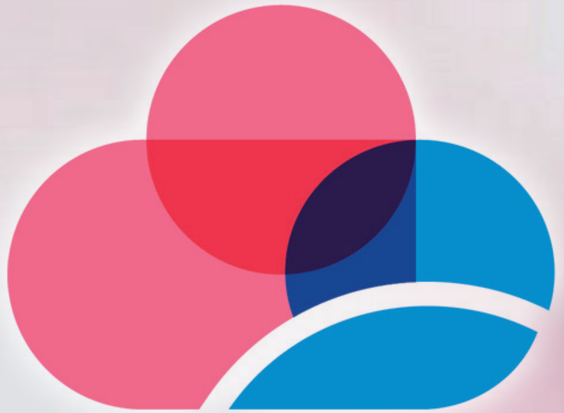
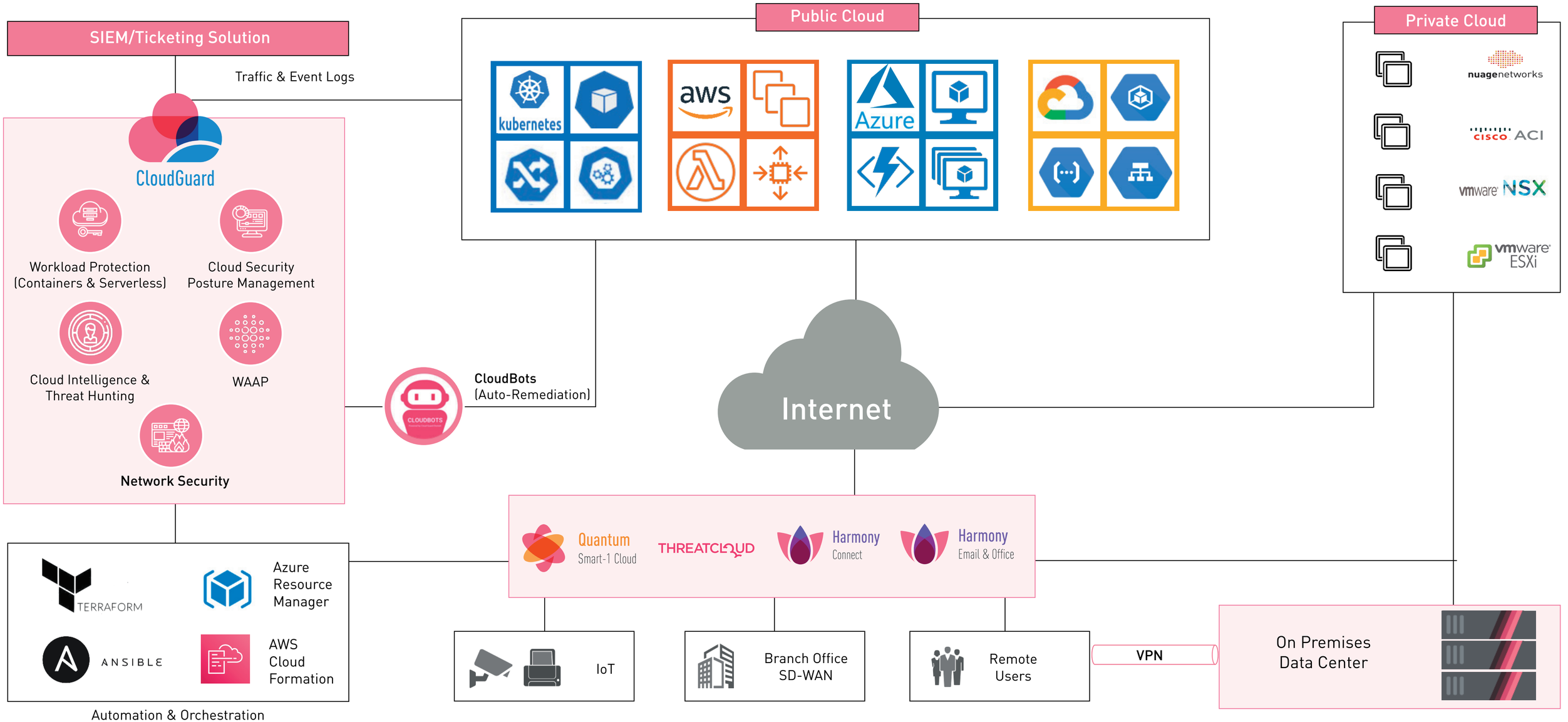
CloudGuard

Architecture Blueprint Diagrams





Network Security

- Advanced Threat Prevention & Traffic Inspection
- Common Policy and Logging Infrastructure
- Unified management of physical and virtual infrastructure
- Automated deployment through IaC
- Dynamic policies map to cloud through tags and metadata
- Support also for Oracle, Alibaba Cloud, IBM, and more

Additional Cloud Security Capabilities

- Continuous Compliance with Industry Frameworks and Best Practices
- Identify misconfigurations in IaaS and PaaS
- Automatic Remediation integrated natively
- Workload Protection for Kubernetes clusters and Serverless functions
- “Shift left” security posture into CI/CD pipeline
- Consumes & correlates cloud native network and audit logs

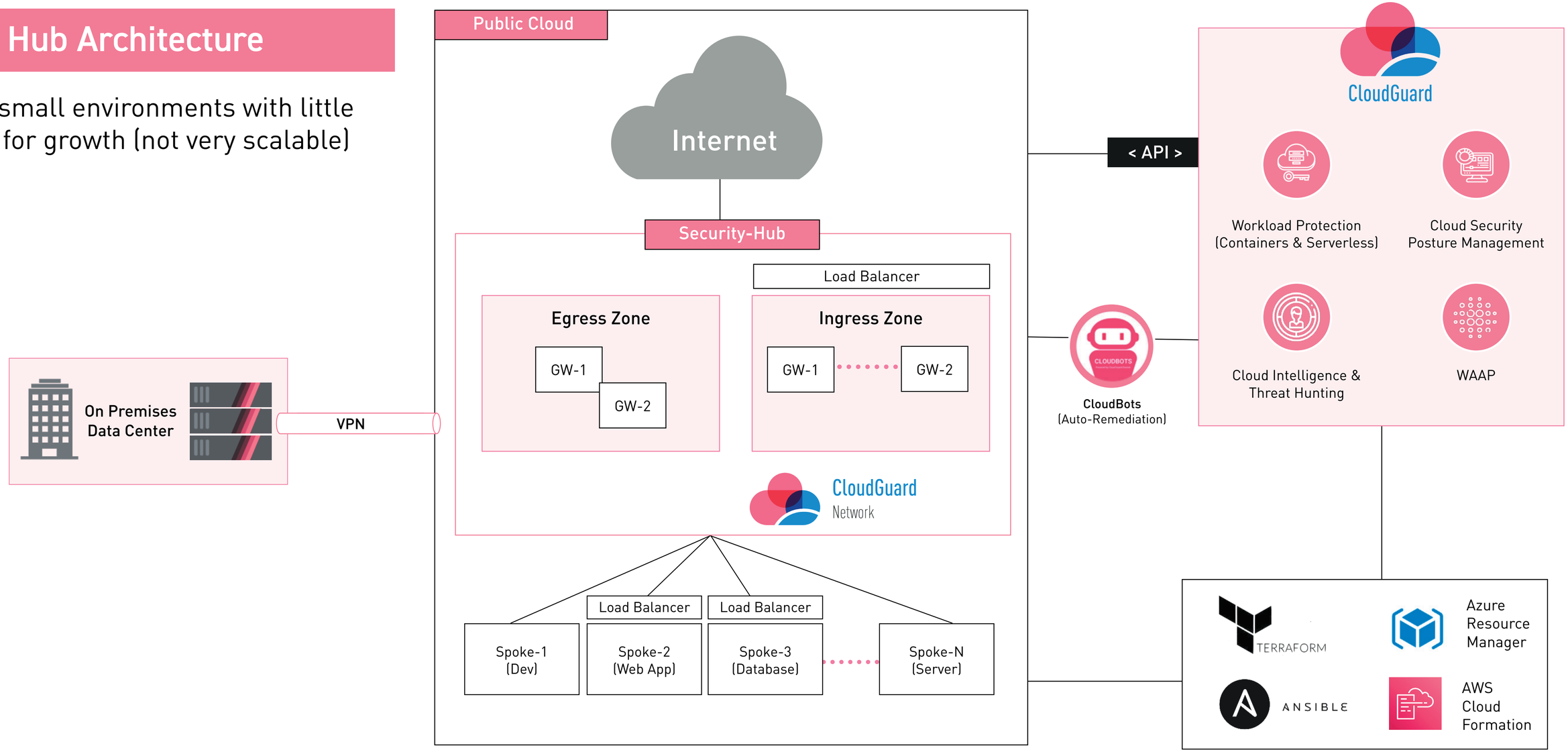
Overall Architecture:

- ThreatCloud delivers real-time dynamic security intelligence from a collaborative cloud driven knowledge base
- Holistic security view
- High Fidelity context for Threat Hunting & Intelligence
- Extensive APIs across the CloudGuard suite

CHECK POINT

Single Hub Architecture

Ideal for small environments with little prospect for growth (not very scalable)



Values

- "Network perimeter" security with Advanced Threat Prevention
- Simple architecture deployment
- Agility, Automation, Efficiency, Elasticity
- Unified management for hybrid environment

