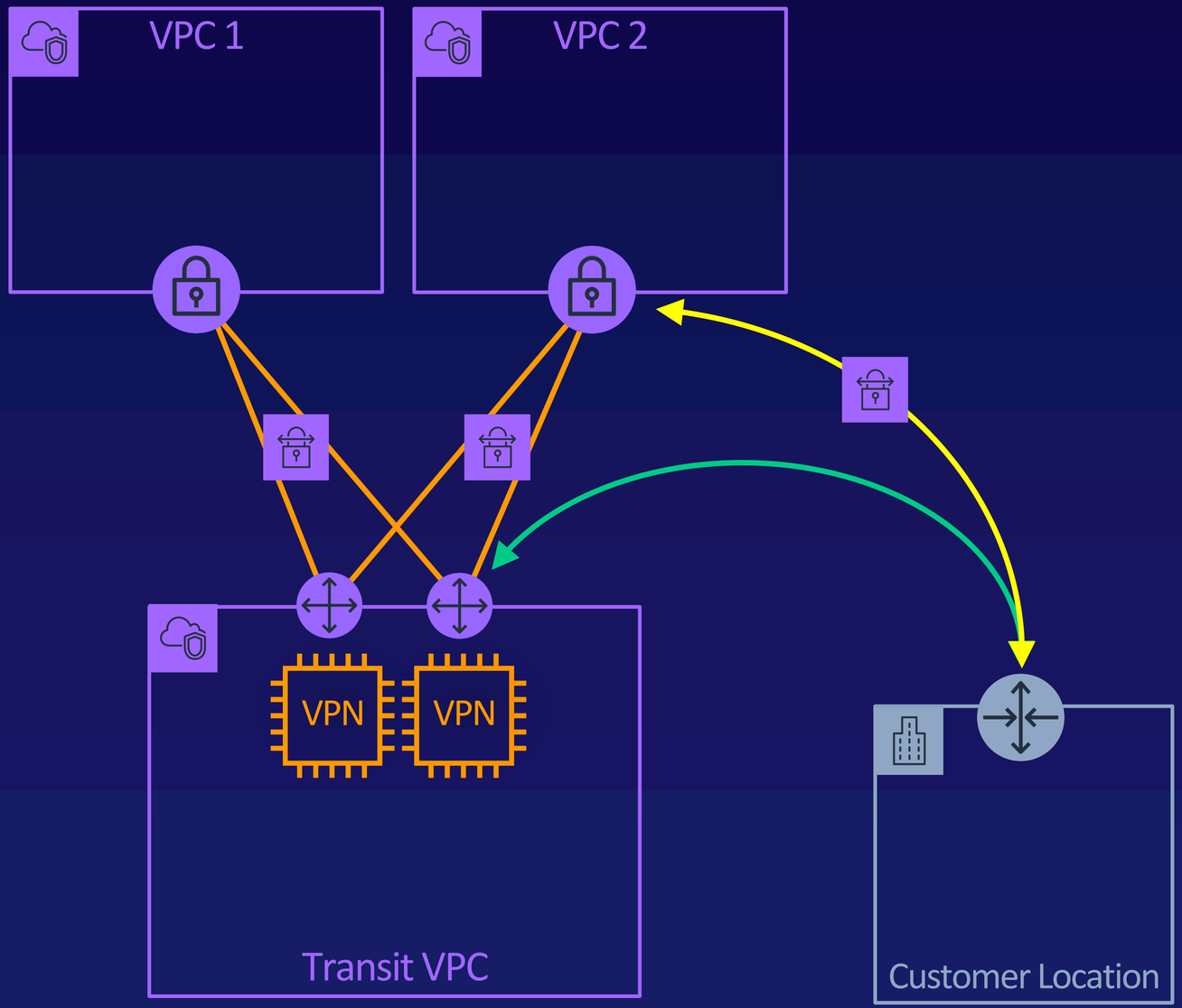
Transit VPCs and Hybrid Connectivity

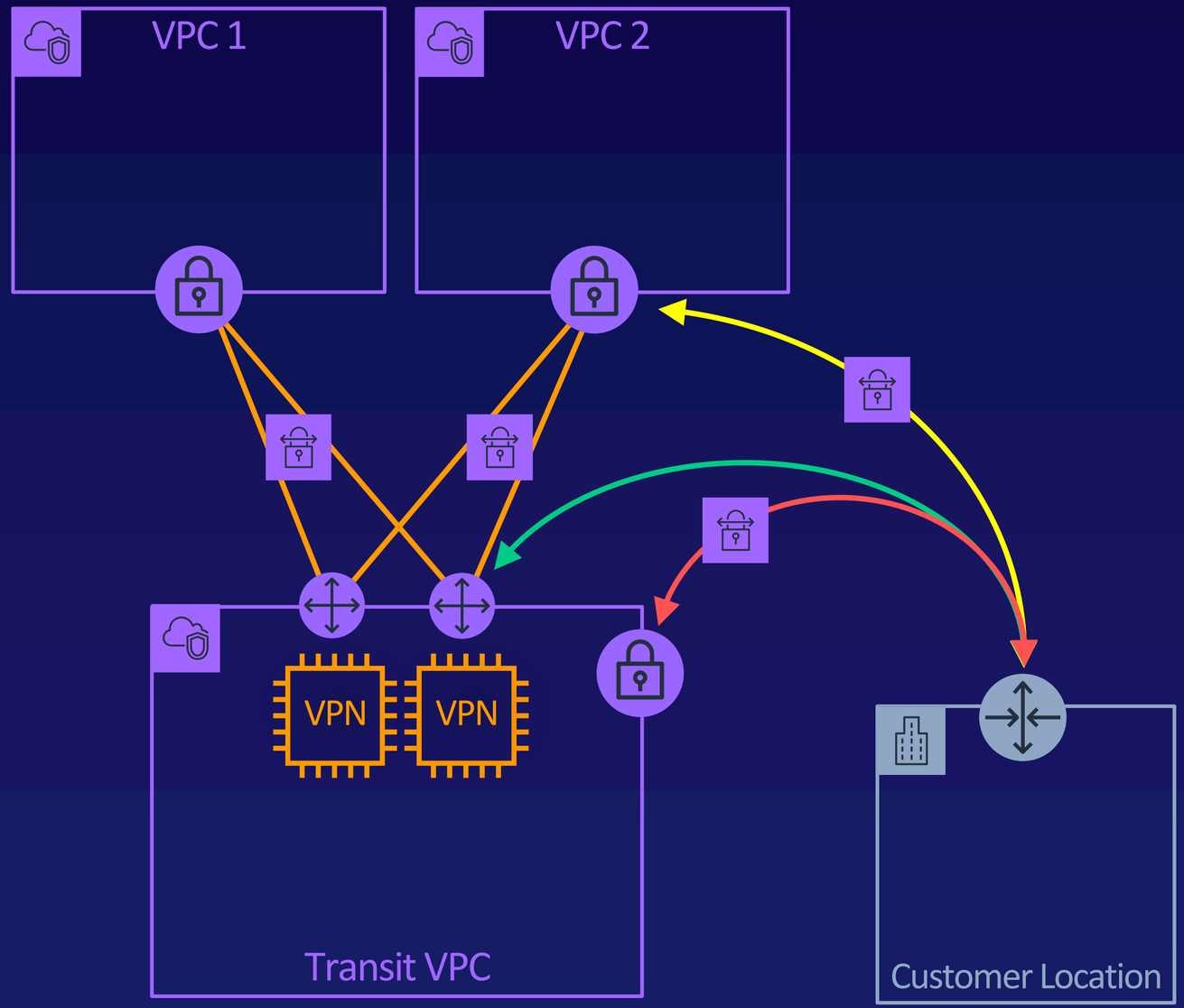
Steven Moran
TECHNICAL INSTRUCTOR

Virtual Private Networks



- VPNs from on-prem networks should connect to the VPN system in the transit VPC
- Optionally, AWS VPN connections may be established with trusted spoke VPCs.

Virtual Private Networks



- AWS VPN connections to a VGW in the transit VPC cannot forward traffic to other VPCs.

