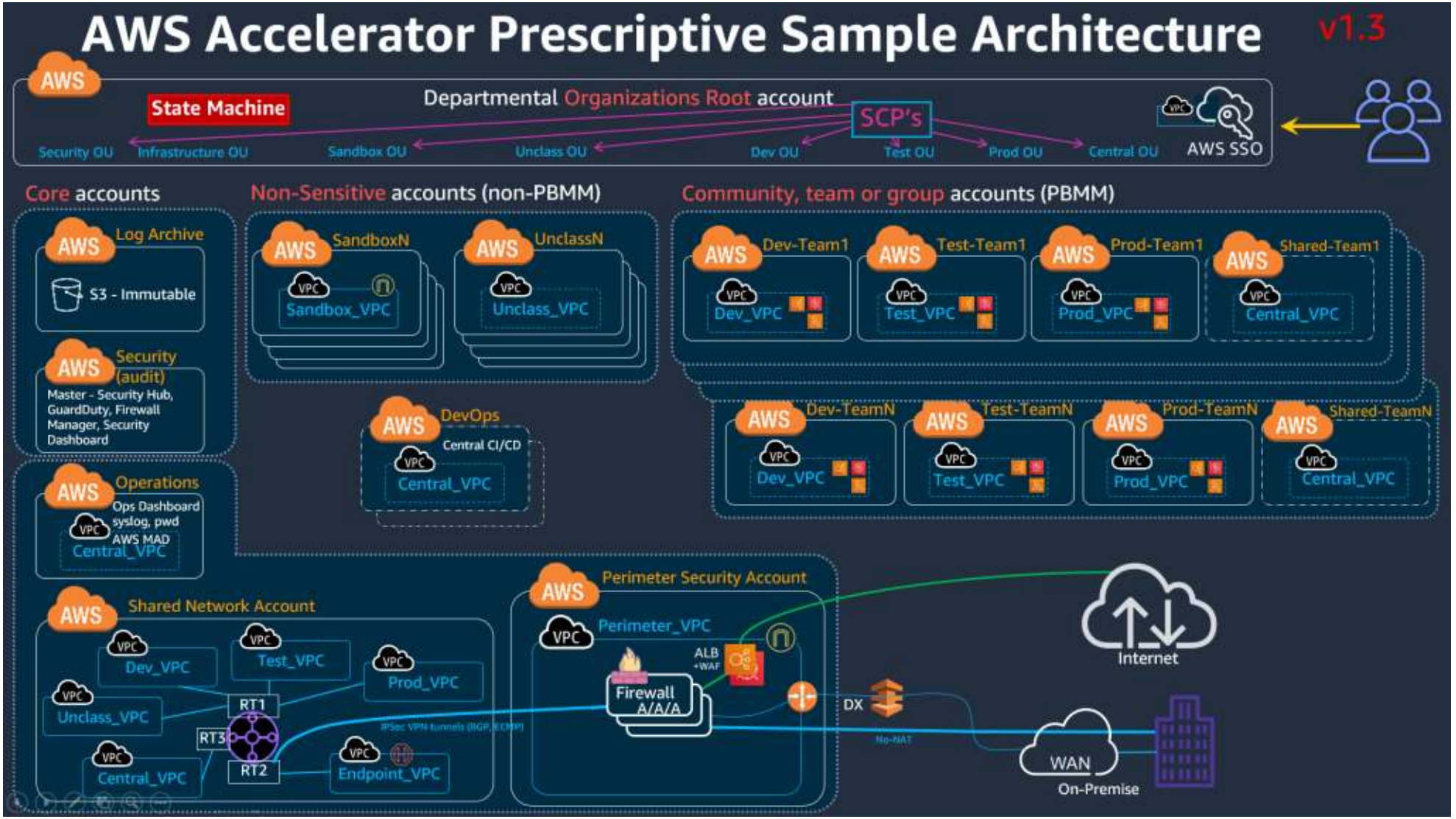
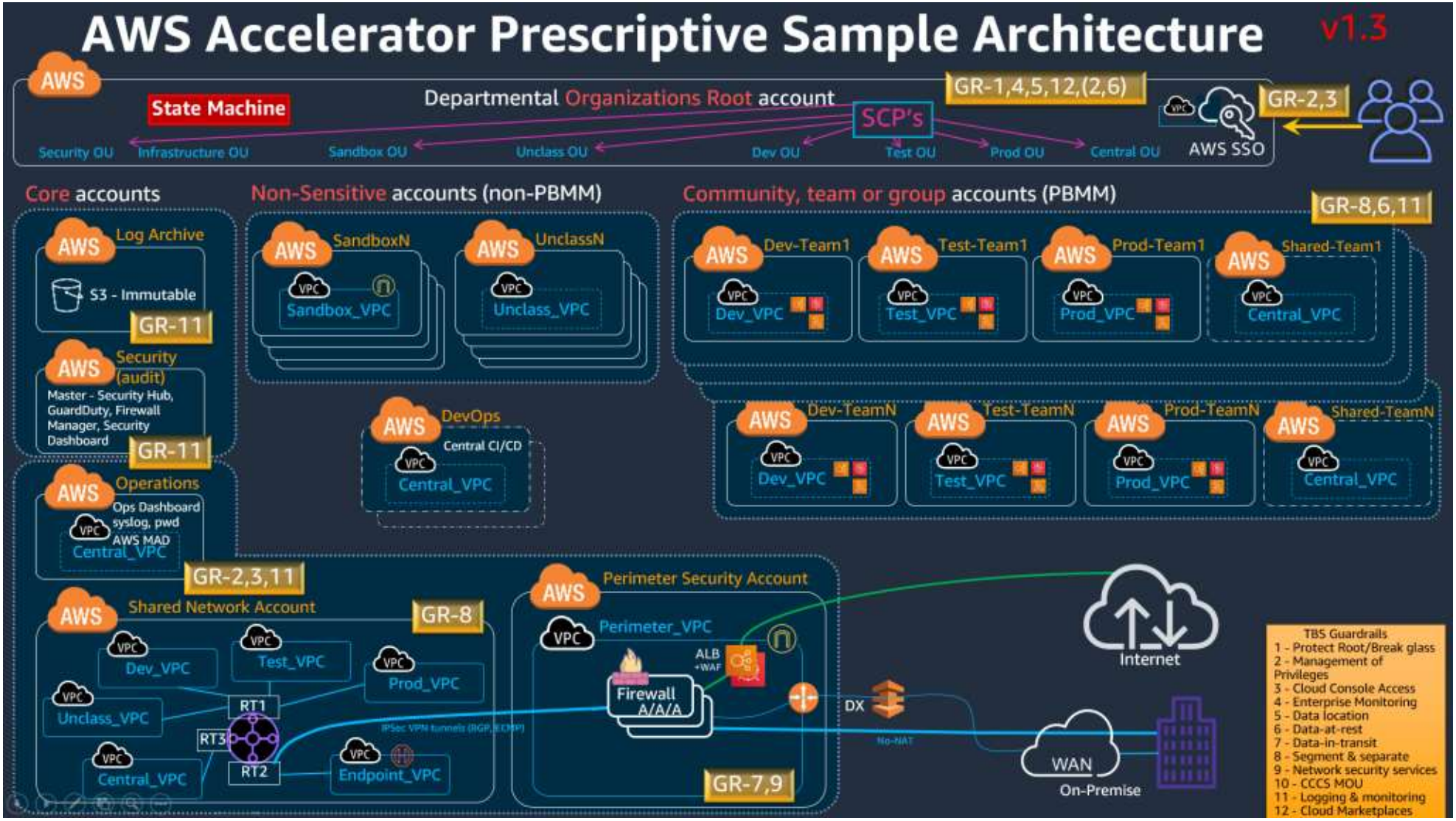
