GCC 2.0 Tech Talks

Government on Commercial Cloud

- AWS GA is coming on **4th May 2022**.
- If and when we talk about Native Services, we will probably cite **AWS only** as these are gearing towards AWS GA preparation.
- Information on Azure will be shared in coming months (to recap, Azure GA will be by Q3 2022).
- All slides will be shared and most of the documentation will also be translated to either Developers Portal (accessible by everyone) or Docs Portal (only accessible by for TechPass account holders).
- All the slides can be shared with existing contractors who are required to manage Projects on GCC as deemed fit by Agencies.
- The series of "Brown Bag" lunch time tech talk is arranged so as to ensure more people can join us in view that some will clash with your meetings. Please feel free to have your lunch while you join us.

For Your Info

- You will be put on mute by default.
- Video should be turned off.

Q&A Segment

- Type in message box when you want to ask a question.
- Wait to be acknowledged by the presenter before speaking.
- Unmute your microphone and state your name and agency clearly.

Session Recording

- Please note that the series of GCC 2.0 Tech Talks will be recorded.
- The video recordings will be made available (in SharePoint).

Let Us Know Your Feedback!

https://form.gov.sg/625cbcecf319210013fe01b3

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg

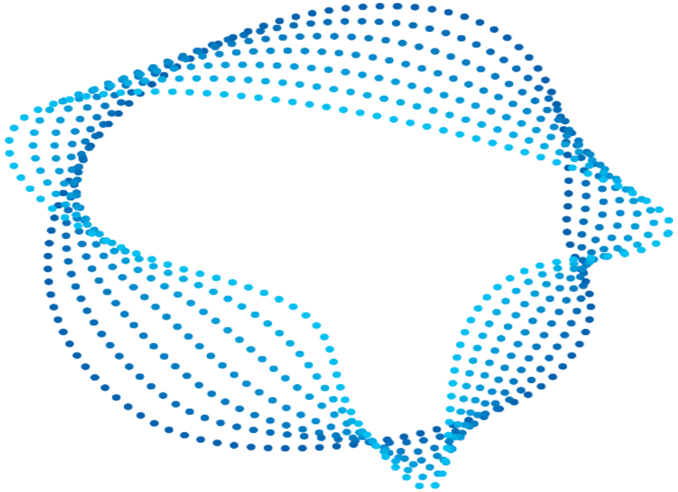
GCC 2.0 Networking Constructs, AWS TGW, Direct Connect & AWS Site to Site(IPSec) VPN

Name: - Cherng Wei & AWS Solutions Architects
Department :- CODEX-GCC & AWS

Date :- 29th Apr 2022(Friday)
Version 1.0

TABLE OF CONTENTS

1. GCC Network Constructs on AWS (Recap)
2. AWS Transit Gateway (TGW)[Agency Managed]
3. Direct Connect(DX)
4. AWS Site to Site IPsec Virtual Private Network (VPN)



Network Constructs on AWS(Recap)

GCC 2.0 Networking Introduction (1/2)

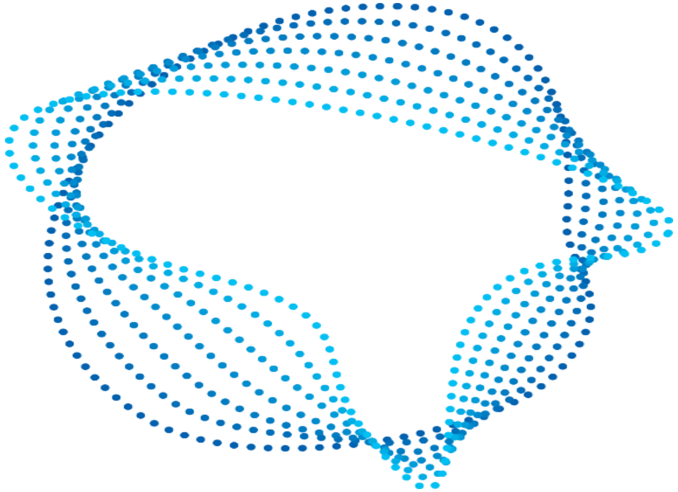
How does GCC 2.0 Network constructs & design differ from GCC 1.0?

- There will be **no GCC provisioned Jumphosts**.
- Workload management activities will be using **CSP Native Workload Administration Tools** (AWS SSM Session Manager, Fleet Manager & Azure Bastion).
- There will be GCC Centrally-managed **GEN Routable[INTRANET] & Non-GEN Routable[Internet]** Compartment with integration to GCC Common Services through AWS Transit Gateway[TGW](also GCC centrally managed).
- The availability of Agency-managed **AWS Transit Gateway (TGW)**.
- **Stronger use of Policy as Code (PaC)** to detect Non-Compliances as opposed to only using Service Control Policies (SCPs). Example include attaching of Internet Gateway (IGW) to an INTRANET (GEN-Routable) compartment, which will be flagged by PaC as non compliant.

GCC 2.0 Networking Introduction(2/2)

