# Multi-Cloud Network Segmentation (MCNS) & FireNet

aviatrix

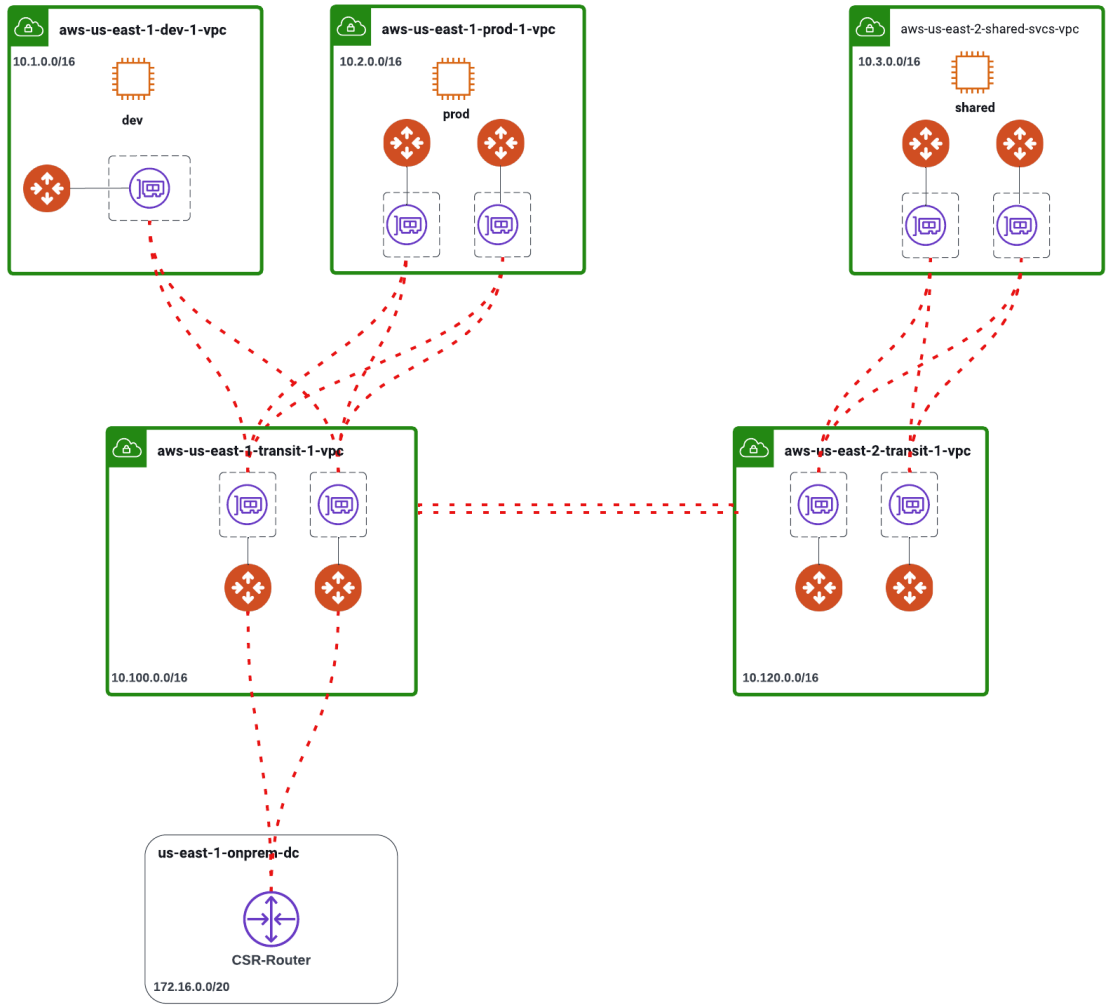
www.aviatrix.com

# Introduction

- **Multi-Cloud Network Segmentation (MCNS):** Aviatrix's MCNS is  the ability to run network domains (i.e., VRFs) where some of them will run isolated whereas other will need to connect to other domains.
- **FireNet:** Aviatrix Firenet is the insertion of L4-L7 services through policy and encompassed creating the L4-L7 device (Checkpoint, PANW, Fortinet), bootstrapping the NGFW and inserting it into the traffic path.
- **Use Cases:**
    - MCNS (Compliance, Security, Operations Best Practices)
        - Dev and Prod workloads running completely isolated on top of a common infrastructure
        - Dev and Prod though isolated from one another will need connectivity to Shared services
        - Extending the network domain to on-prem via Site2Cloud
    - FireNet ( Compliance, Workload Protection, APT)
        - Secure East-West or North-South traffic for production VPCs (Prod-Prod or Prod-Shared Services Communication)
- **Target Individuals**: NetSec, InfoSec

