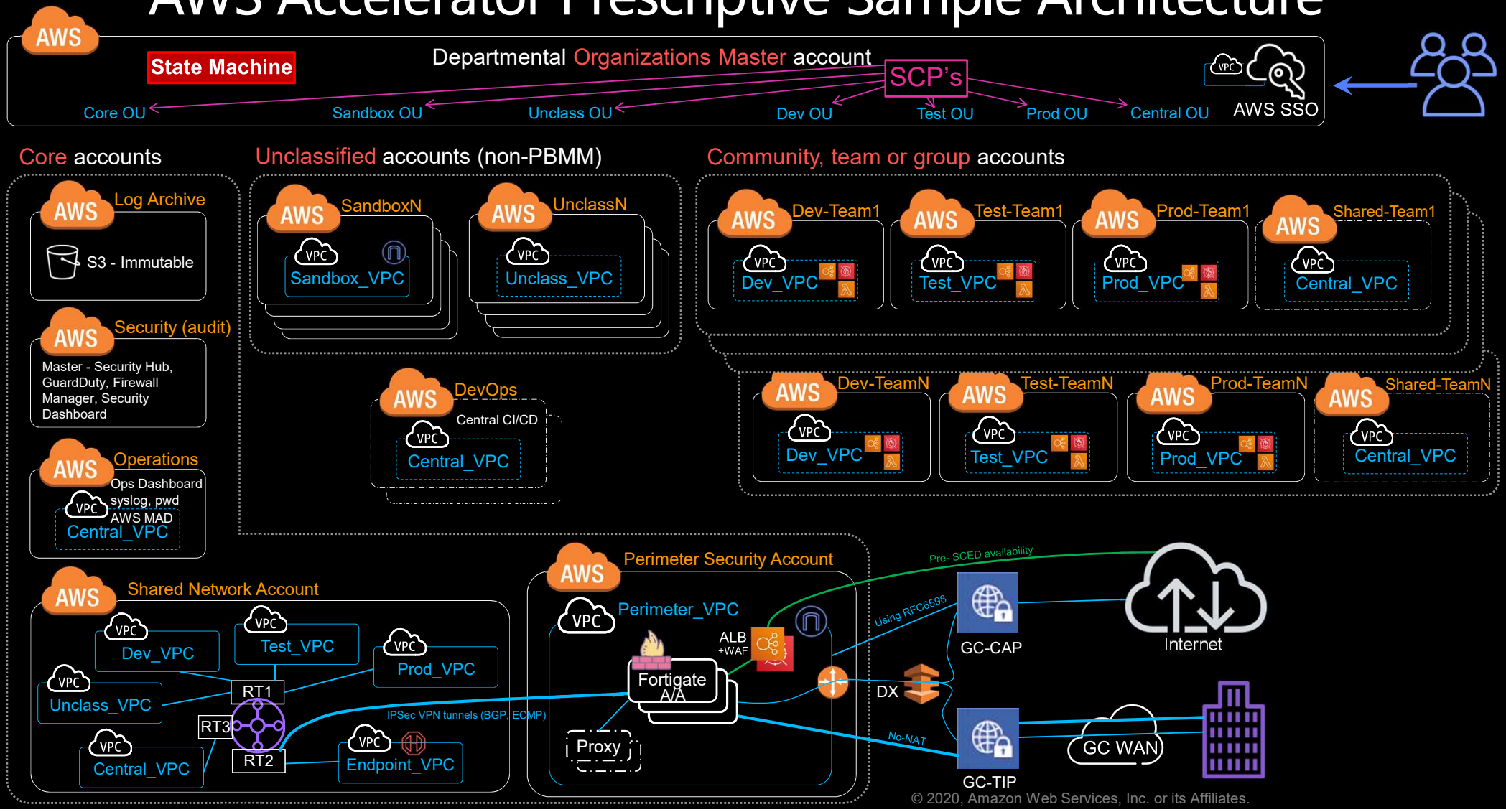
# AWS Accelerator Prescriptive Sample Architecture

v1.2c



# AWS Accelerator Prescriptive Sample Architecture

v1.2c

State Machine

Departmental Organizations Master account

SCP's

GR-1,4,5,12,(2,6)