What are the key improvements and benefits to Agencies

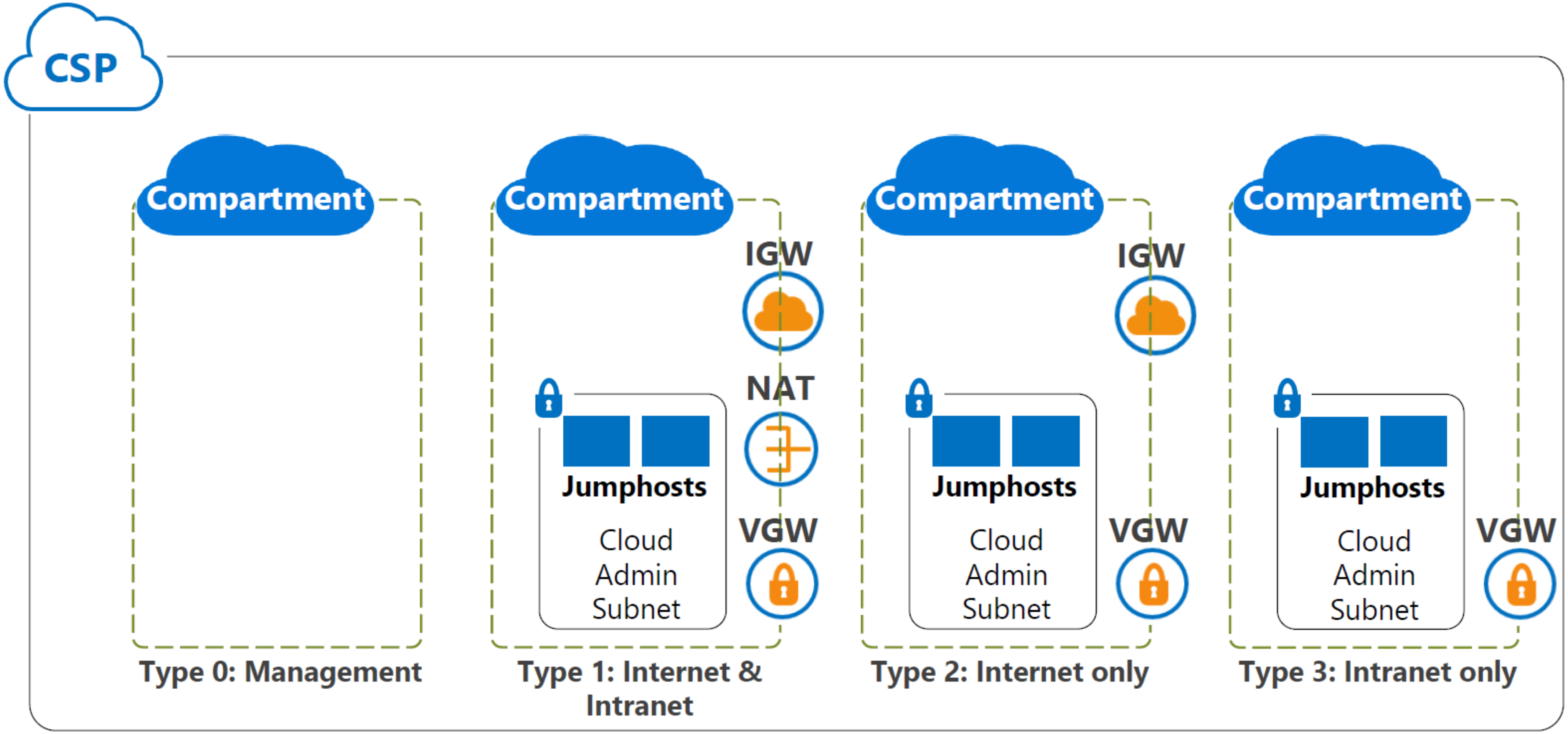
- **No Compartment costs** levied by GCC.
- **No default GCC-provisioned Jumphosts**, which will reduce cloud-spend (VMs operating costs).
- Agencies will have more flexibility (faster time-to-market) to **self-manage networking constructs** in GCC 2.0.
- **Minimal AWS Service Control Policies** (or equivalent) restrictions equates to better configuration flexibility with reduction of Service Requests & Support Requests submissions for faster configuration changes/modifications or implementations.



Types of Network Compartments

GCC 1.0 Network Compartments (Recap)

