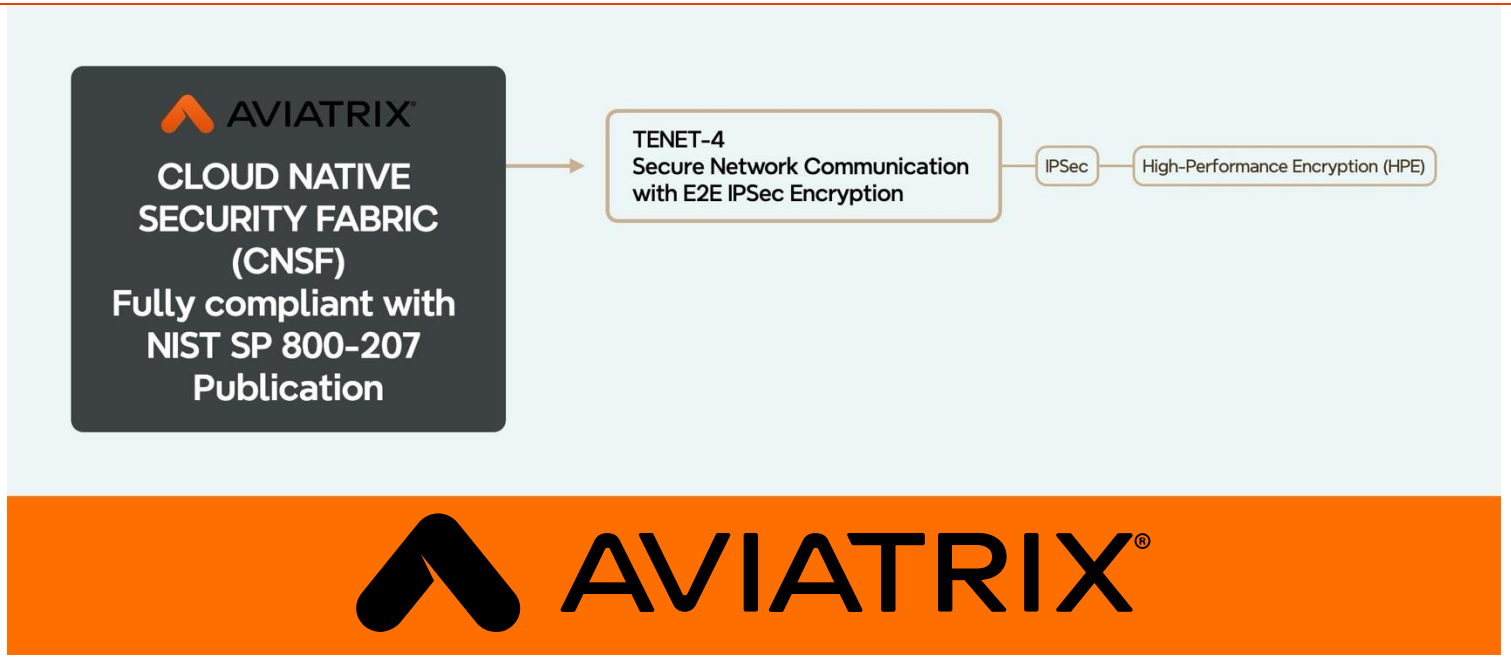
Tenet-4: Secure Network Communication with E2E IPSec Encryption

