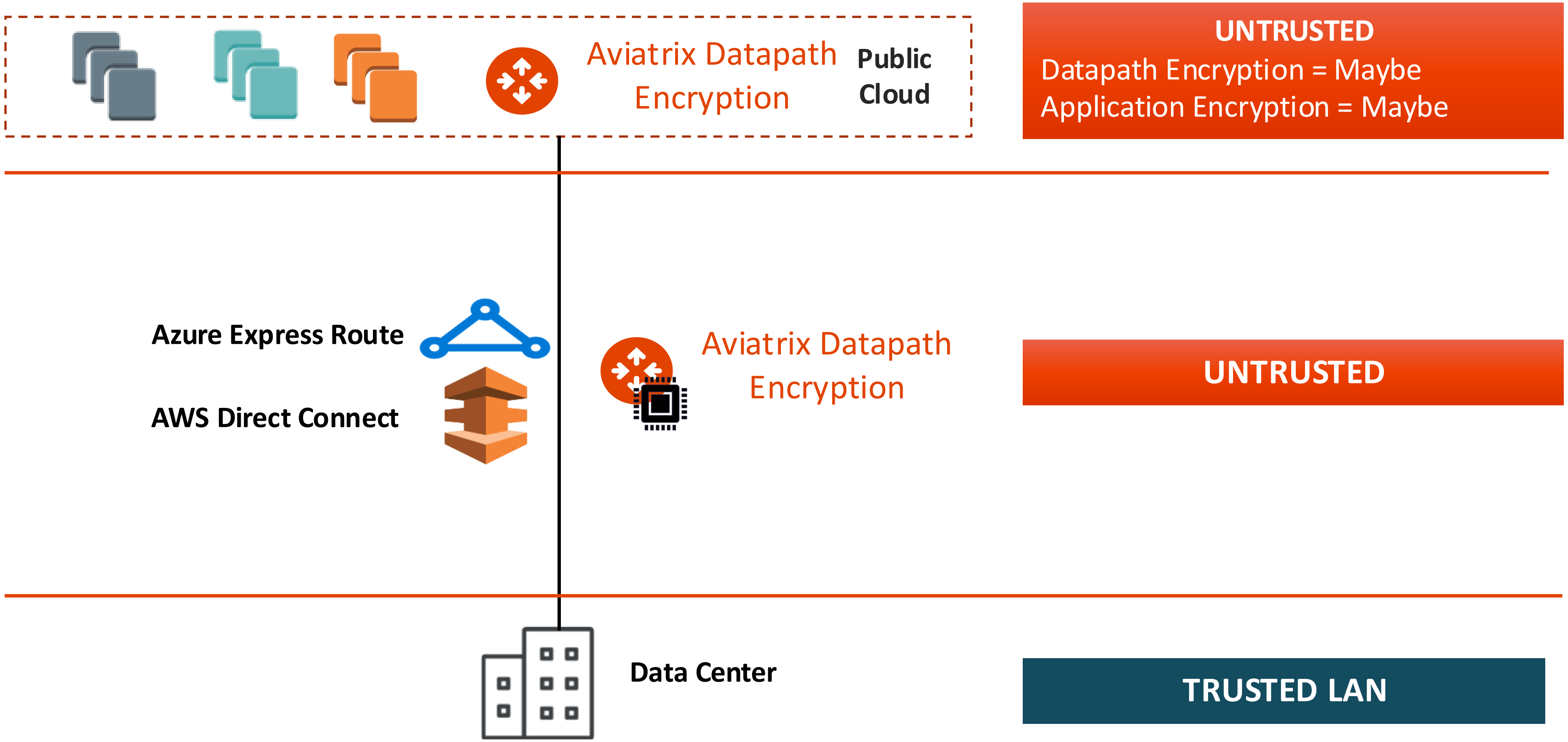
High-Performance Encryption (HPE)

ACE Solutions Architecture Team

Zero Trust – Datapath Encryption

Why?