Direct Connect

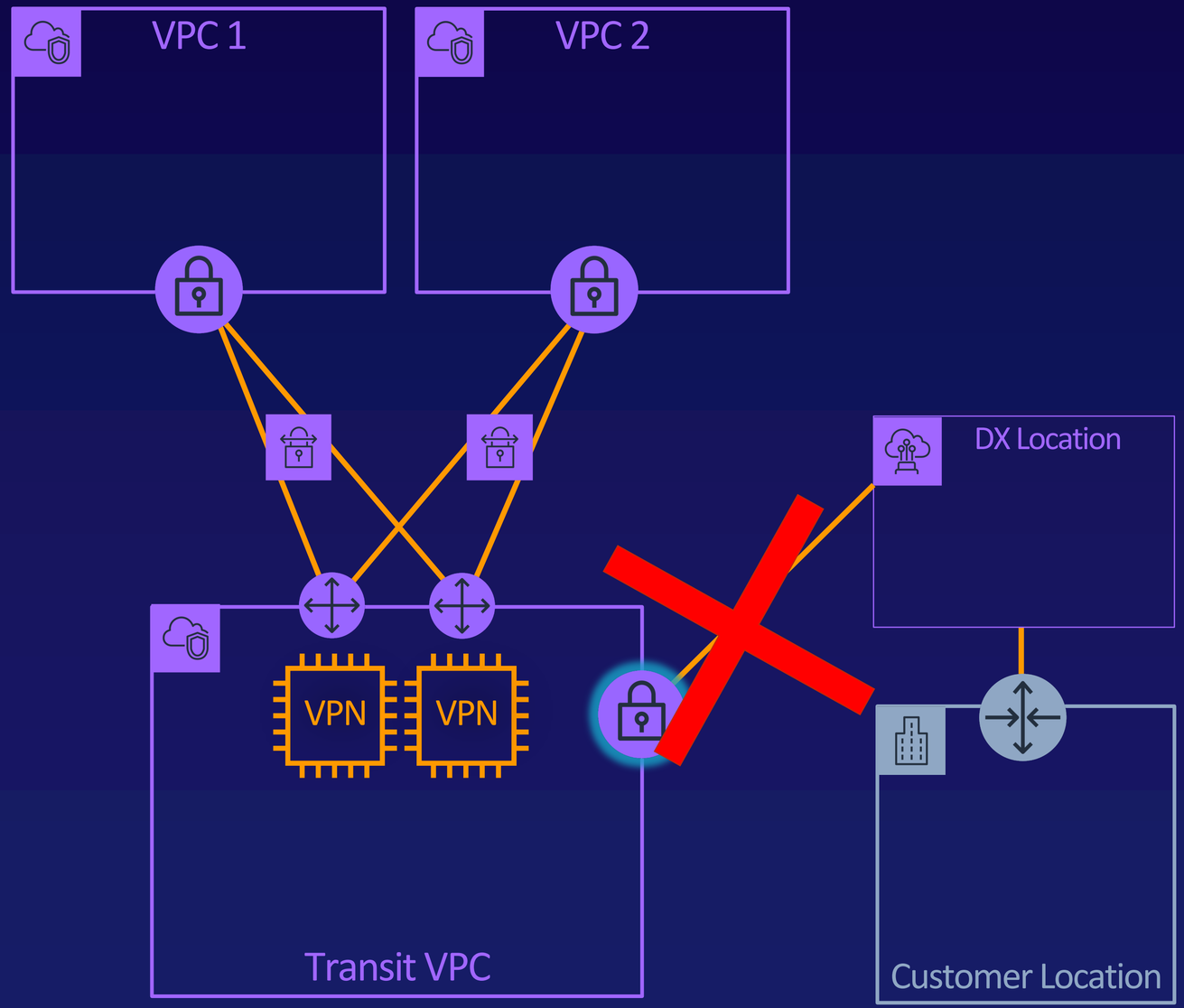
Public VIFs

- Allows access to AWS public services without traversing the internet.

