1.1. Connectivity to on-premises resources

As the bandwidth and throughput requirements for AWS are high, it is proposed to use AWS Direct Connect links in both Datacentres. If the datacentres are not AWS Direct Connect locations, it is necessary to use connectivity services from one of AWS Partners (such as Megaport)

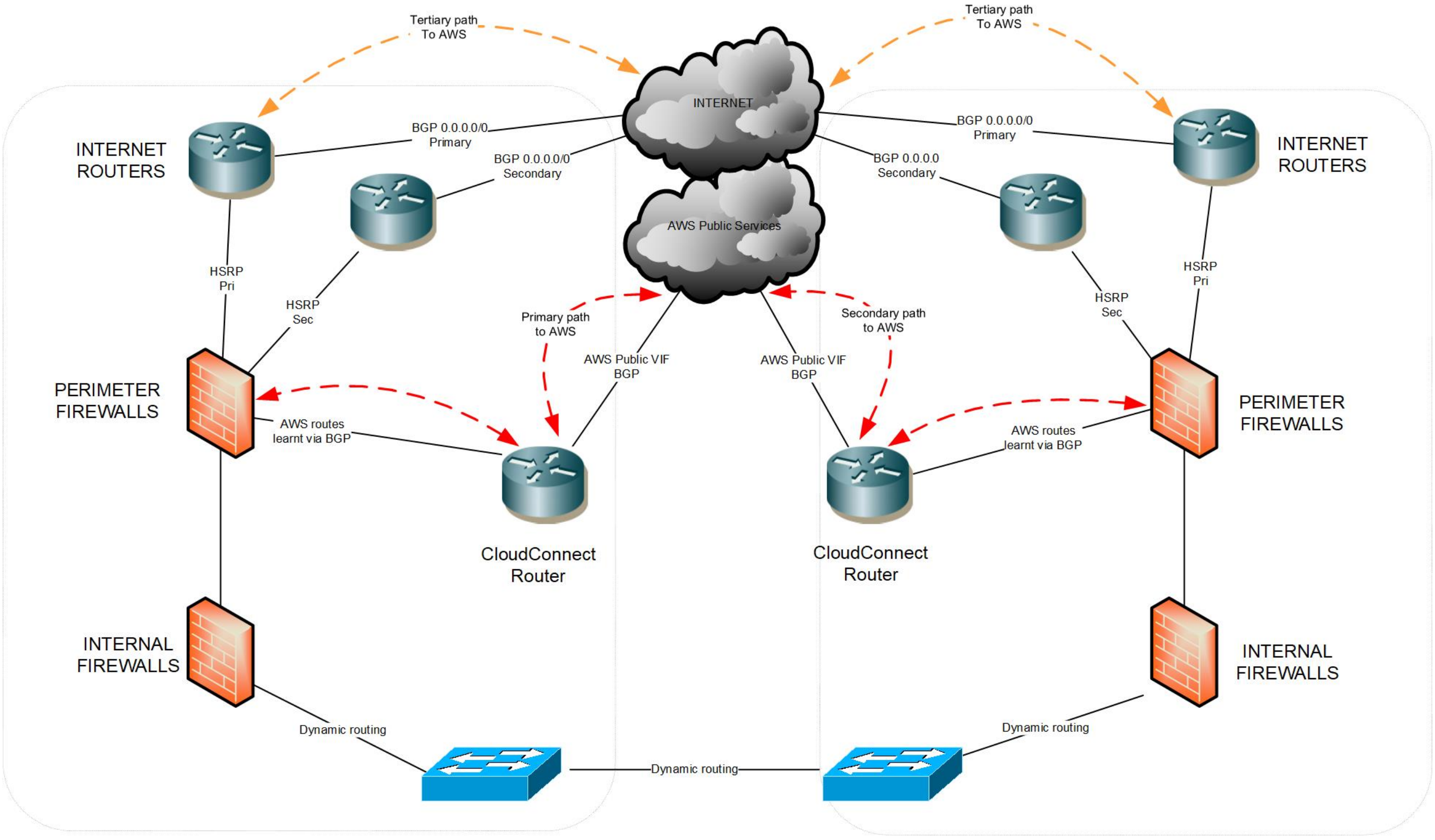
Both private and public VIFs are leveraged.