- Compliance Requirement
- Data Security
- Business Policy
- Native Constructs Routing Scalability Challenges



Aviatrix Datapath Encryption

Public Cloud

UNTRUSTED
Datapath Encryption = Maybe
Application Encryption = Maybe

Azure Express Route

AWS Direct Connect

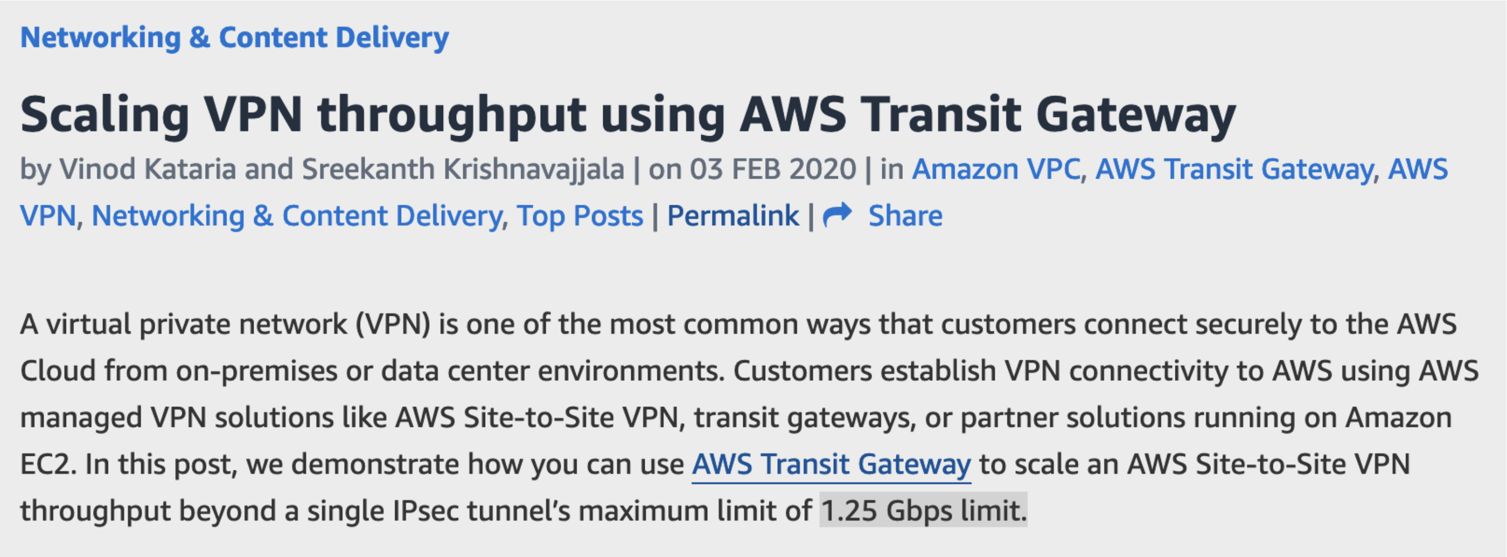
Aviatrix Datapath Encryption

UNTRUSTED

Data Center

TRUSTED LAN

1.25 Gbps IPSec Throughput is industry wide issue

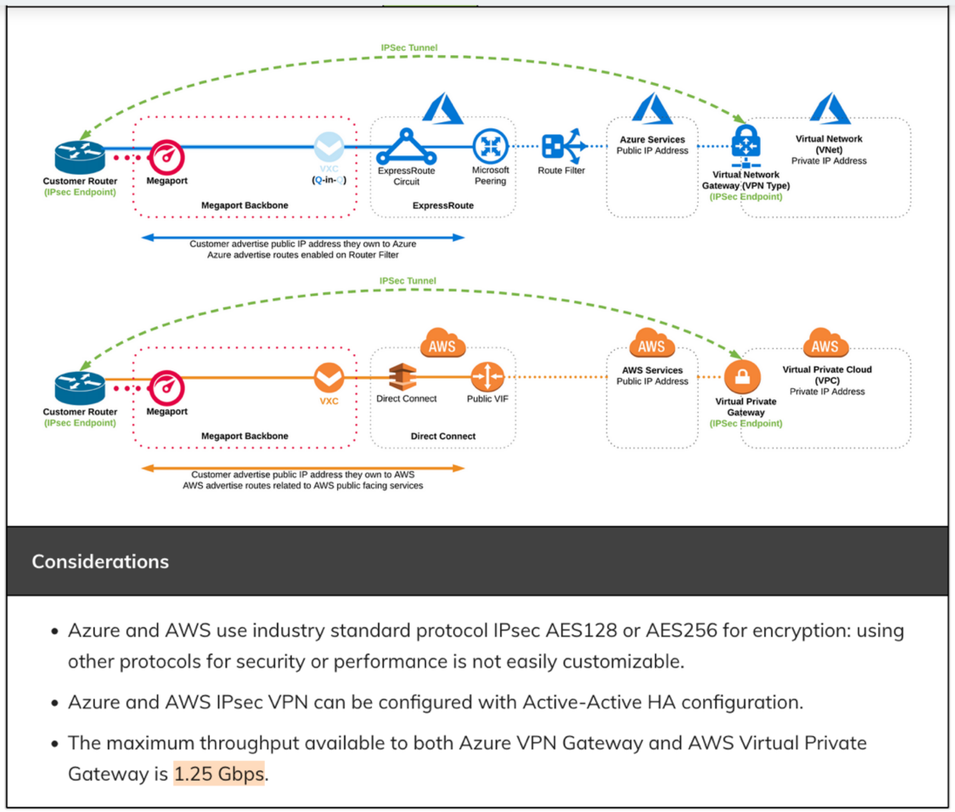


Networking & Content Delivery

Scaling VPN throughput using AWS Transit Gateway

by Vinod Kataria and Sreekanth Krishnavajjala | on 03 FEB 2020 | in Amazon VPC, AWS Transit Gateway, AWS VPN, Networking & Content Delivery, Top Posts | Permalink | Share

A virtual private network (VPN) is one of the most common ways that customers connect securely to the AWS Cloud from on-premises or data center environments. Customers establish VPN connectivity to AWS using AWS managed VPN solutions like AWS Site-to-Site VPN, transit gateways, or partner solutions running on Amazon EC2. In this post, we demonstrate how you can use AWS Transit Gateway to scale an AWS Site-to-Site VPN throughput beyond a single IPsec tunnel's maximum limit of 1.25 Gbps limit.