Private VIFs

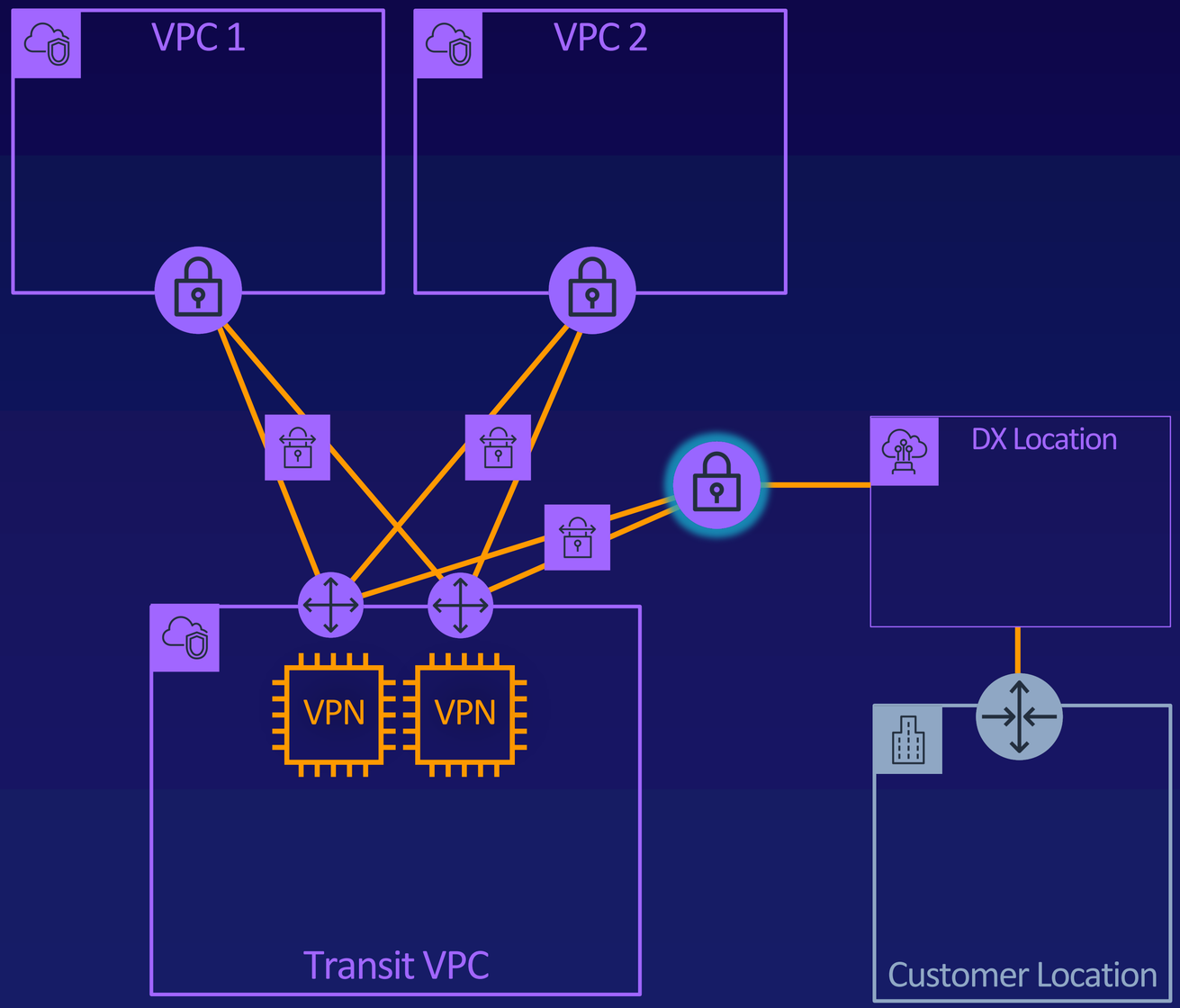
- Can connect to a single VGW to access attached VPC.
- Can connect to a Direct Connect Gateway.
- Up to 10 VGWs in any public region may connect to a DX Gateway.