Private VIF is attached to a Direct Connect Gateway which is also configured as an association with the Transit Gateway. This provides connectivity to the VPC resources.

Public VIFs provide access to AWS Public services from on-premise.

A dedicated router is leveraged as an on-premises device rather than the Border firewall. The reason is that compared to most firewalls, routers usually have better functionality in terms of traffic engineering, routing filtering and manipulation (especially based on BGP community). The same CloudConnect router can be used for different Cloud providers, leveraging either direct connectivity or IPSec VPN tunnels.

The following diagram represents the overall high-level solution. Note this approach will also work with any other directly connect links to Public Cloud resources, such as O365 Expressroute or GCP Direct Peering, as well as VPN failover:



In this architecture the following approach is used to connect to AWS Public Services

- Network prefixes received from AWS and reachable via Direct Connect are dynamically updated using BGP protocol (so no dependency on any third-party tools or APIs) and correctly routed via Expressroute, not via Internet
- Egress AWS traffic is NATted to a distinctive NAT pool, different from the NAT pool used for Internet access to avoid assymentic routing from the AWS cloud
- Firewalls have BGP peering with CloudConnect Routers and the local Internet routers and receive more specific public prefixes from AWS and other public providers

via CloudConnect routers. The default route points to the Internet routers which will be used as a tertiary failover for traffic to the Public Cloud

- Automatic failover between the corporate datacentres (leveraging internal DC infrastructure, usually an IGP or iBGP routing protocols), as well as to the Internet.

1.2. Transit Gateway

This Architecture relies on AWS Transit Gateway Capabilities for providing granular routing segmentation between VPC, on-premises and external networks via the Edge VPC described below.

1.3. Security Domains

This Architecture use a concept of Security Domains. A Security Domain is an abstraction builds upon AWS Transit Gateway route table concept. One or more VPCs are members in a security domain.

VPCs in a security domain can communicate with each other via Transit Gateway. Each security domain has a corresponding route table on Transit Gateway.

Two security domains are not connected by default i.e. a VPC in one domain has no connectivity to another VPC in a different domain. Connection policy must be specified to connect the two domains so that VPCs in each domain can communicate with each other. The Security Domains are conceptually similar to security zones and VRFs in traditional on-premises network segmentation.