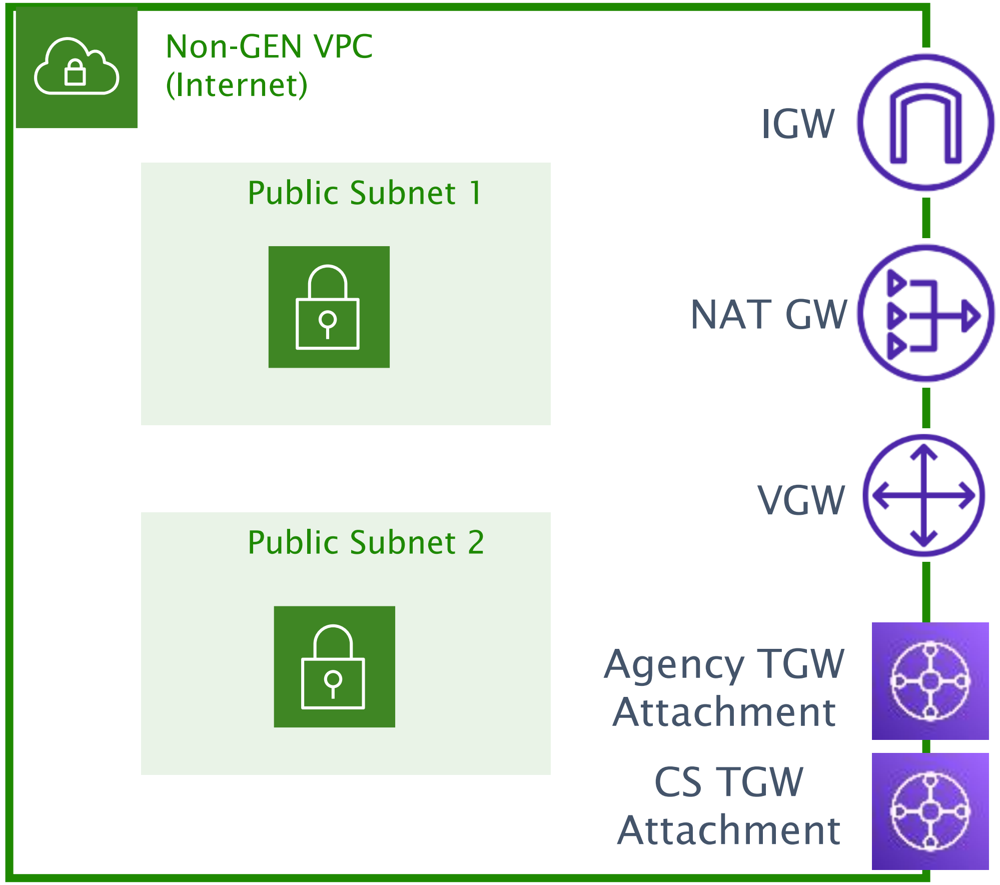
The Four Types of Network Compartments



* Extracted from GCC Foundation Training slide 104

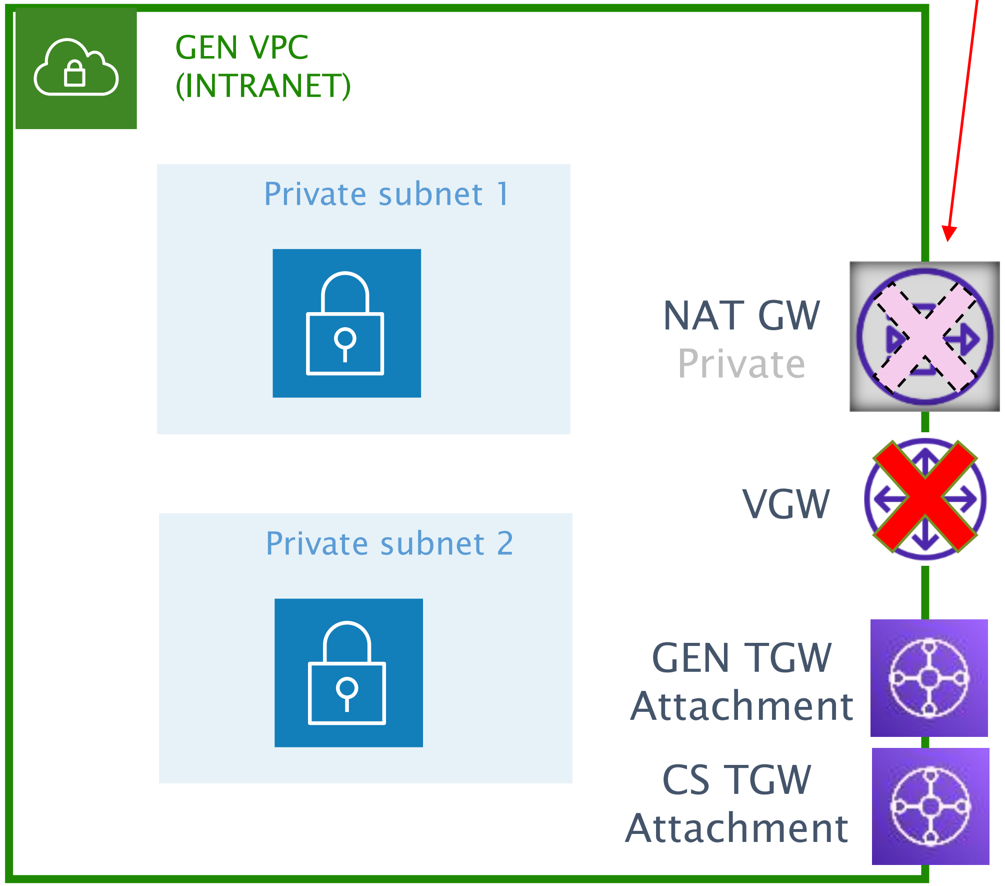
GCC 2.0 Network Compartments

Non-GEN Routable Compartment(Internet)



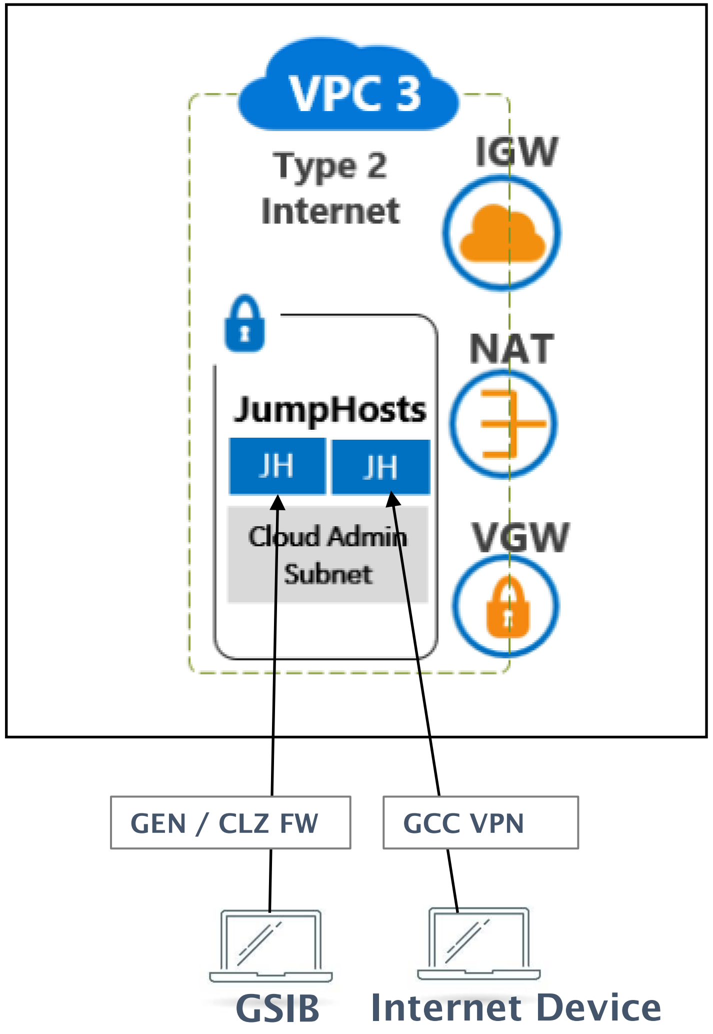
GEN Routable Compartment(INTRANET)

