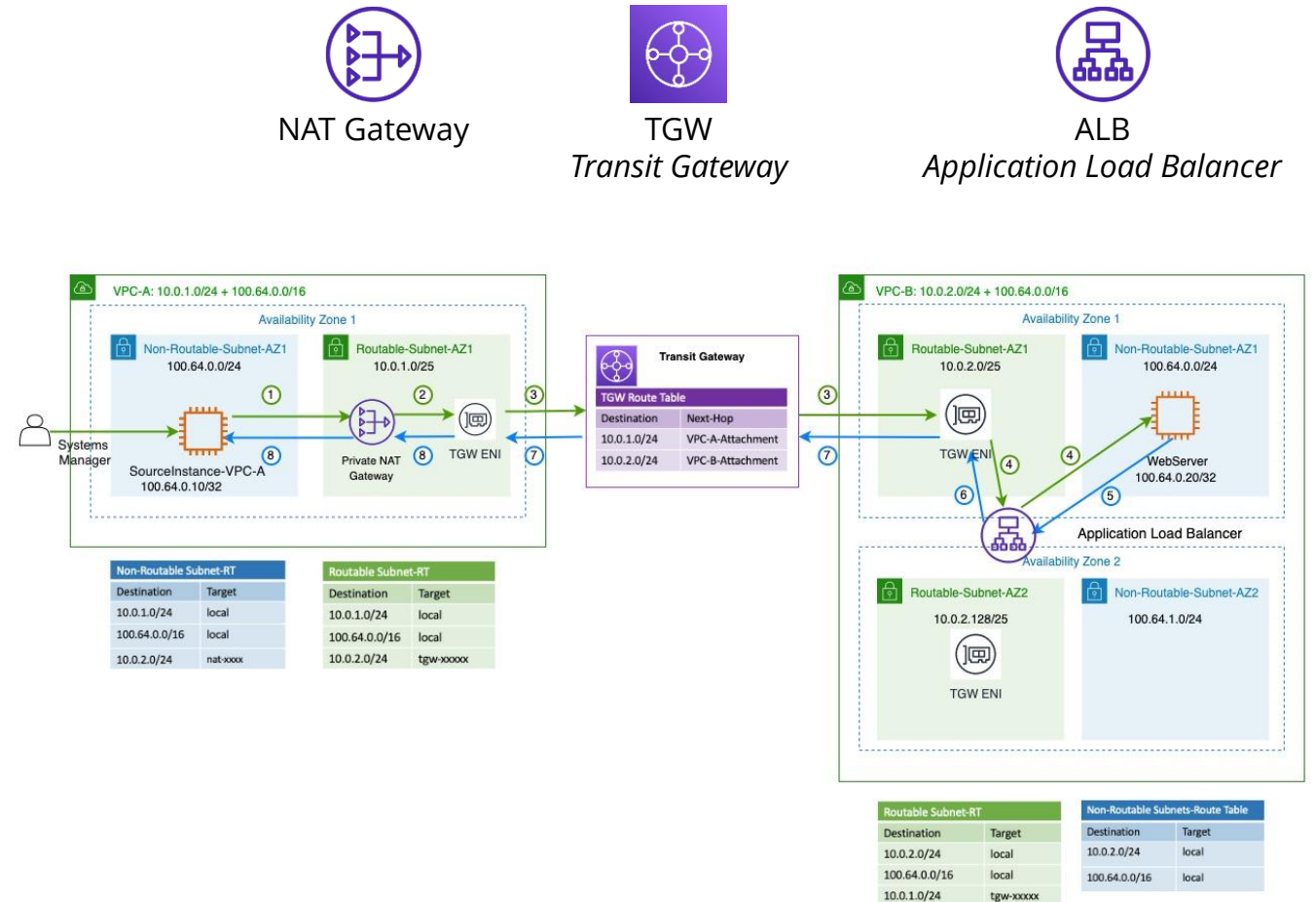
Twitch

Email Updates

AWS Events

Discover the latest AWS events in your region

Learn more >



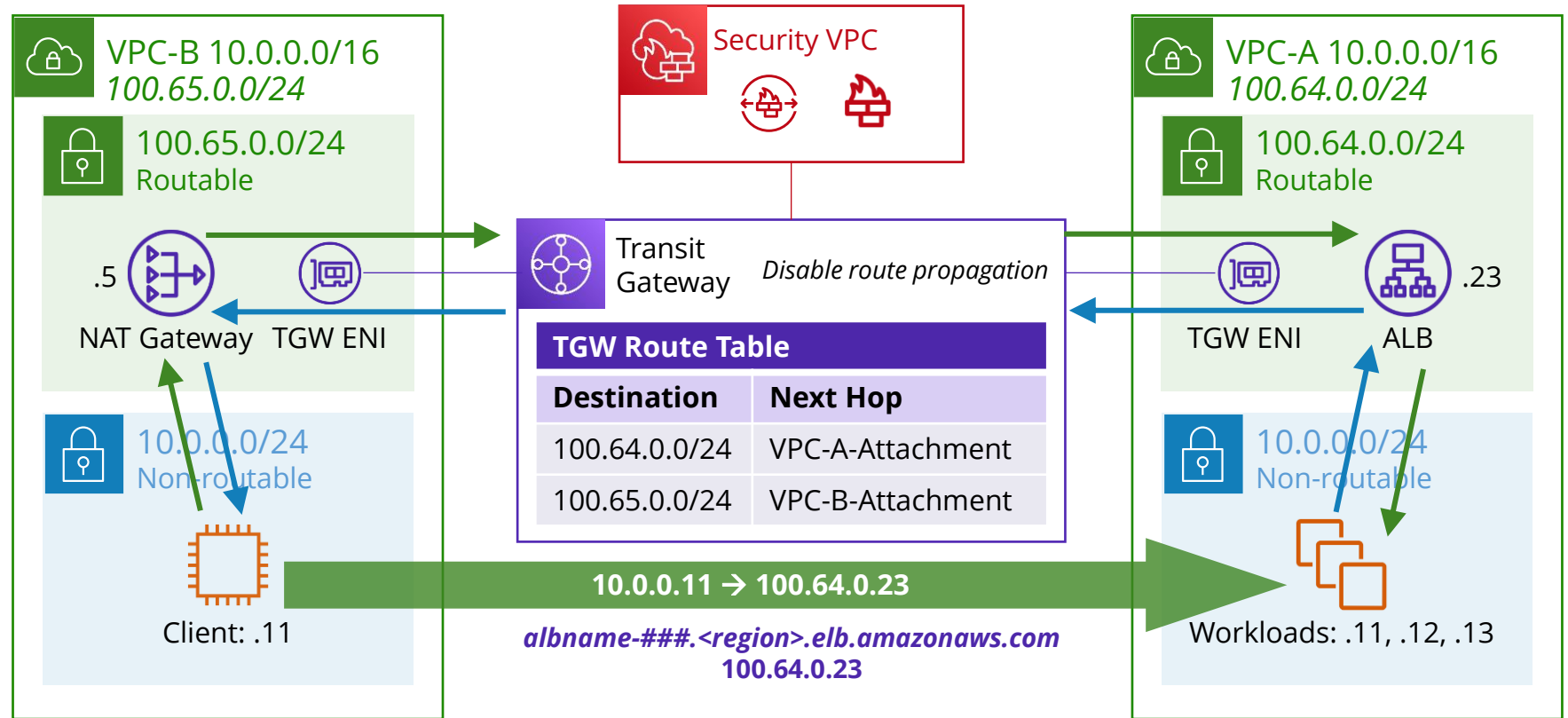
<https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-solve-private-ip-exhaustion-with-private-nat-solution/>



AWS NAT Gateway

<https://github.com/bayupw/terraform-aws-overlapping-nat-gateway-demo>

- ALB & NAT Gateway
- Routable subnets
- Secondary VPC CIDR
- TGW for routable subnets
- TGW security inspection support
- NAT on consumer
- Configure route tables



Non-Routable Subnet RT	
Destination	Next Hop
10.0.0.0/16	local
100.65.0.0/24	local
100.64.0.0/24	nat-xxx

Routable Subnet RT	
Destination	Next Hop
100.65.0.0/24	local
10.0.0.0/16	local
100.64.0.0/24	tgw-xxx