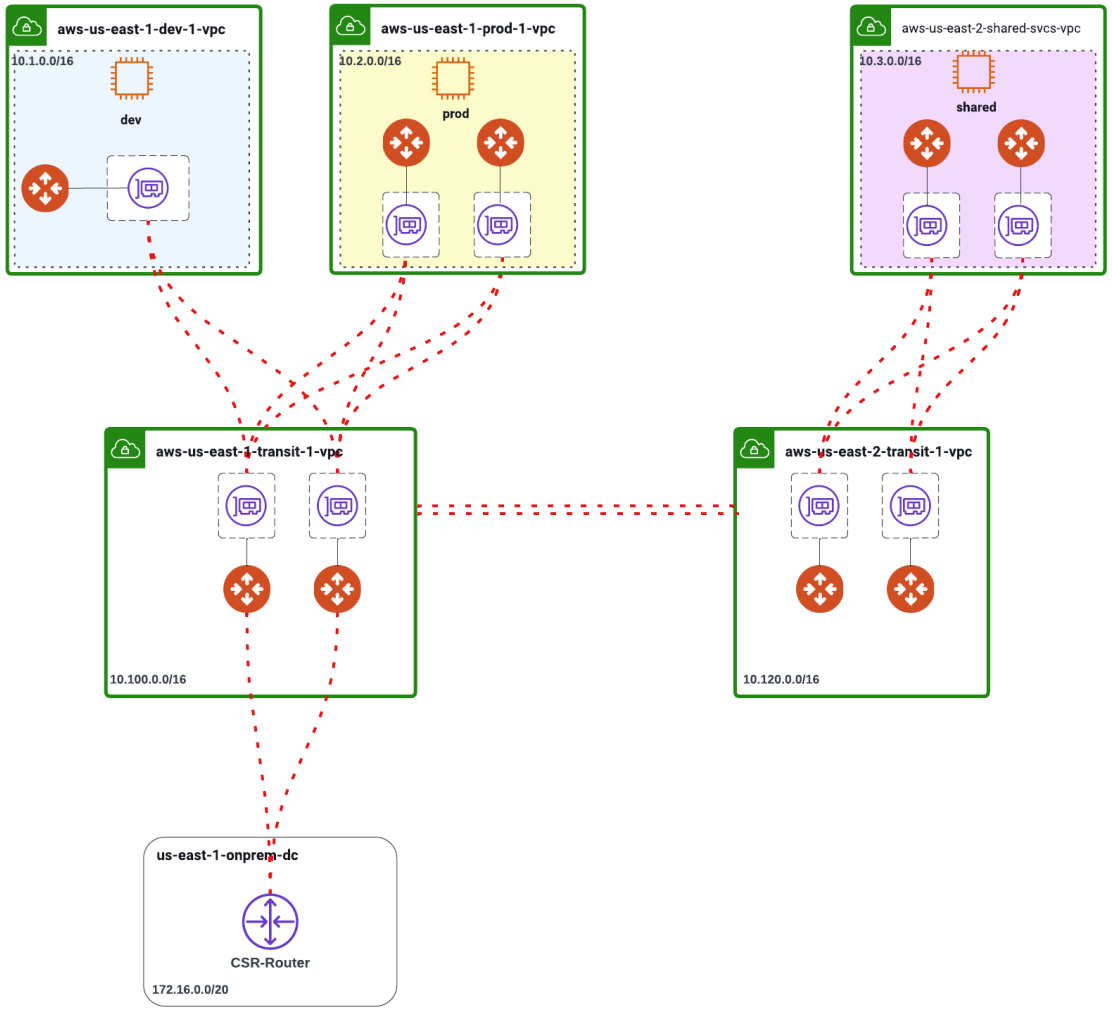
# Initial Topology

- Terraform Code in Github can be found here
- LucidChart Diagram can be found here