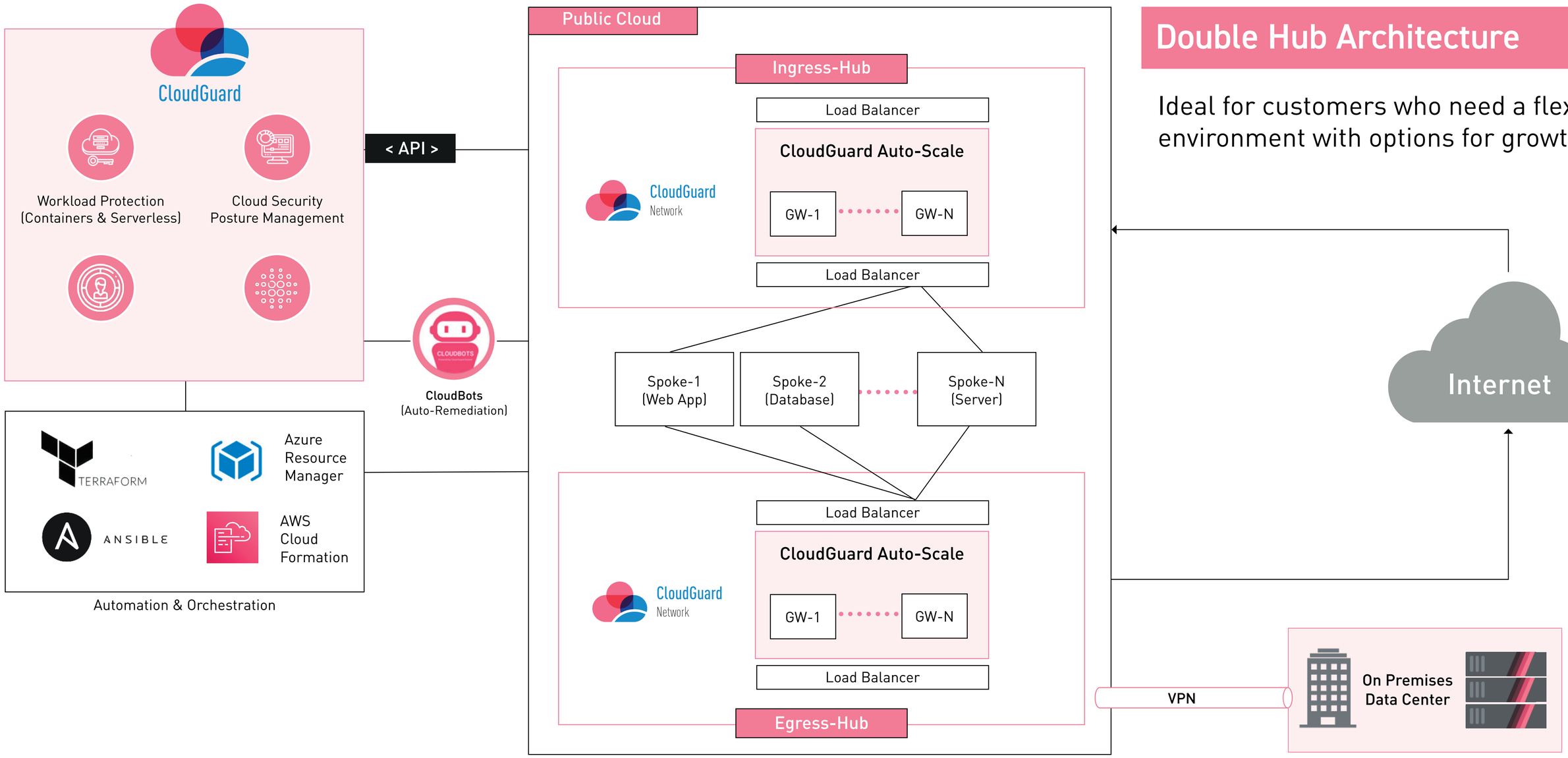
Architecture

- The Single Hub (VPC or vNET) acts as a central point for the security of the entire cloud environment.
- Ingress & Egress Zones for North/South Traffic Inspection
- Ability to add East/West inspection between VPCs, VPN, or MPLS connections
- Flexible deployment templates for single gateway, HA clusters, or Auto-Scaling group
- With Auto-Scaling groups, automatic scale out and scale in based on load and performance
- Spokes represent a virtual network where different assets are deployed.

CHECK POINT

Double Hub Architecture

Ideal for customers who need a flexible environment with options for growth



Values

- Automation of deployment, scaling, and policy enforcement
- Enhance Cloud Native tools with Advanced Threat Prevention
- Ease of enforcement on traffic through cloud networking
- Segmentation of internet facing and private facing traffic

Architecture

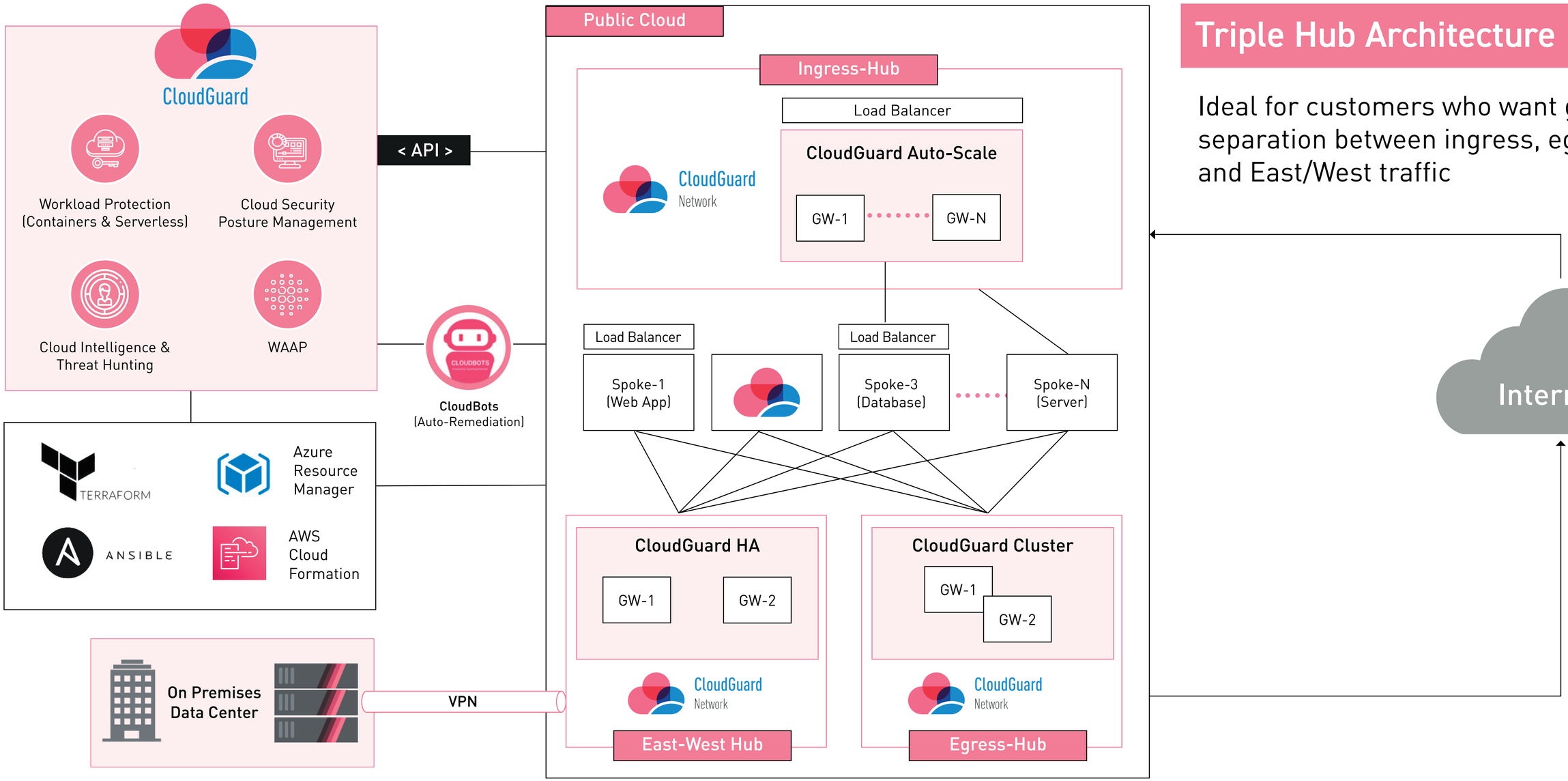
- Double Hub Architecture segments and enforces security controls on traffic entering or exiting a spoke.
- The Ingress Hub deploys Auto-Scaling gateways that handle fluctuating levels of traffic from the Internet.
- The Egress Hub is responsible for East/West traffic between spokes, outgoing traffic to the Internet, and corporate traffic from the On Premises Data Center.
- Flexible deployment options for standalone, clusters, and auto-scaling to meet resiliancy and performance requirements.

This Architecture is the official Check Point recommendation.

CHECK POINT

Triple Hub Architecture

Ideal for customers who want granular separation between ingress, egress, and East/West traffic



Values

- Internet connected North/South traffic uses dedicated security zone
- Options to separate East/West hubs and Egress Hubs
- Separation for performance, change management,and maintenance
- Zero Trust Model

Architecture

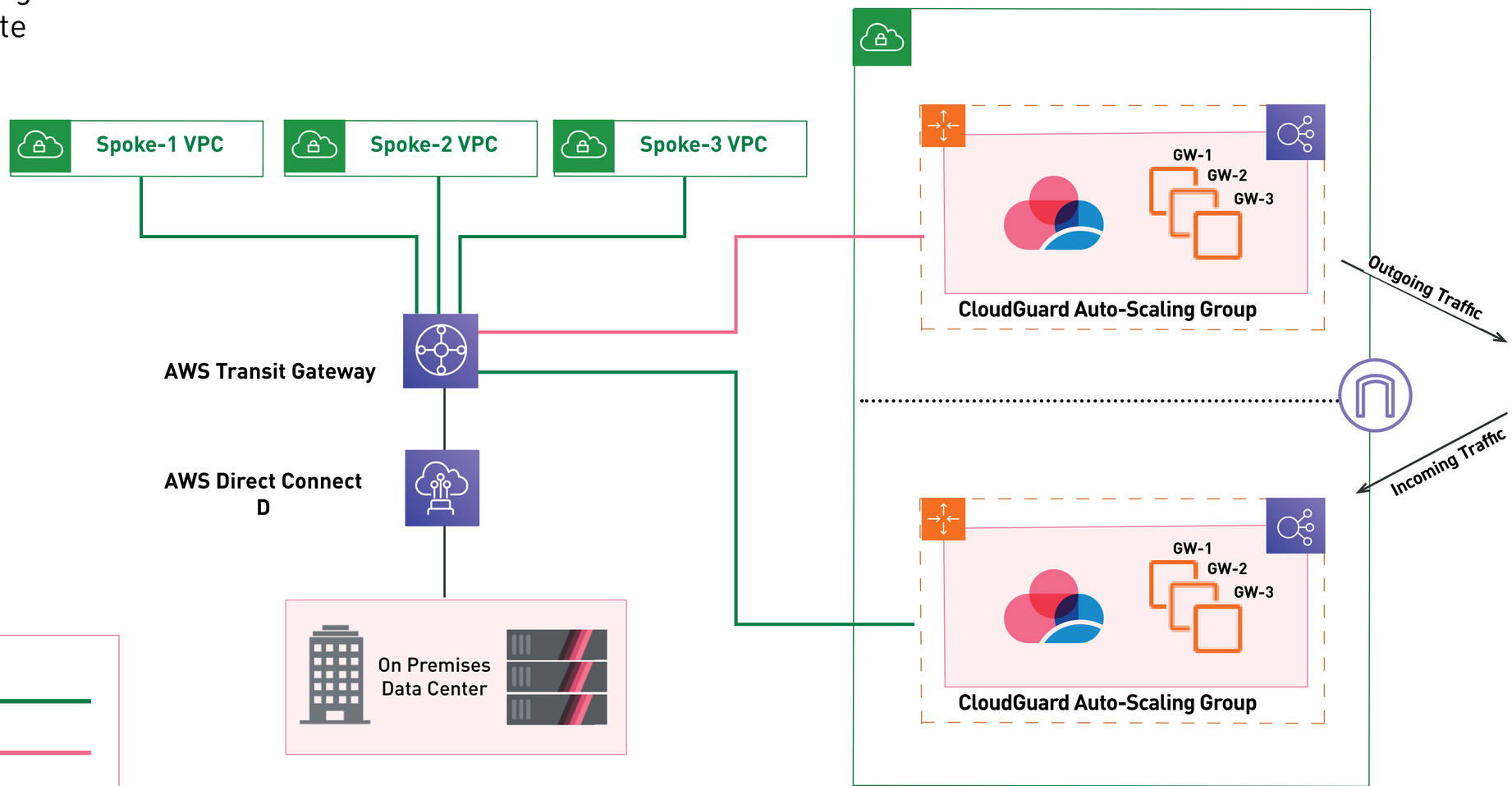
- Triple Hub Architecture offers the most separated architecture and adheres the most to a Zero Trust model.
- This architecture segments the different traffic flows with security controls on each hub.
  - The Ingress Hub deploys Auto-Scaling gateways that handle fluctuating levels of traffic from the Internet.
  - The Egress Hub is responsible for outgoing traffic to the Internet.
  - The East-West Hub handles East/West traffic between the spokes and corporate traffic from the On Premises Data Center
- All deployment templates support agile security policies that dynamically learn from cloud subscriptions through tags and metadata

CHECK POINT™

AWS Architecture Diagrams

Single Security VPC Hub

Ideal for customers who want a single hub to handle security in AWS. Note that this can add complexity.