Direct Connect



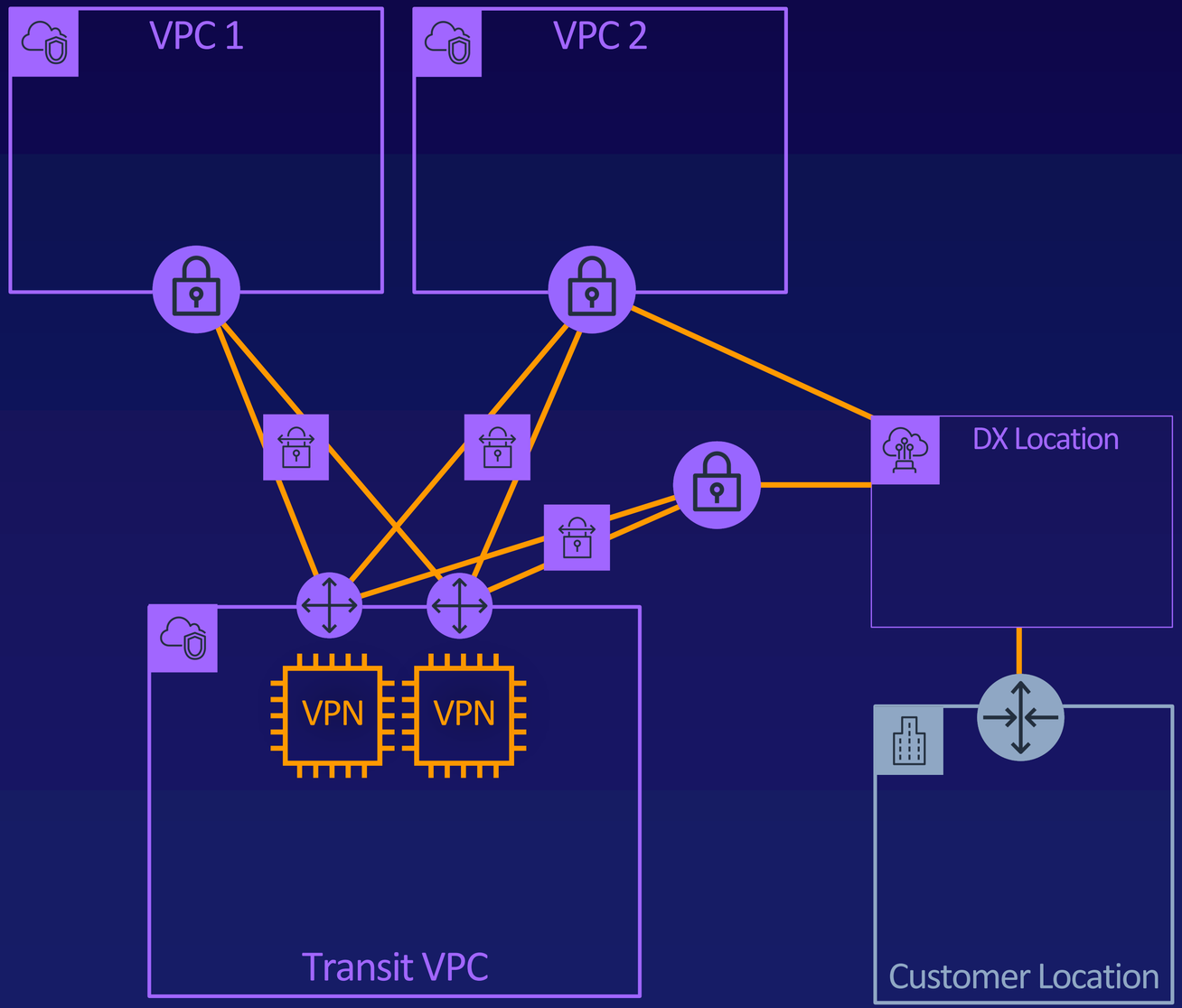
- Connecting a private VIF to a VGW at the transit VPC will create a non-transitive network