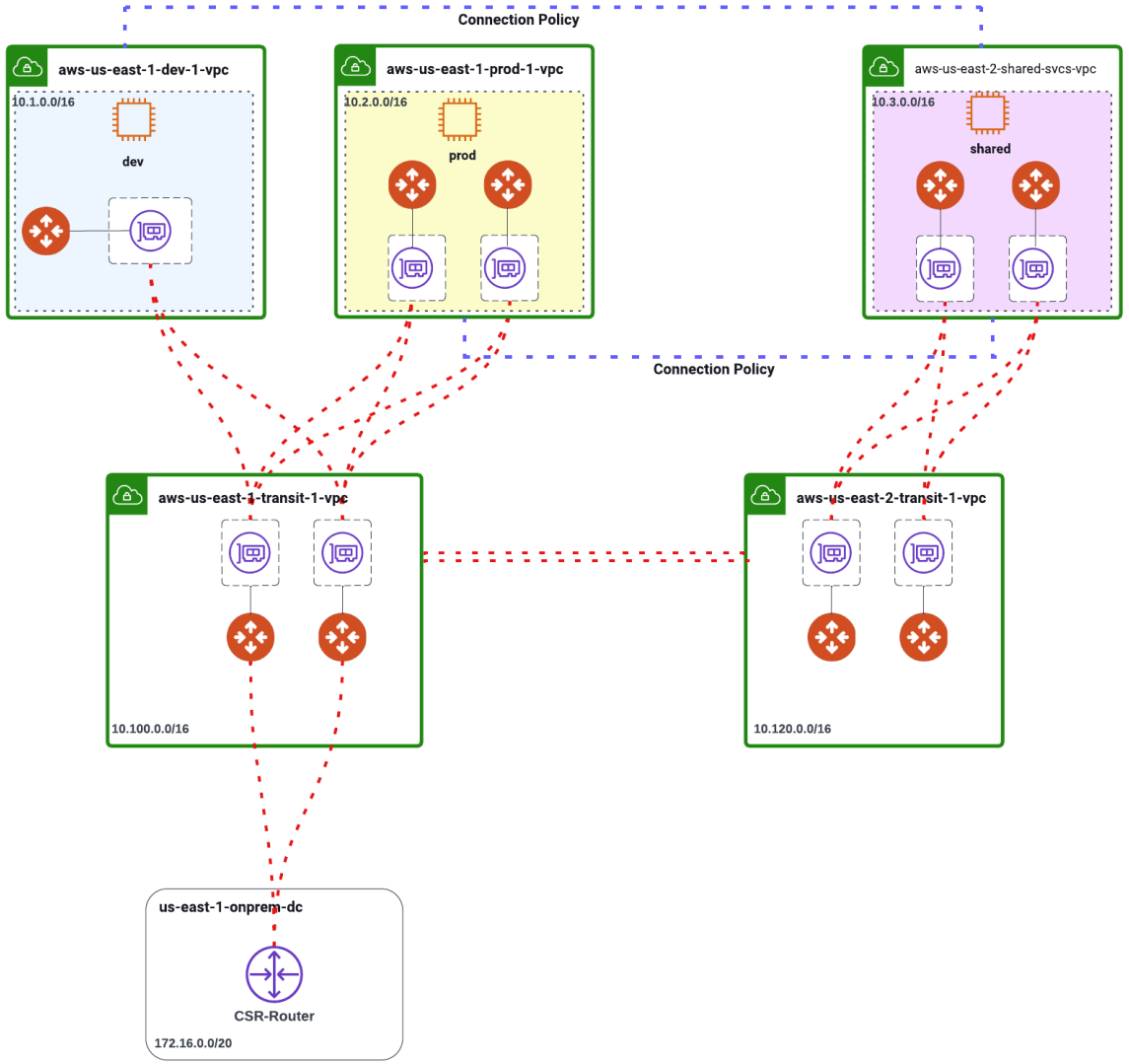
# Step 1: Create Network Domains

- Network Domains Created:
  - Prod
  - Dev
  - Shared-Svcs