Will not be available on GA
Review in progress

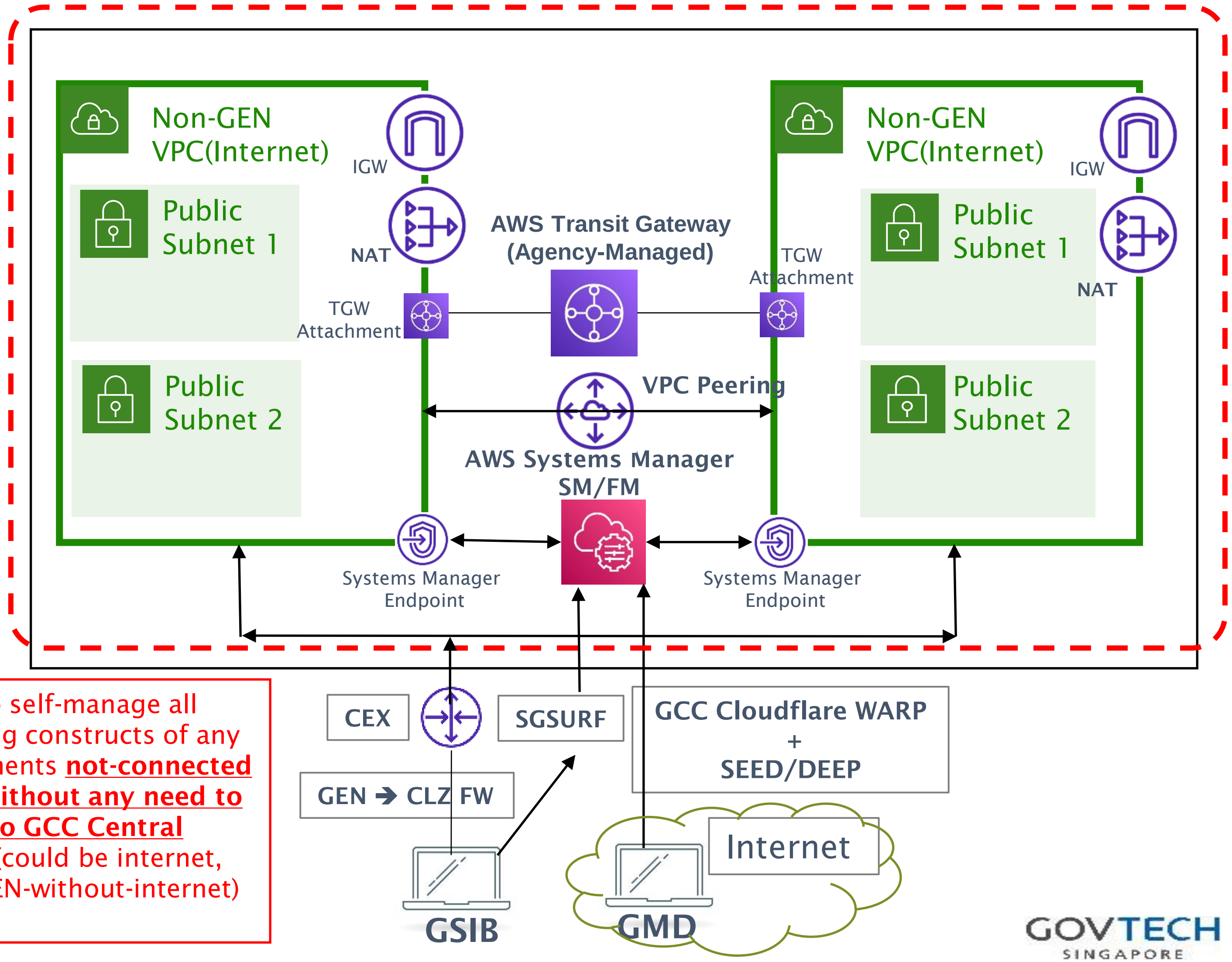


Non-GEN Routable(Internet) Compartments

GCC 1.0



GCC 2.0



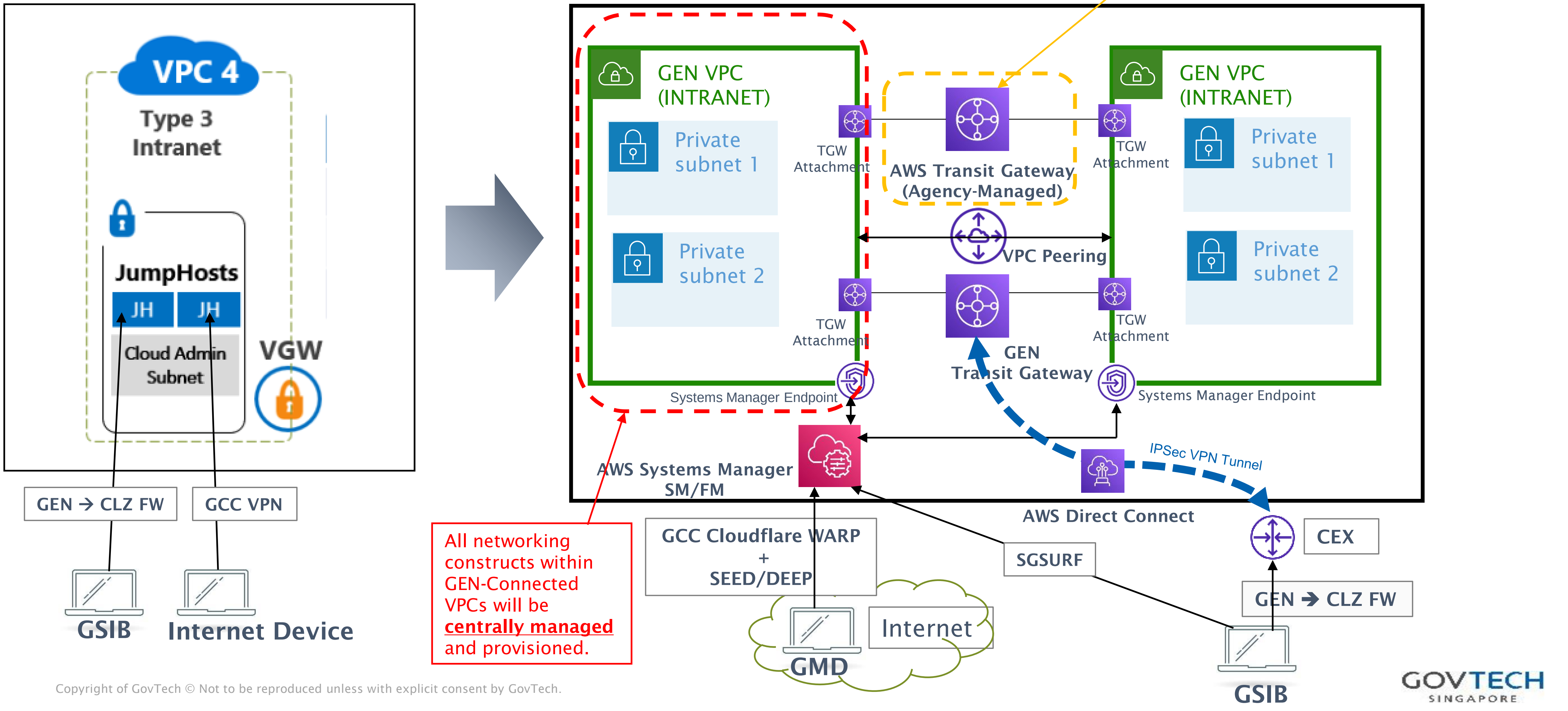
Agency to self-manage all networking constructs of any compartments **not-connected** to GEN, **without any need to connect to GCC Central Services** (could be internet, or Non-GEN-without-internet)