Direct Connect



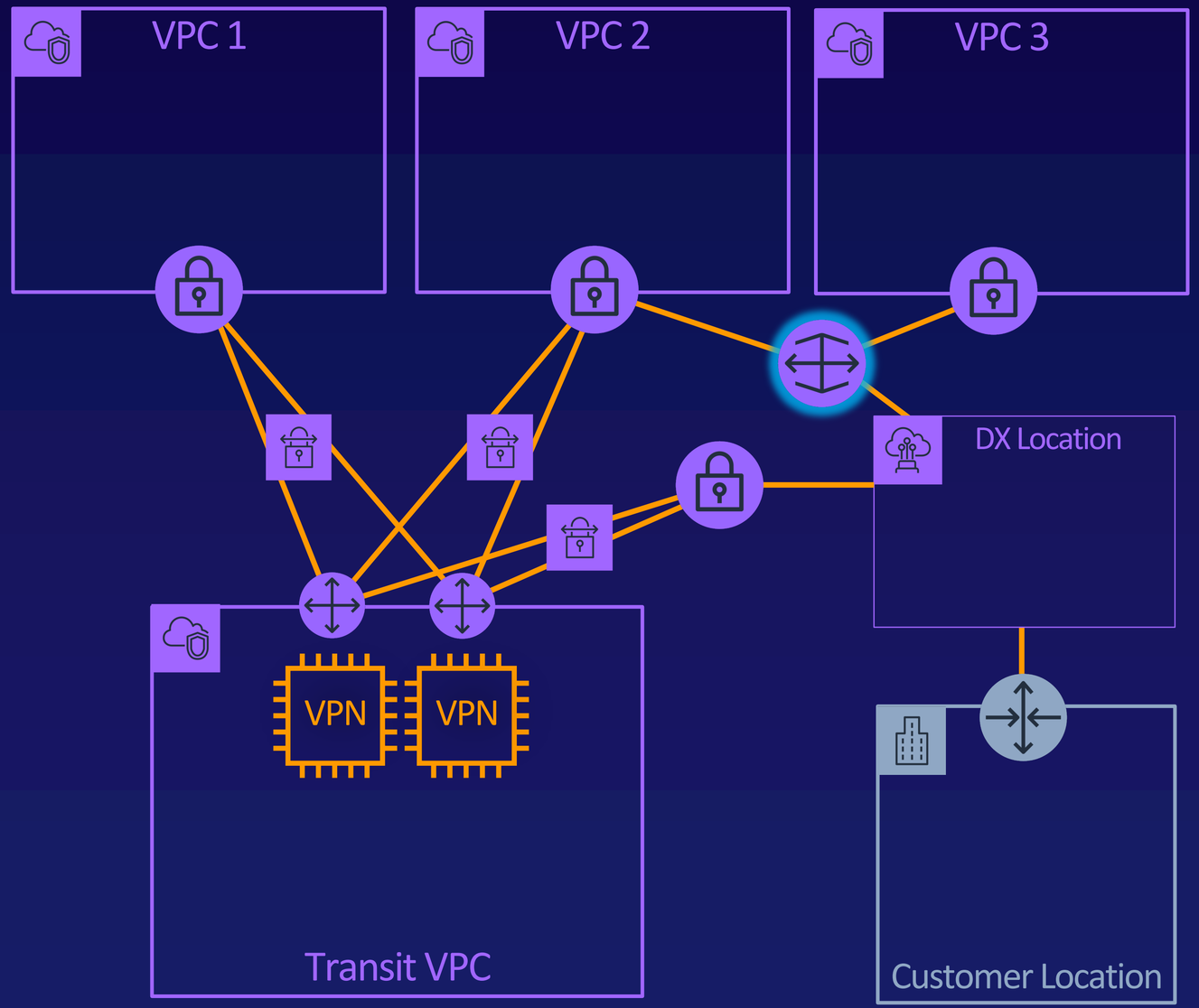
- If Direct Connect traffic must pass through the transit VPC, then a detached VGW must be created in the region the DX location connects to.
- Private VIF is associated with detached VGW.
- The VPN systems in the transit VPC connect with AWS VPN connections.