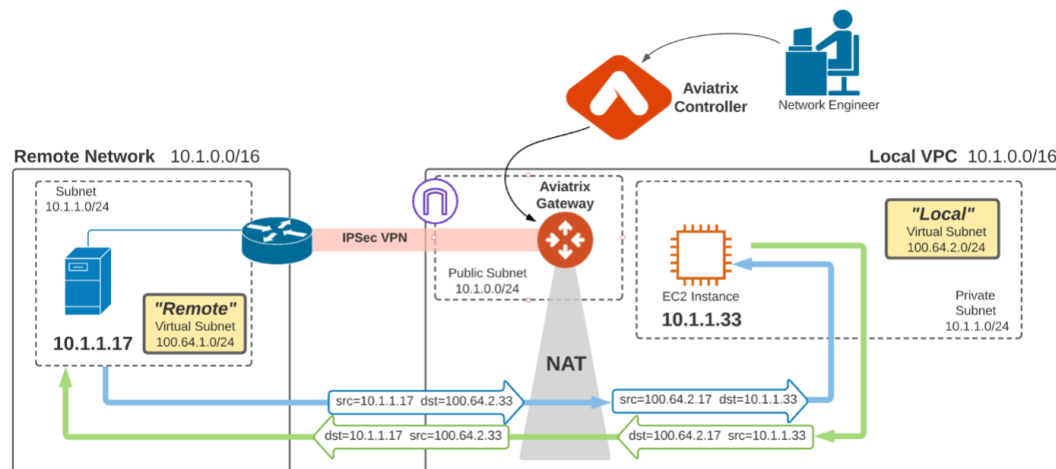
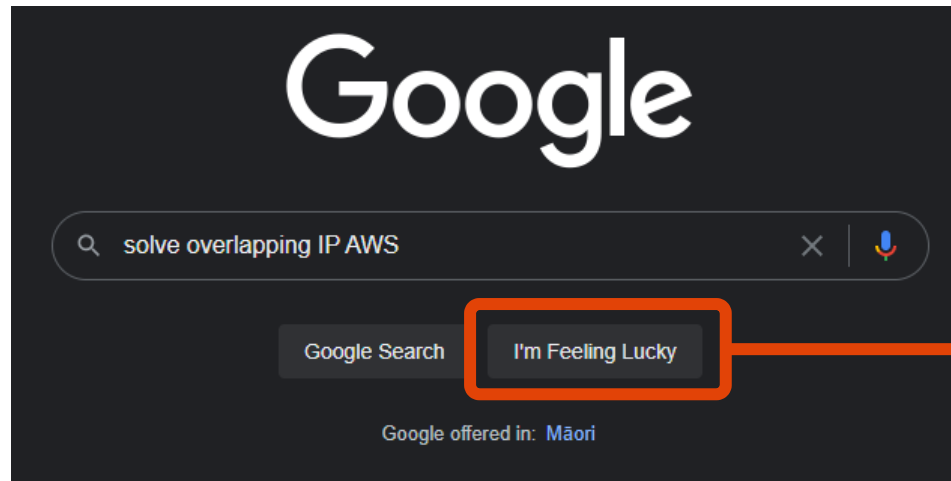
Routable Subnet RT	
Destination	Next Hop
100.64.0.0/24	local
10.0.0.0/16	local
100.65.0.0/24	tgw-xxx

Non-routable Subnet RT	
Destination	Next Hop
10.0.0.0/16	local
100.64.0.0/24	local



3 | Aviatrix Secure Cloud Networking Platform

Google Search: solve overlapping IP AWS



<https://aws.amazon.com/blogs/awsmarketplace/how-to-solve-overlapping-ip-addresses-using-the-aviatrix-cloud-network-platform/>



“

Organizations looking for advanced networking functionality missing from native cloud

...should shortlist Aviatrix.

”

Gartner.

AWS Partner Network (APN) Blog

Gaining Critical Security Insights and Control of Your Traffic with Aviatrix ThreatIQ and ThreatGuard

by James Devine, Jacob Cherkas, and Mandar Alankar | on 05 JAN 2022 | in AWS Marketplace, AWS Partner Network, Customer Solutions, Intermediate (200), Networking & Content Delivery, Security, Thought Leadership | Permalink | Comments | Share

By James Devine, VP Product Management – Aviatrix
Jacob Cherkas, Principal Architect – Aviatrix
Mandar Alankar, Sr. Networking Solutions Architect – AWS

It can be difficult to gain security insights into your cloud infrastructure, especially as architectures grow to encompass multiple availability zones, regions, and clouds.

Aviatrix Systems is an AWS Partner with Competency designations in both [Networking](#) and [Security](#). Aviatrix is uniquely positioned to provide deep insights into network traffic.

This includes security insights that can augment Amazon Web Services (AWS) native security capabilities, such as those found by [Amazon GuardDuty](#), for example.

In a [previous blog post](#), we discussed the advanced visibility and troubleshooting capabilities that Aviatrix brings to AWS customers. In this post, we're excited to detail new capabilities that were recently added to the [Aviatrix Secure Network Platform](#)—ThreatIQ and ThreatGuard.

Threat Detection with ThreatIQ



**Want to work with
Aviatrix Systems?**

[Connect](#)

<https://aws.amazon.com/blogs/apn/gaining-critical-security-insights-and-control-of-your-traffic-with-aviatrix-threatiq-and-threatguard/>

Enterprise customers using Aviatrix

Technology

 ABSOLUTE®

 splunk>

 Informatica®

 genpact

 VERACODE

 MetricStream

 teradata.

 indeed®

 CUJOAI

 XILINX

 workfront®

 ZS

 INFOGIX

 gemalto®
a Thales company

 SHPE®

 VERINT.

 easy
MILE

Financial Services

 ReAssure

 AAA

 Avalara

 TOYOTA
FINANCIAL SERVICES

 WeLab

 FACTSET®

 Jefferies

 SoFi

 XINJA

 AEGON

 APPTIO®

 IPIPELINE®

 FIRST REPUBLIC BANK

 BankUnited

 n e l n e t.

 GUIDEWIRE

Retail

 MONSTER

 Yum!

 Wawa®

 chewy.com

 ellucian.

 Constellation
Brands

 NU SKIN

 Wharton
UNIVERSITY of PENNSYLVANIA

 aviatrix

 COMPASS
GROUP
#AWSAKL

Travel & Hospitality

 HYATT®

 IHG®

 AVIS®

 vacasa

 Republic
Airways

 UNITED
AIRLINES

Manufacturing

 Johnson
Controls

 BAKER
HUGHES
a GE company

 GE

 MUELLER

 PACCAR

Media

 dish CBS

 Charter
COMMUNICATIONS

 SONY
PICTURES

Government



 NASA

 MAXIMUS®

 UNITED
TECHNOLOGIES

Healthcare

 Abbott

 Takeda

 abbvie

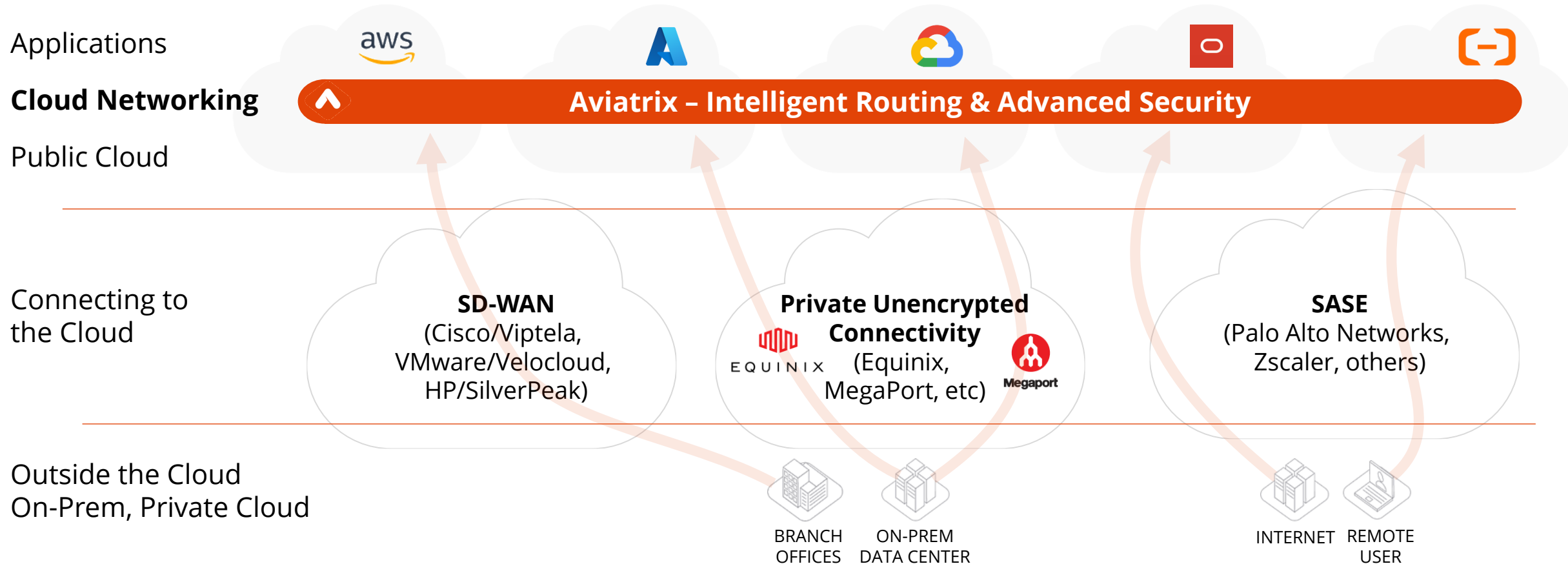
 CENTENE®
Corporation

 robin
HEALTHCARE

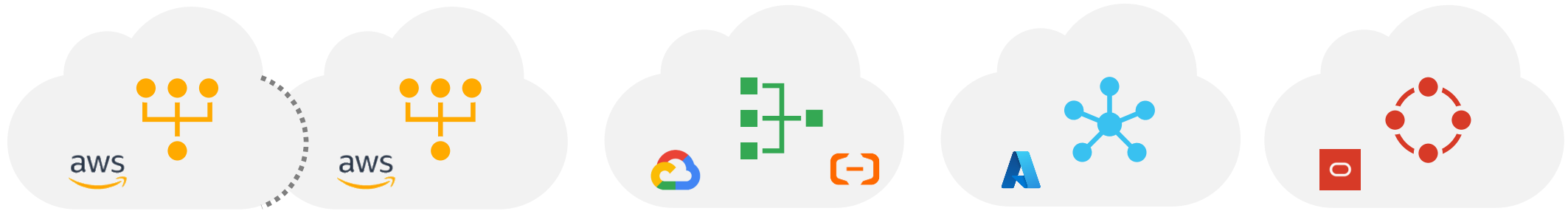
 Biogen.