GEN Routable(INTRANET) Compartments

GCC 1.0

GCC 2.0

Possible for Agency to manage their own TGW



All networking constructs within GEN-Connected VPCs will be **centrally managed** and provisioned.

Network Compartments CIDR & TGW Attachments

	Centrally-Managed CIDR	Agency-Self-Managed CIDR	Centrally-Managed GEN TGW	Centrally-Managed Common-Service TGW	Agency-Managed TGW
Non-GEN Routable (Internet)	Yes			Yes	Yes
GEN-Routable (INTRANET)	Yes		Yes	Yes	*Not Recommended
Non-GEN Routable (Agency Managed) **		Yes			Yes

Note:

- Centrally-managed CIDR will be part of GCC 2.0 Service or Support Request thru' WOG ITSM process. This will include management of both default and additional CIDR IP blocks.
- Centrally managed TGWs will be transparent to Agencies, as all required configuration will be managed centrally by GCC.
- Agencies are strongly encouraged to use Agency-Managed TGW to self manage compartment-to-compartment routing (in lieu of VPC peering).

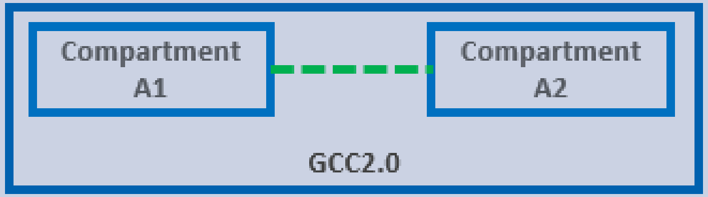
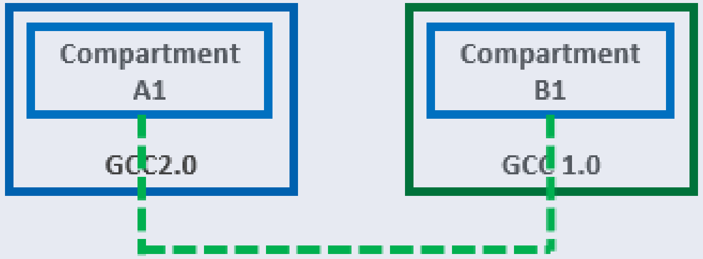
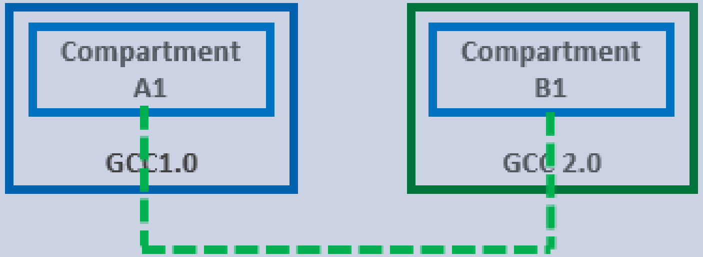
Footnote: Azure does not have an equivalent solution as AWS TGW as the concept of Azure Transit Hub is different. We will advise again on Azure final networking design at a later date.

* Agencies are highly advised to perform their own Risks assessment and acceptance with their own IDSC or CISO on connections that likely might cause bridging between GEN Routable(INTRANET) and Non-GEN Routable(Internet) compartments.

** Agencies can use RFC 1918 IPs **except** 10.0.0.0/8 and RFC 6598 100.64.0.0/10

Network Compartment Peering or TGW attachment Design

Possible scenarios on Compartment Peering & TGW attachment between GCC 1.0 and GCC 2.0

S/N	Source Compartment	Target Compartment	Process	Illustration
1	GCC 2.0	GCC2.0	Agency can use compartment peering or Agency managed TGW for inter-compartment communication within GCC 2.0 AWS. Agencies' need to ensure that they adhere to IM8 policies and PaC will monitor the deviation and alert the Agencies	
2	GCC 2.0	GCC 1.0	Tenant B1's CA to submit Support Request in GCC 1.0 CMP for Tenant B1 AA's Approval to 1) Accept VPC Peering request 2) Accept TGW sharing or create TGW attachments	
3	GCC 1.0	GCC 2.0	Tenant A1's CA to submit Support Request in GCC 1.0 CMP for Tenant A1 AA's Approval to 1) Create VPC Peering request with B1 2) Agency managed TGW sharing or create TGW attachments with B1	

Other Common Scenarios for Network Routing (Specific to AWS)(1/2)