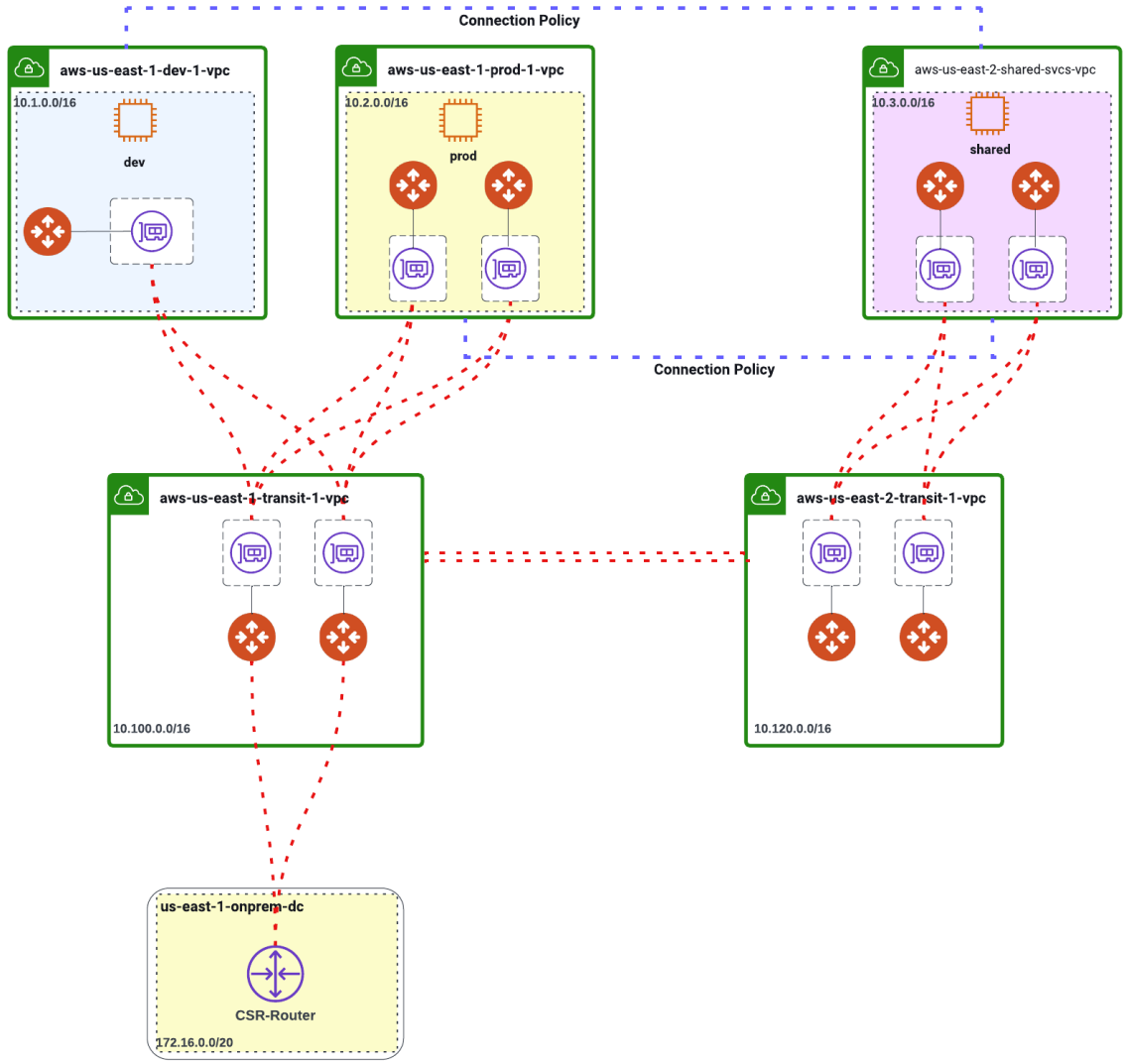
# Step 2: Connection Policies

- Connection Policies are created as follows:
  - Prod – Shared Svcs
  - Dev – Shared Svcs



