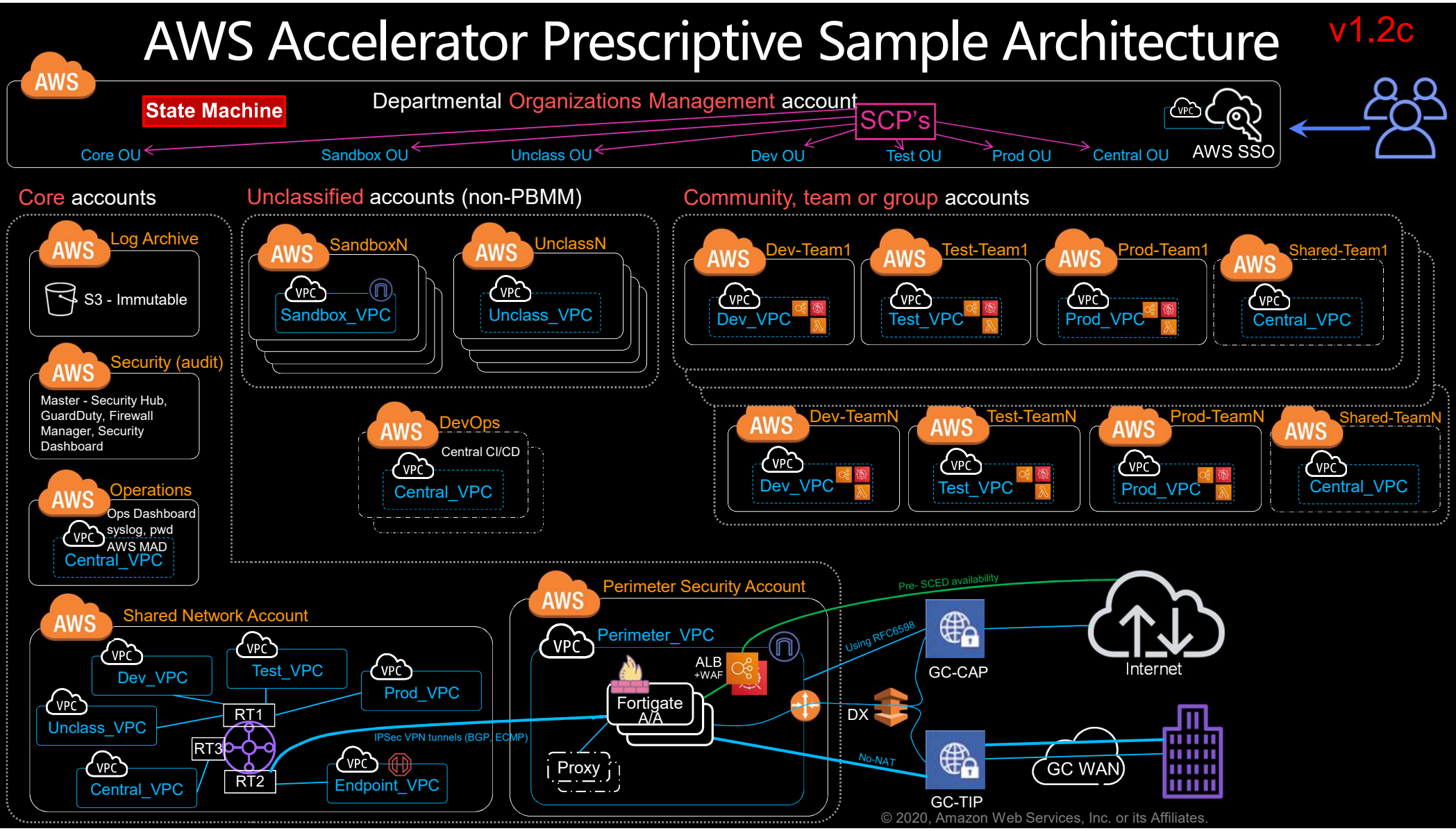
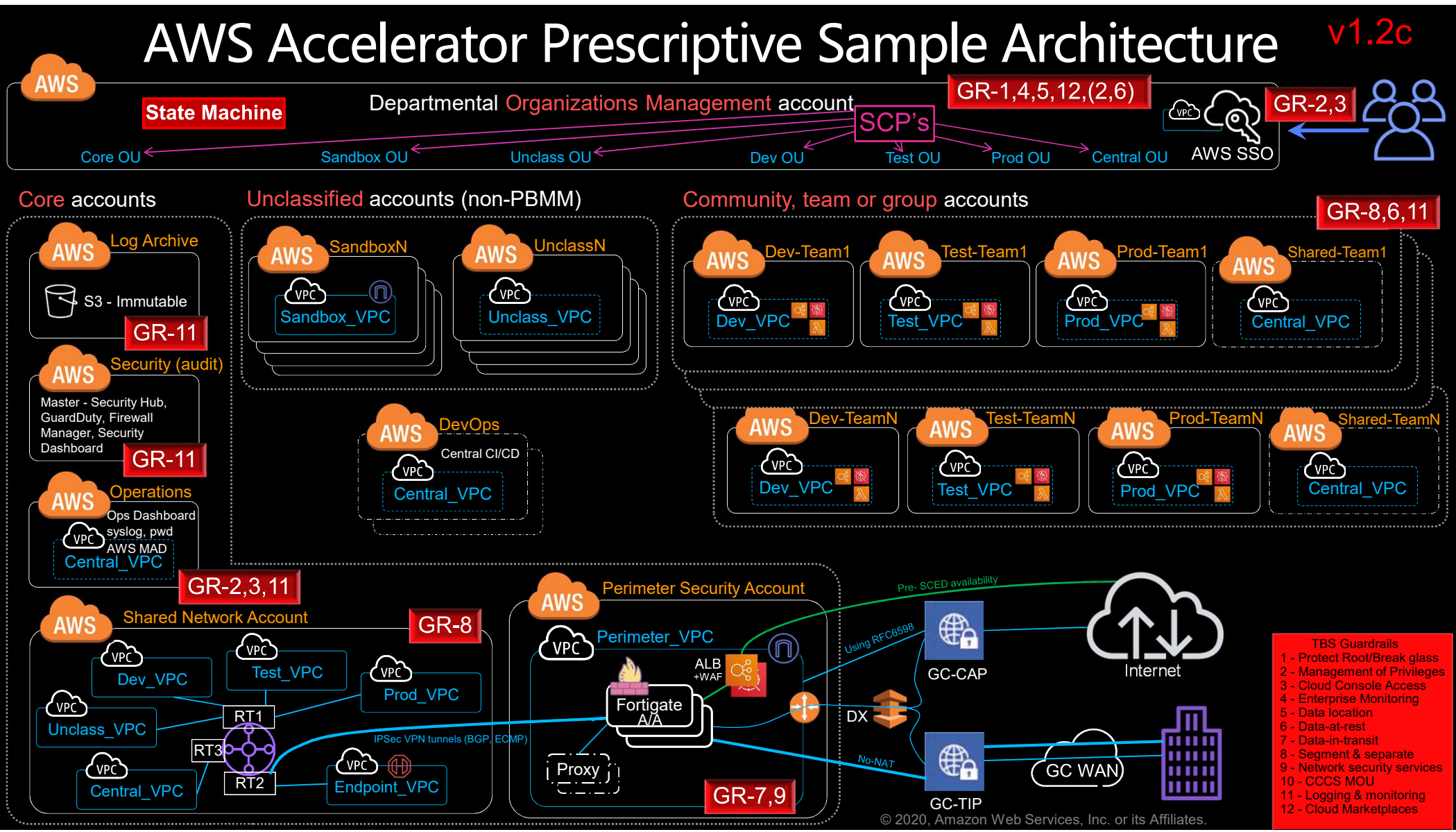
AWS Accelerator Prescriptive Sample Architecture