 medidata

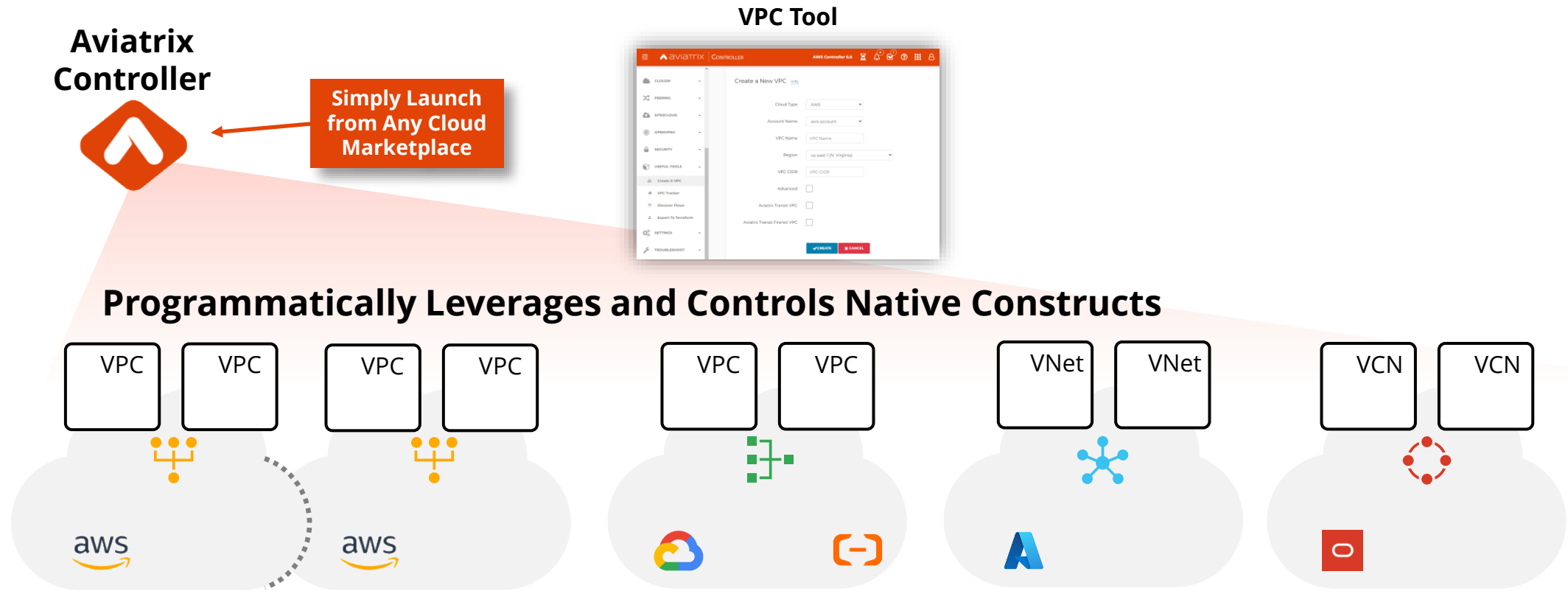
Aviatrix – The Cloud Network Reference Architecture



Cloud Networking with Aviatrix | Cloud Native Integration



Cloud Networking with Aviatrix | Cloud Native Integration



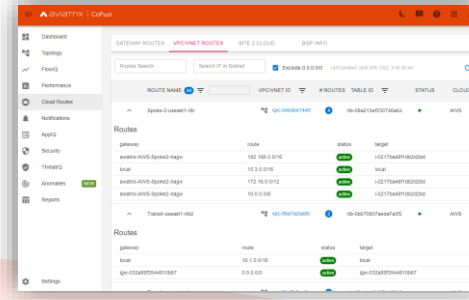
Cloud Networking with Aviatrix | Cloud Routes Management

Aviatrix
Controller

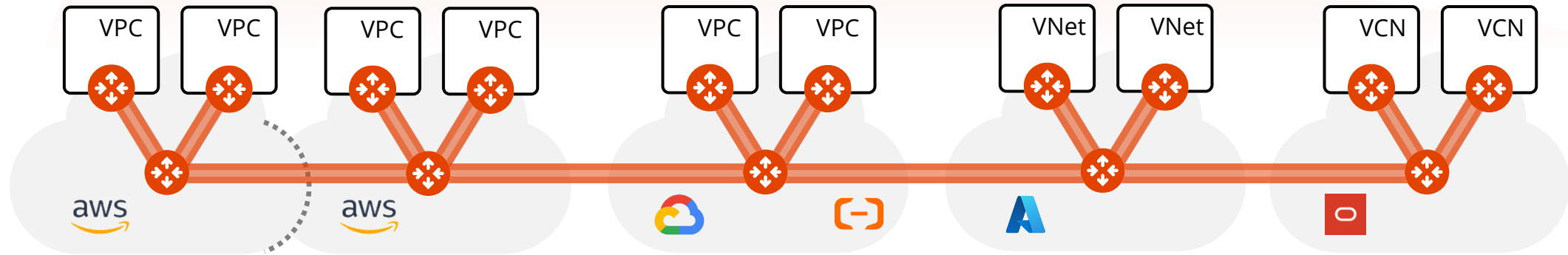


**Adds Networking Management
Advanced Networking and Security on Top In Each Cloud**

Cloud Routes



- Programs and manages Cloud Native Routes
- Turn cloud static routes into dynamic routes
- Single point of management for all cloud routes

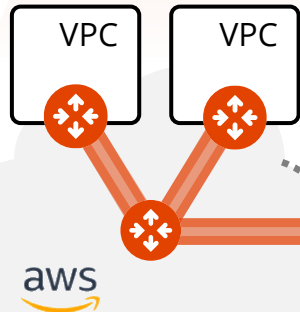


Cloud Networking with Aviatrix | Cloud Routes Management

Aviatrix Controller

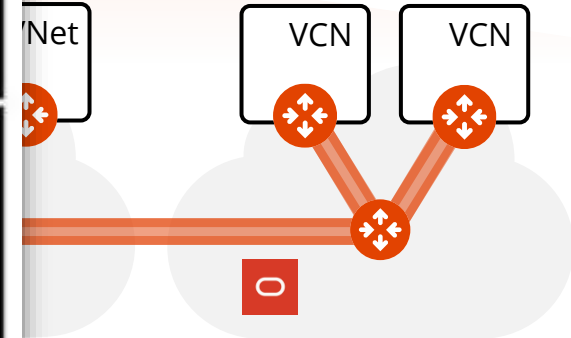


Adds Network
Advanced Network



Cloud Routes Management

- Programs and manages Cloud Native Routes
- Turn cloud static routes into dynamic routes
- Single point of management for all cloud routes