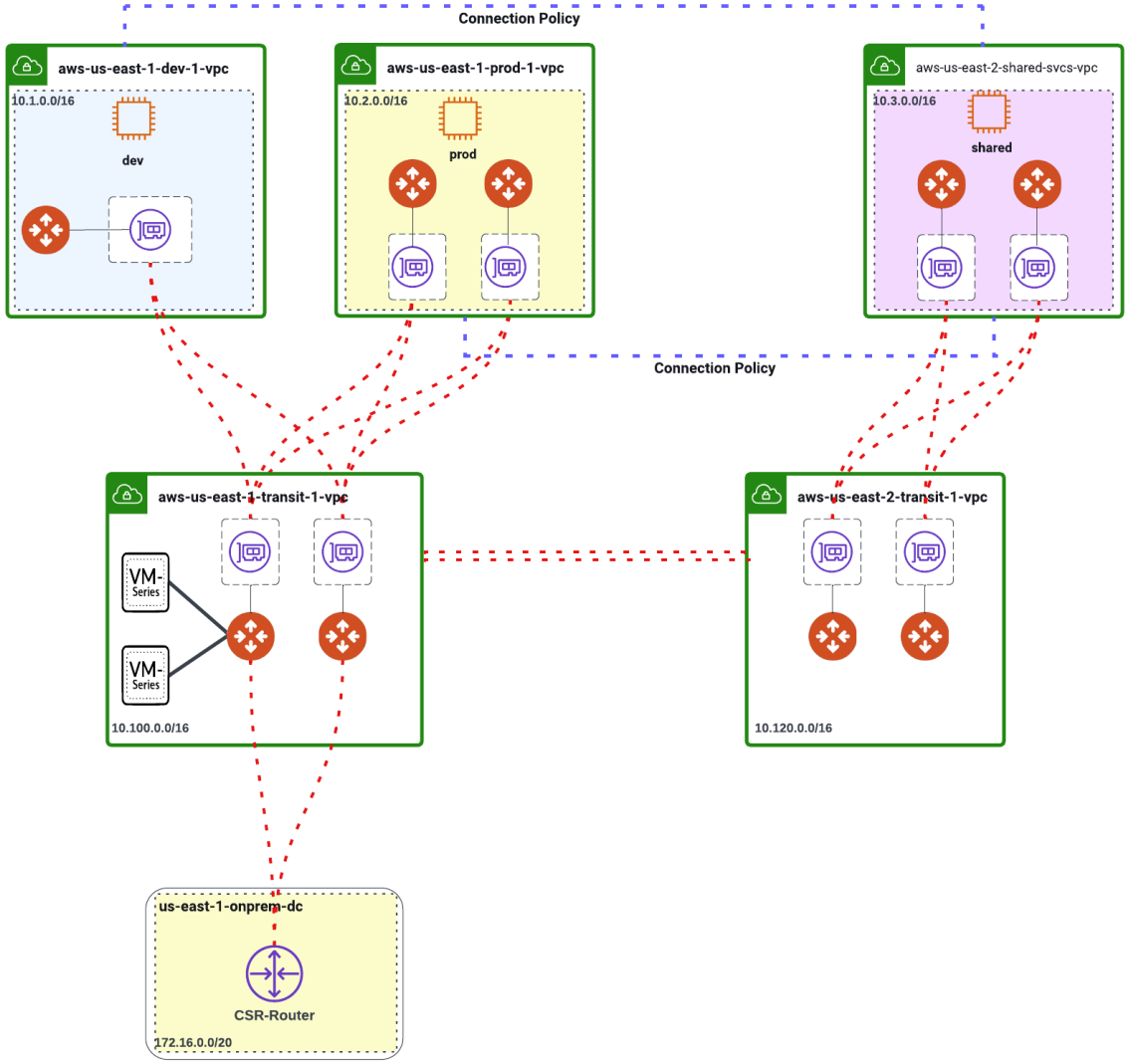
# Step 3: Extending Segmentation to On-Premises

- Prod segment has been extended to on-prem CSR connected via Site-to-Cloud (S2C)



# Step 4: Enable FireNet

- 2 x Palo Alto VM-series FWs are provisioned and inserted into the path
- Inspection Policy for Prod



# Thank You

aviatrix