Network Topology and Connectivity

Azure Foundation Architecture and Hybrid Integration Strategy

Purpose: The next sections provide design considerations based on best practices, Microsoft CAF and Accenture team accumulated experiences implementing Azure network architectures. Additionally, the sections addressing design decisions is based on **ongoing discovery** with Accenture and NewCo team members.

Assumptions

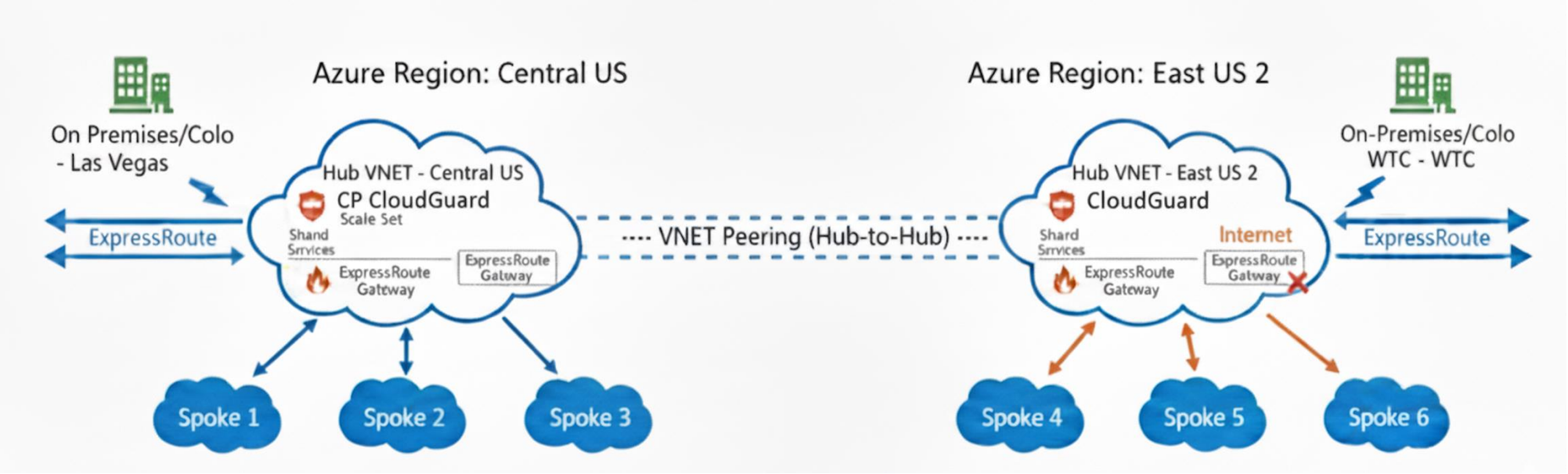
- Prioritizing security from the ground up, no "isolated pockets" of networking without central security.
- Hub NVA firewalls act as the route engine, managing traffic flow and inspection for all intra-Azure and hybrid network traffic
- NewCo Azure environment will be a "greenfield" deployment
- NewCo Azure cloud will be integrated with on-prem network consisting of a shared MPLS and SD-WAN environment that connects all their physical locations back to their data centers.

Azure Network Topology Strategy

Options: Hub-Spoke Architecture vs Azure vWAN

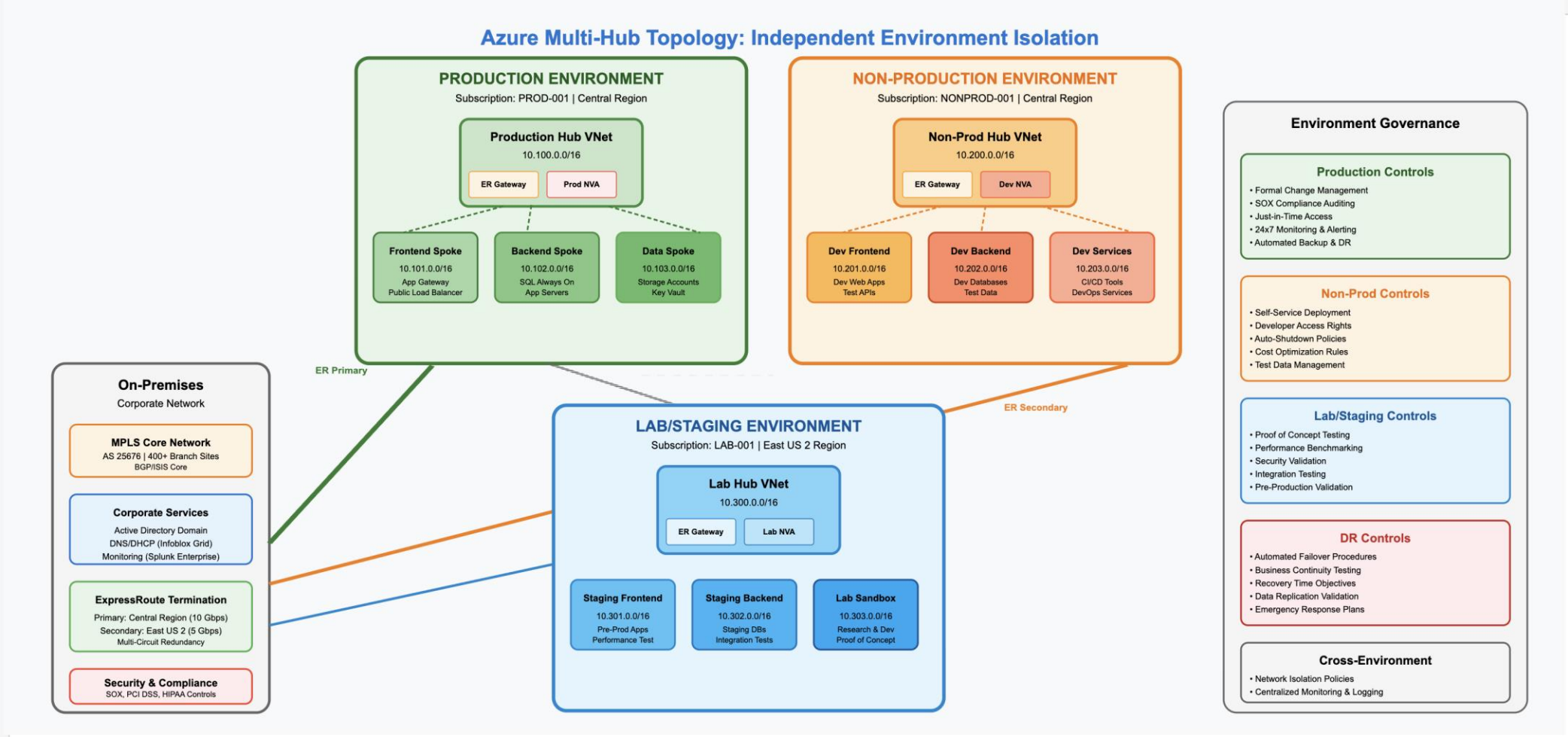
- **Traditional Hub-Spoke** (**recommendation**)
  Unmanaged topology with complete control and proven security patterns
- **Azure vWAN**: Managed service with built-in routing, but less gra

Traditional Hub-Spoke Diagram



Azure Network Topology Strategy

Production and Non-Production Environments Separation



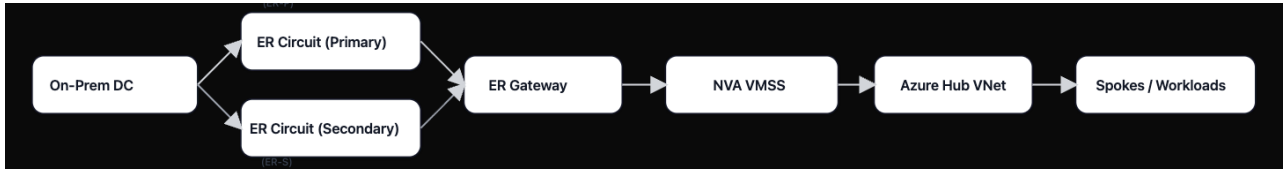
Environments

- Production
- Non-Production
- Lab/Staging

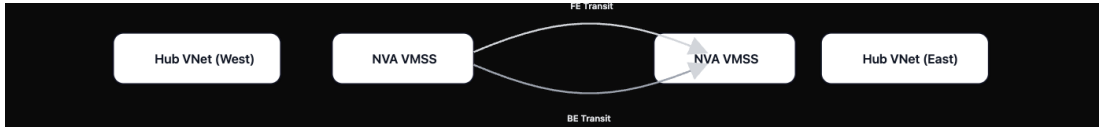
Connectivity Architecture

Network Traffic Flows for Consideration

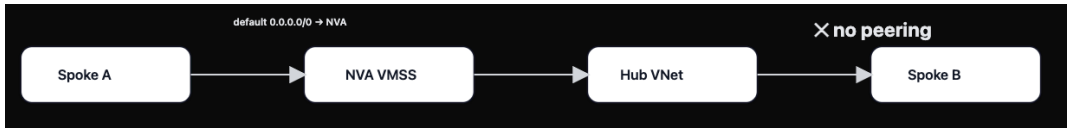
- On-Premises to Azure Hub (regional ExpressRoute Primary and Secondary)