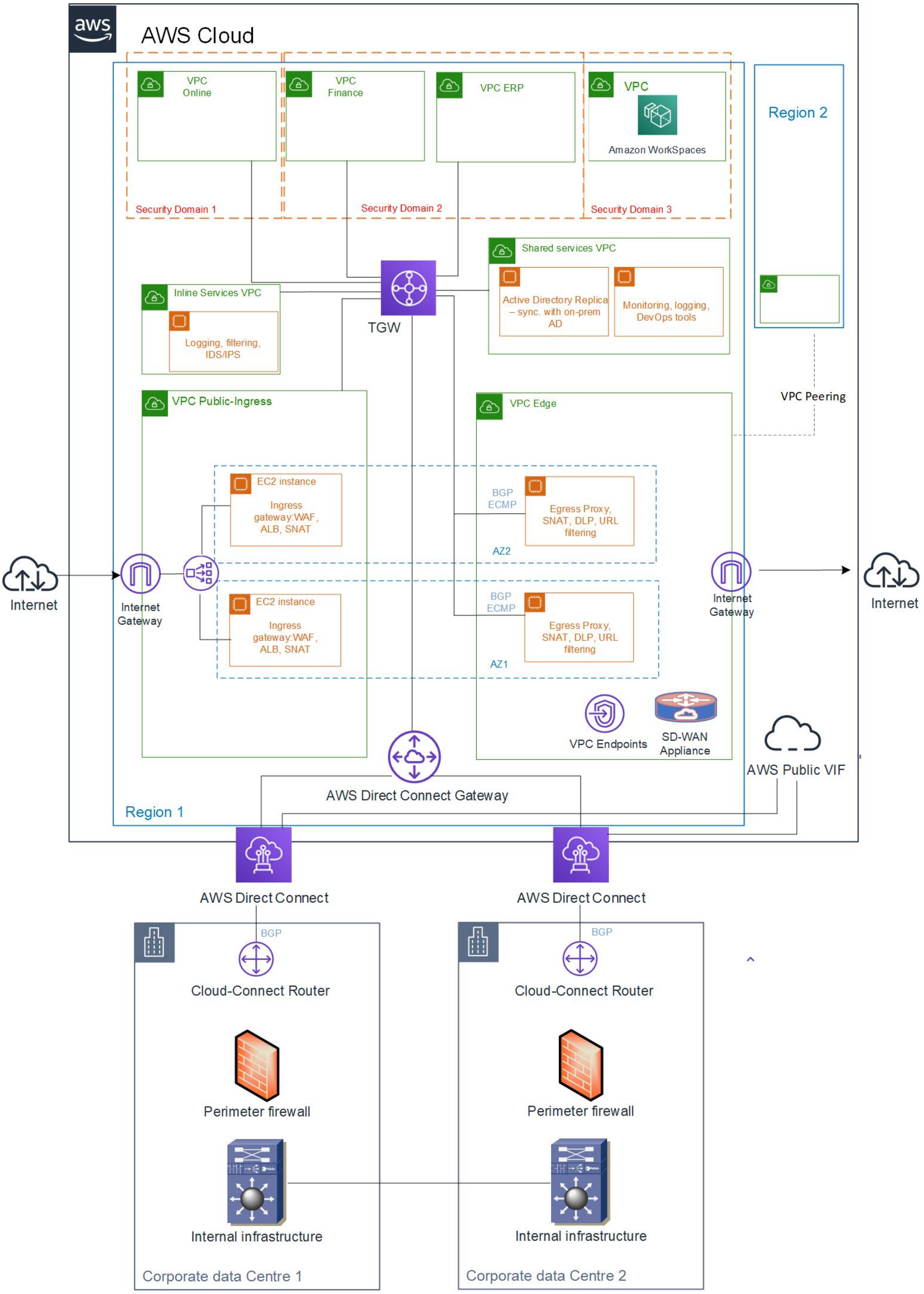
Within the security domain traffic is restricted by using AWS Security Groups and, if necessary, Network ACLs.

In the diagram below, AWS VPCs are grouped into the following domains:

- **Application domains** (split into Security domains, each may contain one or more VPCs in different accounts)
- **Shared Services domain** – Centralised DevOps tools, monitoring, logging. In addition, an EC2 instance running Active Directory Replica for user authentication (this is also needed for AWS Workspaces) is deployed in this VPC.
- **Public-Ingress domain.** The proposed solution places WAF appliance at the Internet perimeter for all inbound connections to web facing applications. Autoscaling groups of EC2 instances will perform two functions, the first being as the inbound firewall, and the second, as the load balancer for the web tier (AWS WAF can also be considered as an alternative solution)
- **Edge domain** providing connectivity to external networks such as:
    - Internet
    - AWS VPC Endpoints (both Interface and Gateway Endpoints)
    - PrivateLink Endpoints to third-party providers
    - Corporate WAN if a SD-WAN appliance is deployed (can be in a different domain)
    - Client VPN access (can be in a different domain)
    - Connectivity to IaaS infrastructure from other Cloud Providers either using SD-WAN or point-to-point IPSec VPN tunnels

The functions of the Edge domain are to perform packet inspection, Content and URL filtering, DLP, IPS/IDS. At least two instances (usually NGFW, can be from the same vendor that NGFW deployed on-premises) which run VPN with BGP ECMP Support are deployed in different AZ. This allows for horizontally scaling, so traffic will be distributed equally across a large number of EC2 instances. SNAT is required on the instances to ensure symmetric traffic flow.