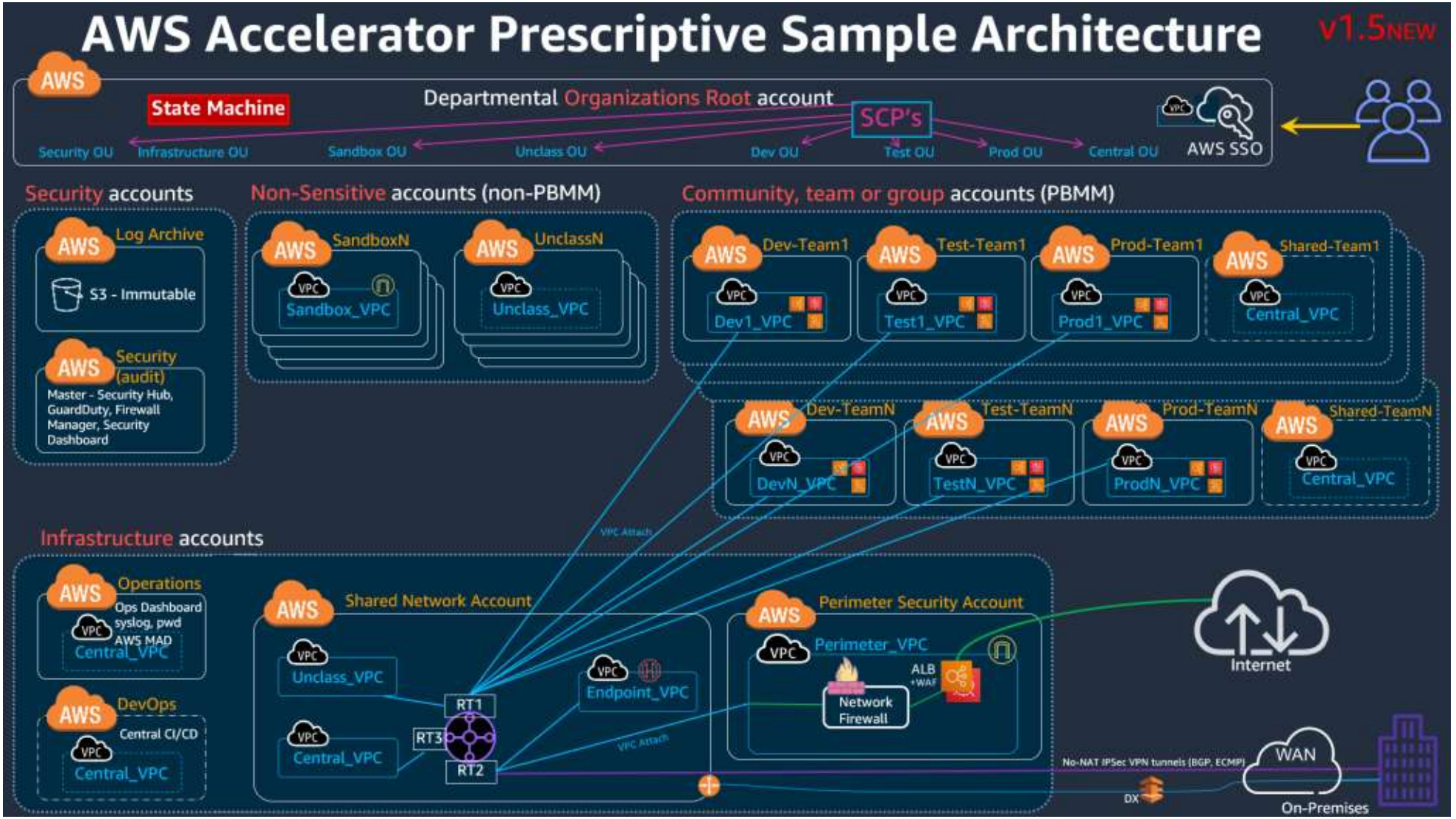
AWS Accelerator Prescriptive Sample Architecture