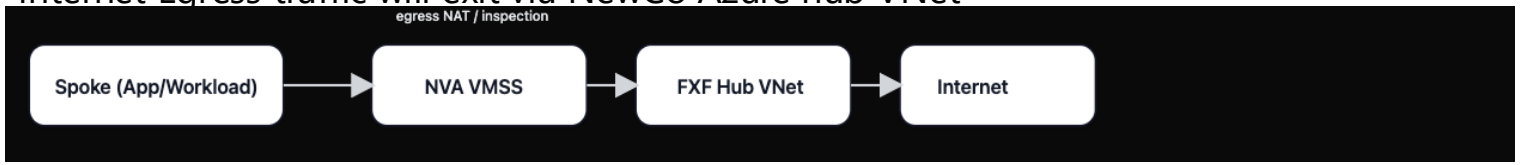
- Hub to Hub inter-region connectivity will use FE and BE transit routes via NVAs between hub vnets



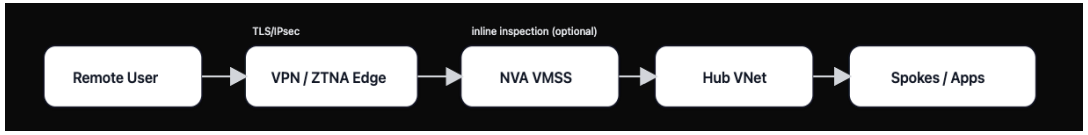
- Spoke to Hub to Spoke connectivity will use default route to NVA (no direct spoke to spoke peering)



- Internet Egress traffic will exit via NewCo Azure hub VNet



- Remote Access



Connectivity Subscription

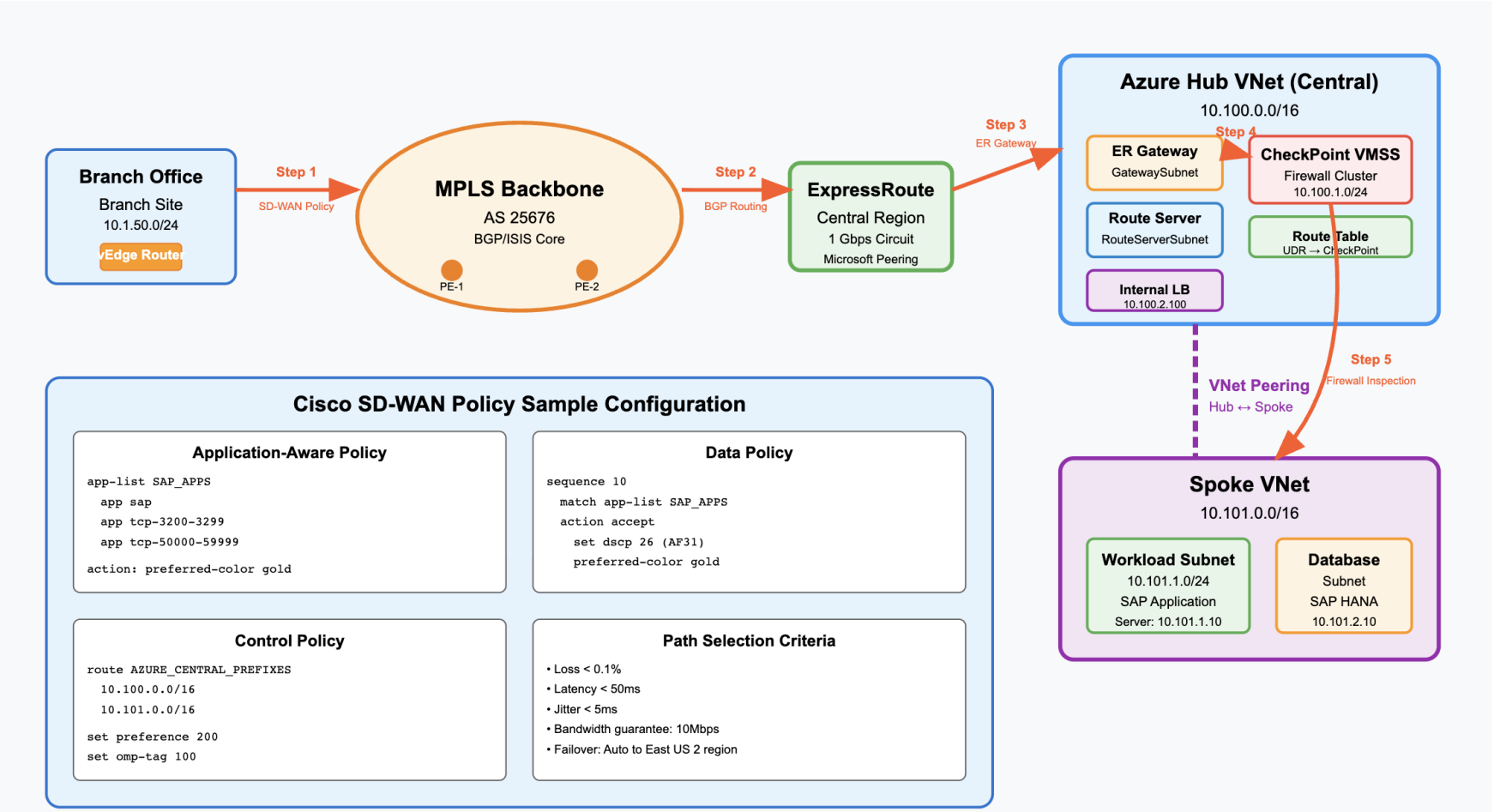
Key Architectural Core Elements

Design Decisions

- Core Infrastructure Subscription - Contains hub vnets, ExpressRoute, CP firewalls, and shared network services
- Hub Subnets: Gateway, Firewall, DNS, Bastion
- Regional Strategy: Dual-region support with Central US primary and East US 2 secondary
- Security Controls: All traffic through hub firewalls, private IP enforcement
- Management Structure: Dedicated management group for core infrastructure
- Workload Subscriptions - Contains application spoke VNets with peering to hubs

Interconnect Architecture

Branch (Edge) to Azure Traffic Flow via ExpressRoute Hub with NVA Inspection



- Branch traffic flows through MPLS backbone (AS 25676) using policies (future state) for routing and path optimization
- ECX ExpressRoute provides dedicated connectivity from MPLS to Azure Hub for inspection
- Hub-and-spoke architecture routes traffic from Azure Central Hub to Spoke VNet workloads