Values

- Simplest deployment possible
- Native automation using Zero Touch Provisioning
- Ease of management and upgrades through templates
- Independent scaling of Ingress and Egress security controls

Architecture

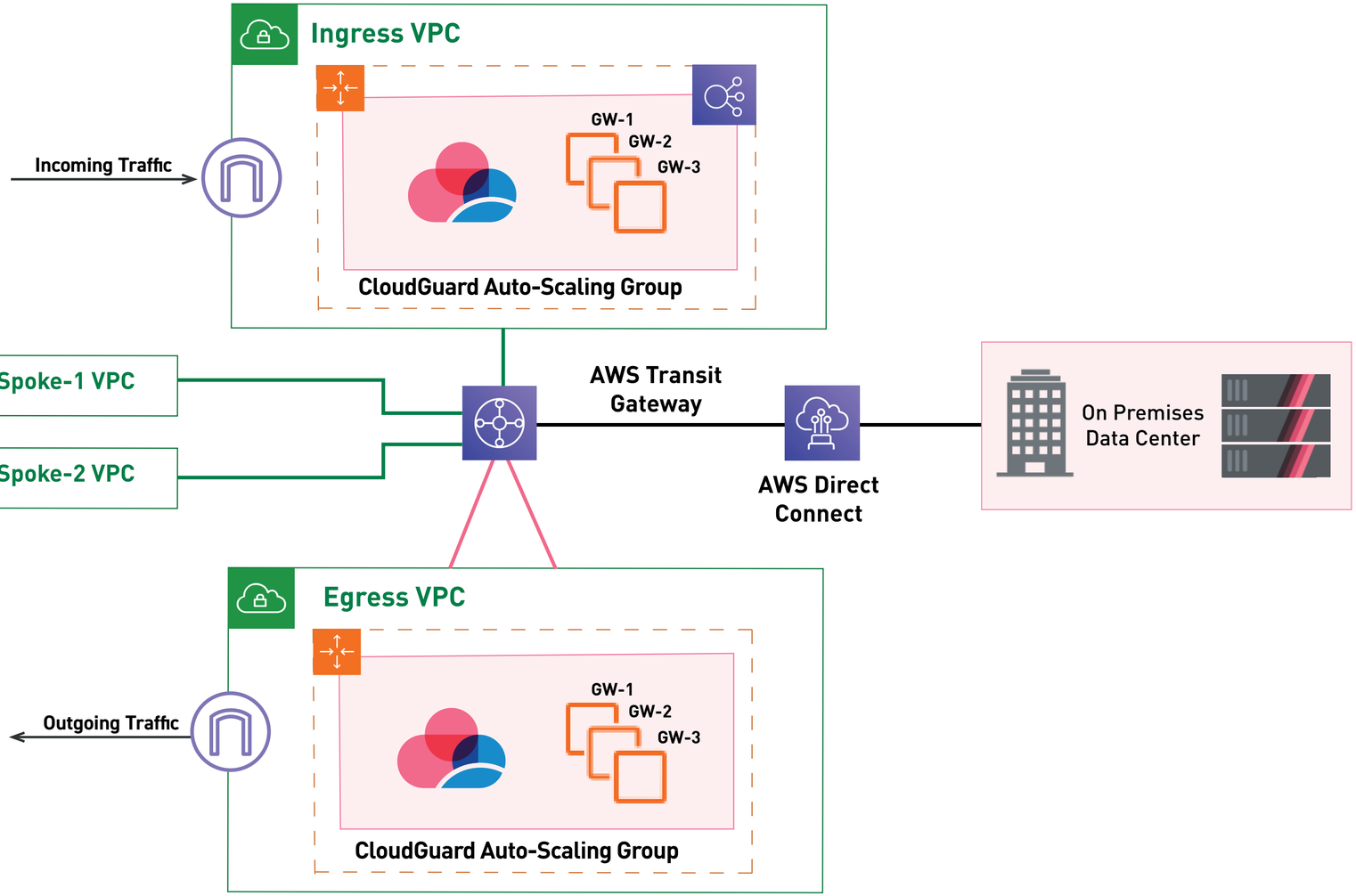
- Transit Gateway acts as a central routing hub, to connect VPCs to Internet GWs, on premises networks, and VPC to VPC
- Security Gateways attach to Transit Gateway using IPsec tunnels and BGP peering
- Seperate Ingress and Egress templates allow for ease of automation and simplified deployment
- The Ingress traffic Auto-Scaling Groups utilize load balancers for Inbound traffic flows
- The Egress traffic Auto-Scaling Groups attach to the Transit Gateway and process outgoing traffic and East/West traffic between the spokes.

CHECK POINT

Two Security VPC - Option 1

Transit Gateway VPC Attachment for Ingress VPC

Ideal for customers who need scalability with ingress/egress and simplified segmentation routing on the TGW Routing Domains



Transit Gateway VPC Attachment

VPN Tunnel

Values

- Separate fault isolation domains
- Horizontal Elasticity via Active/Active load sharing
- Selective traffic steering for some, all, or no traffic
- Scalable East/West and outgoing traffic if required

Architecture

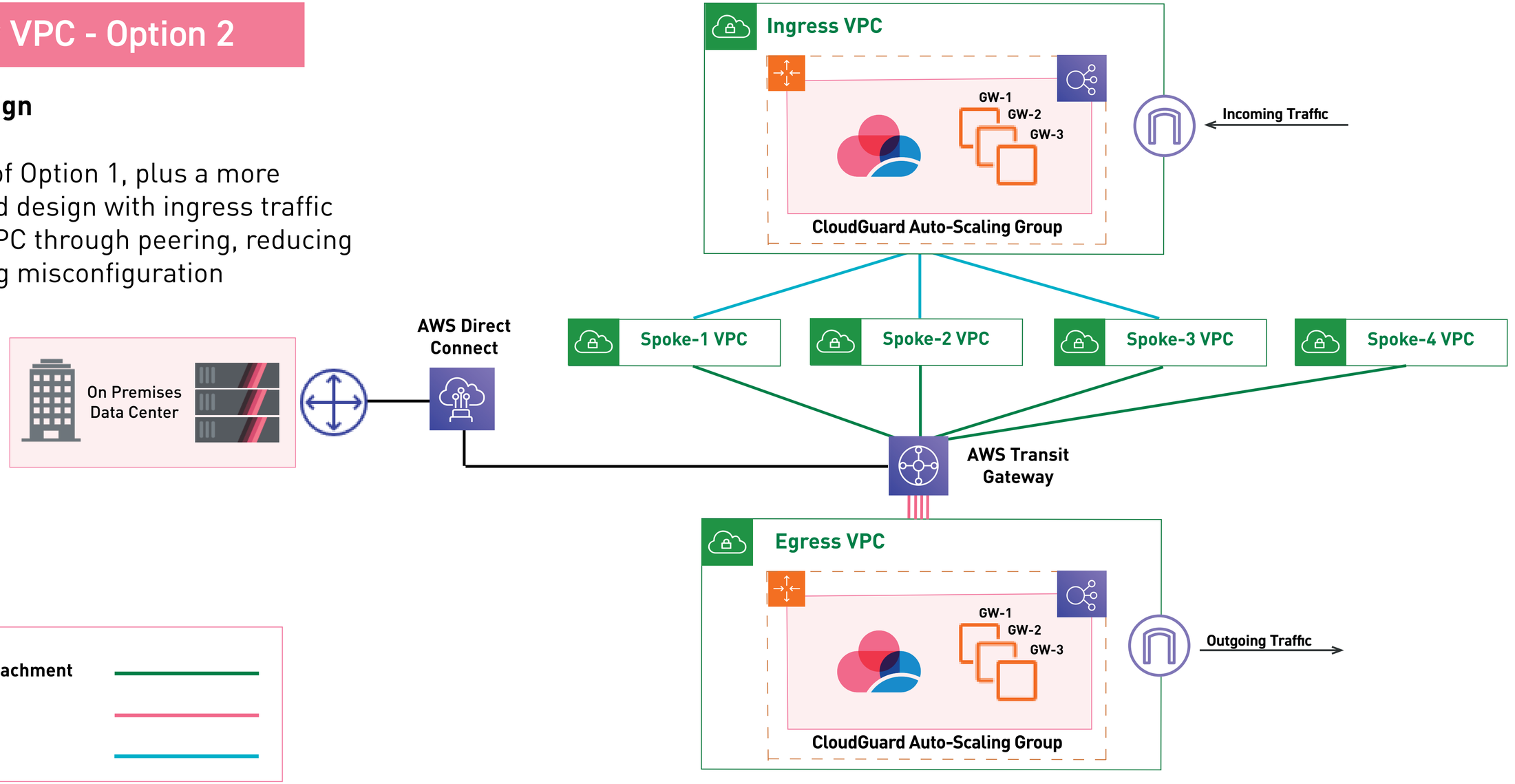
- Multiple VPCs are deployed for Ingress and Egress Security Zones.
- Internet Gateways are attached to CloudGuard Auto-Scaling Groups to allow North/South traffic
- The Ingress Auto-Scale Group attaches to load balancers which can be directly attached, peered, and/or connected via Transit GW.
- The Egress VPC handles outgoing traffic, East/West traffic between the Spoke VPCs, and traffic from the on premises data center.
- Vertical scalability by increasing the size of the CloudGuard instances (2 core, 4 core, 8 core)
- Horizontal scalability by increasing the number of CloudGuard instances within the Scaling Group (changing min and max values)
- Following this best practice enables **handling fluctuating traffic load efficiently and independently.**

CHECK POINT

Two Security VPC - Option 2

Security By Design

All the benefits of Option 1, plus a more security-oriented design with ingress traffic controlled per VPC through peering, reducing chance of routing misconfiguration



Values

- Systematically separate between incoming and outgoing flows
- Ingress traffic flows traverse a shared security zone
- Ingress Auto-Scaling connects through peering
- Spoke VPCs do not contain their own Internet Gateways
- Egress VPC enables on premises to cloud traffic inspection