- **Inline Services** for providing inter-VPC connectivity performing packet filtering, IDS/IPS and logging functions (similar to Edge Domain). Note the network design can be different, as Source NATting may not be appropriate.

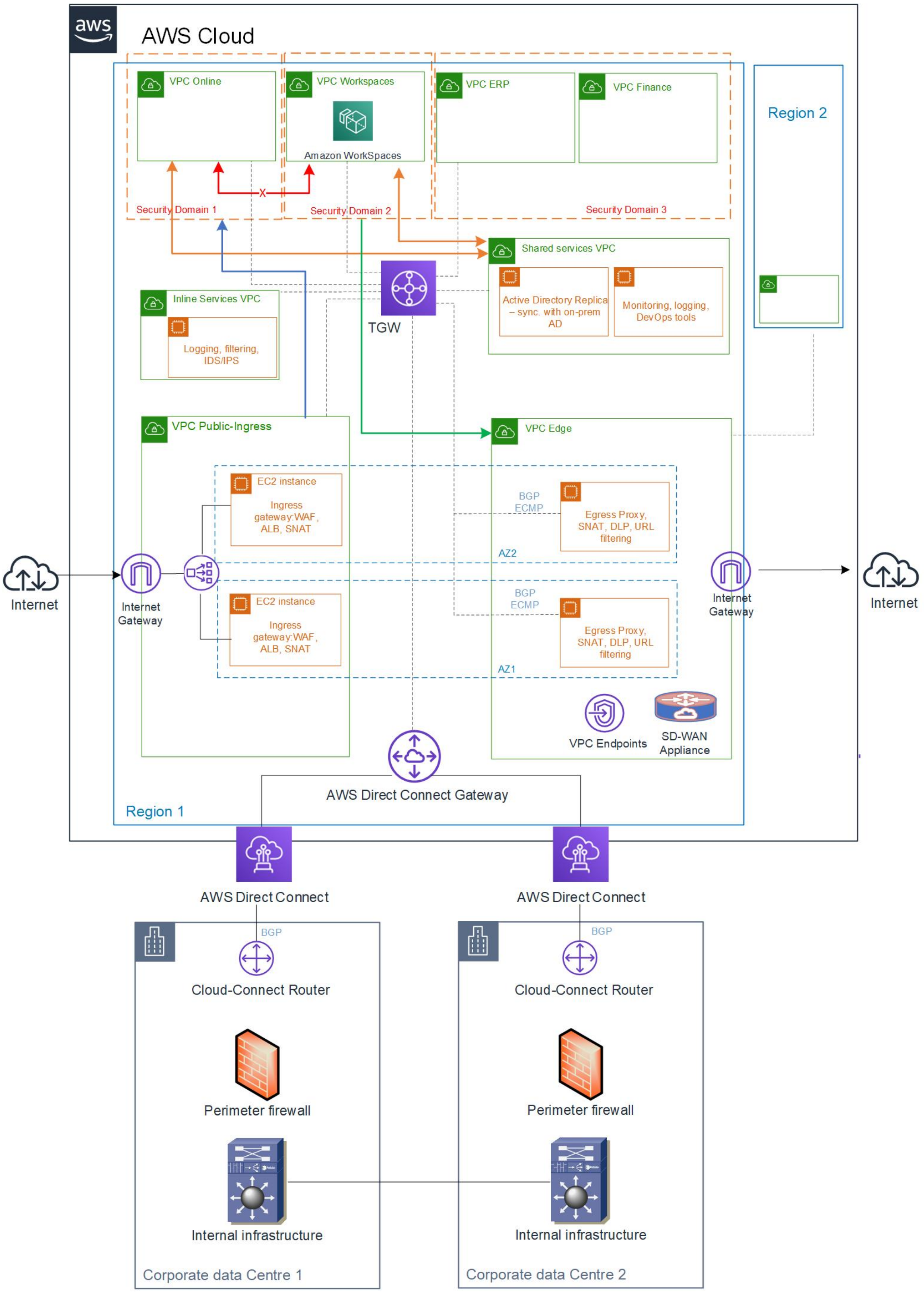

aws
AWS Cloud
VPC Online
VPC Finance
VPC ERP
VPC
Amazon WorkSpaces
Security Domain 1
Security Domain 2
Security Domain 3
Region 2
Shared services VPC
Active Directory Replica – sync. with on-prem AD
Monitoring, logging, DevOps tools
Inline Services VPC
Logging, filtering, IDS/IPS
TGW
VPC Public-Ingress
VPC Edge
VPC Peering
EC2 instance
Ingress gateway:WAF, ALB, SNAT
BGP ECMP