Interconnect Architecture

Key Architectural Core Elements

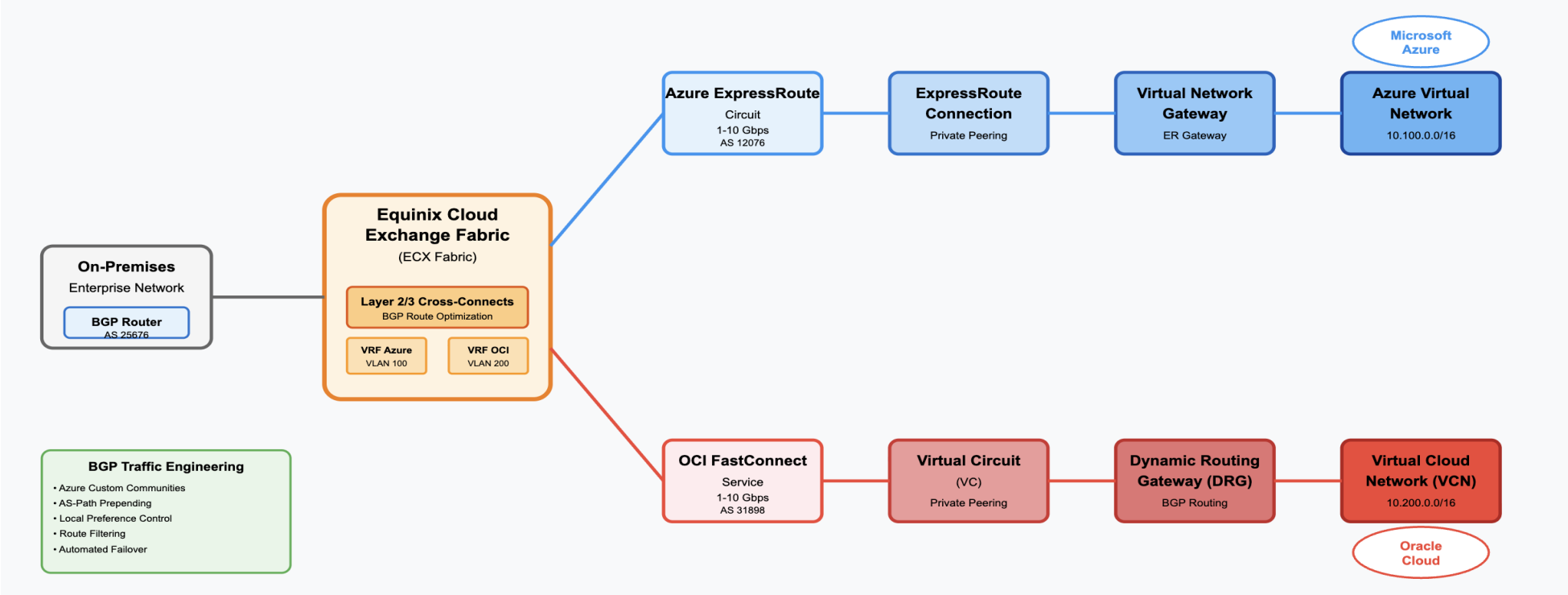
Design Decisions

- ECX serves as primary interconnect leveraging Cloud Exchange for Azure ExpressRoute circuit
- Physical Circuit Isolation/Diversity: engineer dual ExpressRoute circuits with physical geographical diversity Equinix facilities) into MSEE points of presence (POPs)
- Implement a bow-tie topology by cross-connecting dual Azure Express Route circuits from distinct MSEE regions to Azure transit domain, each circuit can reach either hub. Support a FE and BE VNets between hub regions with NVA inspection in path
- VRF-Based Routing: Ingress traffic from SD-WAN managed MPLS core is routed into Azure via a dedicated VRF instance for traffic isolation / separation
- Subnet-Specific Matching: The ingress path is configuration match traffic destined for subnet x.x.x.x, for control, allowing SD-WAN to direct traffic flow towards Azure.
- SD-WAN Azure Labels for Policy Enforcement: A label is applied to the traffic entering Azure cloud policy enforcement.

Interconnect Architecture

Multi-Cloud Interconnect Considerations

- Private interconnect via Equinix Fabric: ECX/Fabric L2 (802.1q) platform for private connect to Azure Express Route and OCI Fast Connect (and other clouds)
- Separate VRFs per cloud (prod/dev) environments distinct virtual circuits; route leaking can happen at NVA
- Azure BGP custom communities provide Azure specific routing intelligence; target specific Azure regions

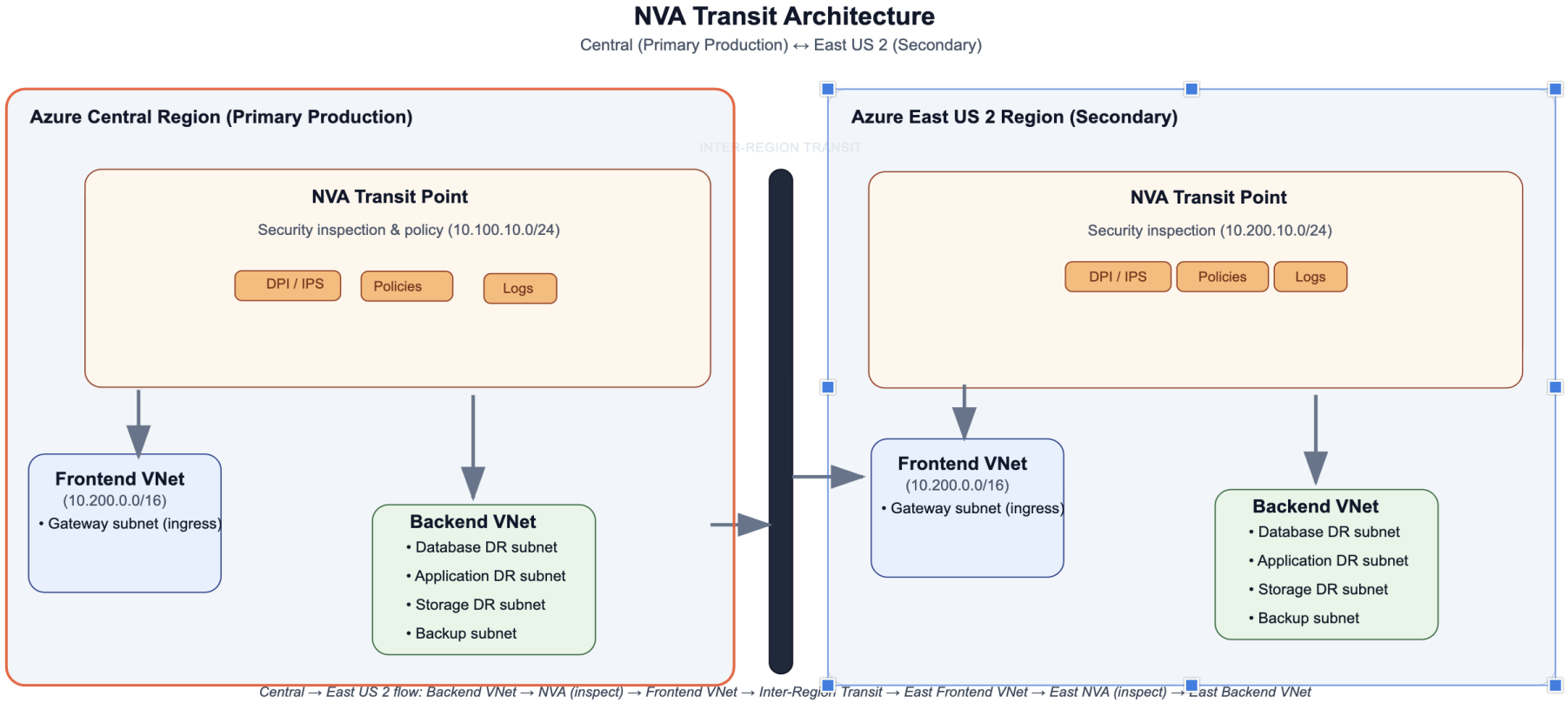


NVA Strategy
Design Recommendations

Checkpoint NVA VMSS

FortiGate NVA VMSS

NVA Strategy



Use Cases

- Database Replication: Always On across regions with security inspection
- Application Failover: Secure failover traffic during disaster scenarios
- Backup & Recovery: Cross-region backup traffic with policy enforcement
- Data Synchronization: Secure sync of critical business data
- Compliance Logging: All inter-region traffic inspected and logged

NVA Security Functions

- Traffic Inspection: Deep packet inspection for all inter-region flows
- Policy Enforcement: Consistent security policies across regions
- Threat Prevention: IPS, malware detection, data exfiltration prevention
- Compliance Logging: Audit trails for regulatory requirements
- Bandwidth Control: QoS and rate limiting for different traffic types

All region-to-region traffic passes through centralized NVA checkpoints; design favors HA, security, and DR readiness.

Check Point VMSS for scalable, security, policy management.