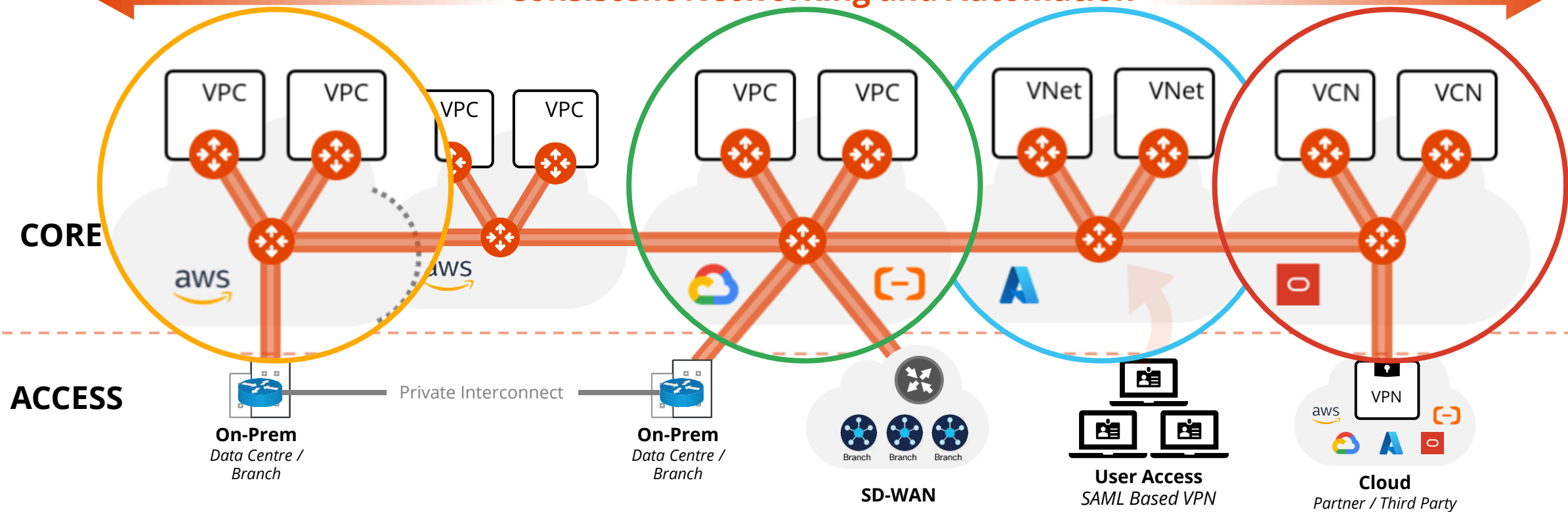
Cloud Networking with Aviatrix | Consistent Networking

Aviatrix
Controller



Single Terraform Multi-Cloud Provider

Consistent Networking and Automation



Cloud Networking with Aviatrix | Consistent Network Operations

Aviatrix
Controller



Aviatrix
CoPilot



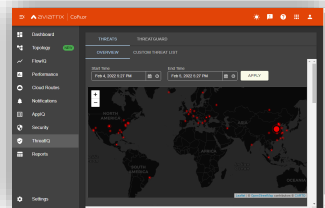
Topology Mapping



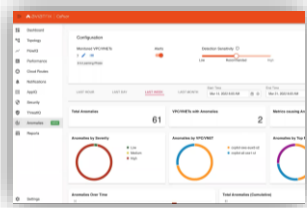
NetFlow



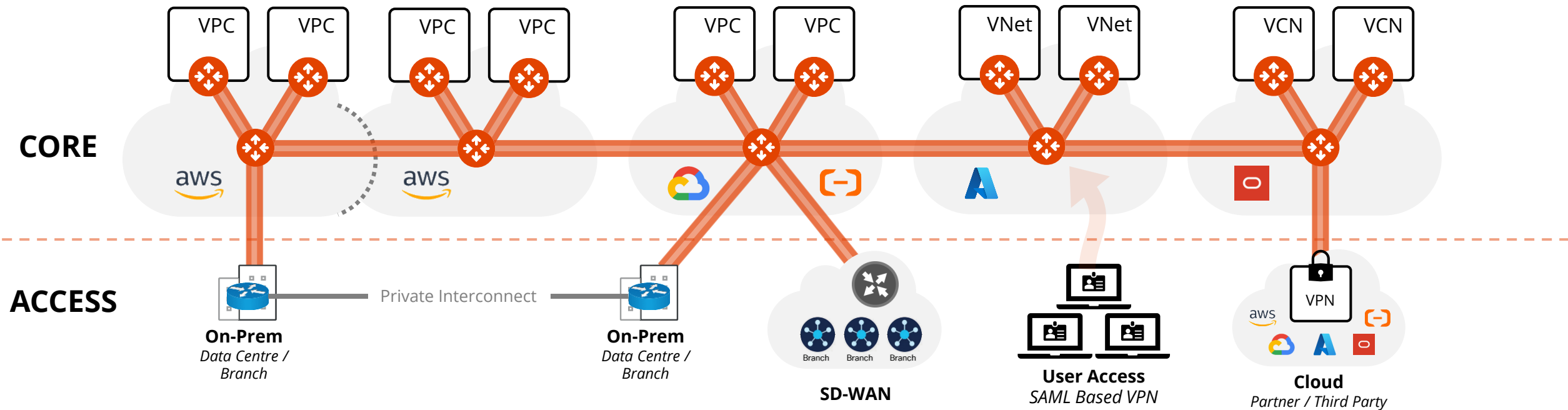
Threat Intelligence



Anomaly Detection



Consistent Visibility and Troubleshooting



Cloud Networking with Aviatrix | Threat Intelligence with Remediation

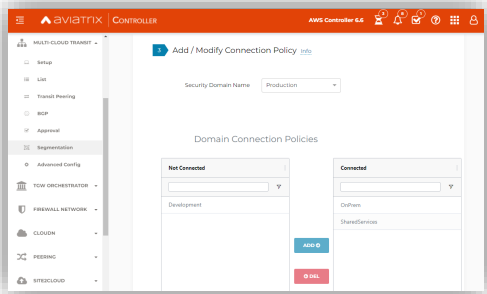
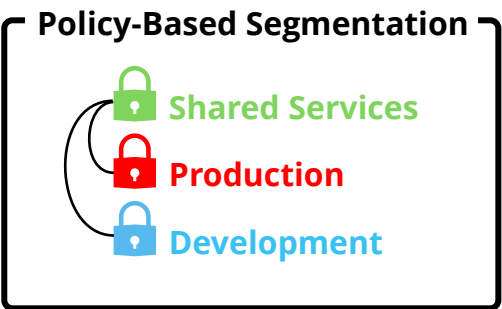


Cloud Networking with Aviatrix | Automatic Remediation

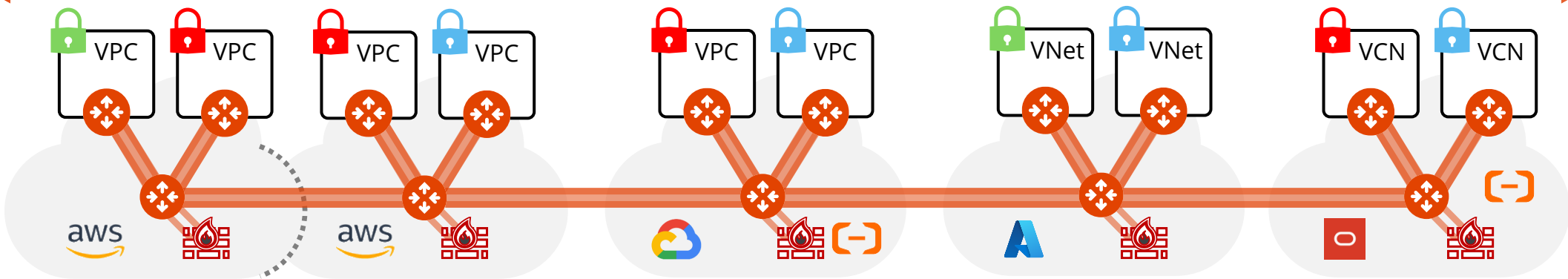


Cloud Networking with Aviatrix | Consistent Security

Aviatrix
Controller



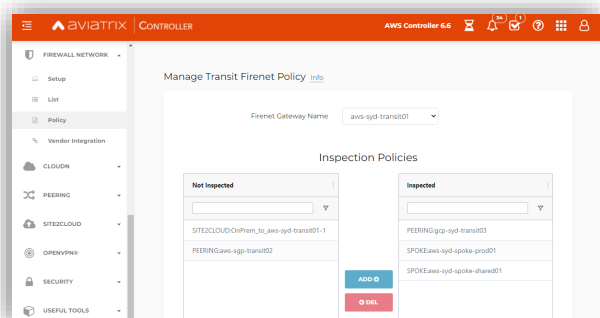
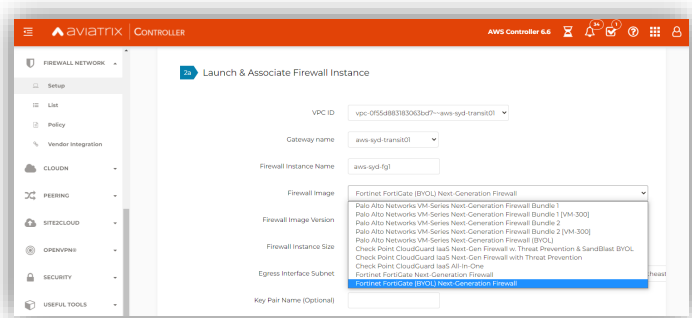
Consistent Policy-Based Security