Shared VPC Architecture

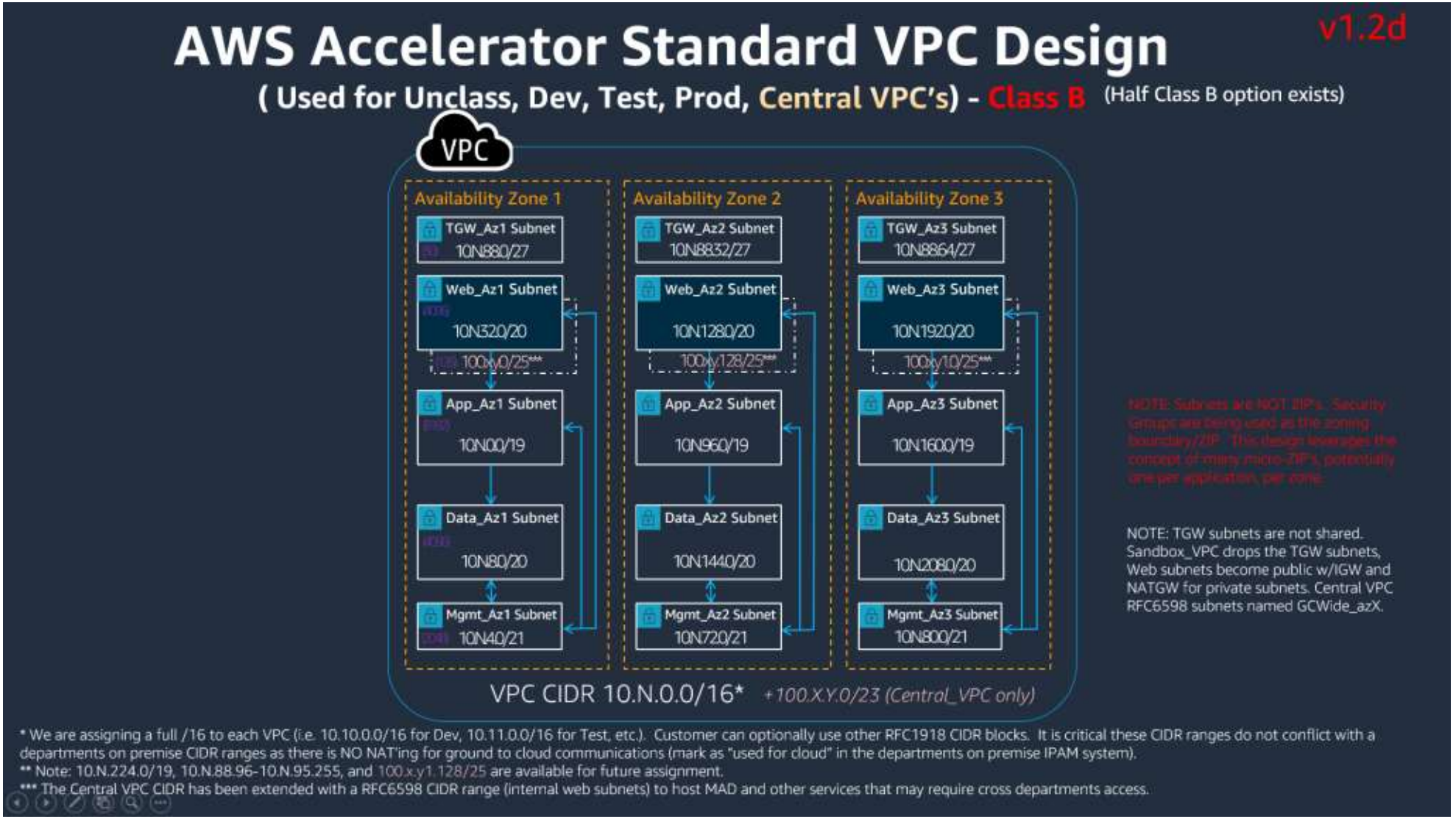


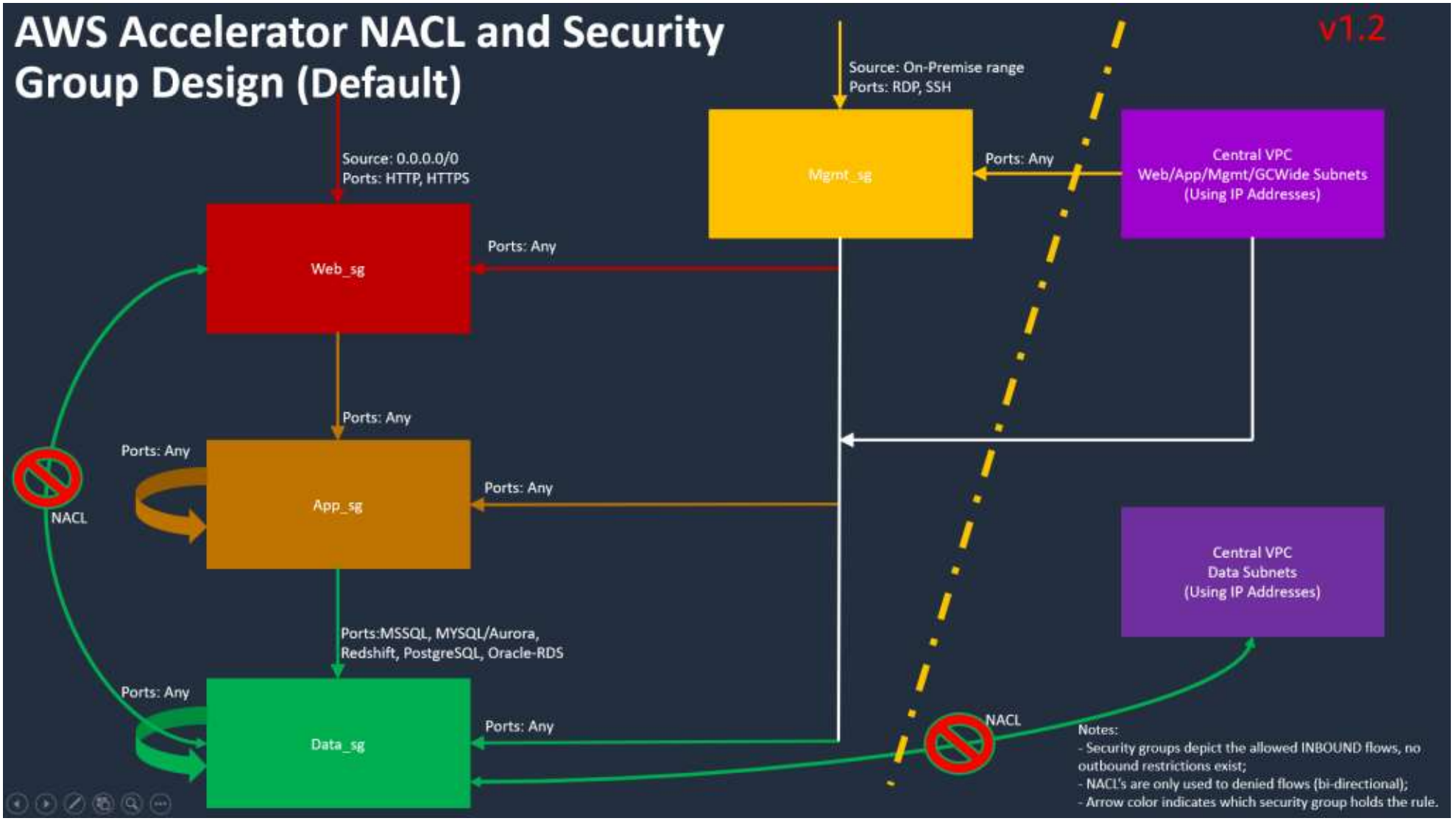

AWS Accelerator Prescriptive Sample Architecture
v1.3
AWS
State Machine
Departmental Organizations Root account
GR-1,4,5,12,(2,6)
SCP's
GR-2,3
AWS SSO
Security OU
Infrastructure OU
Sandbox OU
Unclass OU
Dev OU
Test OU
Prod OU
Central OU
Core accounts
Non-Sensitive accounts (non-PBMM)
Community, team or group accounts (PBMM)
GR-8,6,11
Log Archive
S3 - Immutable
GR-11
Security (audit)
Master - Security Hub, GuardDuty, Firewall Manager, Security Dashboard
GR-11
SandboxN
Sandbox_VPC
UnclassN
Unclass_VPC
Dev-Team1
Dev_VPC
Test-Team1
Test_VPC
Prod-Team1
Prod_VPC
Shared-Team1
Central_VPC
DevOps
Central CI/CD
Central_VPC
Dev-TeamN
Test-TeamN
Prod-TeamN
Shared-TeamN
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
RT1
RT3
RT2
Central_VPC
Endpoint_VPC
IPSec VPN tunnels (BGP, 8 CIDR)
Perimeter Security Account
Perimeter_VPC
ALB +WAF
Firewall A/A/A
GR-7,9
DX
No-NAT
Internet
WAN
On-Premise
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