- VMSS in hub VNets auto-scaling based on traffic demand
- Azure Firewall NOT considered due BGP peering functionality

OR

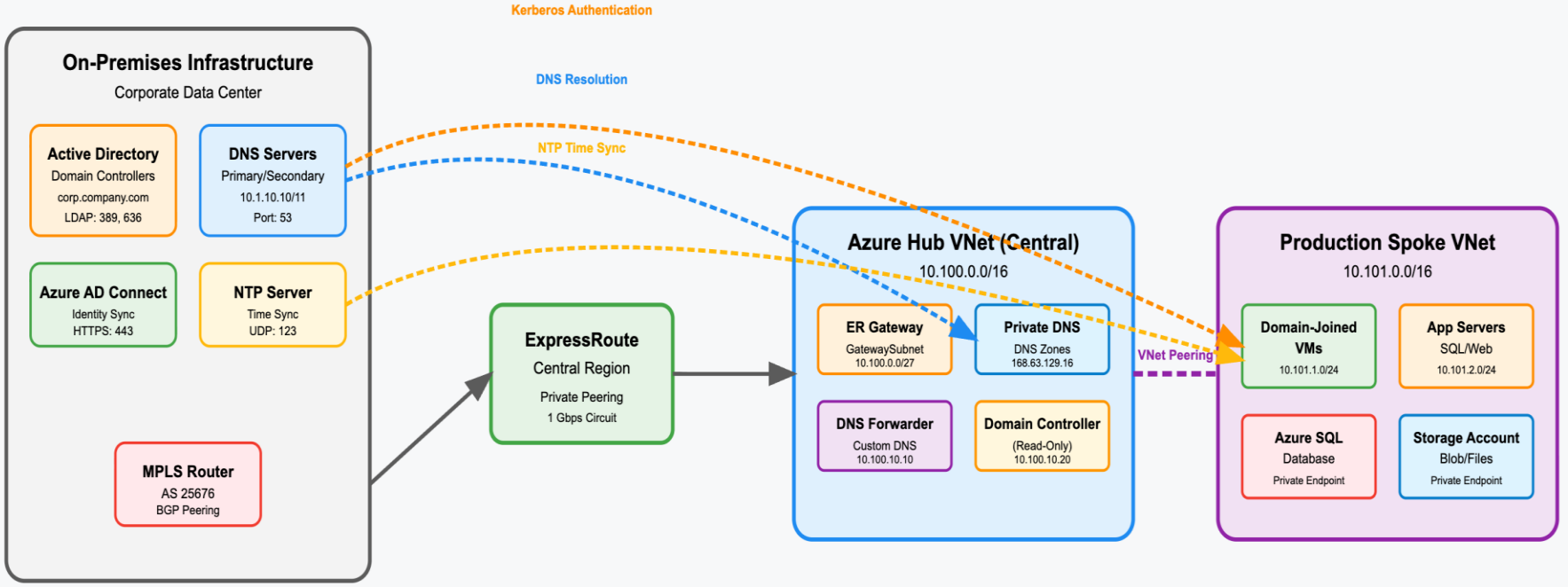
FortiGate VMSS

- Works with Cisco SD-WAN policies, Zscaler native integration for L7
- Terraform, REST API and Ansible modules enable IaC deployments
- eBGP peering with Azure Route Server route exchange between on-prem MPLS core(s)
- VMSS scaling based on metrics (CPU, memory, session count, etc)

Alternate Option

Azure DNS Services

Design Considerations



- Deploy DNS forwarder VMs in Hub VNet, configure conditional forwarding to on-premises
- Azure private DNS zones to all VNets

Internet Egress

Design Considerations

Option 1: Internet Egress via NewCo Azure Cloud (Recommended)

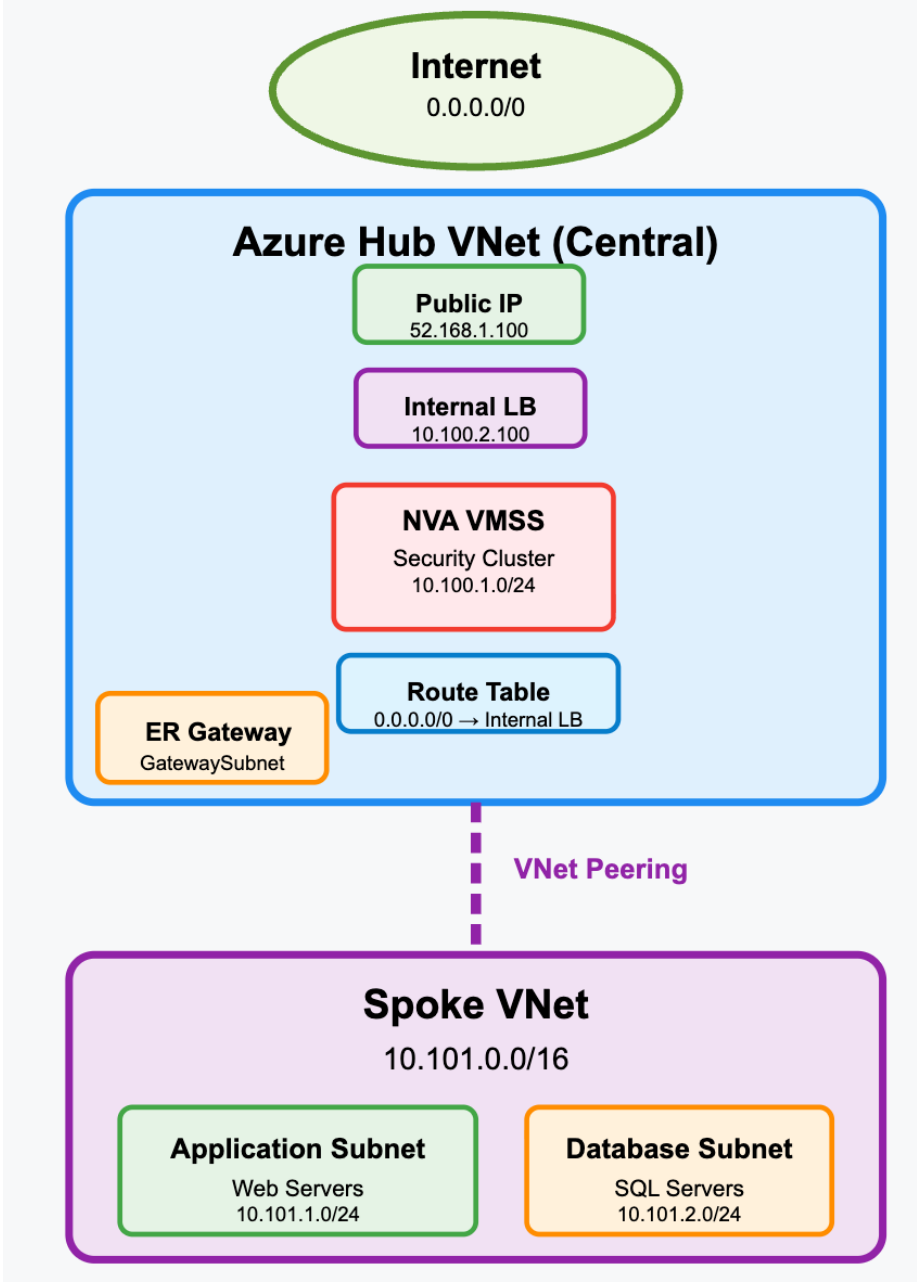
- This solution provides immediate access to established security policies, threat intelligence, and logging (via NVA) deployed in Azure

Option 2: Internet Egress via NewCo SDWAN DIA:

- This solution provides access to established security policies, threat intelligence, and centralized logging infrastructure deployed on-prem with SD-WAN control