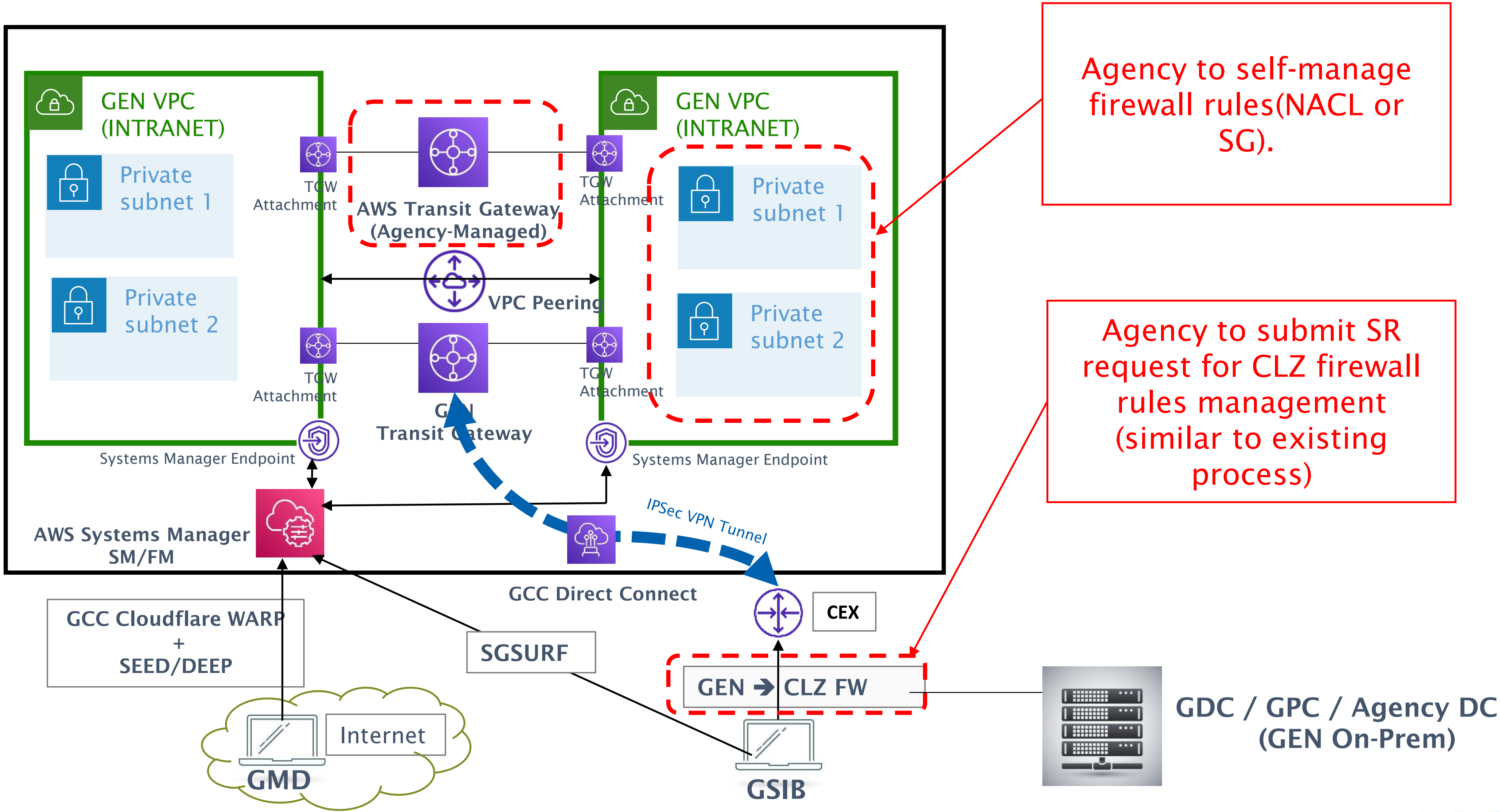
S/N	Routing Scenario	Routing Method	Consideration for Agencies
1	Between Agencies' GEN Routable[INTRANET] compartments and GEN(On-Premise)	GEN TGW to route the traffic to GEN(On-Prem) and vice versa	Agencies required to manage all firewall rules within compartment and at CLZ (same consideration as GCC 1.0 today).
2	Inter-CSP communication between AWS and other CSPs **(applicable to GEN Routable[INTRANET] compartments only)**	GEN TGW and CLZ (Cloud Landing Zone) router	Agencies required to manage all firewall rules at compartment and perform the proper routing within their compartment(same consideration as with GCC 1.0 today).
3	Inter-compartment communication within GCC 2.0 AWS and between GCC 2.0 AWS and 1.0 AWS the relevant SR (e.g GCC 1.0 CMP SM)	Compartment peering or Agency managed TGW for all inter-compartment communication	Where possible, Agencies are advised to use TGW to manage all routing. If VPC peering is required, the high-level steps as highlighted in preceding slide may be required.
4	Between GCC Common Services and Agencies' GCC 2.0 AWS new compartments (GEN routable[INTRANET] and Non-GEN routable[Internet] compartments)	GCC Common Services TGW	Agencies need to manage firewall rules within their compartment. Route association and other networking configuration and rules at TGW will be managed centrally.

Other Common Scenarios for Network Routing (Specific to AWS)(2/2)

S/N	Routing Scenario	Routing Method	Consideration for Agencies
5	Between GCC 2.0 AWS Agency managed compartment (Non WOG connectivity with Link Landing Zone) and GCC 2.0 Non-GEN Routable(Internet) compartments.	Compartment Peering	The scenario of Agency-self-managed Direct Connect (known as Non-WOG connectivity today) will still be supported, its treated as no difference to Non-GEN Routable(Internet) compartment in GCC 2.0.
6	Between GCC 2.0 AWS GEN[INTRANET] & Non-GEN[Internet] compartments and External organization compartments.	Compartment Peering or Agency Managed TGW attachment	Agencies need to thoroughly review + perform own risk assessment & whitelist the External organization at PaC, otherwise PaC will monitor the deviation and alert the Agencies Connectivity between GEN Routable[INTRANET] compartment and External Organization account is not allowed(similar to GCC 1.0).