Considerations

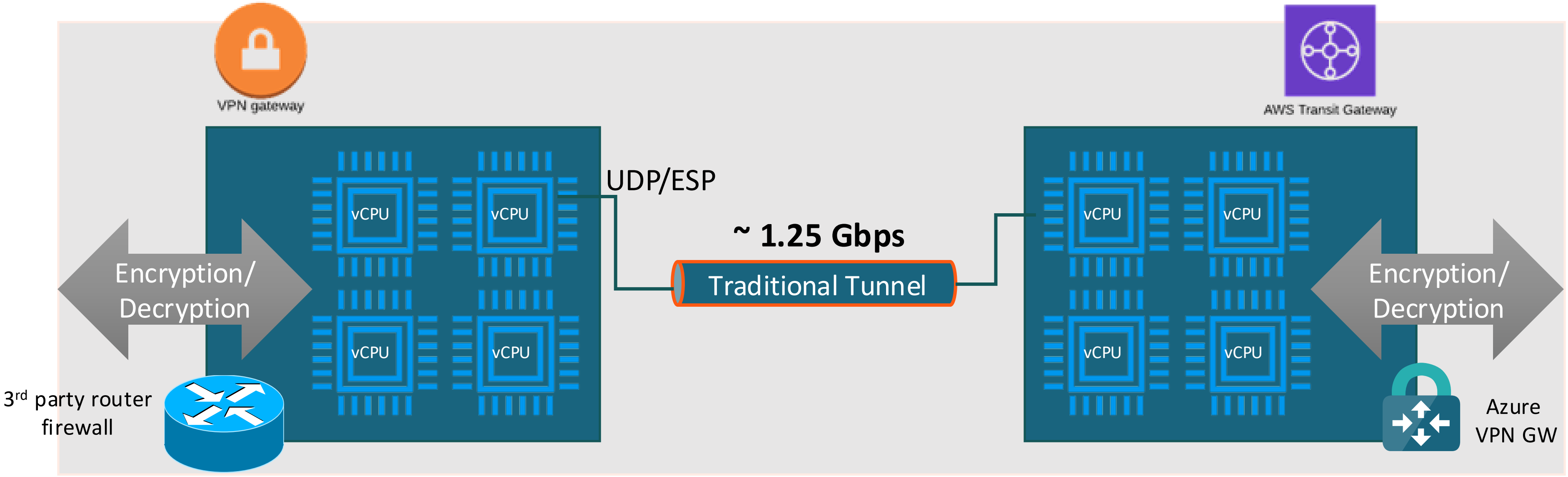
- Azure and AWS use industry standard protocol IPsec AES128 or AES256 for encryption: using other protocols for security or performance is not easily customizable.
- Azure and AWS IPsec VPN can be configured with Active-Active HA configuration.
- The maximum throughput available to both Azure VPN Gateway and AWS Virtual Private Gateway is 1.25 Gbps.

https://docs.megaport.com/cloud/megaport/cloud-native-vpn-encryption/

https://aws.amazon.com/blogs/networking-and-content-delivery/scaling-vpn-throughput-using-aws-transit-gateway/

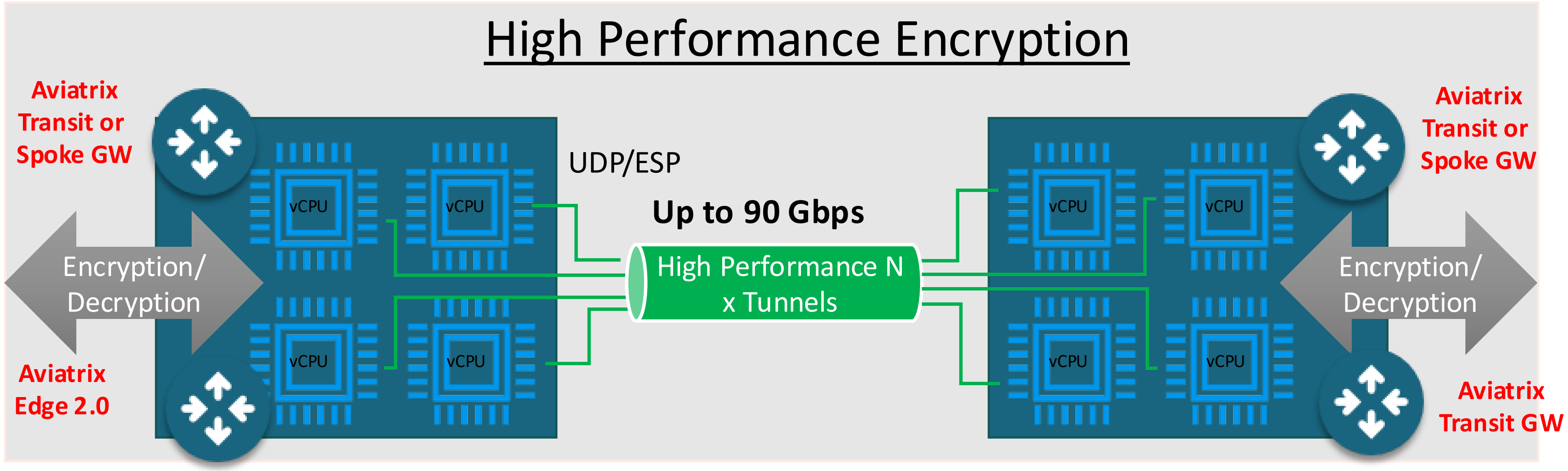
Without Aviatrix: Encryption / IPsec Performance Limitations