Spoke VPC Architecture



VPC and Security Group Patterns

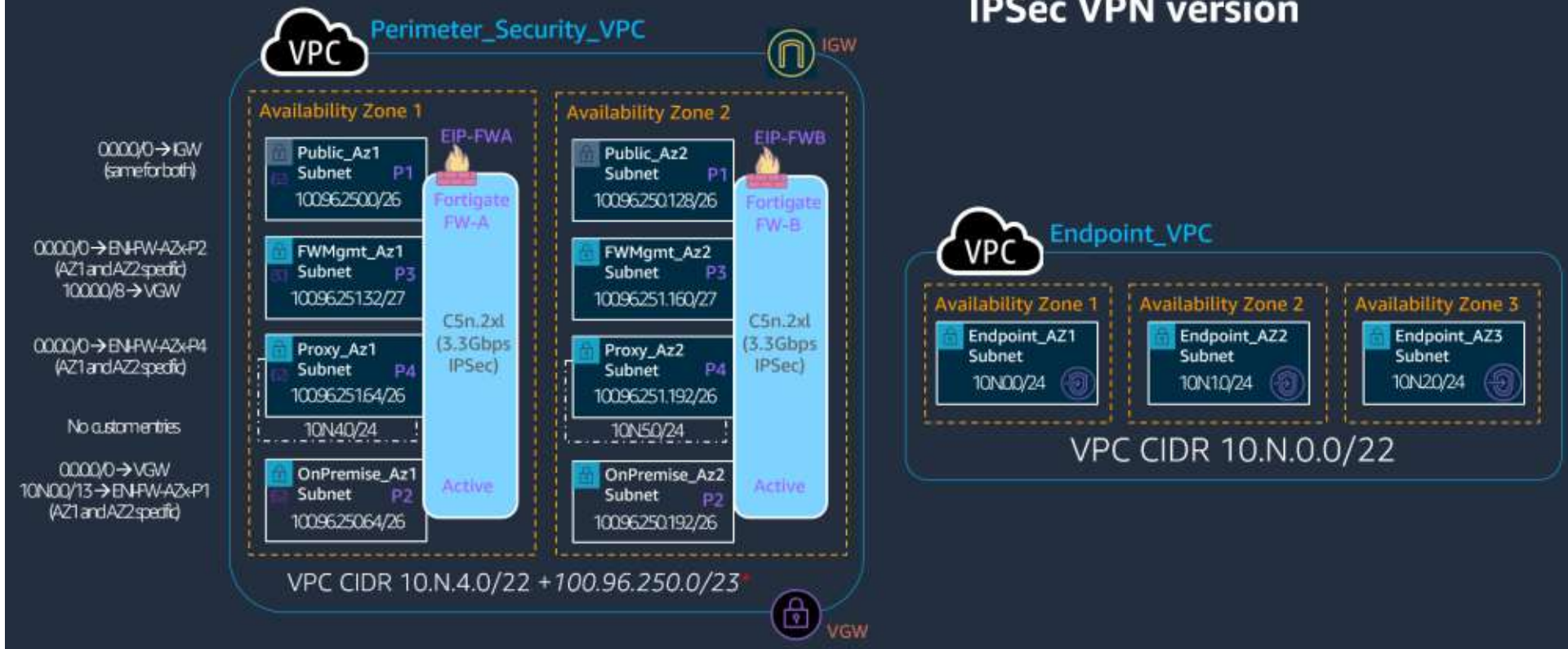



AWS Accelerator NACL and Security Group Design (Default)
v1.2
Source: On-Premise range
Ports: RDP, SSH
Source: 0.0.0.0/0
Ports: HTTP, HTTPS
Mgmt_sg
Ports: Any
Central VPC
Web/App/Mgmt/GCWide Subnets
(Using IP Addresses)
Web_sg
Ports: Any
Ports: Any
Ports: Any
NACL
App_sg
Ports: Any
Central VPC
Data Subnets
(Using IP Addresses)
Ports:MSSQL, MYSQL/Aurora,
Redshift, PostgreSQL, Oracle-RDS
Ports: Any
Data_sg
Ports: Any
NACL
Notes:
- Security groups depict the allowed INBOUND flows, no outbound restrictions exist;
- NACL's are only used to denied flows (bi-directional);
- Arrow color indicates which security group holds the rule.

AWS Accelerator Specialty VPC Designs

v1.2

IPSec VPN version



* 100.96.250.0/23 is a sample RFC 6598 block; customers must each use their own block assigned by SSE. Departments also need SSE to assign unique BGP ASNs.