Architecture

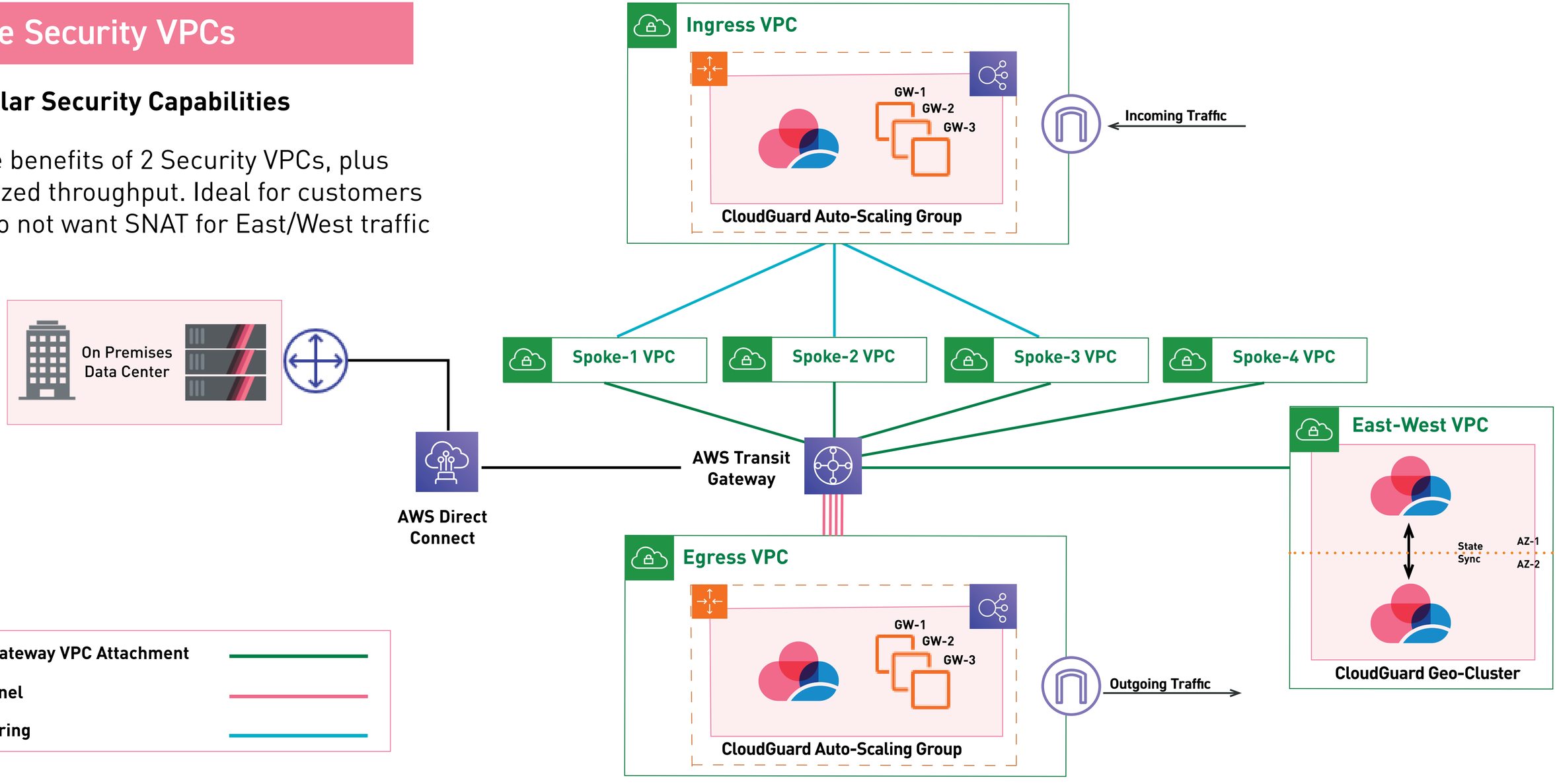
- The Ingress VPC is peered to the Spoke VPCs, making it so there is no direct connection between the Ingress Hub and the Transit Gateway.
- Selective control for Ingress traffic on a per VPC basis through peering
- Inter-VPC traffic attaches to Transit Gateway, where Layer 3 manipulation allows insertion of Layer 4-7 Security
- The Egress VPC handles outgoing traffic, East/West traffic between the Spoke VPCs, and traffic from the on premises data center.
- Selective performance sizing should be considered for non Auto-Scaling deployments

CHECK POINT

Three Security VPCs

Granular Security Capabilities

All the benefits of 2 Security VPCs, plus optimized throughput. Ideal for customers who do not want SNAT for East/West traffic



Values

- Cross AZ State Synchronization anf Stateful Failover
- Elimination of SNAT for East/West and Corporate traffic flows
- Common use case for East/West or Direct Connect where SNAT is undesirable
- Greater granularity over network flows (security is enforced separately based upon direction of traffic)
- Isolation of Security Zones provide autonomy

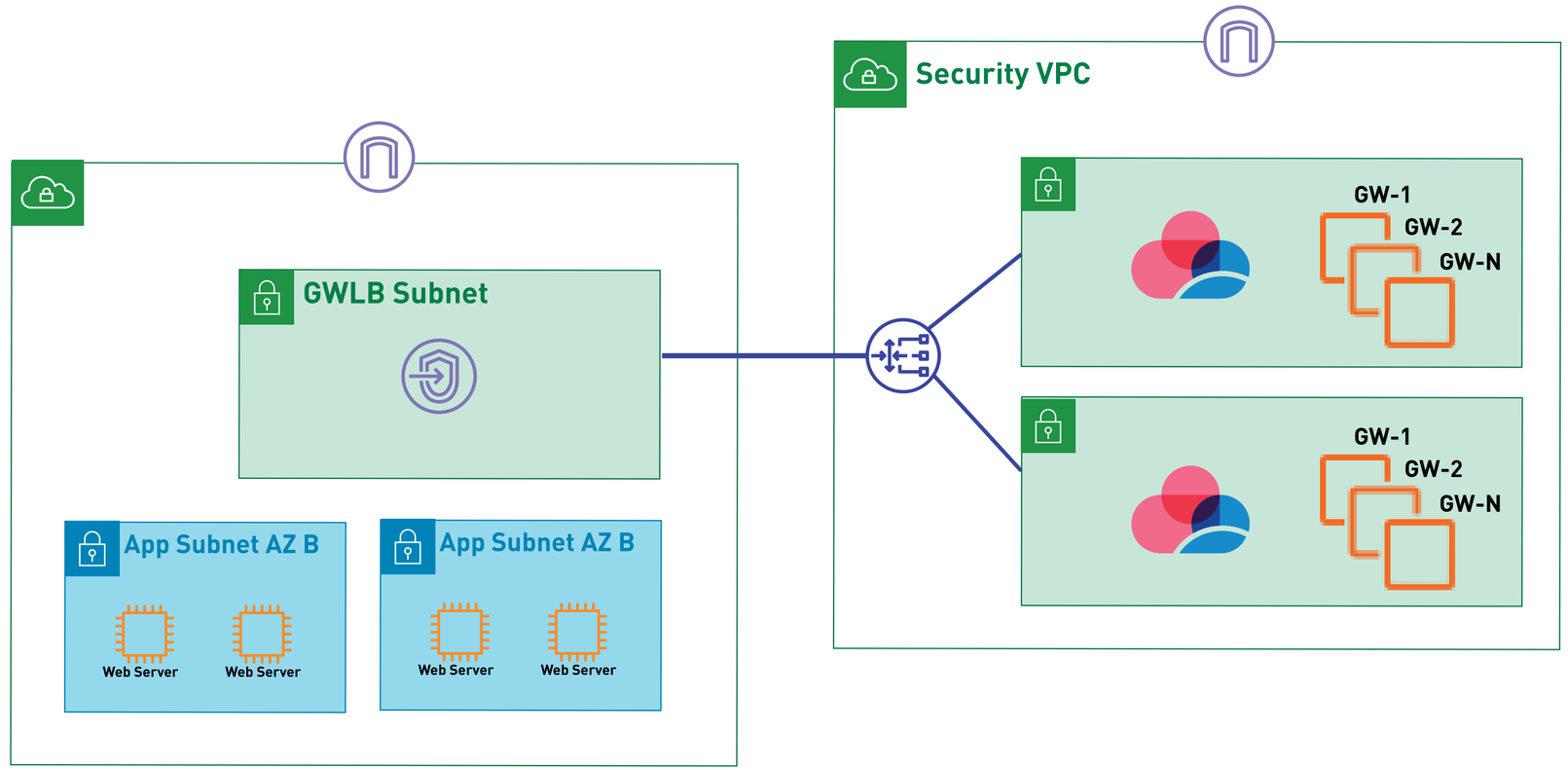
Architecture

- Independent VPC for East/West and Direct Connect usage uses Active Standby
- CloudGuard Geo-Cluster supports stateful failover where the member that needs to become active automatically changes the routing table in the TGW. This method of failover is faster and takes less API time than the classic cluster failover method. Alternatively, Auto-Scaling Group can be deployed in the East West VPC.
- Creation of separate East/West VPC isolates performance, change control, and policy management from egress security requirements. East/West and Direct Connect have isolation and eliminated need for SNAT