Insert NextGen Firewall

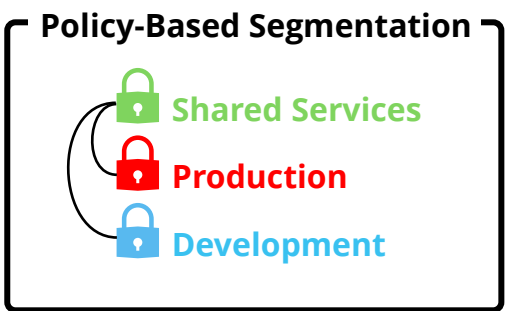


Bring your own Firewall

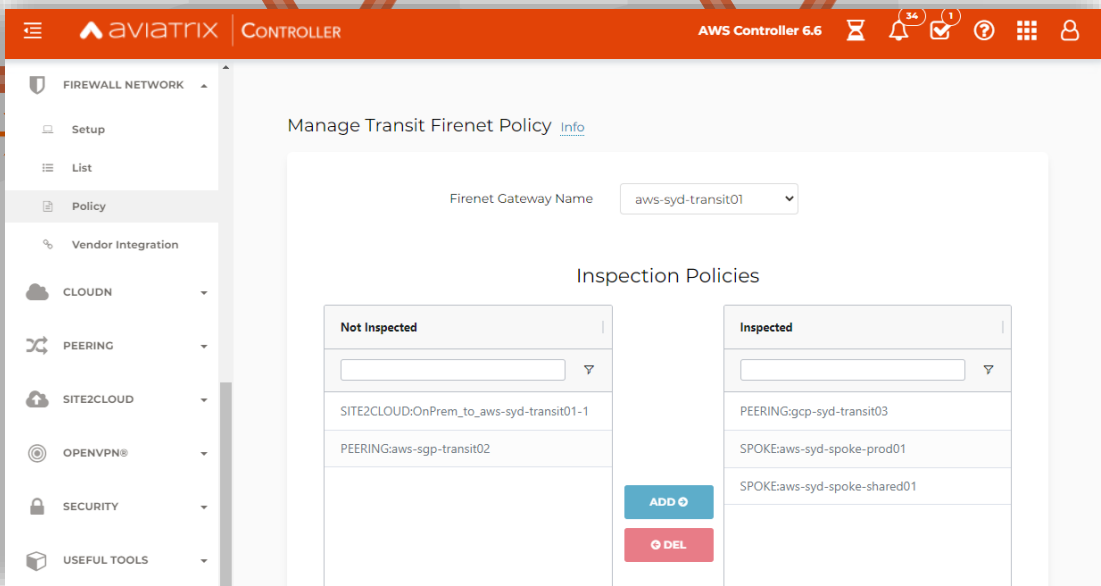
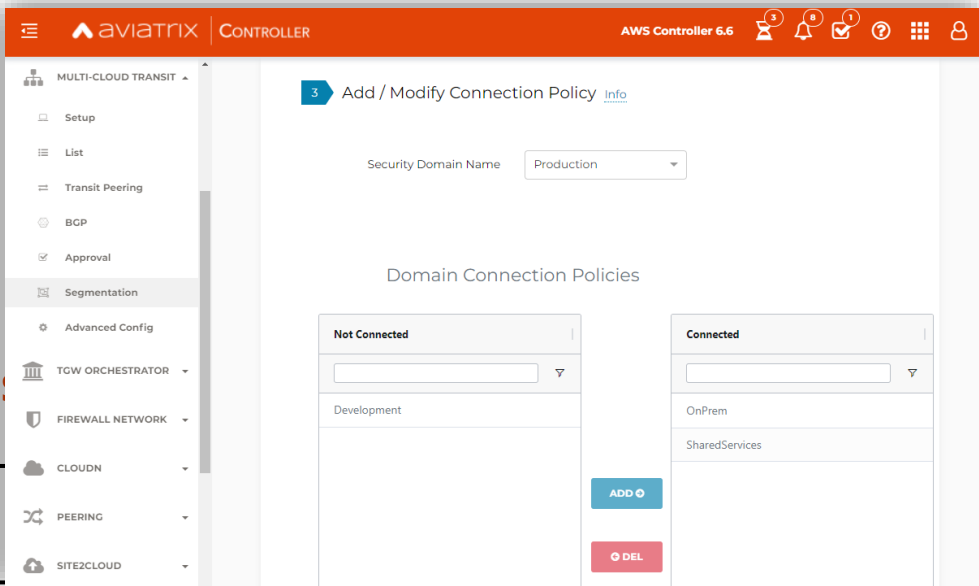
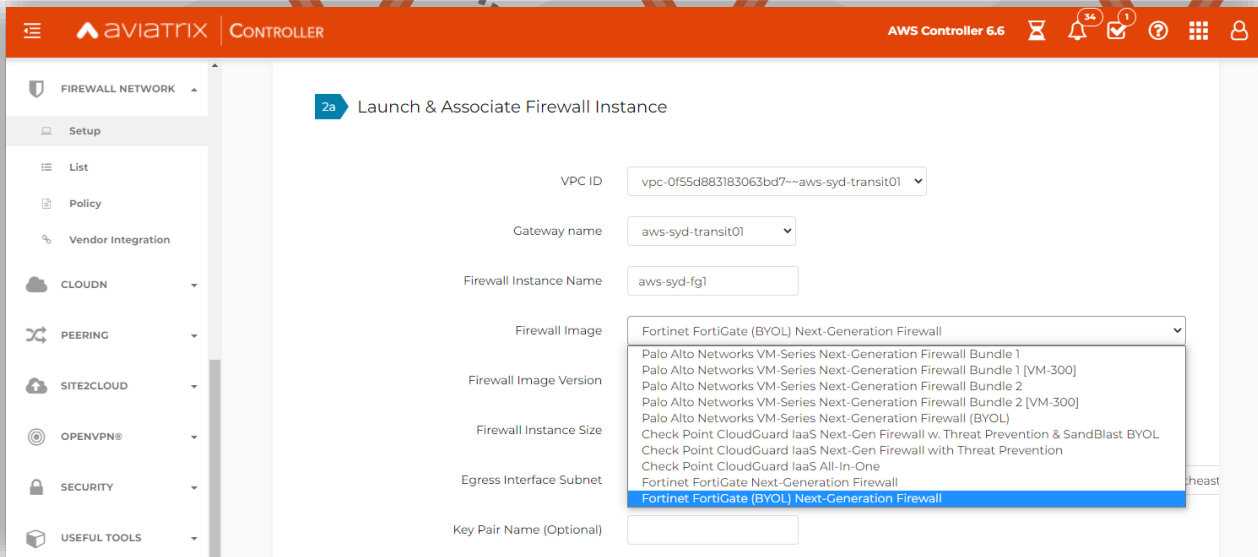
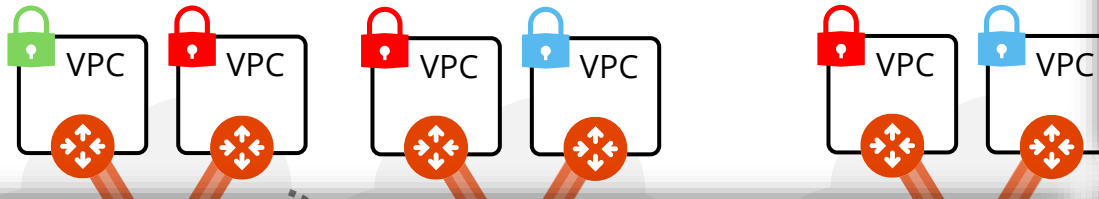


Cloud Networking with Aviatrix | Consistent Security

Aviatrix
Controller



Consistent Policy-Based



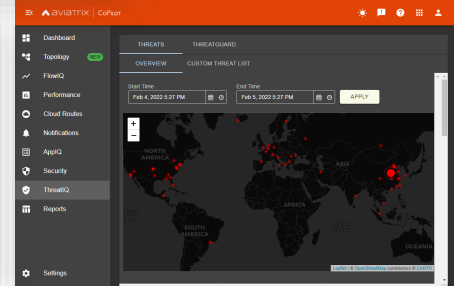
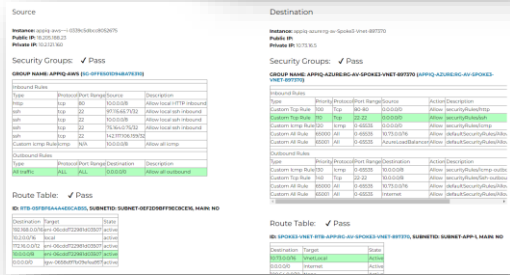
Start With A Single, Simple Initial Use Case