Option 3: NewCo Internet Egress via Existing OldCo DIA

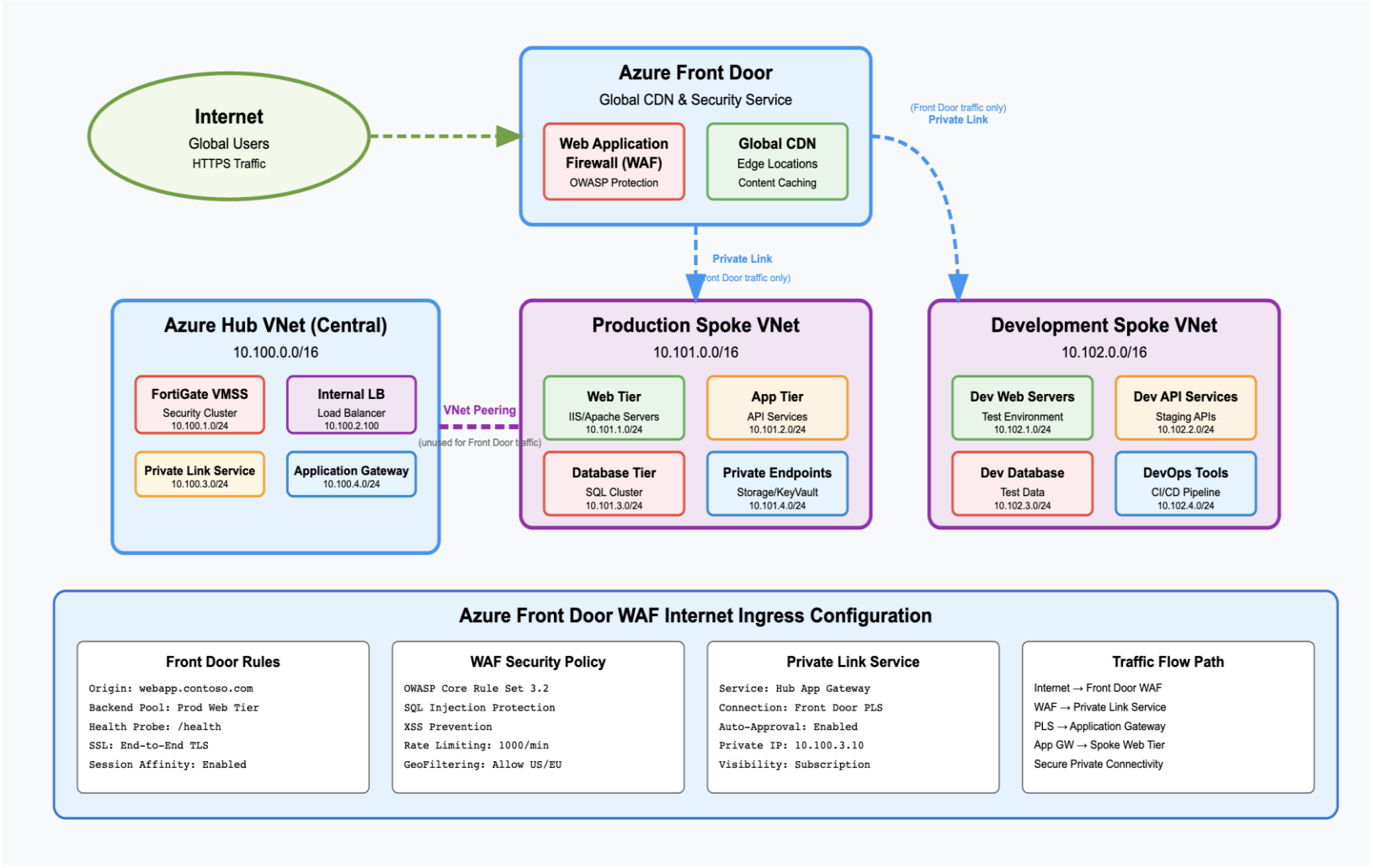
- NewCo workloads leverages existing NewCo Azure tenant internet egress points (Azure OldCo) for outbound connectivity rather than establishing dedicated internet breakouts



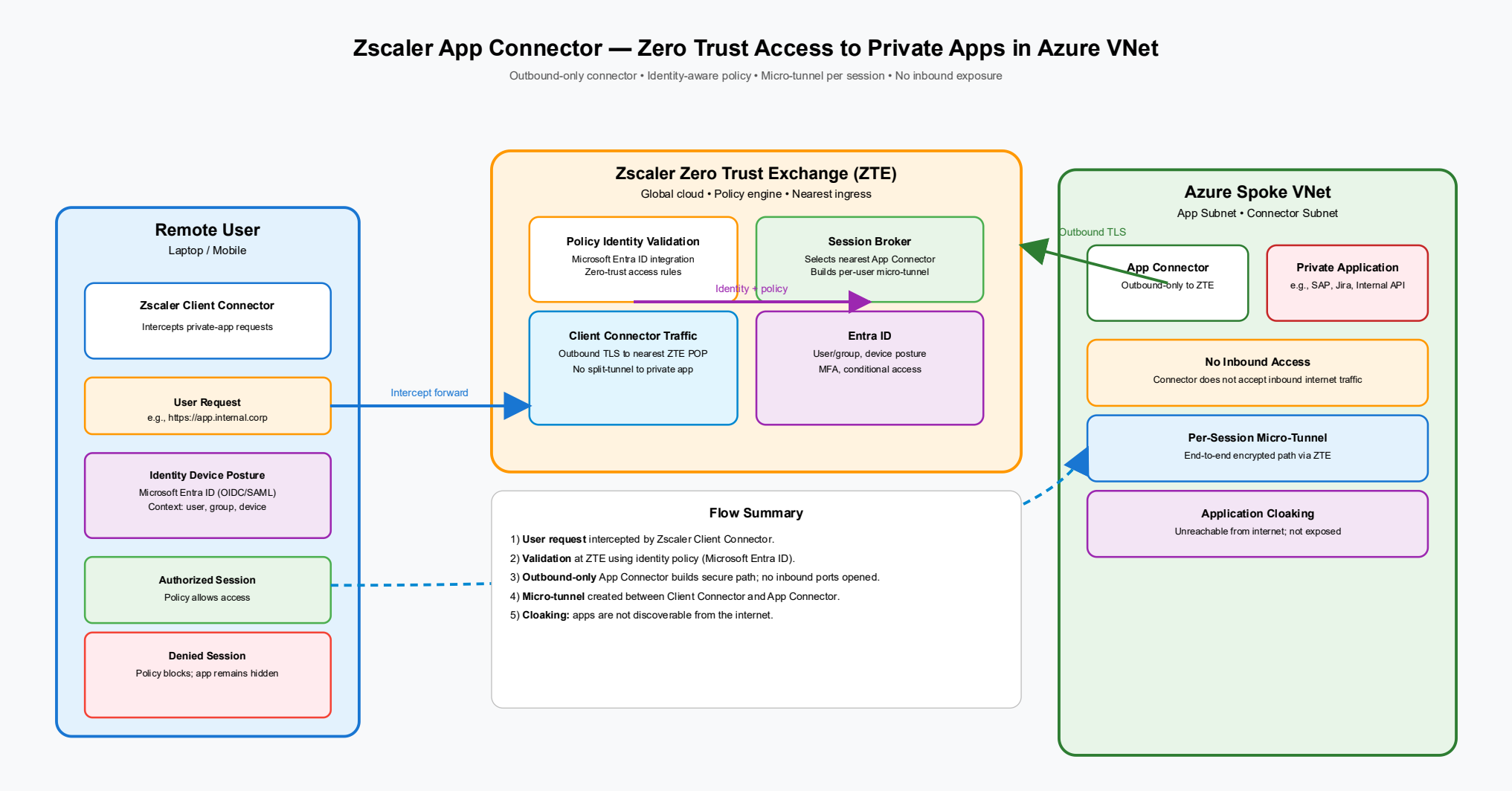
Internet Ingress Strategy (Post-TSA)