CHECK POINT

Gateway Load Balancer

Ideal for customers without the requirement for E/W traffic inspection



GWLB connection to endpoints

Values

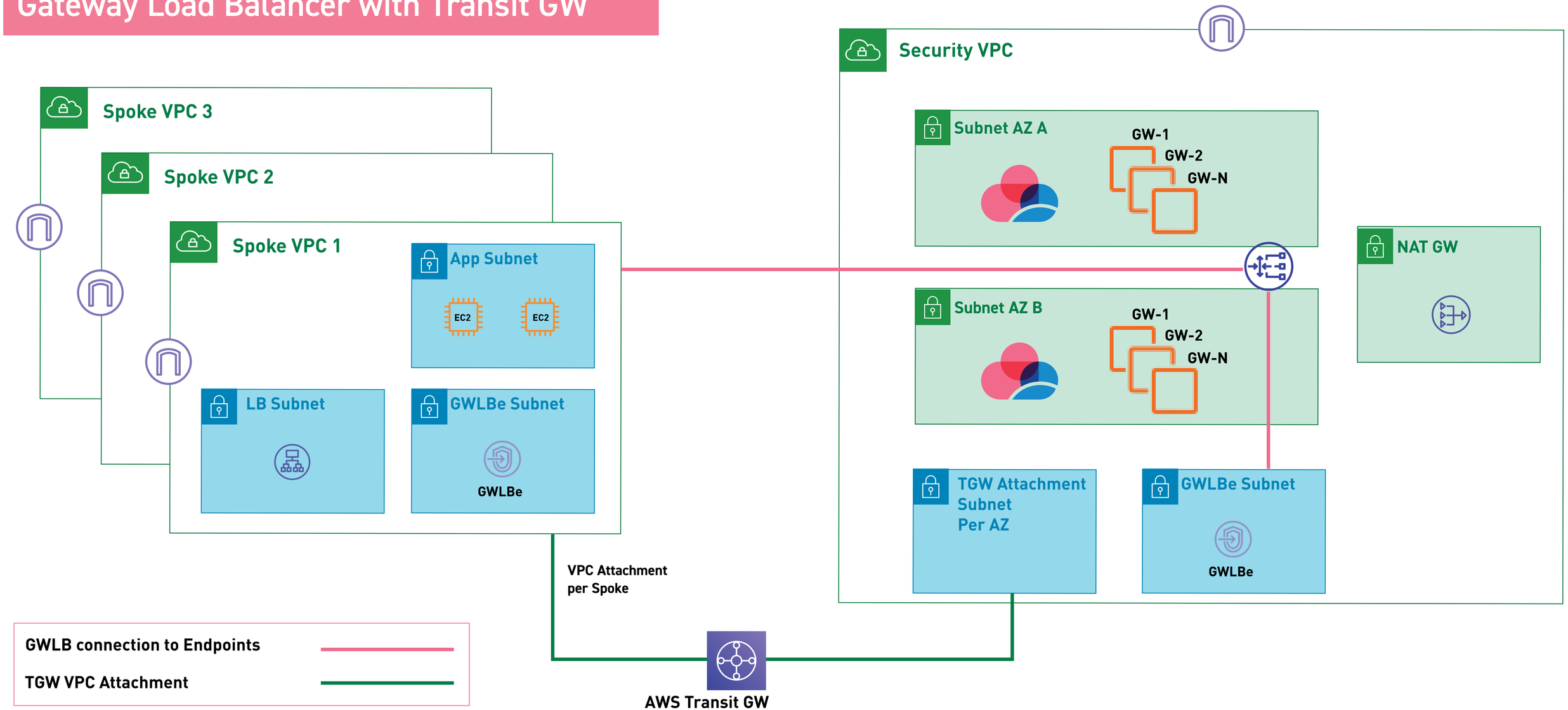
- Simple per hop routing directs traffic to Security VPC for inspection
- SNAT is not required for GWLB, so original traffic is seen at CG Gateways

Architecture

- GWLB Endpoint is deployed in it's own subnet in the Consumer VPC
- This endpoint will forward all ingress (via Ingress routing edge attachment to IGW) and egress traffic to the GWLB
- GWLB automatically forwards traffic to CG Auto-scaling GWs for enforcement and inspection
- Deploy an Application Load Balancer in Consumer VPC for SSL Termination

CHECK POINT™

Gateway Load Balancer with Transit GW



Values

- SNAT not required to view original outbound, E/W, or encrypted inbound traffic
- Simple per hop routing directs traffic to Security VPC for inspection
- Combined with TGW, eliminates need for IPSec/ BGP/ECMP tunnels

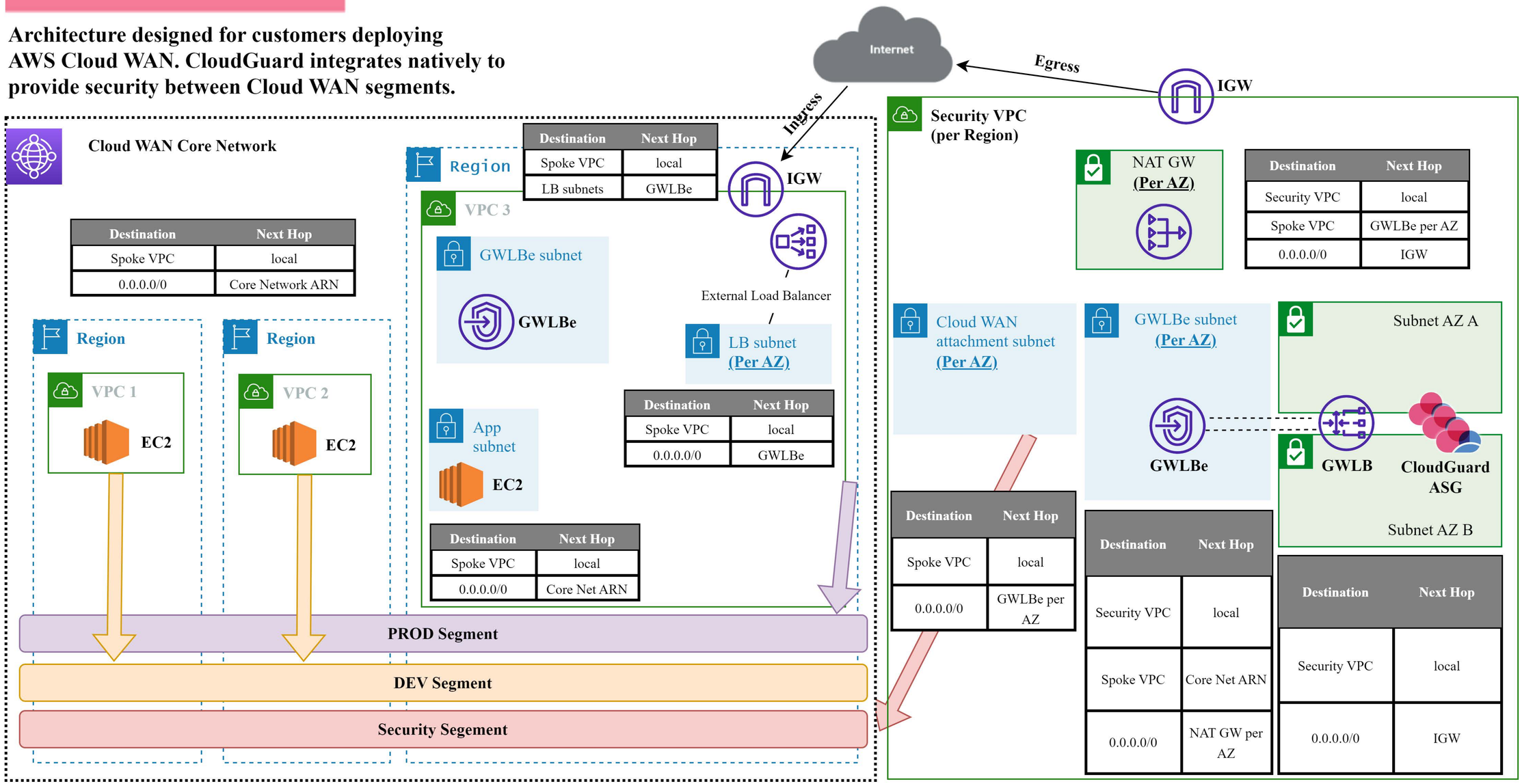
Architecture

- The GWLBe in the Spoke VPCs will forward ingress traffic to the GWLB and automatically to CG enforcement via ingress routing edge attachment to IGW
- IGW must be deployed in every spoke for this inbound inspection
- For SSL offloading of ingress traffic, deploy an Application Load Balancer subnet per AZ
- The GWLBe in the Security VPC forwards egress and E/W traffic to the GWLB and automatically to CG enforcement
- A NAT GW is deployed per AZ to handle outbound traffic NAT translation

CHECK POINT

Cloud WAN

Architecture designed for customers deploying AWS Cloud WAN. CloudGuard integrates natively to provide security between Cloud WAN segments.



Values

- **Prevent advanced threats and reduce your attack surface by enabling segmentation and blocking lateral attacks while giving you greater visibility of all Cloud WAN connected segments**
- **Seamless integration with AWS Cloud WAN**
- **Centralized security policy management across hybrid and multi-cloud**

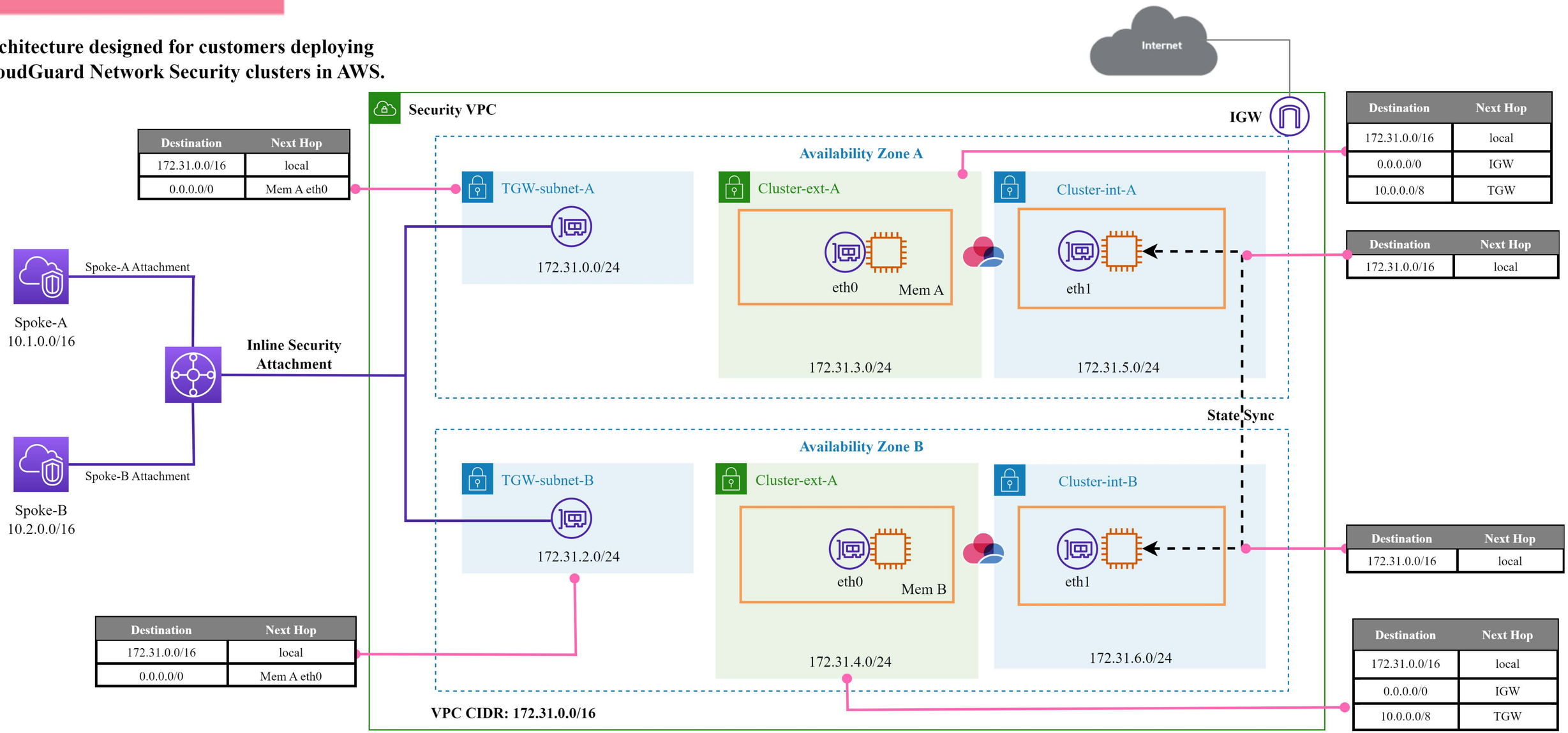
Architecture

- **Use one security VPC for each region to prevent cross-region charges.**
- **The region's CloudGuard Network Security GWLB/ASG pool inspects the inbound traffic without traversing through the Cloud WAN segments**
- **Outbound traffic egresses from the same region the traffic originated from**
- **Supports all traffic flows**

CHECK POINT™

Cross AZ Cluster

Architecture designed for customers deploying CloudGuard Network Security clusters in AWS.