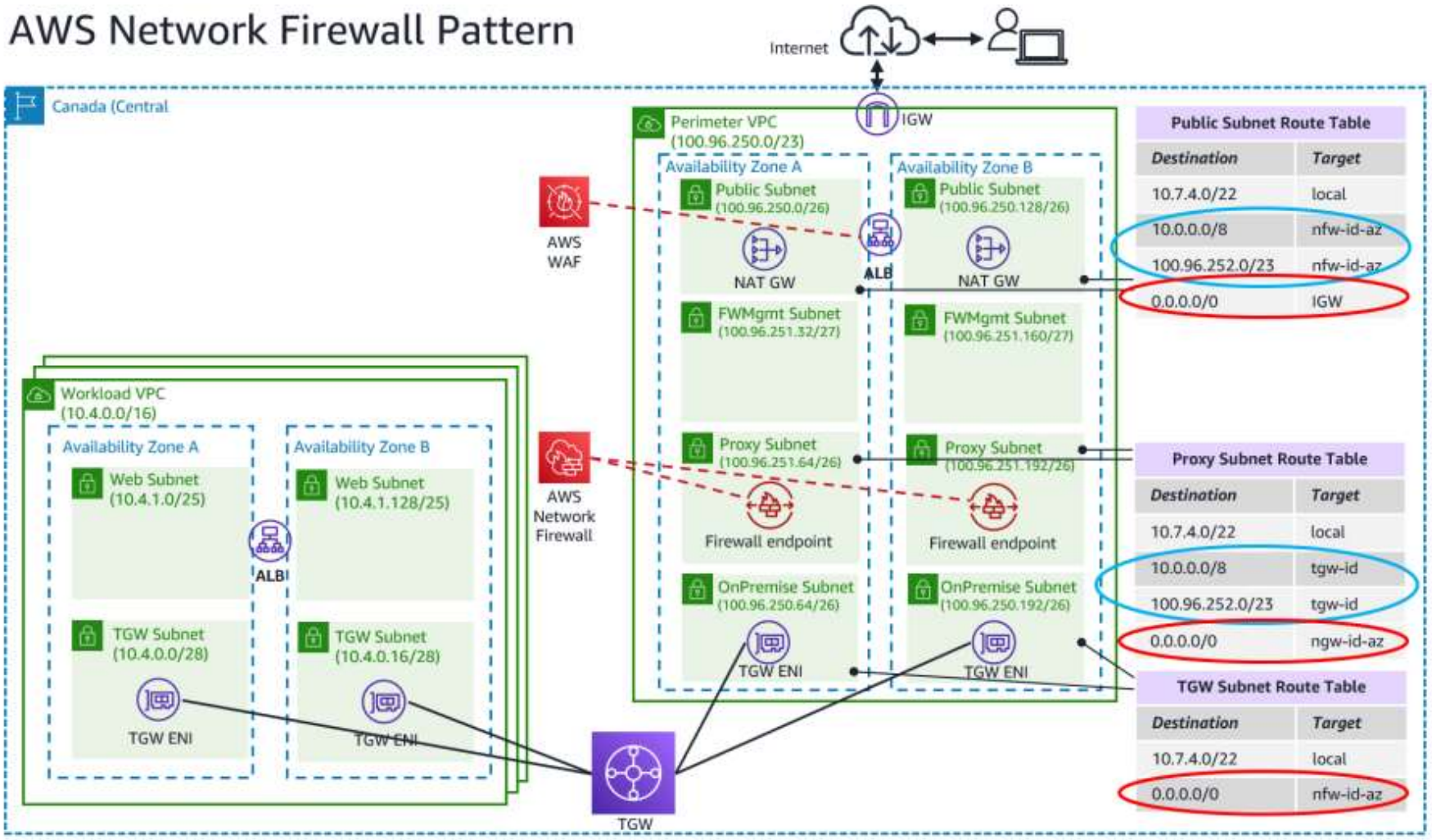
** Note: 10.n.4.0/22 must be used to created VPC as you cannot extend a 100.* subnet block, this is a FortiSandbox detonation subnet