Aviatrix Controller

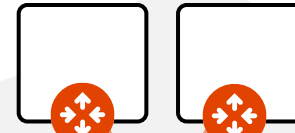


Aviatrix CoPilot



Visibility & Operations

High-Availability
Hub-n-Spoke

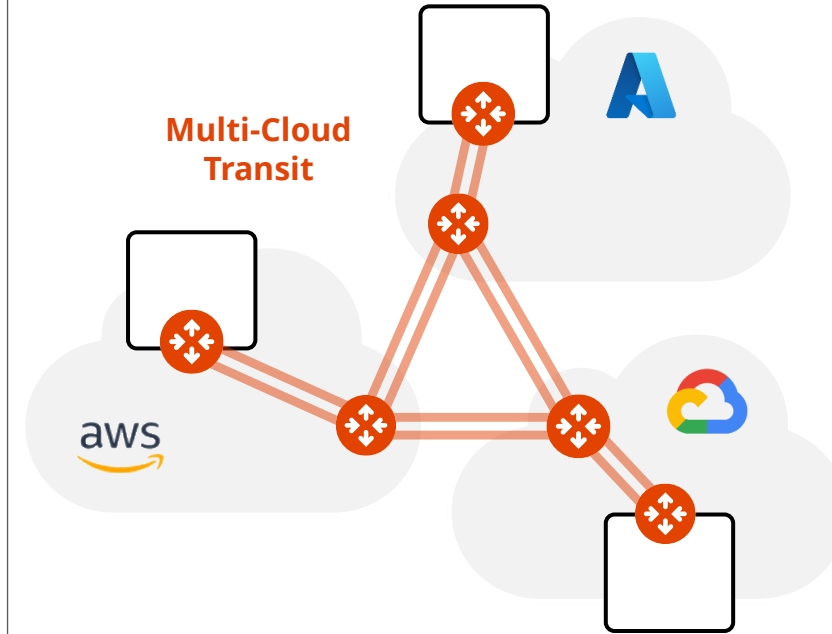


Securing
Private
Connectivity
with
HPE



Data Center-to-Cloud

Multi-Cloud
Transit



Secure User Access
User VPN
(SAML)



Internet



Compliance



Egress FQDN
Filtering

Advanced
NAT

10.0.0.0/16

10.0.0.0/16

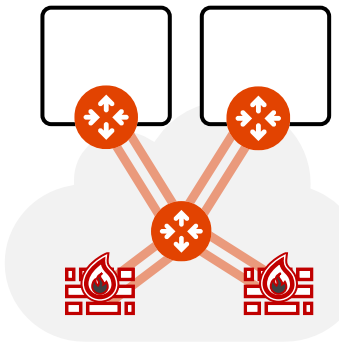
Overlapping IPs

10.0.0.0/16

Next-Gen Firewall
Service Insertion
(FireNet)

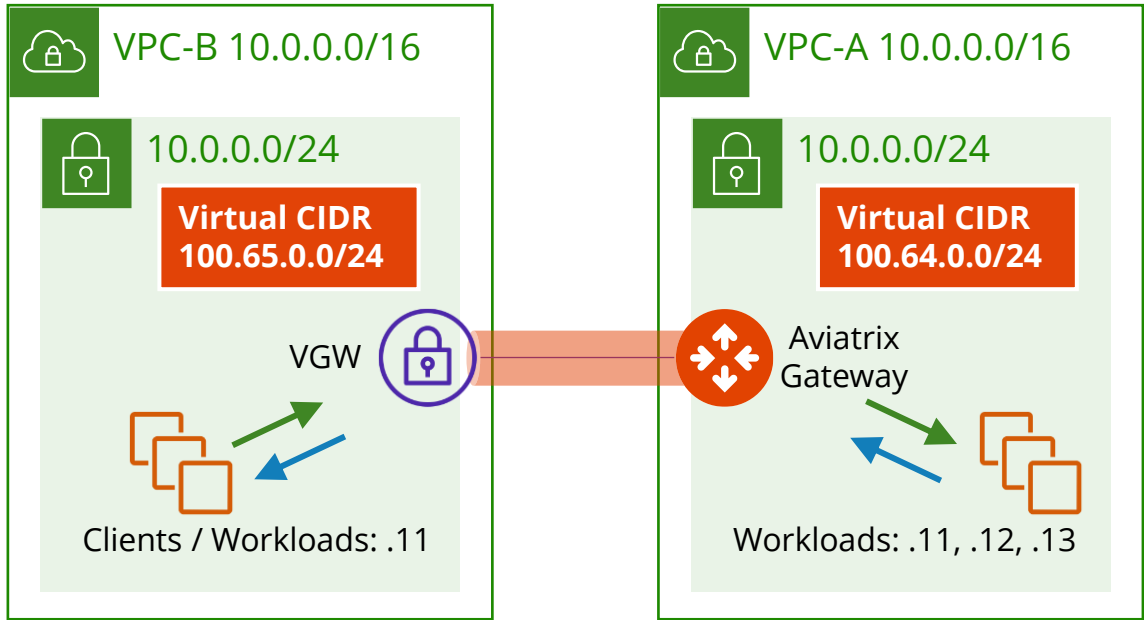


Bring your own Firewall





- Virtual CIDR
- Bidirectional or Unidirectional – flexible NAT options
- No NAT on consumer side
- DNS handled outside Aviatrix e.g. Route 53