Egress Proxy, SNAT, DLP, URL filtering
AZ2
Internet
Internet Gateway
Internet Gateway
Internet
EC2 instance
Ingress gateway:WAF, ALB, SNAT
BGP ECMP
Egress Proxy, SNAT, DLP, URL filtering
AZ1
VPC Endpoints
SD-WAN Appliance
AWS Public VIF
AWS Direct Connect Gateway
Region 1
AWS Direct Connect
AWS Direct Connect
BGP
Cloud-Connect Router
BGP
Cloud-Connect Router
Perimeter firewall
Perimeter firewall
Internal infrastructure
Internal infrastructure
Corporate data Centre 1
Corporate data Centre 2

1.4. Traffic flows

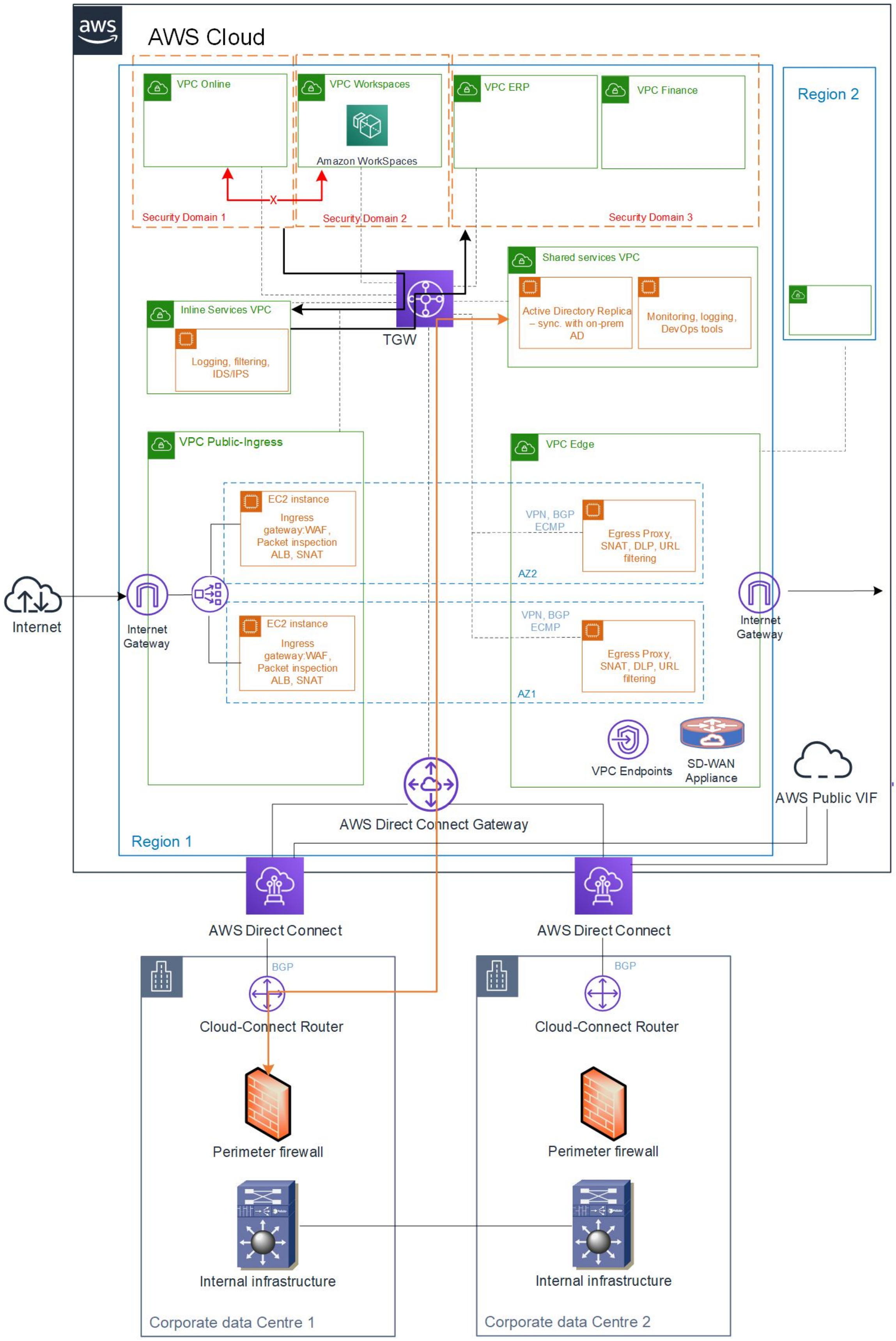
Each VPC in the same domain can communicate with each other via AWS Transit Gateway.