Design Considerations

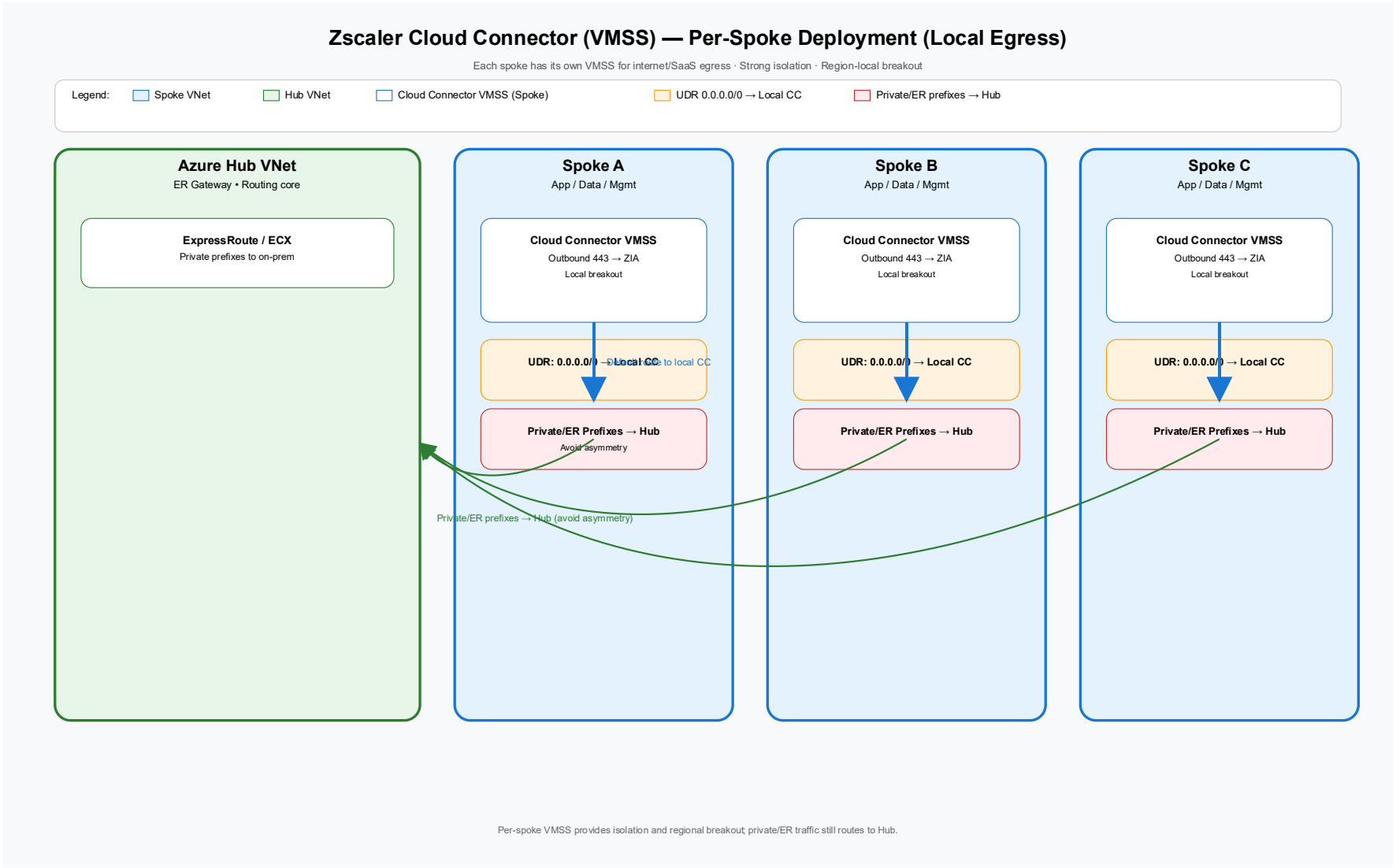
- Azure Front Door with Private Link (PL) and spoke LB
- No hub transit for Internet ingress or hair-pinning through NVAs
- Security at the edge using WAF
- Traffic uses Microsoft backbone
- Anycast edges for availability and failover.



Remote Access

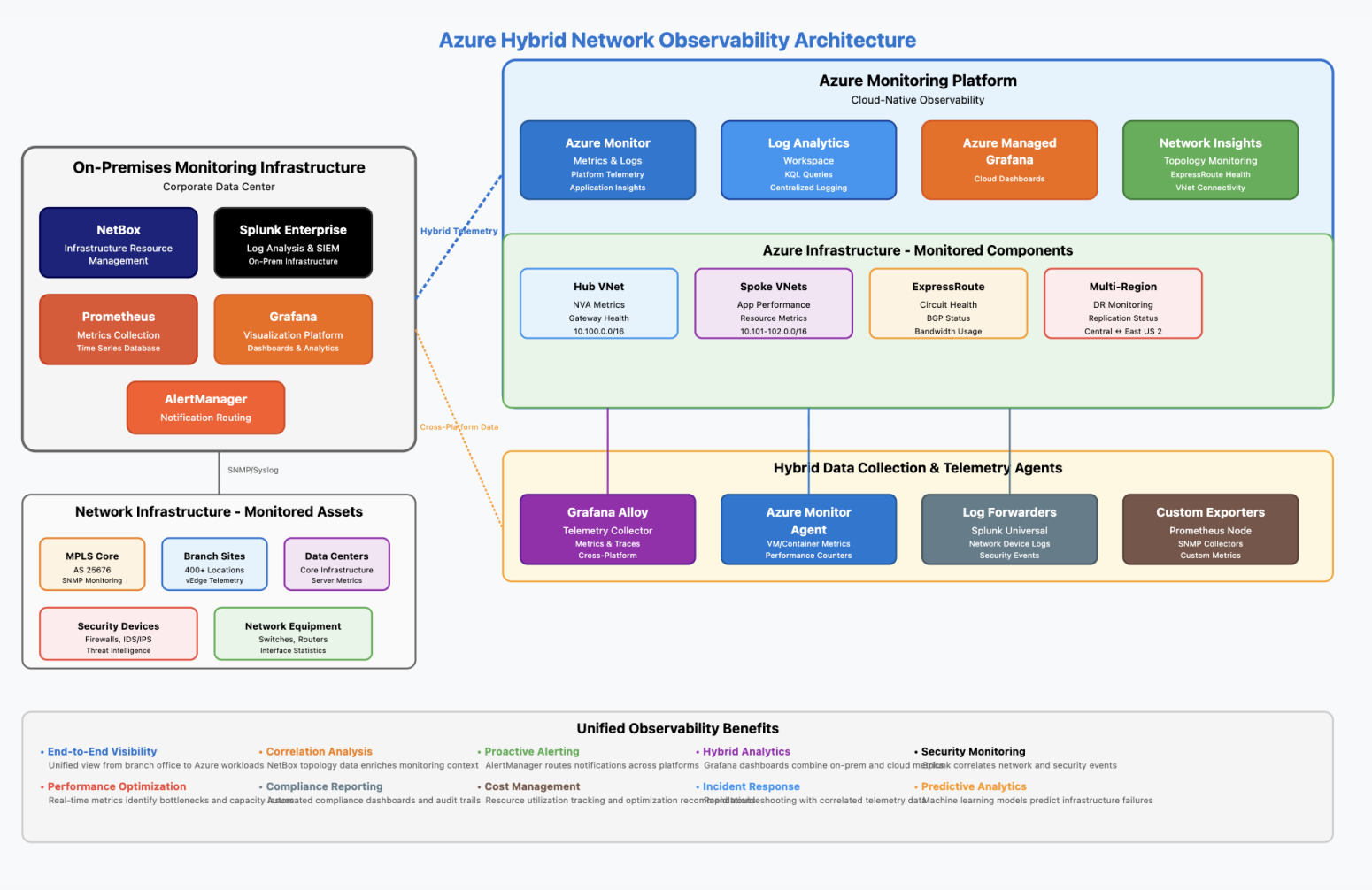


Remote Access



Observability and Monitoring

Core Elements



Option 1: Hybrid Extension of On-Premises Solution

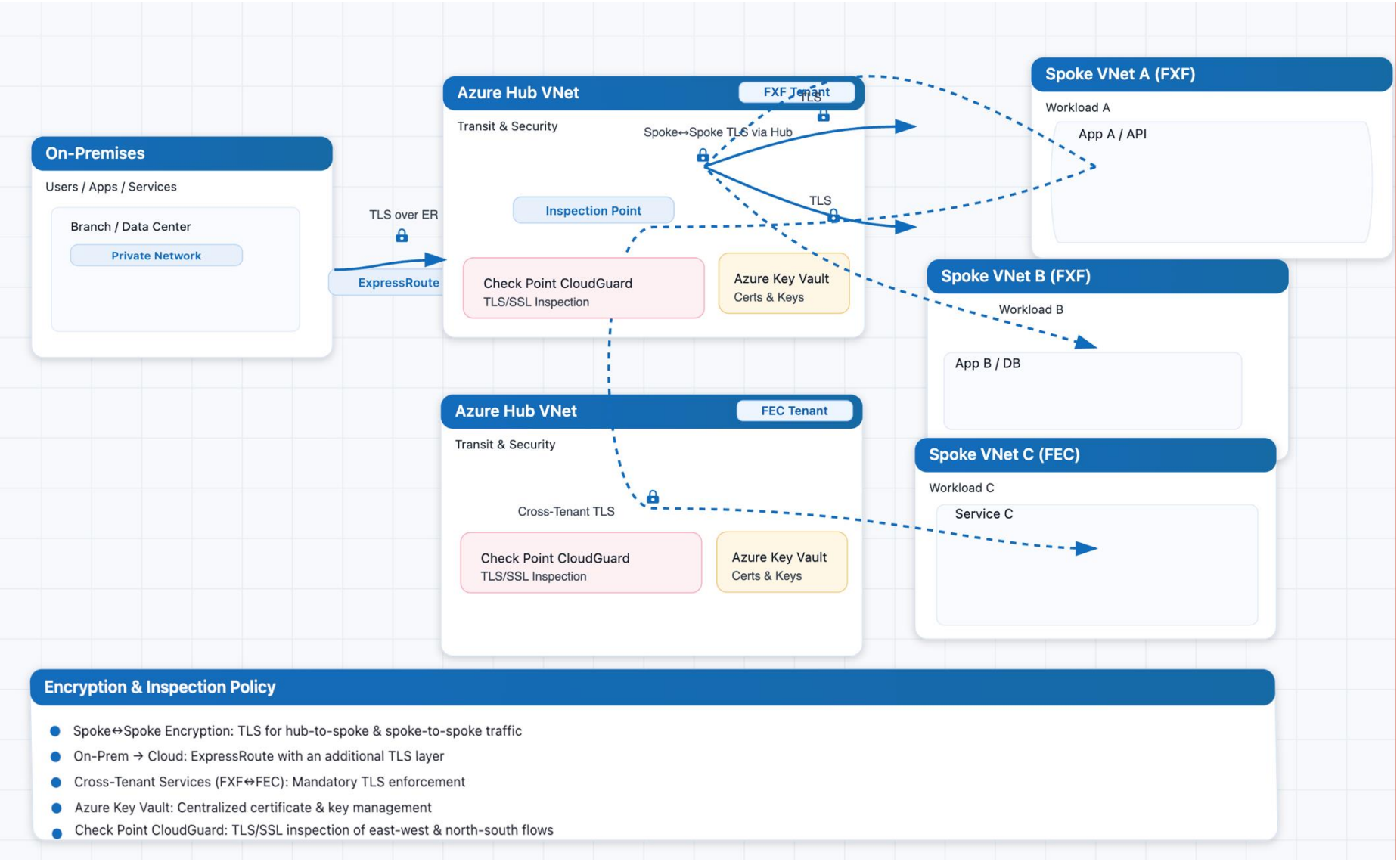
- Federated Monitoring with the existing monitoring stack: Extend current Prometheus/Grafana/Splunk infrastructure to Azure through Azure Monitor integration and Prometheus federation to exporter/collectors *Azure*