GR-2,3

Core OU | Sandbox OU | Unclass OU | Dev OU | Test OU | Prod OU | Central OU

AWS SSO

## Core accounts

- Log Archive
  - S3 - Immutable
  - GR-11
- Security (audit)
  - Master - Security Hub, GuardDuty, Firewall Manager, Security Dashboard
  - GR-11
- Operations
  - Ops Dashboard
  - syslog, pwd
  - AWS MAD
  - Central_VPC
  - GR-2,3,11
- Shared Network Account
  - GR-8
  - Dev_VPC
  - Test_VPC
  - Prod_VPC
  - Unclass_VPC
  - Central_VPC
  - Endpoint_VPC
  - RT1
  - RT2
  - RT3
  - IPSec VPN tunnels (BGP, ECMP)

## Unclassified accounts (non-PBMM)

- SandboxN
  - Sandbox_VPC
- UnclassN
  - Unclass_VPC
- DevOps
  - Central CI/CD
  - Central_VPC

## Community, team or group accounts

GR-8,6,11

- Dev-Team1
  - Dev_VPC
- Test-Team1
  - Test_VPC
- Prod-Team1
  - Prod_VPC
- Shared-Team1
  - Central_VPC
- Dev-TeamN
  - Dev_VPC
- Test-TeamN
  - Test_VPC
- Prod-TeamN
  - Prod_VPC
- Shared-TeamN
  - Central_VPC

## Perimeter Security Account

- Perimeter_VPC
- ALB +WAF
- Fortigate A/A
- Proxy
- GR-7,9

Pre- SCED availability

Using RFC6598

No-NAT

DX

GC-CAP

GC-TIP

Internet

GC WAN

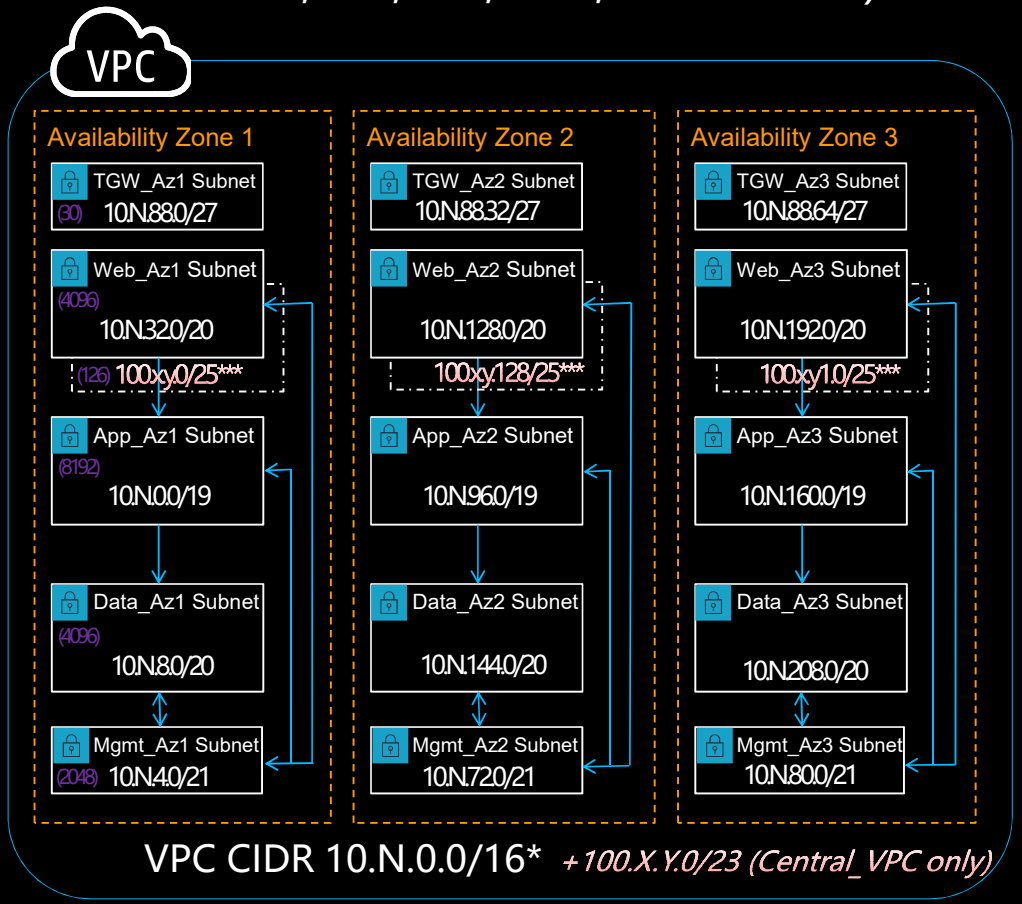
TBS Guardrails

1 - Protect Root/Break glass
2 - Management of Privileges
3 - Cloud Console Access
4 - Enterprise Monitoring
5 - Data location
6 - Data-at-rest
7 - Data-in-transit
8 - Segment & separate
9 - Network security services
10 - CCCS MOU
11 - Logging & monitoring
12 - Cloud Marketplaces