v1.2c



AWS Accelerator Prescriptive Sample Architecture

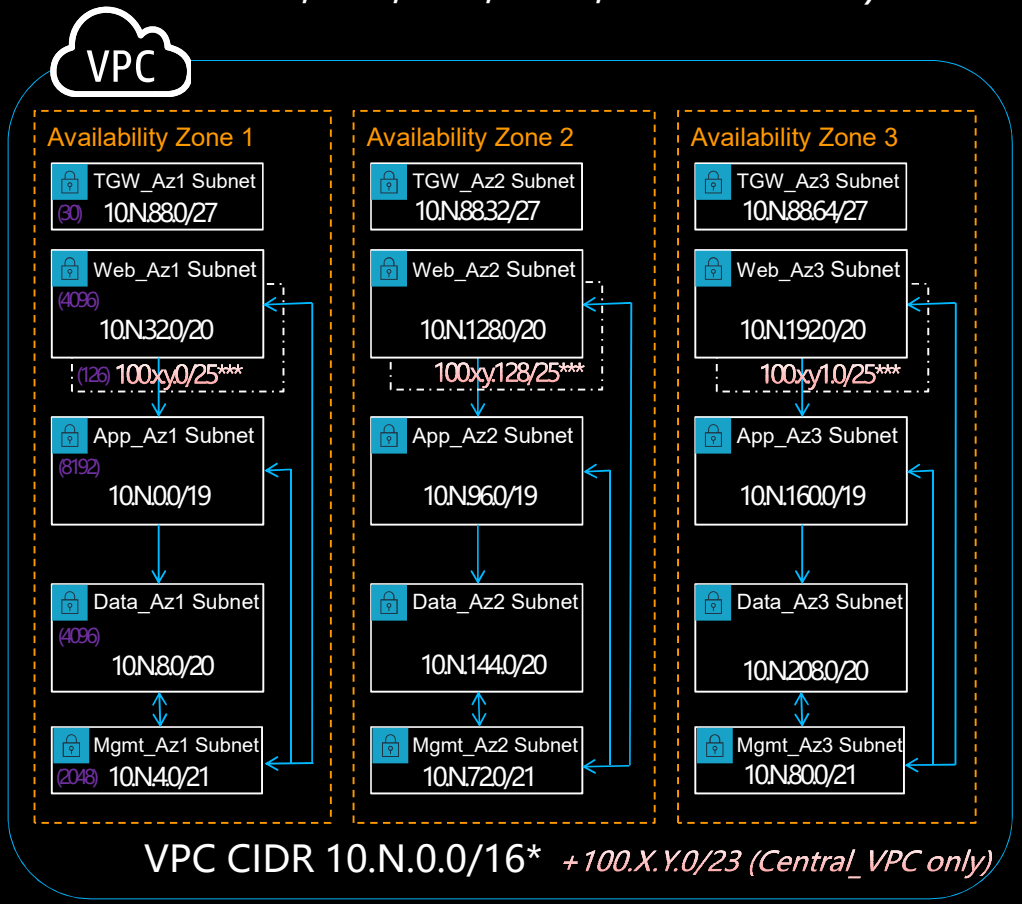
v1.2c



AWS Accelerator Standard VPC Design

v1.2

(Used for Unclass, Dev, Test, Prod, Central VPC's) - Class B (Half Class B option exists)