VPCs in Online VPC domain cannot communicate with VPCs in Finance VPC (so no East-West Traffic is allowed by default), while all VPCs can communicate with Shared service domain and Edge domain.

This is shown on the diagram below:



If there is a requirement to connect two VPCs directly, an Inline services domain can be used. Traffic to on-premises IP addresses is not directed via the Inline services or Edge Domain, as it is be inspected by the on-premises Perimeter firewall:



1.5. Cross-region Connectivity

Cross-region Connectivity is achieved via VPC peering between Edge VPCs in different Regions. An alternative solution is to leverage Private VIFs in different regions, but this solution has some limitations (VGWs should be in the same account)

1.6. Azure and GCP connectivity

Since GCP/Azure have low bandwidth requirements, it is assumed the direct connectivity is not needed at this stage, and VPN tunnels built from the two main Datacentres would be enough. Due to the same reason, traffic from any sources including branches and AWS VPC to Azure and GCP IaaS resources (which use private IP addresses) is backhauled to the local Datacentres, inspected and then directed via the VPN tunnels.

Traffic to Microsoft and Google SaaS applications and API endpoints available via Internet use the local Internet access (including traffic from AWS IaaS workloads). Security is provided on the application level (TLS encryption, API keys, PKI, etc)

However, if this requirement changes in the future, direct links can be deployed for the Datacentres, and SD-WAN appliances can be deployed in Azure and GCP to providing direct access for Stores and Warehouses. Leveraging the existing Architecture described in this document, this will not require any network redesign.

1.7. Security

To further secure AWS workloads and corporate data the following is recommended:

- AWS provide a good list of general security recommendations in their Whitepapers
- AWS-native tools such as AWS Guard Duty, AWS Inspector, as well as automated frameworks utilising these tools should be used
- Workload firewall and host-based IDS/IPS, centrally managed
- Centralised logging and application visibility
- It is also worth considering Cloud Access Security Broker (CASB) solutions