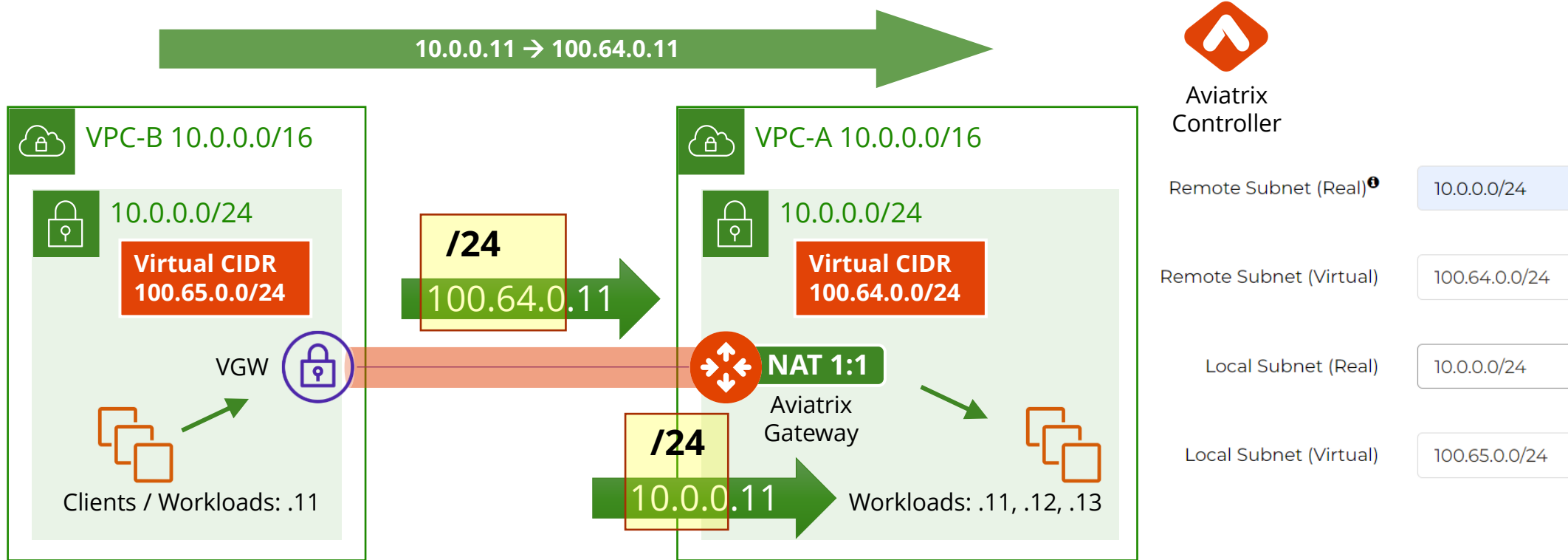


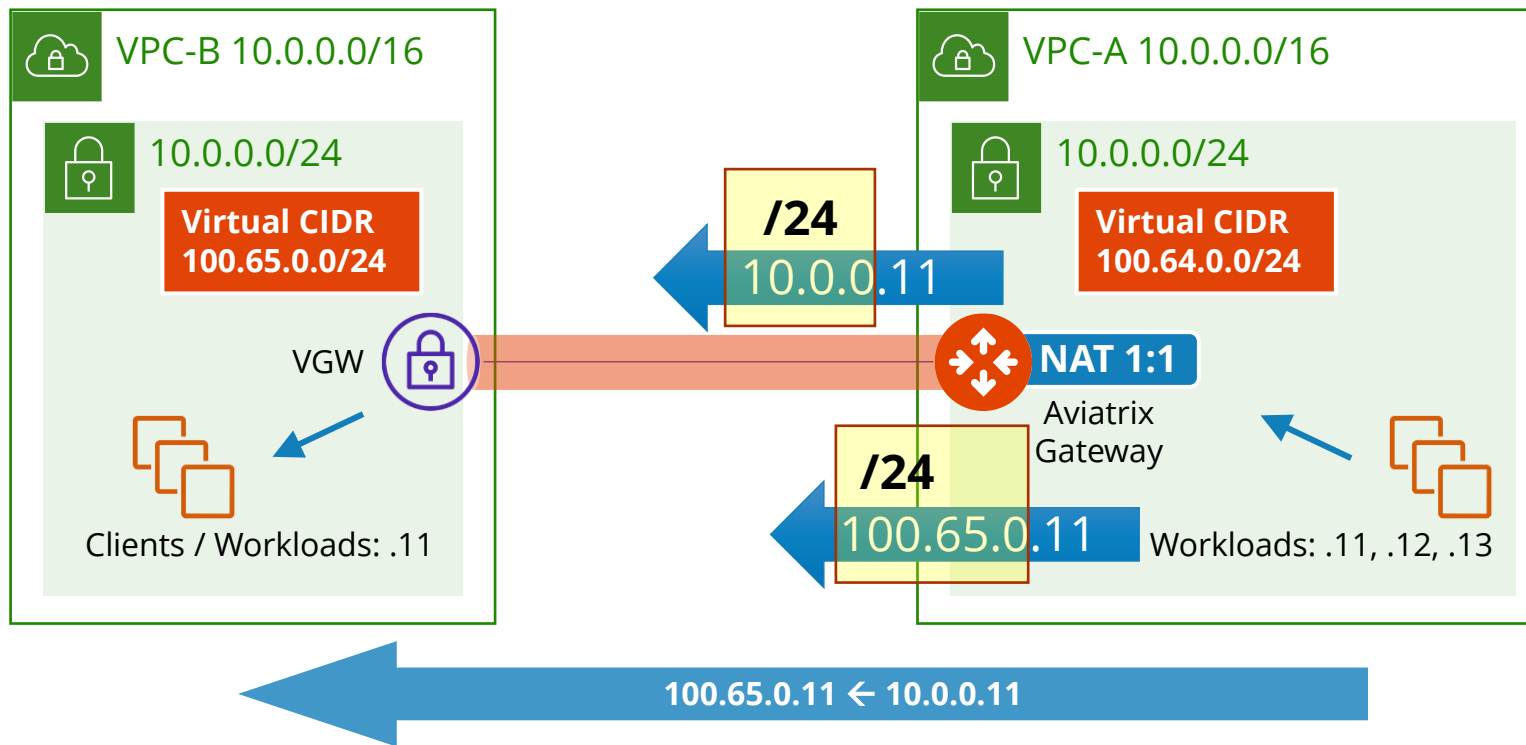
Aviatrix
Controller

Remote Subnet (Real)	10.0.0.0/24
Remote Subnet (Virtual)	100.64.0.0/24
Local Subnet (Real)	10.0.0.0/24
Local Subnet (Virtual)	100.65.0.0/24

Routable Subnet RT	
Destination	Next Hop
10.0.0.0/16	Local
100.64.0.0/24	vgw-xxx

Route Table	
Destination	Next Hop
10.0.0.0/16	local
100.65.0.0/24	eni-xxx





Aviatrix
Controller

Remote Subnet (Real) ⓘ

10.0.0.0/24

Remote Subnet (Virtual)

100.64.0.0/24

Local Subnet (Real)

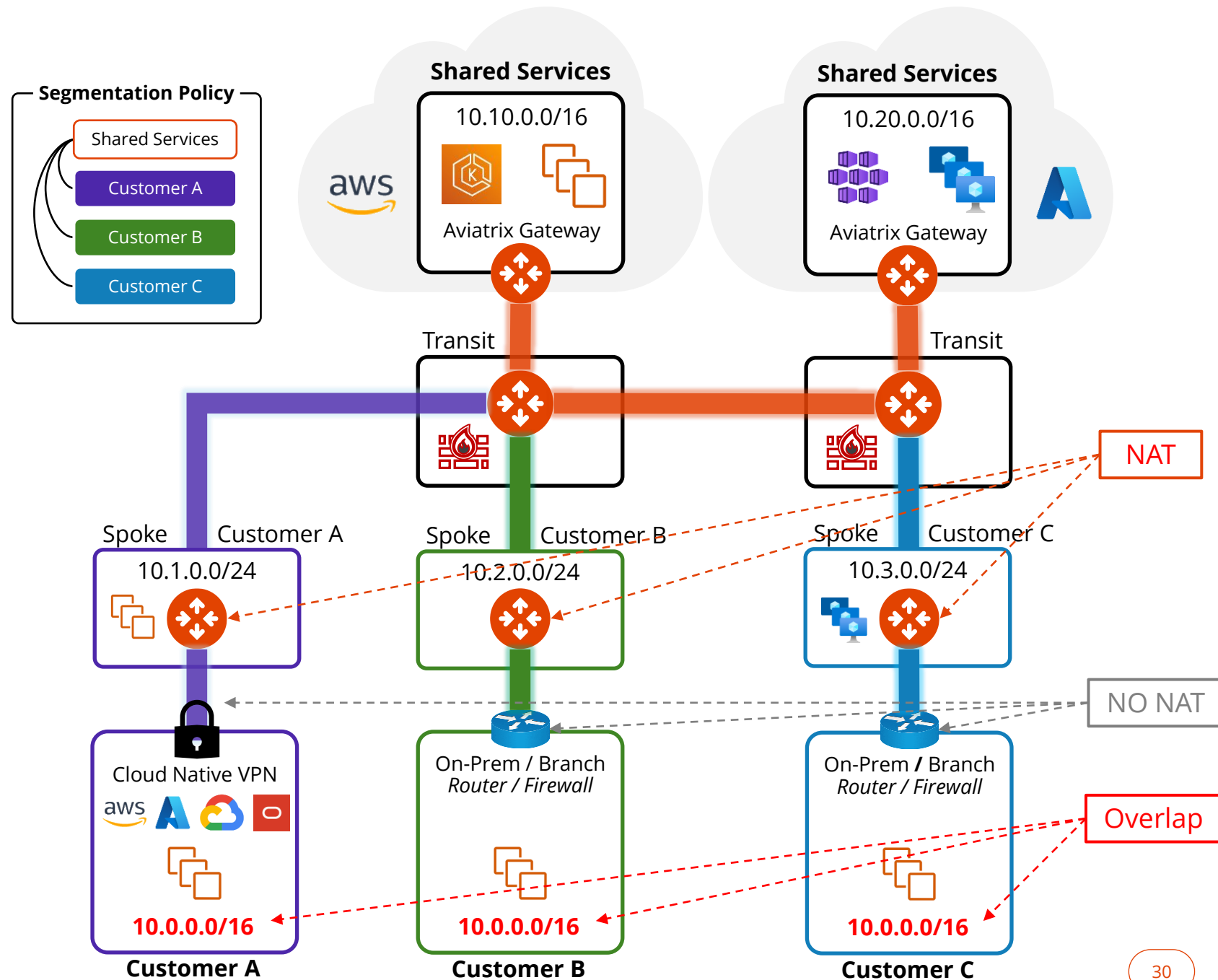
10.0.0.0/24

Local Subnet (Virtual)

100.65.0.0/24

SaaS Provider Use Cases

- Policy based segmentation to segregate customer traffic
- Next-Gen Firewall Service Insertion in Transit
- Overlapping IPs and NAT support
- No NAT on customer side
- Multi-Cloud Ready



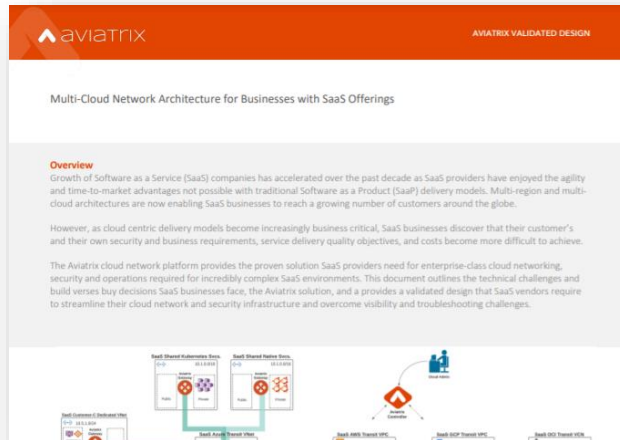
Demo



Additional Resources

SaaS Provider Case Study

<https://aviatrix.com/resources/all-content/saas-customer-case-study>



SaaS Provider Infrastructure | AviaTrix Validated Design

<https://aviatrix.com/resources/all-content/aviatrix-validated-design-saas-providers-infrastructure>



TechTalk | SaaS Provider Use Cases with Demo

<https://youtu.be/XkOIYfi7ELO>



Summary

Summary & Key Takeaways



AWS PrivateLink

- NLB + VPCE
- Unidirectional TCP traffic
- No NAT configuration (Auto SNAT on NLB)
- Bypass TGW and security inspection VPC



AWS NAT Gateway

- NAT Gateway + ALB
- Secondary CIDR (Routable) + TGW
- Unidirectional TCP / UDP
- Security Inspection VPC support
- NAT on consumer side
- Route table configuration



Aviatrix



- Virtual CIDR
- Advanced NAT on provider side
- Bidirectional / unidirectional
- Multi-cloud support
- Advanced network/security features:
 - Network operational visibility
 - Packet capture, dynamic topology mapping
 - Network segmentation
 - Micro-segmentation
 - Next-Gen Firewall Inspection