- All software-based IPsec VPN solutions have maximum performance of 2Gbps depending on ciphers used
- Software Routers use single core and establish only one tunnel
- Packet can only use single core despite availability of multiple cores



Solution: Aviatrix High Performance Encryption (HPE)

- Aviatrix Controller automatically builds multiple tunnels between Aviatrix devices
- Uses all available CPU cores
- IPsec encryption performance can be up to 90 Gbps



High Performance Encryption
Aviatrix Transit or Spoke GW
Aviatrix Edge 2.0
Encryption/ Decryption
vCPU
UDP/ESP
Up to 90 Gbps
High Performance N x Tunnels
Aviatrix Transit or Spoke GW
Aviatrix Transit GW
Encryption/ Decryption

High Performance Encryption used to be called **INSANE MODE**

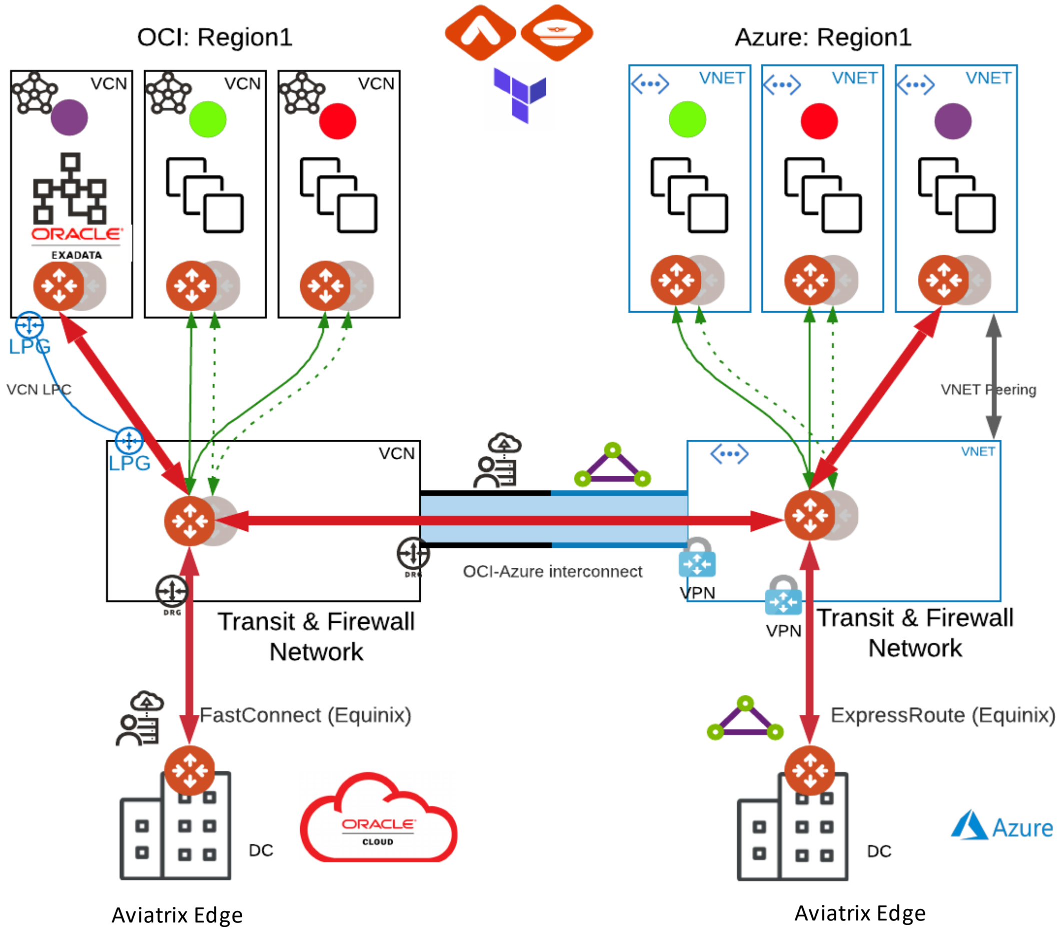
Instance sizes that support High Performance Encryption