Direct Connect



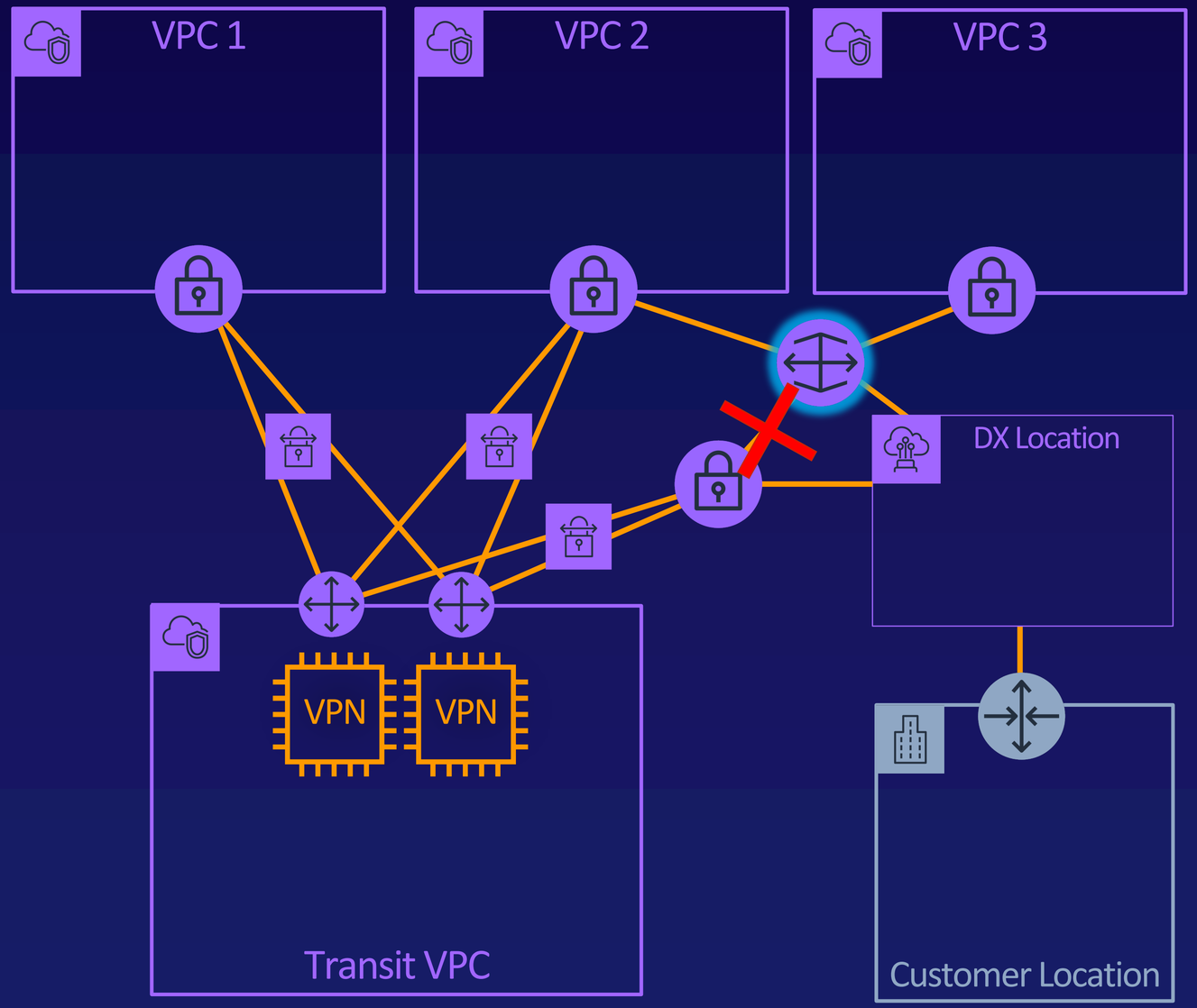
- If spoke VPCs must be accessed directly, new private VIFs could be connected to their VGWs directly.

Direct Connect



- If spoke VPCs must be accessed directly, new private VIFs could be connected to their VGWs directly.
- Direct Connect Gateway can be used to connect to multiple spoke VPCs.

Direct Connect



- If spoke VPCs must be accessed directly, new private VIFs could be connected to their VGWs directly.
- Direct Connect Gateway can be used to connect to multiple spoke VPCs.
- DX Gateway cannot associate with floating VGW.

Jumbo Frame Roundup

- Traffic with a larger MTU than the network can support will be fragmented.

- Enabling “Do Not Fragment” IP header flag will cause large traffic to be dropped instead.

Jumbo Frame Roundup

- Default size: 1500 bytes
- Max supported MTU sizes:
  - VPC: 9100
  - DX Private VIF: 9100
  - DX Transit VIF: 8500
  - DX Public VIF: 1500
  - VPC Peering: 1500
  - Internet: 1500

Fast Takeaways

VPN tunnels from on-prem should terminate at the transit VPC EC2 VPN system.

DX connections to the transit VPC must use a detached VGW in order for the connection to remain transitive.

Spoke VPCs can be connected through a DX Gateway.

Be mindful of MTU mismatch.