Aviatrix Learning and Hands-on Lab Workshop Events

Aviatrix Certified Engineer (ACE) Multi-Cloud Networking Certification



<https://aviatrix.teachable.com/>

Free Voucher code: AWSAKL



ACE IaC

Aviatrix + Terraform, GitHub Actions
\$9.95 w/ code **ACEINFRASTRUCTURE**

<https://aviatrix.teachable.com/p/aviatrix-ace-iac>



<https://events.aviatrix.com/aviatrixtestflight-june>

Aviatrix Test Flight

- 2PM – 3.30PM NZST
- 90 minutes session
- Hands-on lab



<https://events.aviatrix.com/immersiondays>

<https://events.aviatrix.com/mayawsaviatriximmersionday>

Cloud Networking and Network Security Immersion Day

- Co-presented by AWS
- 6 hours session
- Hands-on lab



Bayu Wibowo



EMAIL
bwibowo@aviatrix.com

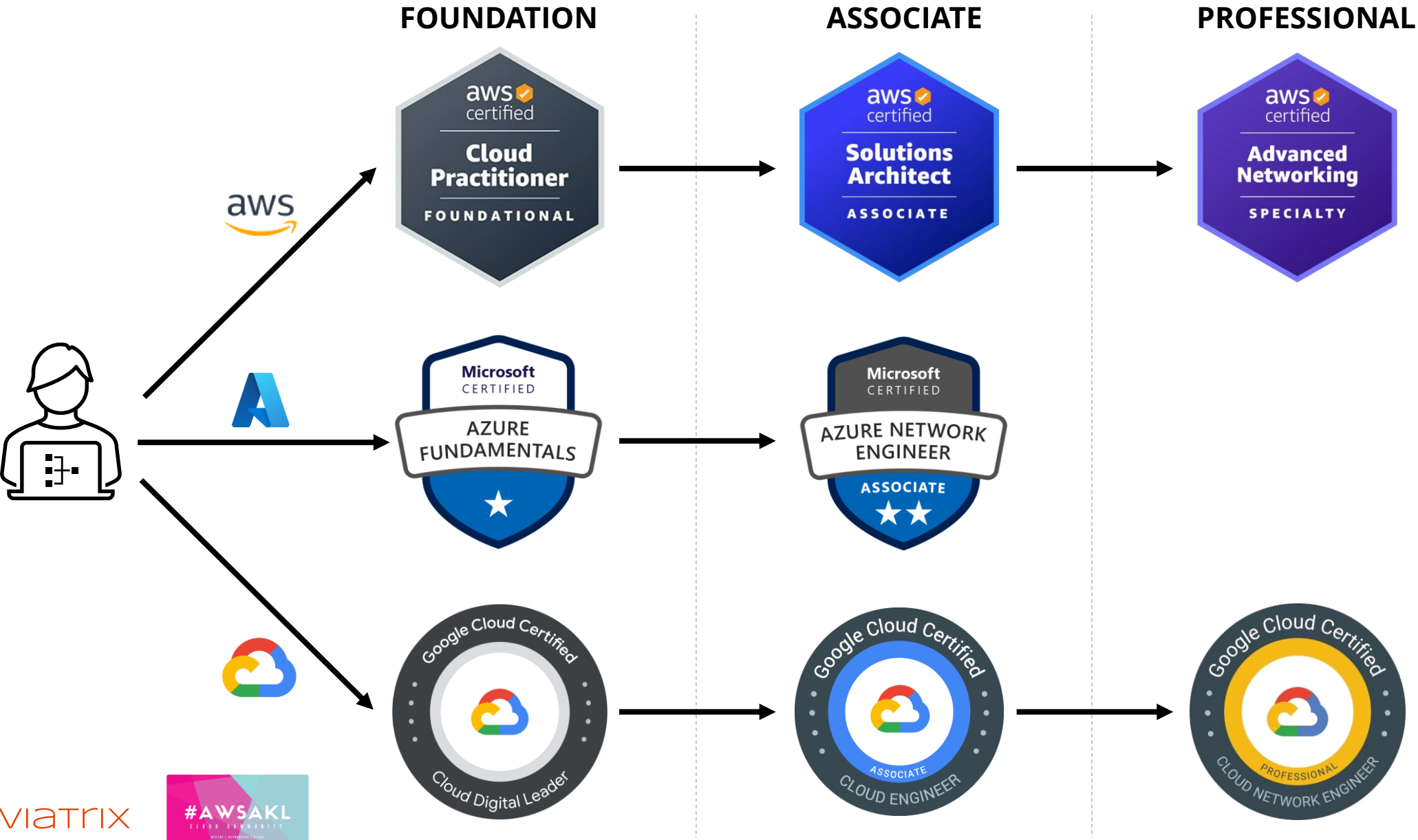


WEBSITE
www.aviatrix.com

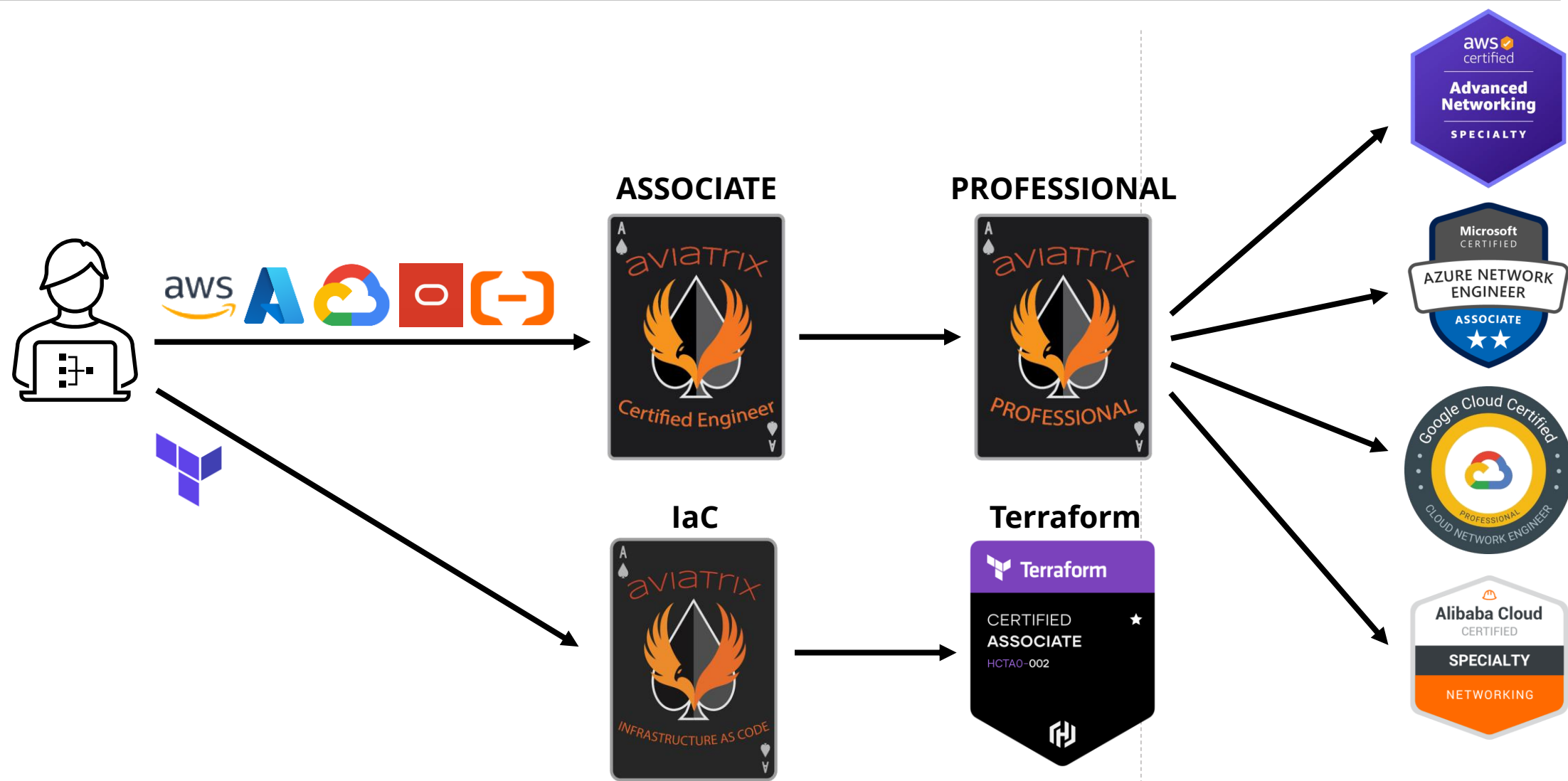


PHONE
+64 21 410 534

Cloud Networking Certification Path



Cloud Networking Certification Path with Aviatrix



Aviatrix Leads Cloud Learning for Networking, Security and Ops Teams

Deploy in minutes ~ \$1 / hour



<https://community.aviatrix.com/t/g9hx9jh>

Need Help?

info@aviatrix.com

docs.aviatrix.com

aviatrix.com →



Customised Architectural Design Session



Schedule an In-Person or Virtual Design Session

bwibowo@aviatrix.com

<https://www.linkedin.com/in/bayupw/>

Weekly TechTalks Webinar



Secure Cloud Networking Topics Discussed Weekly

<https://aviatrix.com/techtalks/>