Option 2: Azure-Native Observability with Hybrid Integration

- Implement Azure Monitor, Log Analytics, and Application Insights platform for all Azure resources with data federation to on-premises Splunk/Prometheus.
- This design consideration utilizes native Azure capabilities, automated scaling insights, and integration while implementing custom logic apps and Azure Functions to replicate critical metrics to existing Prometheus instances

Network Encryption

Core Elements



- **Spoke to Spoke Encryption** - TLS for hub-to-spoke and spoke-to-spoke traffic
- **On-Premises to Cloud Encryption** - ExpressRoute with additional TLS layer
- **Cross-Tenant Security Enforcement** - Mandatory encryption for NewCo/OldCo tenant services
- **Azure Key Vault** - Centralized management
- **Check Point** performs TLS/SSL inspection

Network Segregation Strategy

Core Elements

Network Segmentation Strategy	Implementation Details
Hub-Spoke Isolation with Centralized Security	All spoke vnets connected to hub through vnet peering with User-Defined Routes (UDRs) forcing traffic through Check Point CloudGuard VMSS firewalls for inspection, logging, and policy enforcement before reaching destinations
Zero Trust Spoke-to-Spoke Communication	Direct spoke-to-spoke connectivity prohibited through disabled gateway route propagation and explicit firewall rules required for any inter-spoke communication, ensuring complete traffic visibility and granular access control
Environment-Based Network Boundaries	Production and non-production environments maintained in separate hub vnets with dedicated ExpressRoute circuits and firewall instances, preventing cross-environment traffic except through approved firewall policies with comprehensive audit logging
Private IP Enforcement and Public Access Control	Azure Policy prohibits public IP creation on resources with all internet egress routed through hub firewalls via 0.0.0.0/0 UDR configurations, while internet ingress limited to specific application spokes through Azure Front Door with WAF integration

Questions and Feedback

Next Steps

NetBox

Design Considerations

Recommendation

Multi-Cloud Visibility

- For unified Azure / Oracle / On-Prem documentation
- Future state, business goals modeling and capacity planning.
- Model relationships across Azure subscriptions and management groups
- Single view of clouds ER/FC circuits and Equinix cross-connects. Right size circuits
- DNS modeling for on-prem and Azure cloud resolution chains

Observability Strategy

NetBox

- Topology aware
- Dynamic network Monitoring

Azure Network Topology Strategy

Core Elements

Appendix

Network Architecture Foundation

- Traditional Hub and Spoke: Selected over Azure vWAN for complete control
- Dual Regional Design: Central US (primary) and East US 2 (secondary)
- VRF Segmentation: Azure as distinct VRF for routing isolation
- Zero Trust Design: Security-first architecture from day one

Security Architecture

- Check Point CloudGuard VMSS: Auto-scaling firewall clusters
- Private IP Enforcement: Azure Policy prohibits public IPs
- TLS 1.3 Encryption: All traffic flows encrypted in transit
- Centralized Inspection: All traffic through hub firewalls

Management Structure

- Core Infrastructure Subscription: Hub VNets and shared services
- Workload Subscriptions: Application spoke VNets
- Management Groups: Core Infra, Production, Non-Production
- Policy Enforcement: Automated governance and compliance

Connectivity Infrastructure

- Equinix Cloud Exchange: Primary interconnect for ExpressRoute and OCI
- Dual ExpressRoute: Physical diversity with bow-tie topology
- Cisco SD-WAN Integration: Catalyst overlay with 8000V edge devices
- Site-to-Site VPN: Backup connectivity for resilience

Automation Deployment

- Infrastructure as Code: Terraform primary, Bicep/ARM as alternatives
- Pipeline Deployment: Automated CI/CD with gates and approvals
- Subscription Vending: Standardized provisioning workflows
- Policy as Code: Governance automation and drift prevention

Observability Strategy

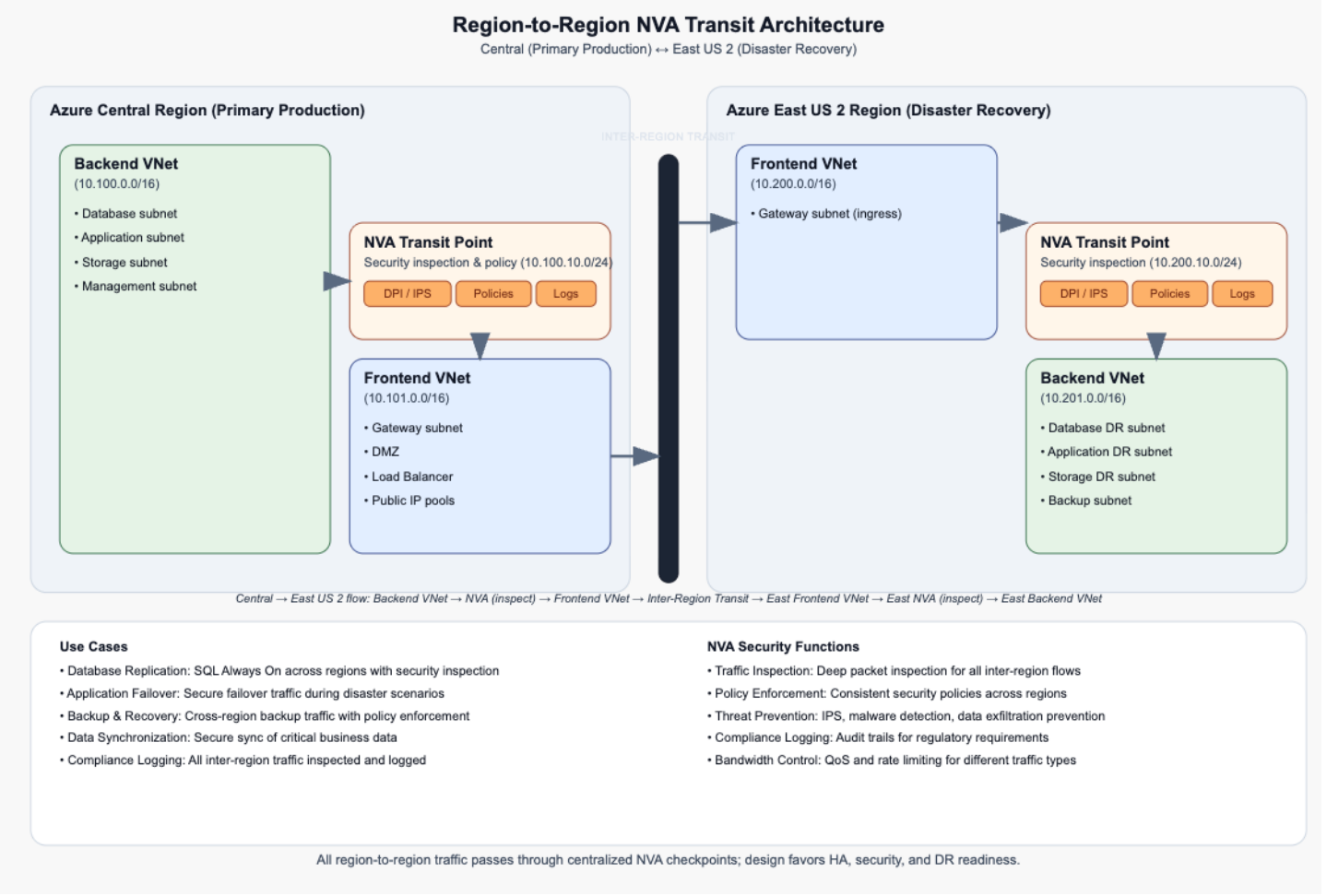
- Hybrid Monitoring: Extend Prometheus/Grafana or Azure-native
- Log Analytics Consolidation: Reduce from 17 to fewer workspaces
- Network Watcher: Azure-native network monitoring
- SIEM Integration: Existing Splunk or Azure Sentinel options