Cloud Provider	Instance SIZES that suppoort HPE
AWS	t3 (spoke), t3a (spoke), c5 (spoke and transit), c5n (spoke and transit), c6in (spoke and transit)
Azure	Standard (except for B1ms, B2s, B4ms, B8ms, D1_v2, D2_v2, DS1_v2, DS2_v2, D2s_v3, D4s_v3, F2s_v2, F4s_v2)
GCP	n1-standard (except for standard-1 and standard-2), n1-highcpu (except for highcpu-2)
OCI	All instance sizes

- *Caveat:* the number of tunnels that are created depends on the gateway instance size.

High Performance Encryption (HPE)

1. Between the Cloud (over DirectConnect, ExpressRoute, FastConnect, Cloud Interconnect) to the DC via:
   - Aviatrix **Edge**
2. Between networks in one cloud (same or different regions)
   - Automatic VPC/VNet/VCN peering to build required underlay
3. Between networks in different clouds
   - Requires private underlay (e.g., Equinix, Epsilon, Megaport, OCI-Azure Interconnect)
   - Over Public Internet (v6.4)



Aviatrix Edge will be discussed in Site2Cloud module

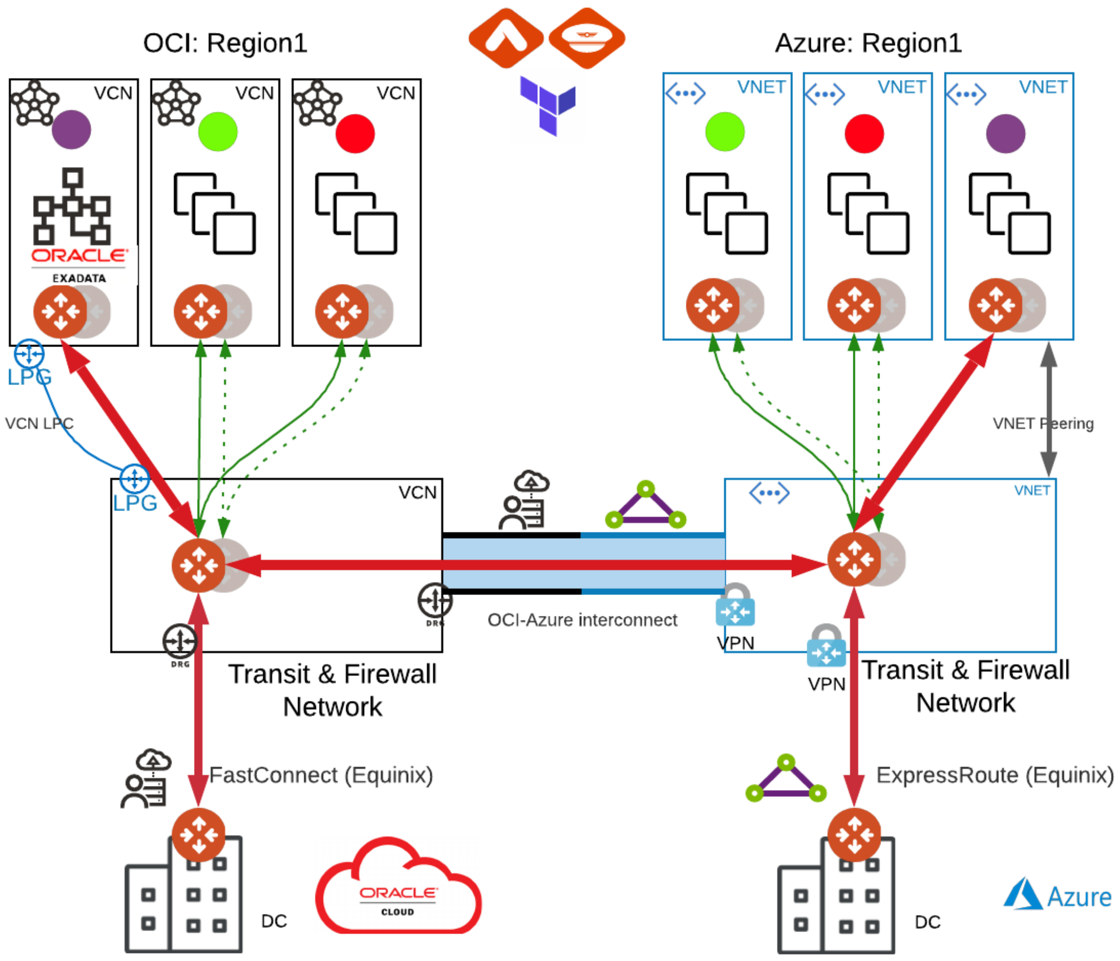
HPE Peering – Public or Private IP?