*** 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)

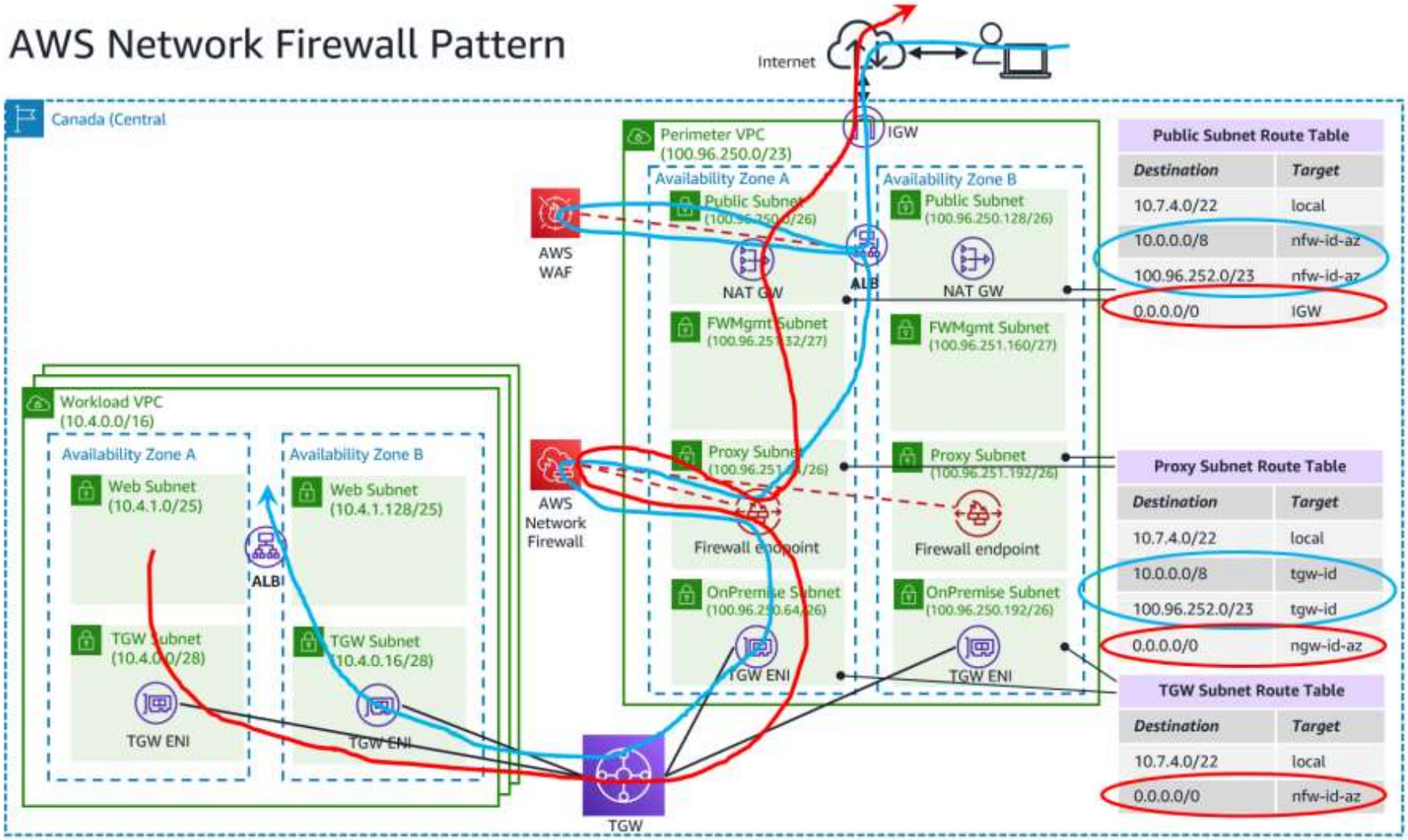
aws migrations

Additional Perimeter Patterns



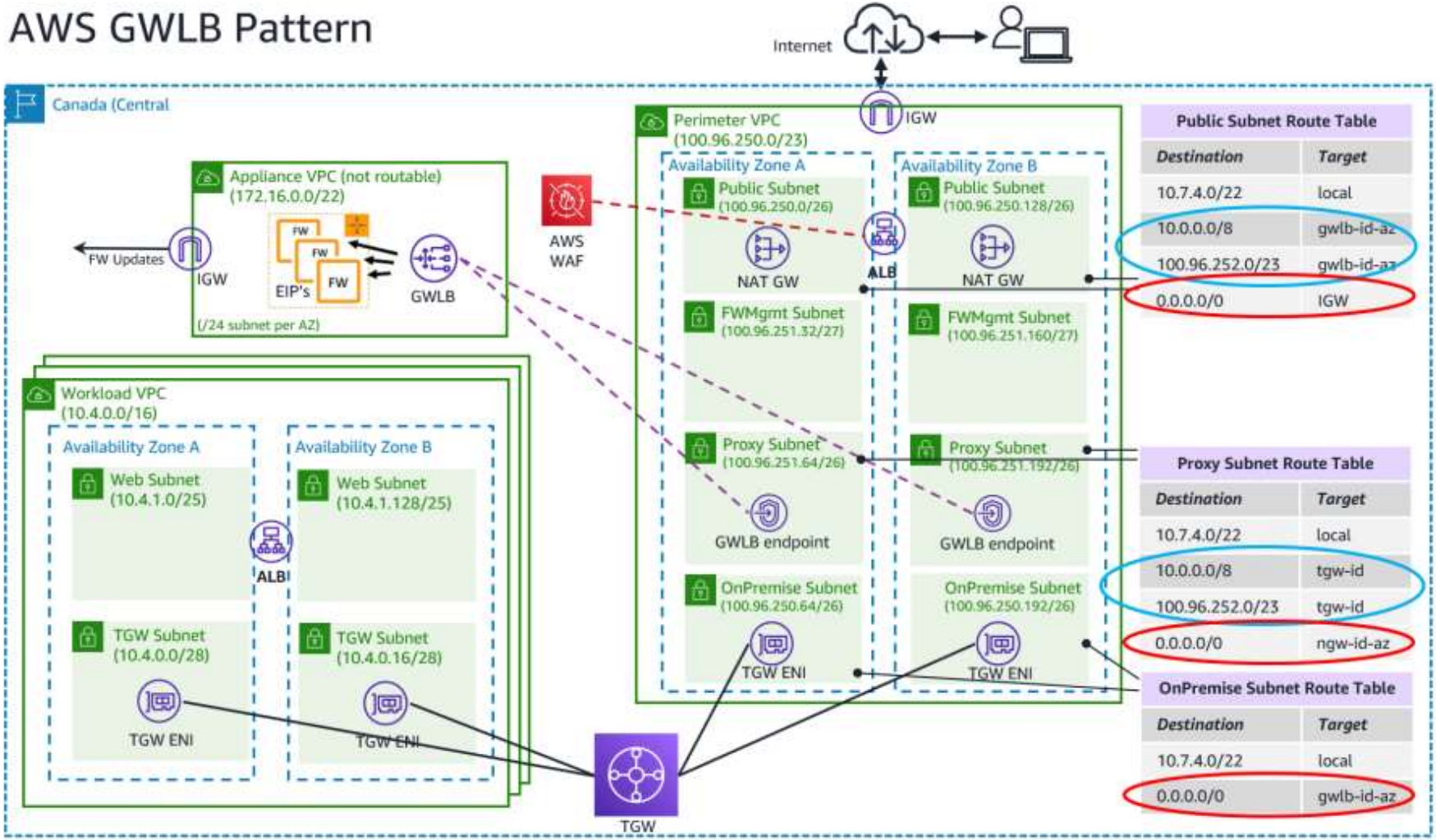
NOTE1: Distinct route tables required per AZ, which targets the local AZ's nfw, gwlb or ngw endpoint