Security and Operational Visibility

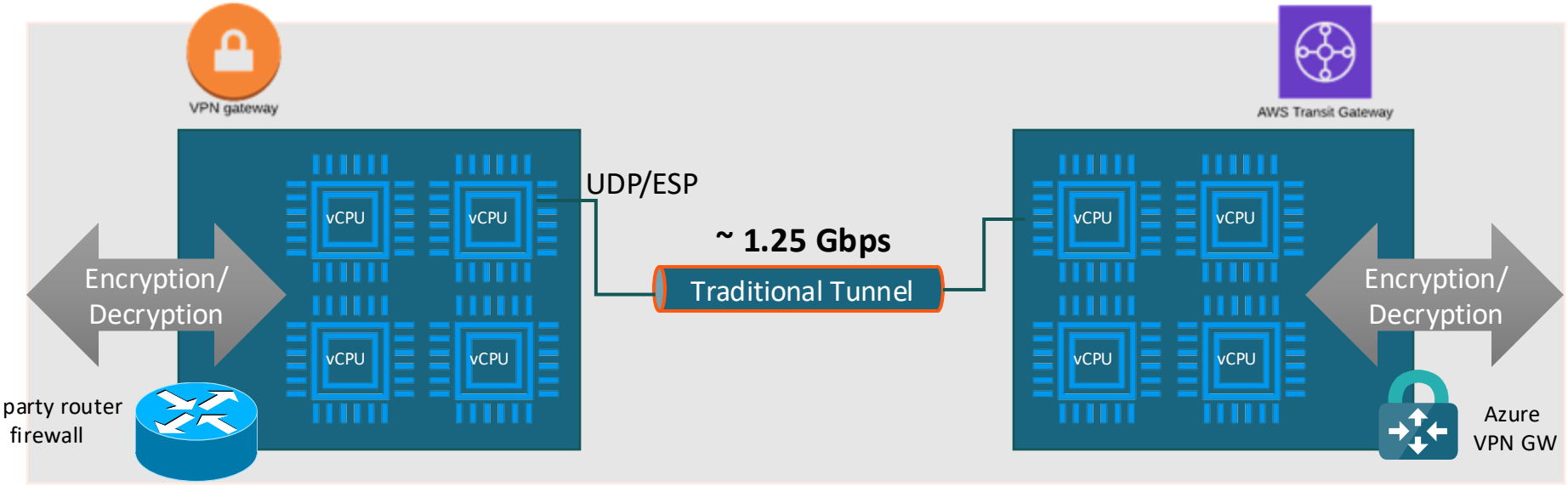
Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

All communication is secured regardless of network location. Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other nonenterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.



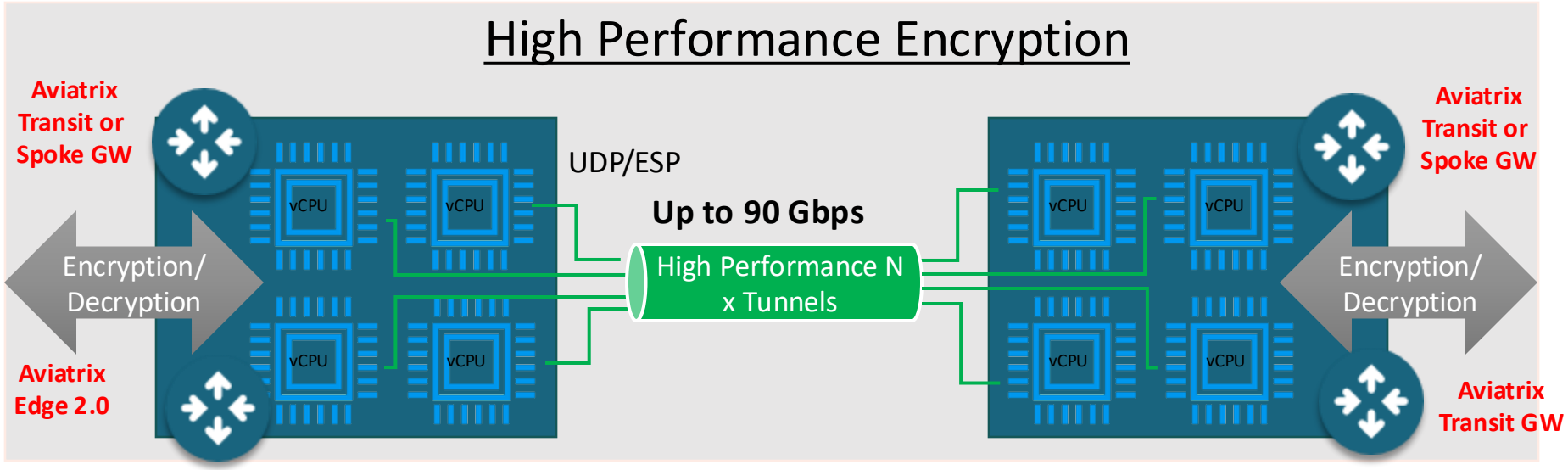
Without Aviatrix: Encryption / IPsec Performance Limitations