Region to Region Architecture Strategy

Design Considerations

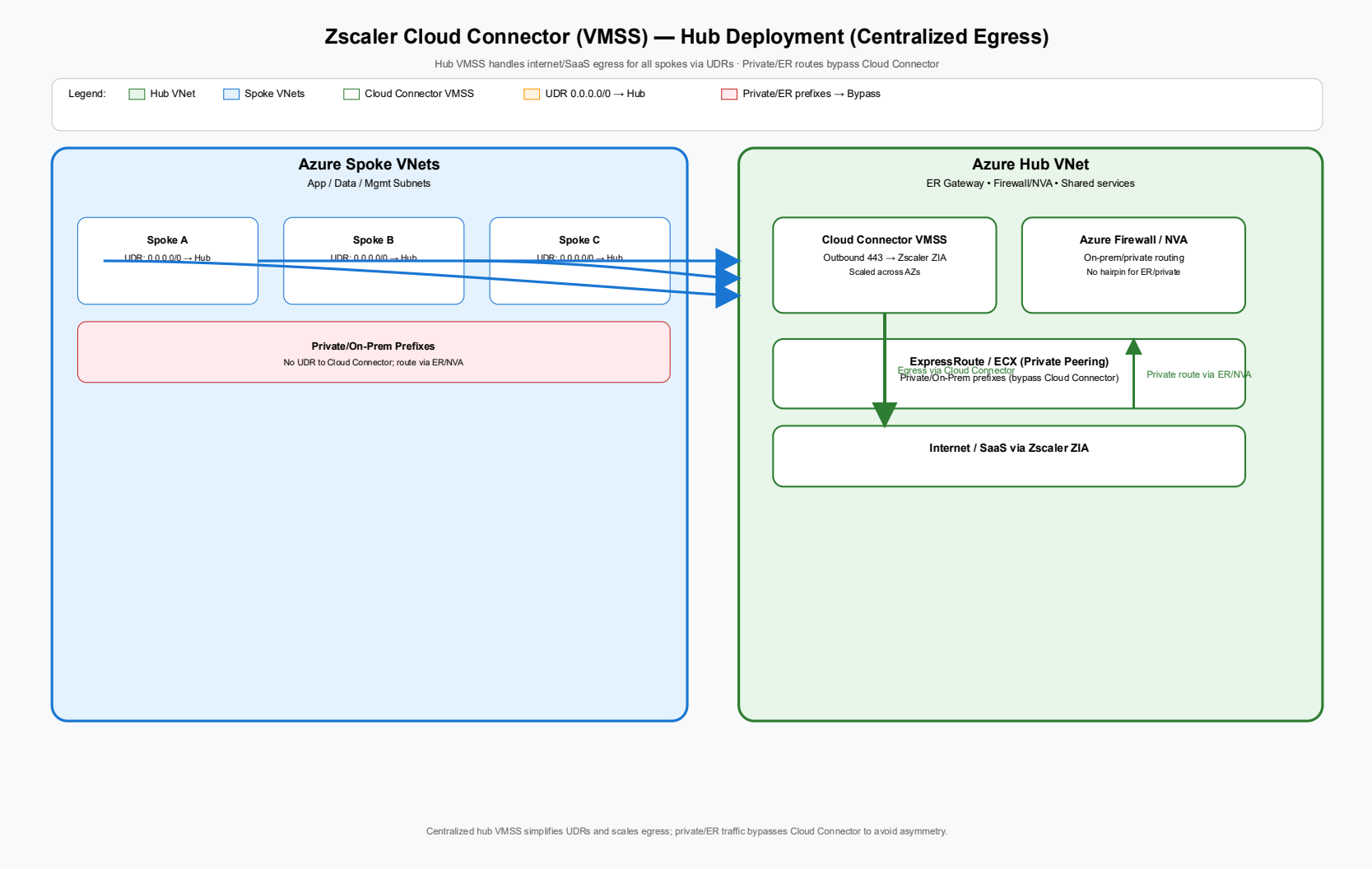
Recommendations are based on compilation of NIST (SP 800-207) and CAF guidelines

- NVAs are security transit points to/from both regions with inspection at ingress and egress FE and BE vnet peering
- Aligns with NIST zero trust model for continuous resource identification and CAF workloads using identity, policy, security controls
- Central boundary security and segmentation with policies, monitor and control communications at external/internal boundaries, enforce approved info flows
- FE can failover (no BE impact), replication can be send over single vnet instead so not impact day to day prod workloads
- Internet traffic only on FE vnet



Remote Access

ZScaler Hub VNet Deployment



IP Addressing and Management

Design Considerations

Option 1: Hybrid IPAM with Gradual Azure Native Transition

- Phased IPAM Migration Strategy: Maintain Infoblox as the authoritative source for all IP allocations during initial Azure deployment as a secondary system for cloud-native subnet management.

Option 2: Azure Native IPAM with Infoblox Integration

- Azure IPAM as Primary with Infoblox Federation: Implement Azure as the primary IP address management platform for all cloud resources while maintaining Infoblox integration for on-premises DNS/DHCP services
- Use API for synchronization. This design decision provides centralized visibility and integrates well with PowerShell/Terraform automation pipelines

- Site to Site VPN (can be used as backup for telco delays)
- Internet Ingress traffic

Hub-and-Spoke Architecture – A traditional Azure topology where a central hub VNet provides shared services (firewalls, gateways) to multiple spoke VNet hosting workloads.
Azure vWAN (Virtual WAN) – Microsoft-managed networking service with simplified routing and connectivity, but less granular control compared to hub-and-spoke.
ExpressRoute – A private, dedicated connection between on-premises infrastructure and Azure, offering predictable latency and reliability compared to internet VPN.
Site-to-Site VPN – Secure IPsec tunnel between on-premises networks and Azure VNets, often used as a backup to ExpressRoute.
Equinix Cloud Exchange (ECX) – Interconnection service used to link Azure ExpressRoute circuits with other clouds or on-premises networks.
SD-WAN (Software-Defined WAN) – Overlay technology that uses software policies to manage connectivity across MPLS, internet, and cloud networks.
Check Point CloudGuard VMSS – Cloud-native firewall solution deployed as a Virtual Machine Scale Set for scalable security enforcement in Azure.
NVA (Network Virtual Appliance) – Virtualized network function (e.g., firewall, router) running in Azure for traffic inspection and routing.
UDR (User-Defined Route) – Custom route table in Azure that forces traffic through a specific path, typically through a firewall.
VRF (Virtual Routing and Forwarding) – Logical routing table segmentation for traffic isolation across multiple tenants or environments.

Zero Trust – Security model that assumes no implicit trust; all traffic must be verified, inspected, and explicitly allowed.
TLS 1.3 – Latest version of Transport Layer Security, ensuring data encryption in transit.
Azure Key Vault – Managed service for secure storage and management of cryptographic keys and certificates.
Observability – End-to-end monitoring strategy using metrics, logs, and traces (e.g., Prometheus, Grafana, Azure Monitor, Log Analytics).
L2 802.1Q - Ethernet standard that adds a small “tag” so multiple isolated networks (VLANs) can share the same physical link.