# AWS Accelerator Standard VPC Design

v1.2

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



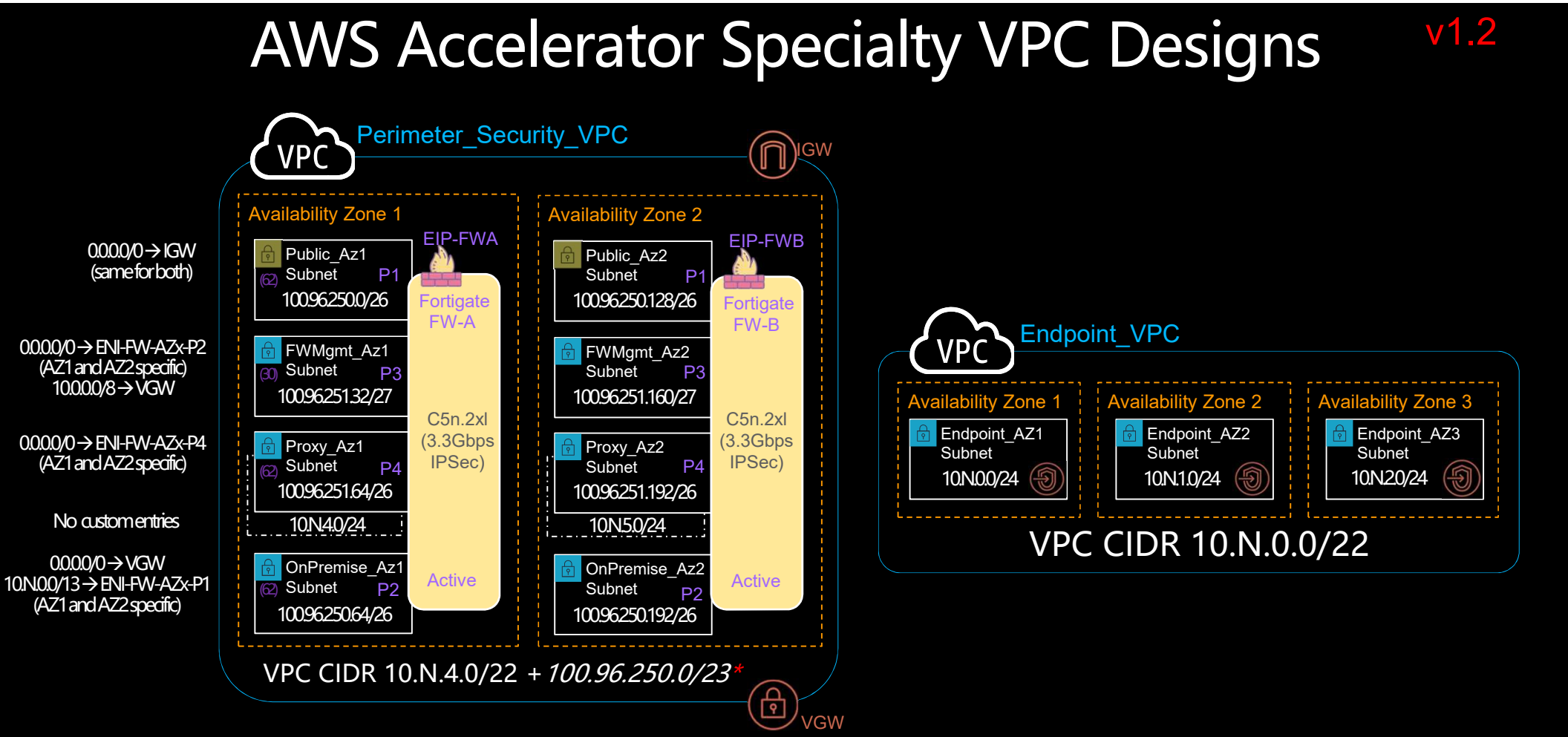

NOTE: Subnets are NOT ZIP's. Security Groups are being used as the zoning boundary/ZIP. This design leverages the concept of many micro-ZIP's, potentially one per application, per zone.

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