Destination	Next Hop
172.31.0.0/16	local
0.0.0.0/0	Mem A eth0

Destination	Next Hop
172.31.0.0/16	local
0.0.0.0/0	IGW
10.0.0.0/8	TGW

Destination	Next Hop
172.31.0.0/16	local

Destination	Next Hop
172.31.0.0/16	local

Destination	Next Hop
172.31.0.0/16	local
0.0.0.0/0	IGW
10.0.0.0/8	TGW

Values

- **Simplifies VPC connections**
- **Provides a security cluster which synchronizes connections, prevents interruptions in case of failure, and uses the full 50 Gb/s network throughput**
- **Easy to deploy through the use of a CloudFormation template**

Architecture

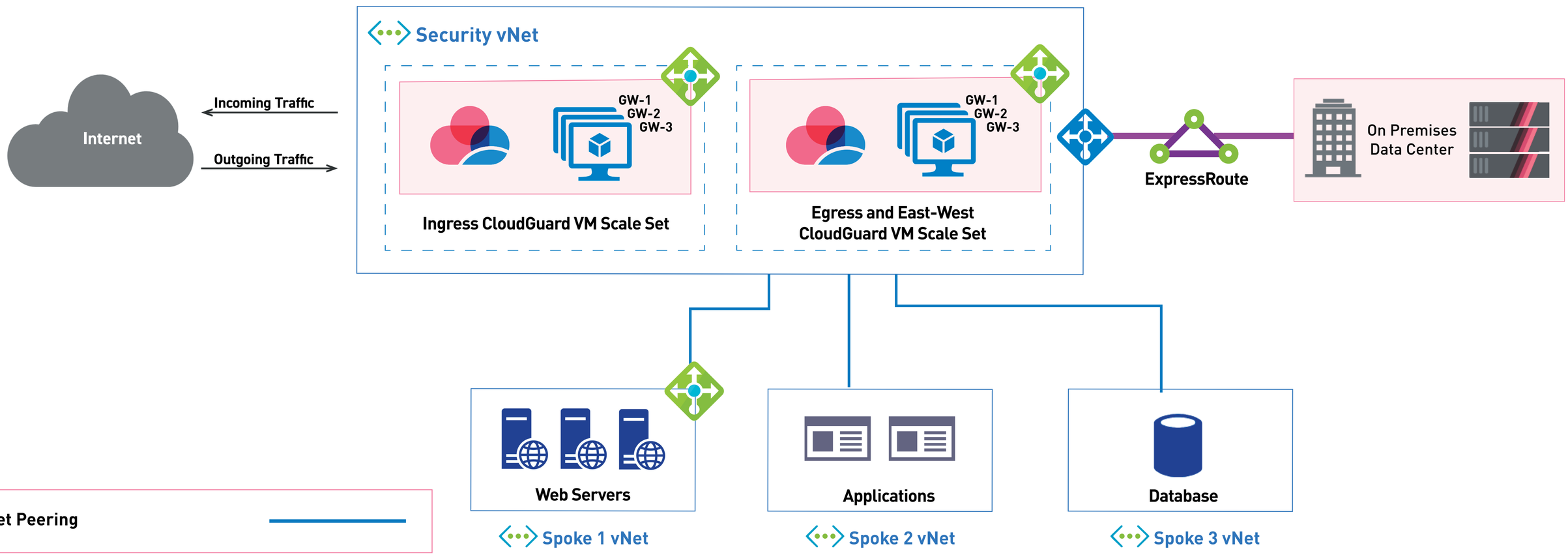
- **Security VPC with the CloudGuard Network Cross AZ Cluster members deployed in different Availability Zones**
- **Sync between the Cross AZ Cluster members**
- **Public routing tables associated with public subnets**
- **Private routing table associated with the private subnets with a default route to the Active member private interface (eth1)**
- **Ingress routing integration: The routing table associated with the IGW contains routes to private subnets trough the Active member public interface (eth0)**

CHECK POINT™

Azure Architecture Diagrams

Single Security vNet

Ideal for customers who want very simple routing that works for both small and large environments



Values

- Incredible scalability and resiliency
- Highly automated
- Intra-vNET and micro segmentation simplified through use of UDRs
- Inter and Intra vNET Security Deployments supported
- Ability to do host to host micro-segmentation
- On demand and elastic remote access

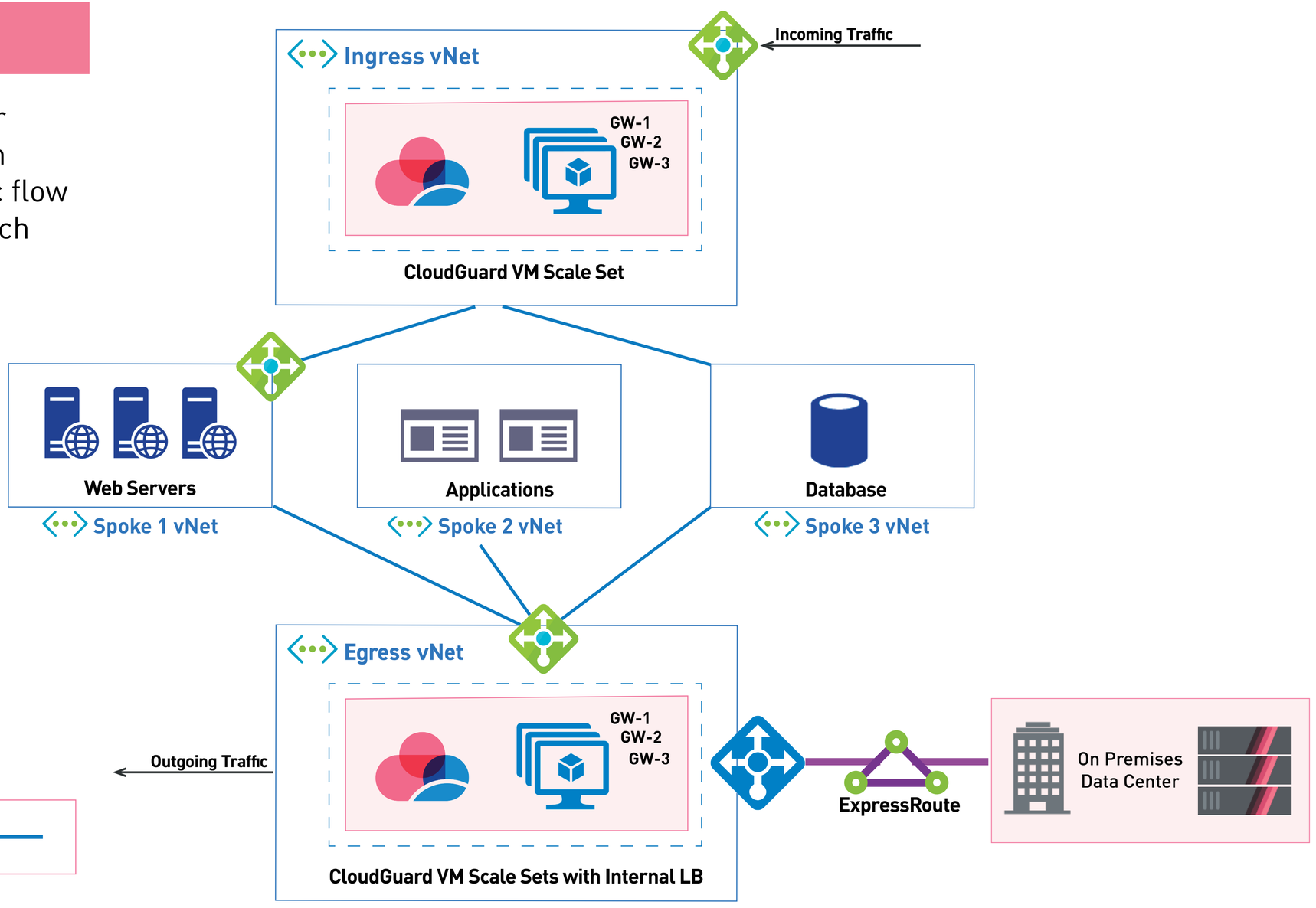
Architecture

- All security controls are deployed in one vNET.
- Inbound traffic flows through an External Load Balancer hosting the public IP addresses.
- Outbound traffic flows match UDRs which can be sent to single GWs, HA clusters, and/or VMSS
- With VMSS, UDRs point to the Microsoft standard load balancer attached to HA ports comprised of a CloudGuard VMSS
- Such UDRs eliminate the need for route table manipulation during failover, heavily reducing downtime
- VMSS with UDRs can be used inter or intra vNETS, ExpressRoutes, VPN, and/or micro-segmentation

CHECK POINT

Two Security vNet

Ideal for customers desiring better segmentation for traffic flows, with ability to easily send desired traffic flow to a dedicated hub and choose which spokes are exposed to internet.