- **HPE in the same cloud**
  - Will use *CSP-native peering* so the tunnels will be built over private IPs.

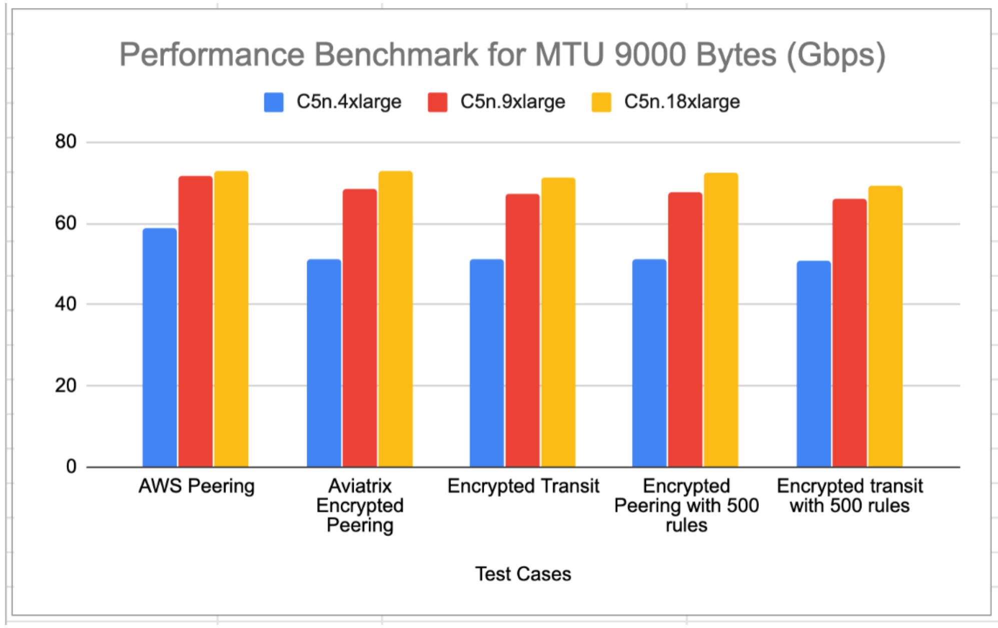
- **HPE across different clouds**
  - Supported over private circuits (Direct Connect, Express Route, Cloud Interconnect, Fast Connect).
  - Supported over internet (AWS, Azure, GCP, OCI).