Routing Scenario 1

Between Agencies' GEN Routable[INTRANET] compartments and GEN (on-premise)

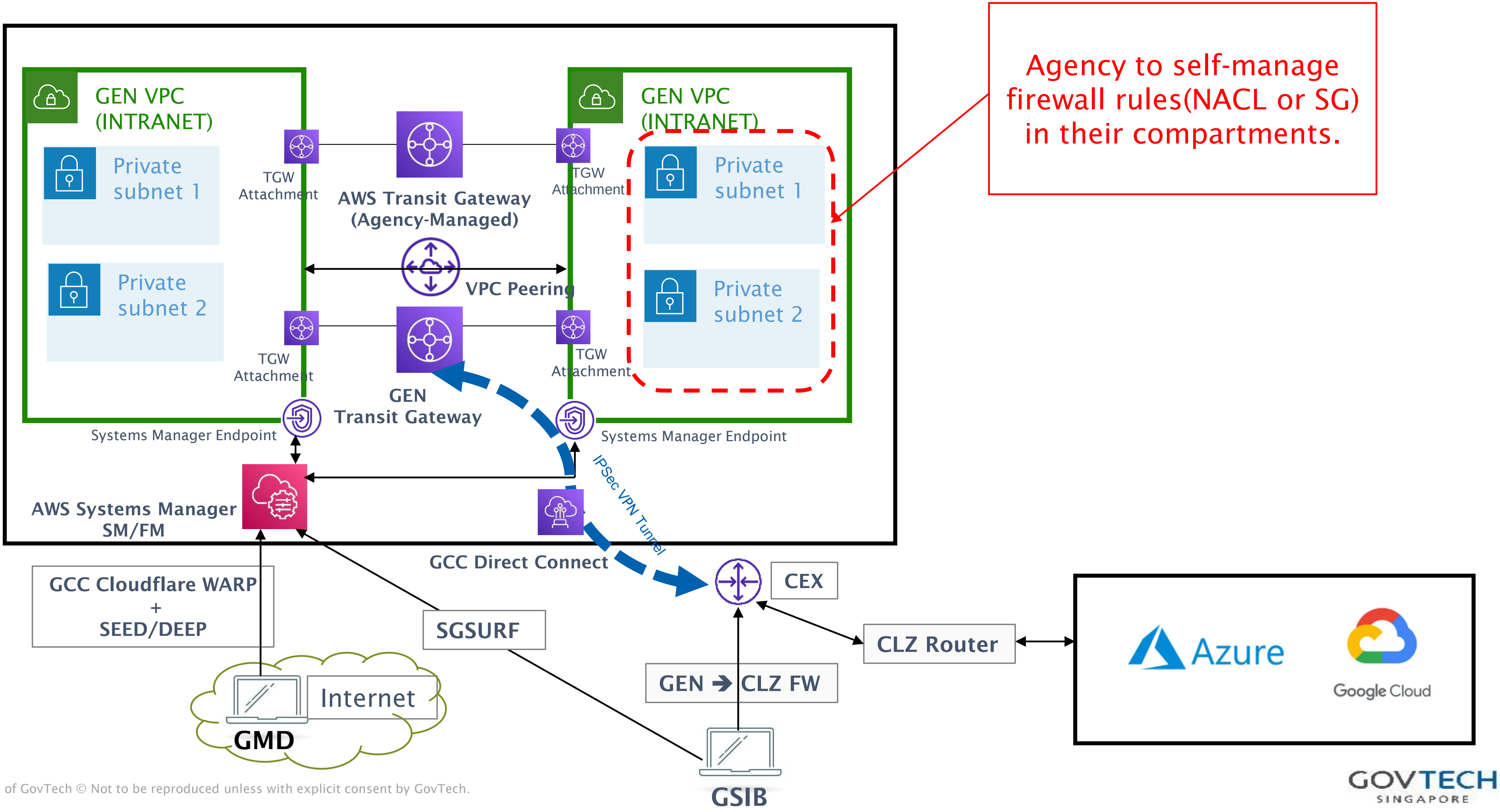


Agency to self-manage firewall rules(NACL or SG).

Agency to submit SR request for CLZ firewall rules management (similar to existing process)

Routing Scenario 2

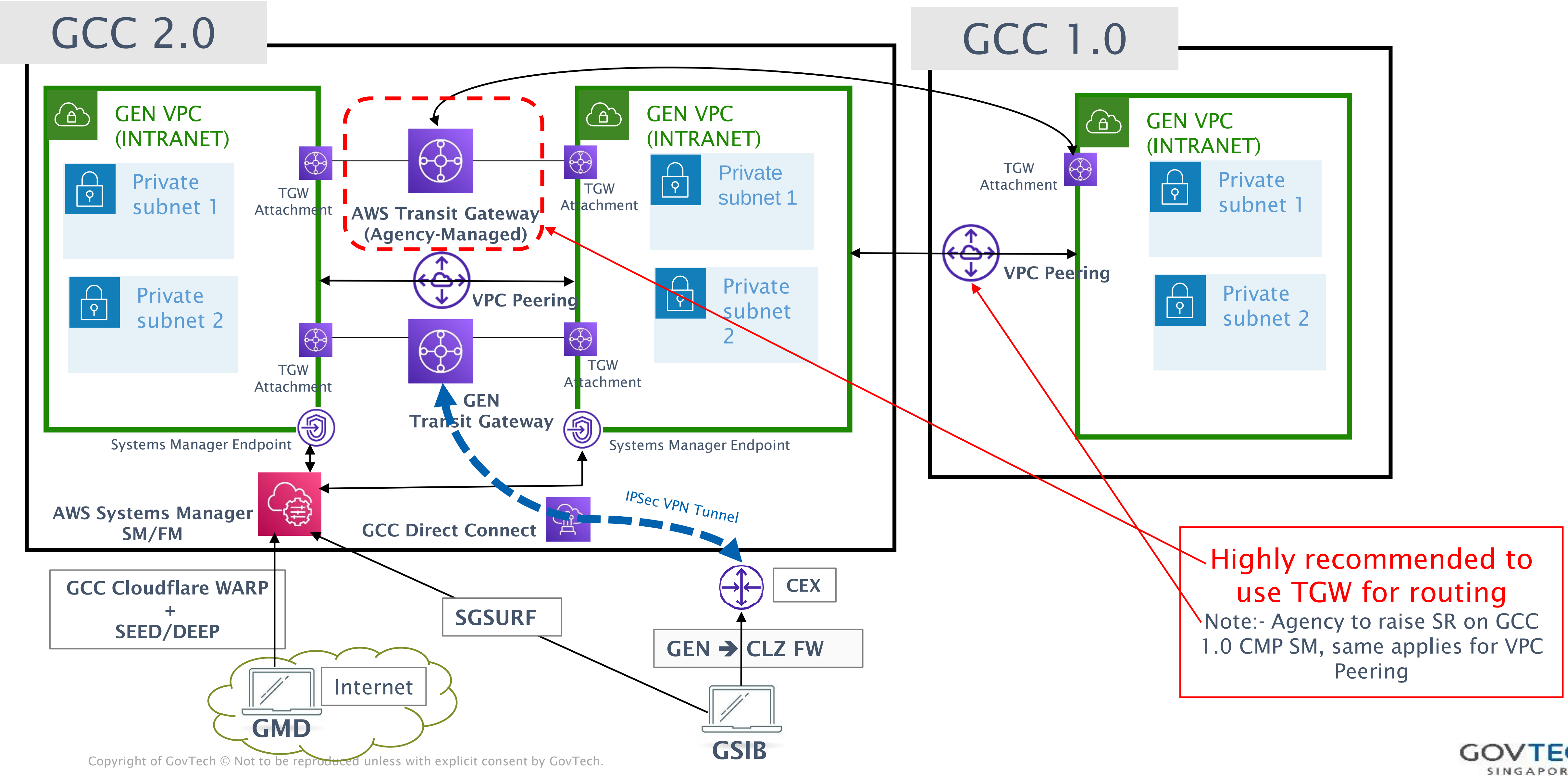
Inter-CSP communication between AWS and other CSPs (applicable to GEN routable compartments only)