Values

- Security by design – Zero Trust Model
- Systematically separate between incoming and outgoing traffic flows
- Traffic flow isolation for performance and policy optimization
- On demand and elastic remote access

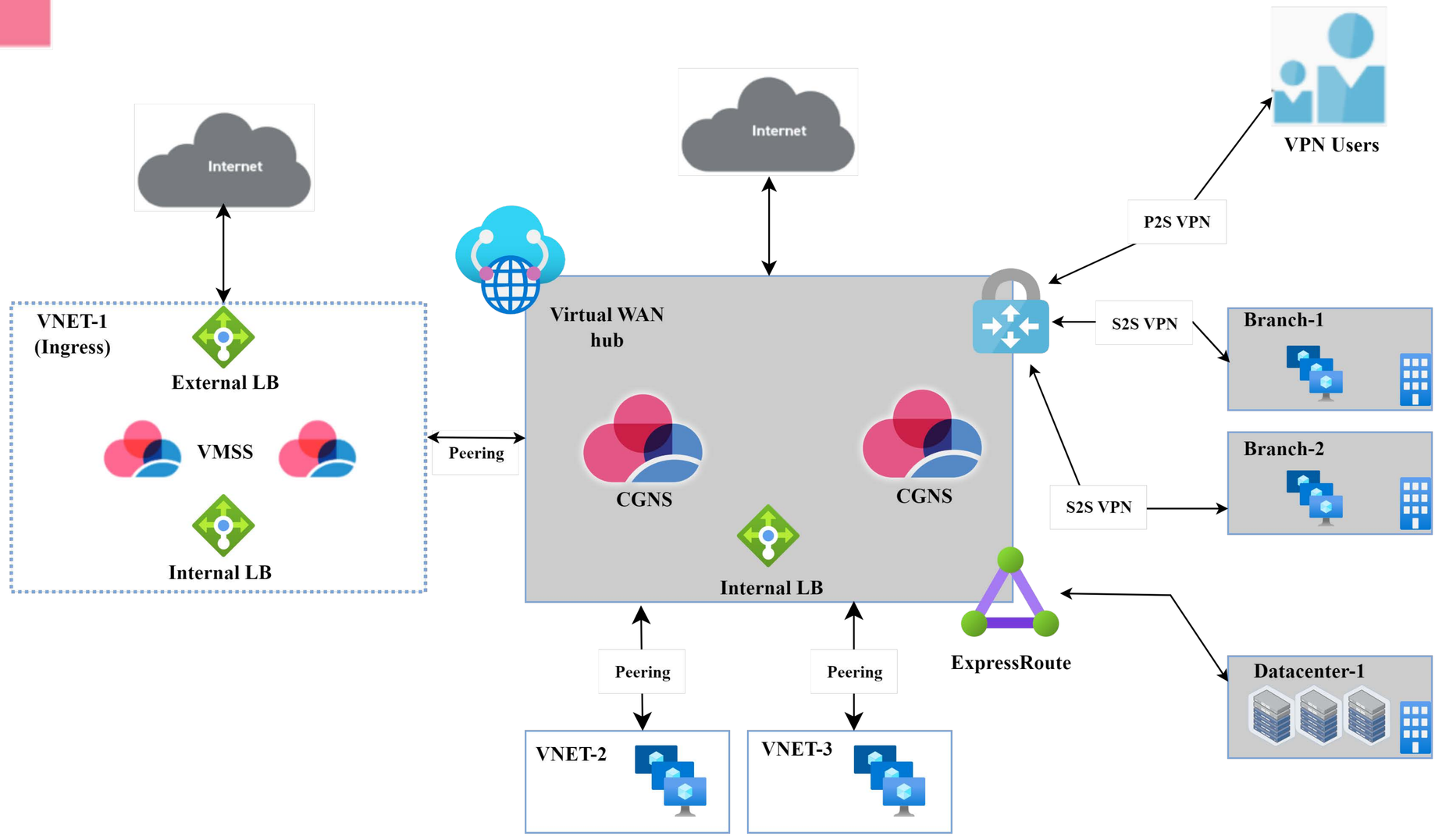
Architecture

- Two vNETs with separate security controls. All the vNETs are connected through peering.
- Security by design. Spokes which do not require Internet connection are not peered to the Ingress vNET, preventing the risk for a routing configuration error. This can be addressed also with CloudGuard CSPM.
- In the Ingress vNET, Inbound traffic flows through an External Load Balancer hosting the public IP addresses.
- The Egress vNET handles East/West traffic, outgoing traffic, and the communication to the on premises data center.
- ARM Templates for single GW, HA Cluster, and/or VMSS are available to meet performance and availability options

CHECK POINT

Virtual WAN

Architecture designed for customers deploying Azure Virtual WAN. CloudGuard integrates natively to provide security within the hub.



Values

- Prevent advanced threats and reduce your attack surface by enabling segmentation and blocking lateral attacks while giving you greater visibility of all Virtual WAN connected spokes
- Seamless integration with Azure Virtual WAN managed application via the Routing Intent feature
- Globally available Remote Access VPN
- Centralized security policy management across hybrid and multi-cloud

Architecture

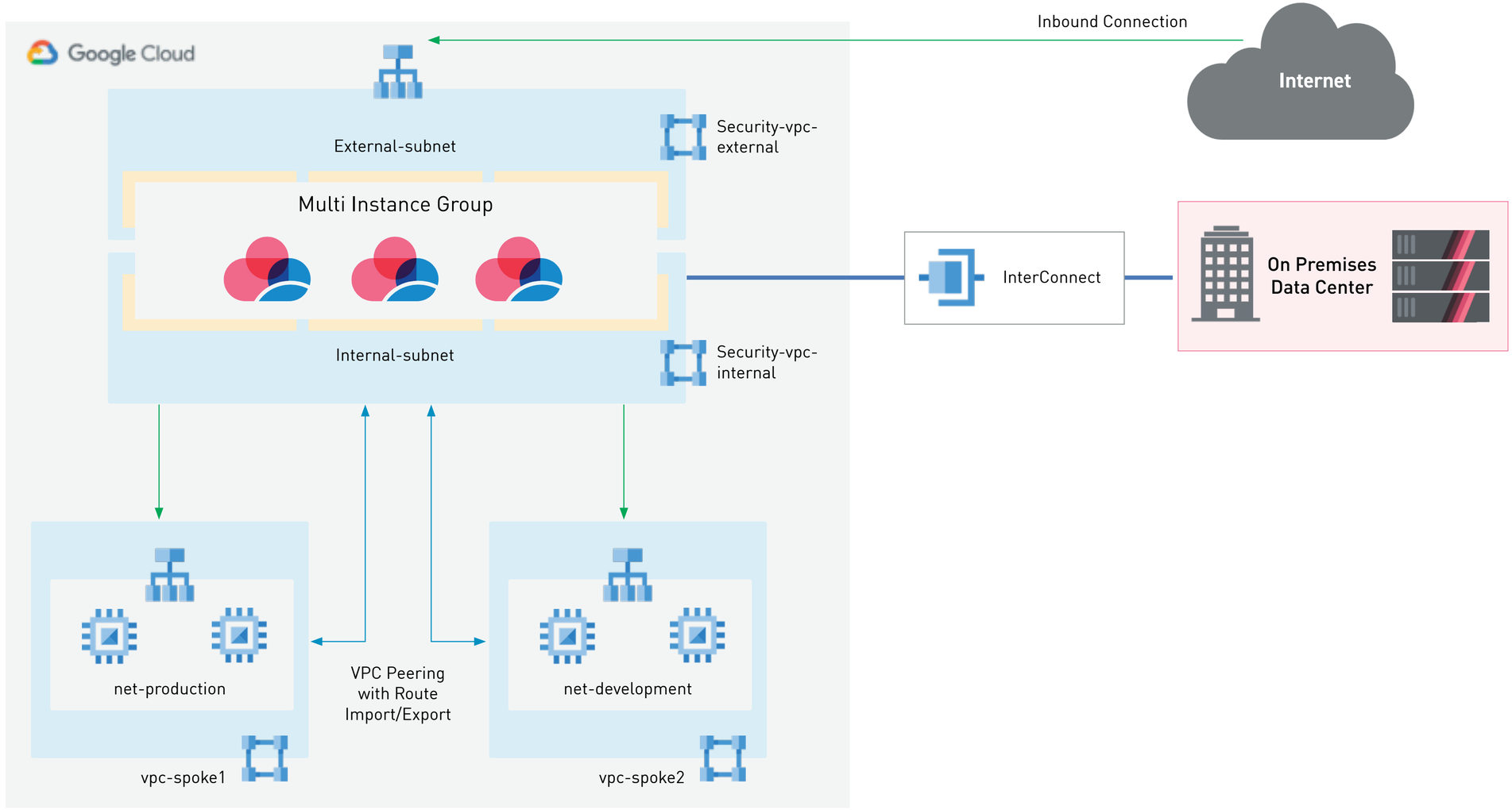
- One Virtual WAN Hub per region
- Managed hub & spoke WAN by Azure as a service
- CloudGuard Network Security is provided via an Azure Managed Application and located in the middle of the fabric allowing customers to steer relevant traffic to it for security inspection
- Supports East/West, Egress, Remote Access VPN, and ExpressRoute traffic flows
- Ingress traffic requires a dedicated VNET which is then peered with the Virtual WAN Hub
- Consumption-based pricing model

CHECK POINT

GCP Architecture Diagrams

Inbound MIG

Ideal for customers who need a dynamic and scalable solution to handle unpredictable inbound traffic flows



Values

- Grows with demand for ingress automatically
- Take full advantage of compute that's provisioned. No idle compute, only when needed
- Scalable deployment for exposing back-end applications/services with Multi Instance Group (MIG)

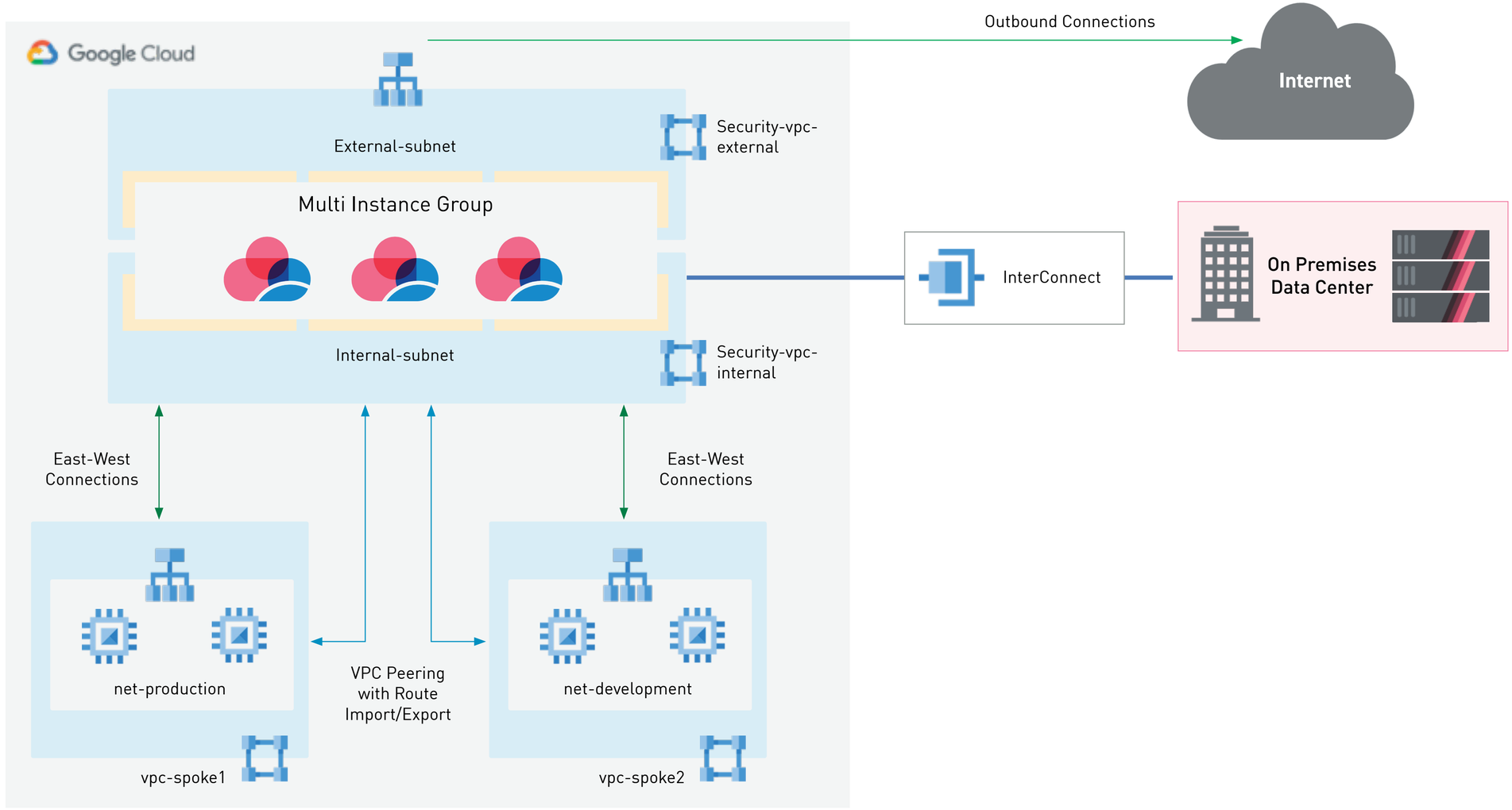
Architecture

- Automatically provisioned MIG instances with Cloud Management Extension (CME)
- MIGs are deployed in both the external and internal VPC, with interfaces in both
- Load balancer on the external subnet of the external VPC receives inbound connections from the internet and distributes across the MIG instances
- Back End Spoke VPCs are peered to the internal VPC
- Traffic automatically forwarded from MIGs to back-end internal load balancer serving the spokes.