HPE Performance – Matching the Speed of the Underlay

https://docs.aviatrix.com/HowTos/insane_mode_perf.html

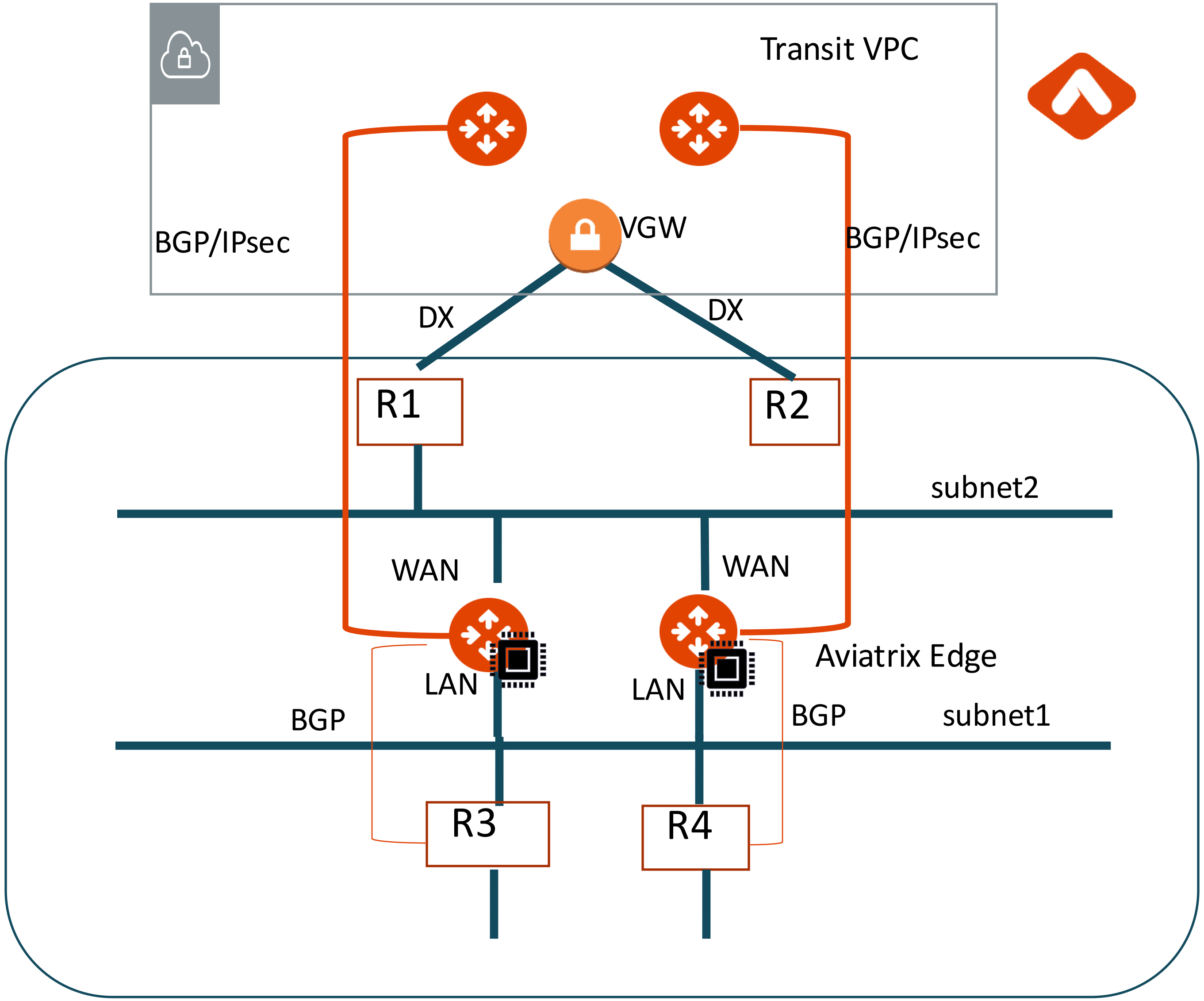


- ~90 Gbps in-region in AWS
  - 9000 MTU supported
- Line-Rate (~9.6 Gbps) over single 10 Gbps Direct Connect or ExpressRoute



Architecture over Direct Connect and Other Private Circuits

https://docs.aviatrix.com/HowTos/CloudN_insane_mode.html



© Aviatrix Certified Engineer

Next: ActiveMesh