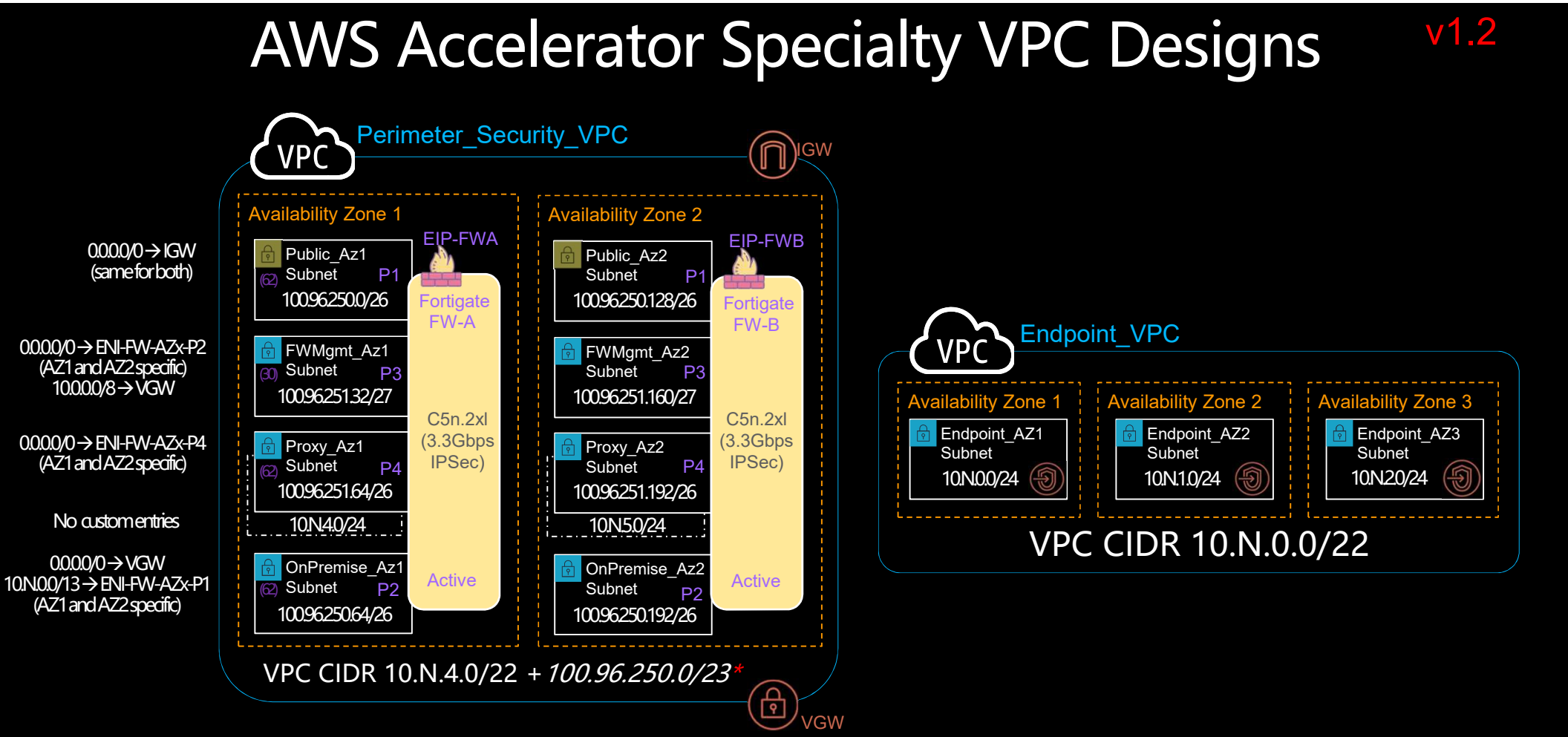
NOTE: Subnets are NOT ZIP's. Security Groups are being used as the zoning boundary/ZIP. This design leverages the concept of many micro-ZIP's, potentially one per application, per zone.

NOTE: TGW subnets are not shared. Sandbox_VPC drops the TGW subnets, Web subnets become public w/IGW and NATGW for private subnets. Central VPC RFC6598 subnets named GCWide_azX.

* We are assigning a full /16 to each VPC (i.e. 10.10.0.0/16 for Dev, 10.11.0.0/16 for Test, etc.). Customer can optionally use other RFC1918 CIDR blocks. It is critical these CIDR ranges do not conflict with a departments on premise CIDR ranges as there is NO NAT'ing for ground to cloud communications (mark as "used for cloud" in the departments on premise IPAM system).
** Note: 10.N.224.0/19, 10.N.88.96-10.N.95.255, and 100.x.y1.128/25 are available for future assignment.
*** The Central VPC CIDR has been extended with a RFC6598 CIDR range (internal web subnets) to host MAD and other services that may require cross departments access.

AWS Accelerator Specialty VPC Designs

v1.2



* 100.96.250.0/23 is a sample RFC6598 block, customers must each use their own block assigned by SSC. Departments also need SSC to assign unique BGP ASN's.
** Note: 10.n.4.0/22 must be used to created VPC as you cannot extend a 100.* subnet block, this is a FortiSandbox detonation subnet
*** Additional 100.96.252.0/23 needed for the overlay network (Fortigates inside VPN tunnel). Before GCCAP available, Public subnet will hold ELB's for public facing applications.
**** Remaining available addresses: 100.96.251.0/27 and 100.96.251.128/27 (32 per AZ)

AWS Accelerator NACL and Security Group Design (Default)

v1.2