CHECK POINT

Outbound and E/W Traffic MIG

Ideal for customers without publically facing assets who have no need for VPN.



Values

- Good for something that grows with demand for E/W and egress
- Active/active load sharing takes advantage of all the GCP Compute and Check Point licenses
- Scalable deployment with Multi Instance Group handling E/W and Egress flows

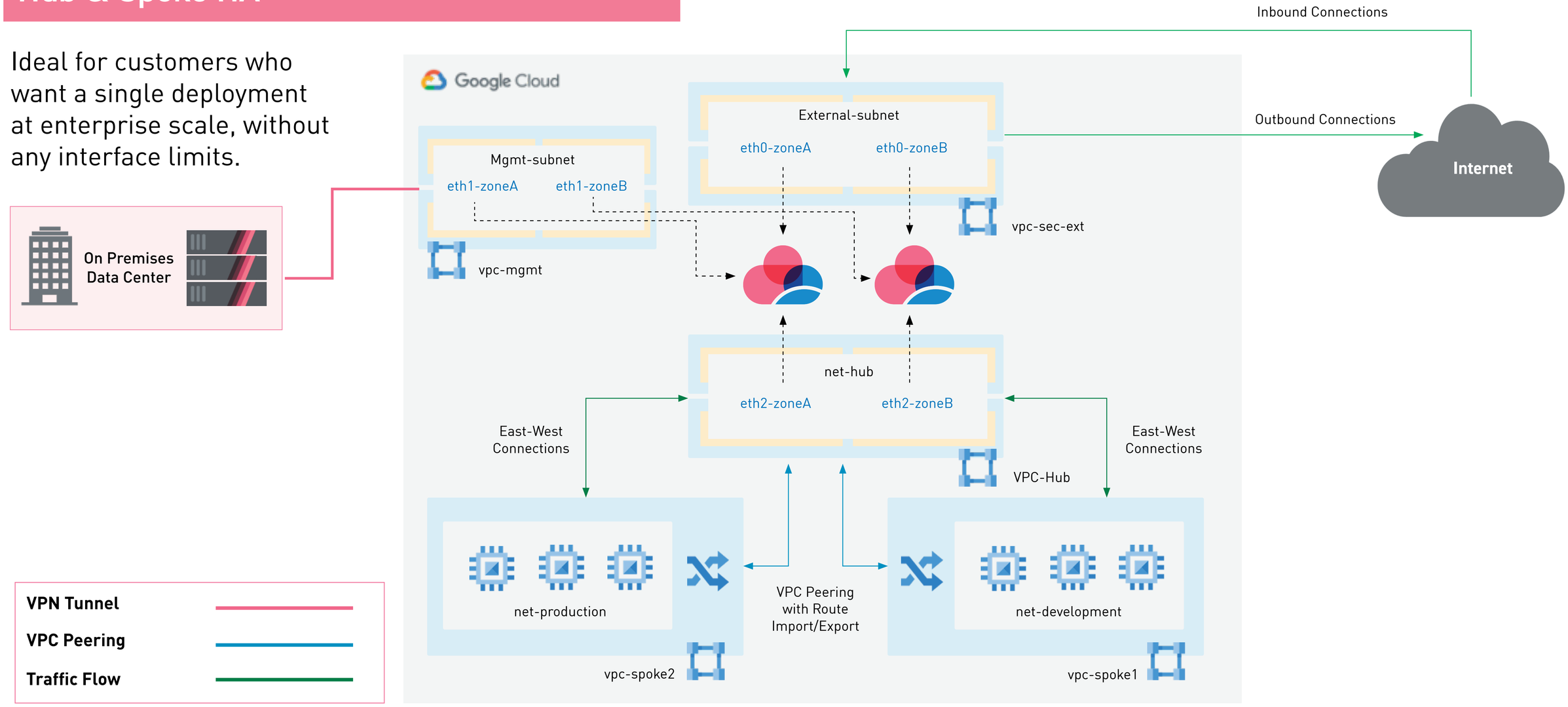
Architecture

- All VPCs must be in the same region for this architecture
- Egress and E/W traffic relies on internal TCP/UDP load balancer in the internal Security VPC
- All spoke VPCs have a default route pointing to the internal load balancer
- Route exchange (import/export) between spoke and security internal VPC
- Does not support ingress flows
- Note that Outbound Autoscaling solution to be released later this year will replace this

CHECK POINT

Hub & Spoke HA

Ideal for customers who want a single deployment at enterprise scale, without any interface limits.



Values

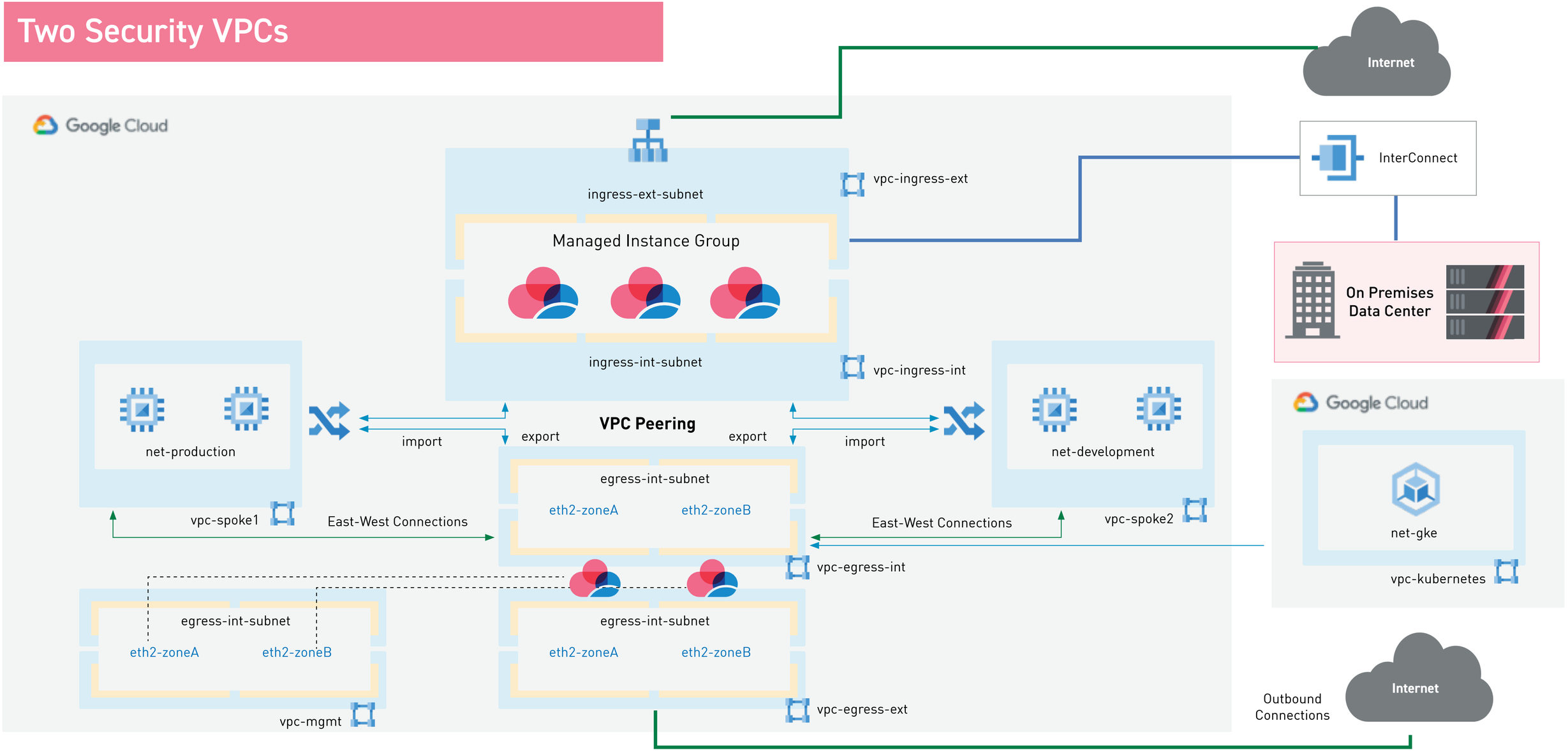
- Good for something that grows with demand for E/W and egress
- Active/active load sharing takes advantage of all the GCP Compute and Check Point licenses
- Scalable deployment with Multi Instance Group handling E/W and Egress flows

Architecture

- All VPCs must be in the same region for this architecture
- Egress and E/W traffic relies on internal TCP/UDP load balancer in the internal Security VPC
- All spoke VPCs have a default route pointing to the internal load balancer
- Route exchange (import/export) between spoke and security internal VPC
- Does not support ingress flows
- Note that Outbound Autoscaling solution to be released later this year will replace this

CHECK POINT

Two Security VPCs



Values

- Security by design – Zero Trust Model
- Good for something that grows with demand for N/S, E/W and ingress/egress
- Active/active load sharing takes advantage of all the GCP Compute and Check Point licenses
- Systematically separate between incoming and outgoing traffic flows
- Traffic flow isolation for performance and policy optimization

Architecture

- Supports multiple regions when the Cloud Interconnect terminates on a Security/Shared VPC
- Multiple VPCs are deployed for North/South, East/West Ingress and Egress Security Zones.
- Vertical scalability by increasing the size of the CloudGuard instances (2 core, 4 core, 8 core)
- Horizontal scalability by increasing the number of CloudGuard instances within the Managed Instance Group - “MIG” (changing min and max values)
- Supports static or dynamically learned routes to be exported to peer VPC networks benefitting from centralized configuration and allowing for scalable VPC network growth.
- Following this best practice enables handling fluctuating traffic load efficiently and independently.

CHECK POINT