AWS Network Firewall Pattern



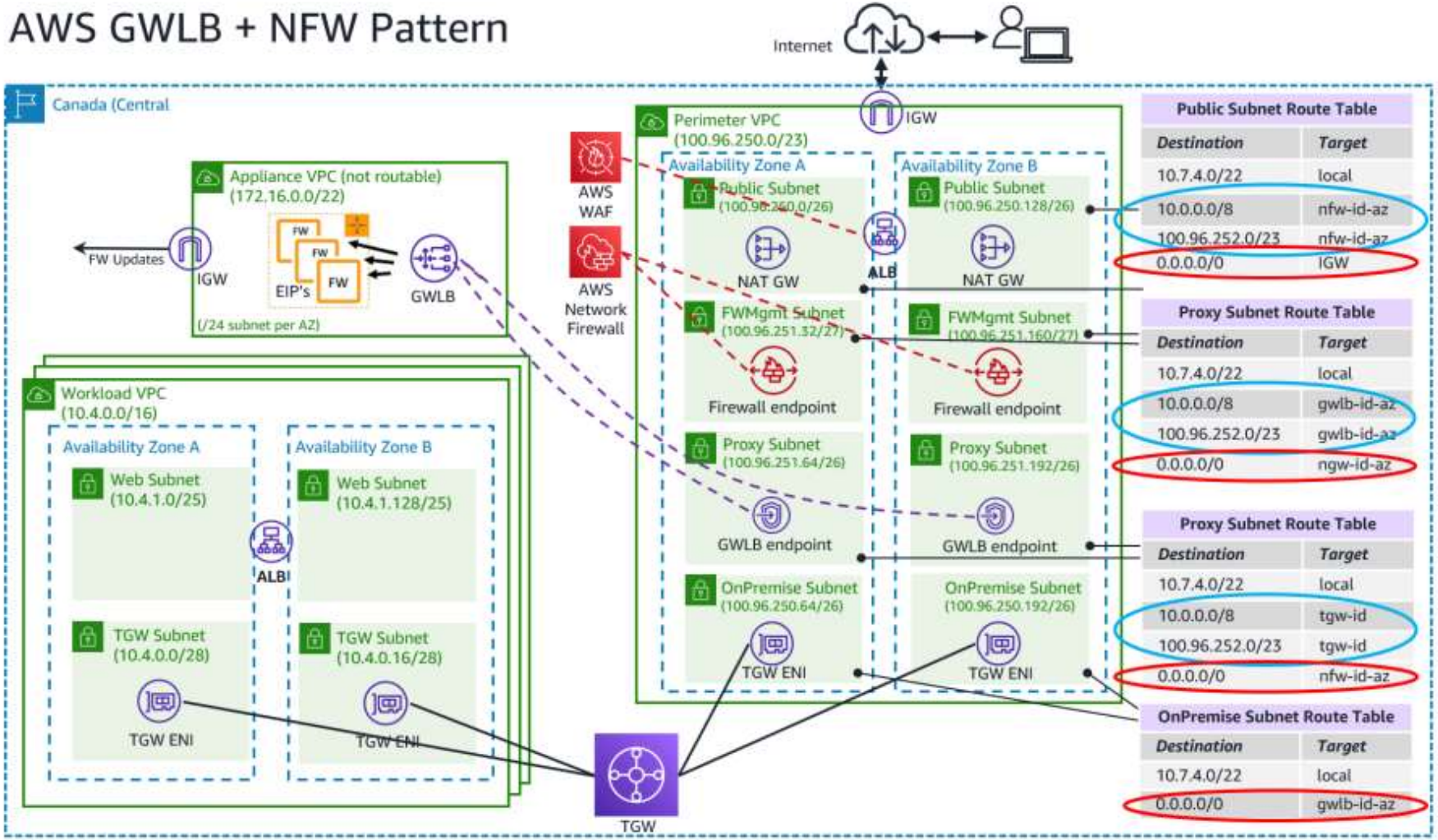
NOTE1: Distinct route tables required per AZ, which targets the local AZ's nfw, gwlb or ngw endpoint

AWS GWLB Pattern



NOTE1: Distinct route tables required per AZ, which targets the local AZ's nfw, gwlb or ngw endpoint

AWS GWLB + NFW Pattern



NOTE1: Distinct route tables required per AZ, which targets the local AZ's nfw, gwlb or ngw endpoint