- 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 used to be called **INSANE MODE**

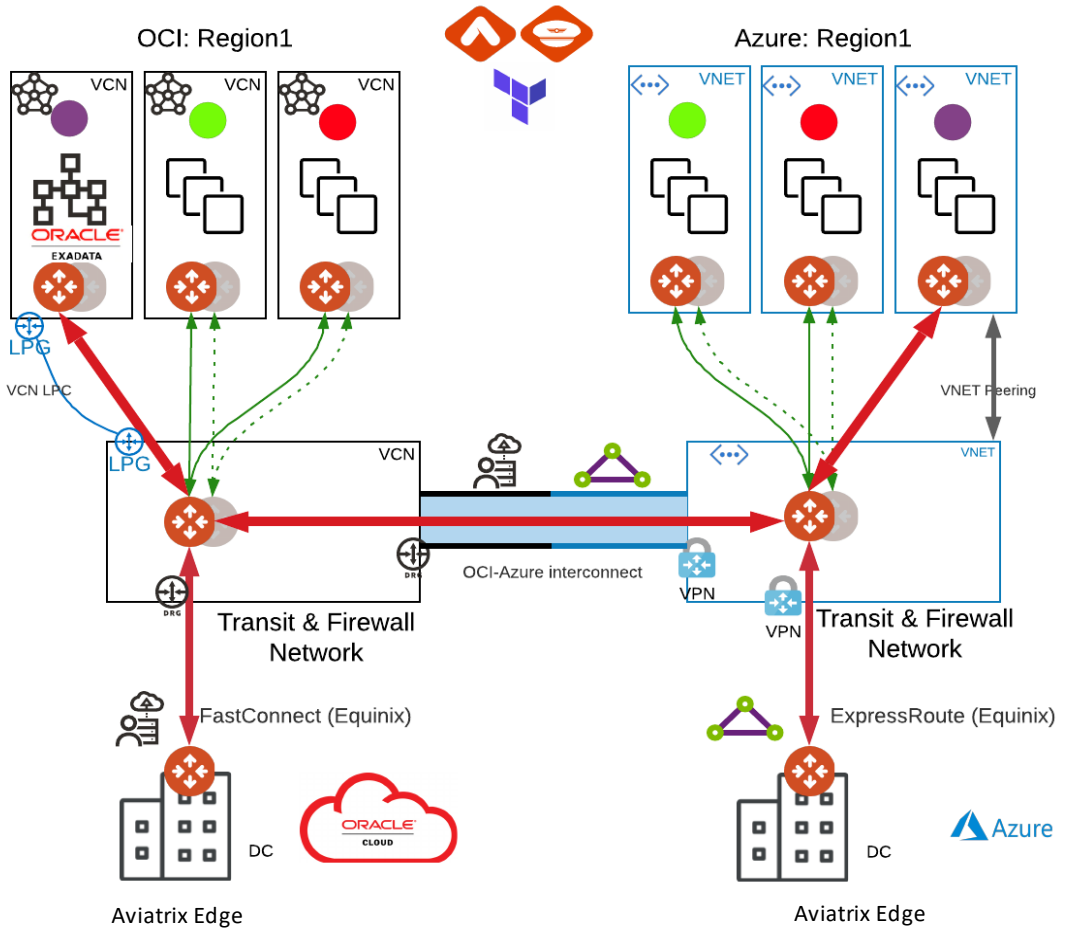
Instance sizes that support High Performance Encryption

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

Next: Tenet-5 Operational and Security Visibility