Agency to self-manage firewall rules(NACL or SG) in their compartments.

Routing Scenario 3

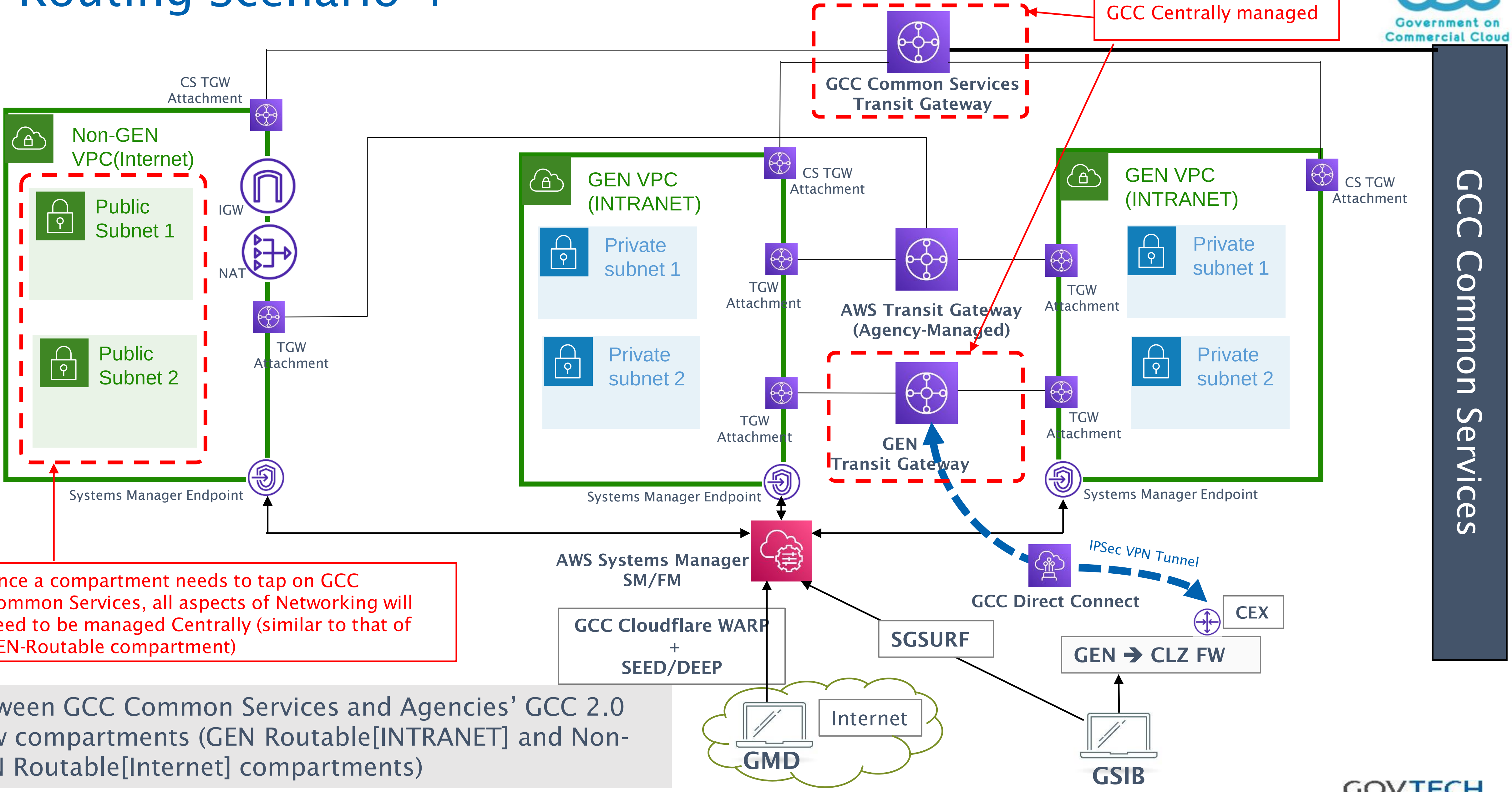
Inter-compartment communication within GCC 2.0 AWS and between GCC 2.0 AWS and 1.0 AWS



Highly recommended to use TGW for routing

Note:- Agency to raise SR on GCC 1.0 CMP SM, same applies for VPC Peering

Routing Scenario 4



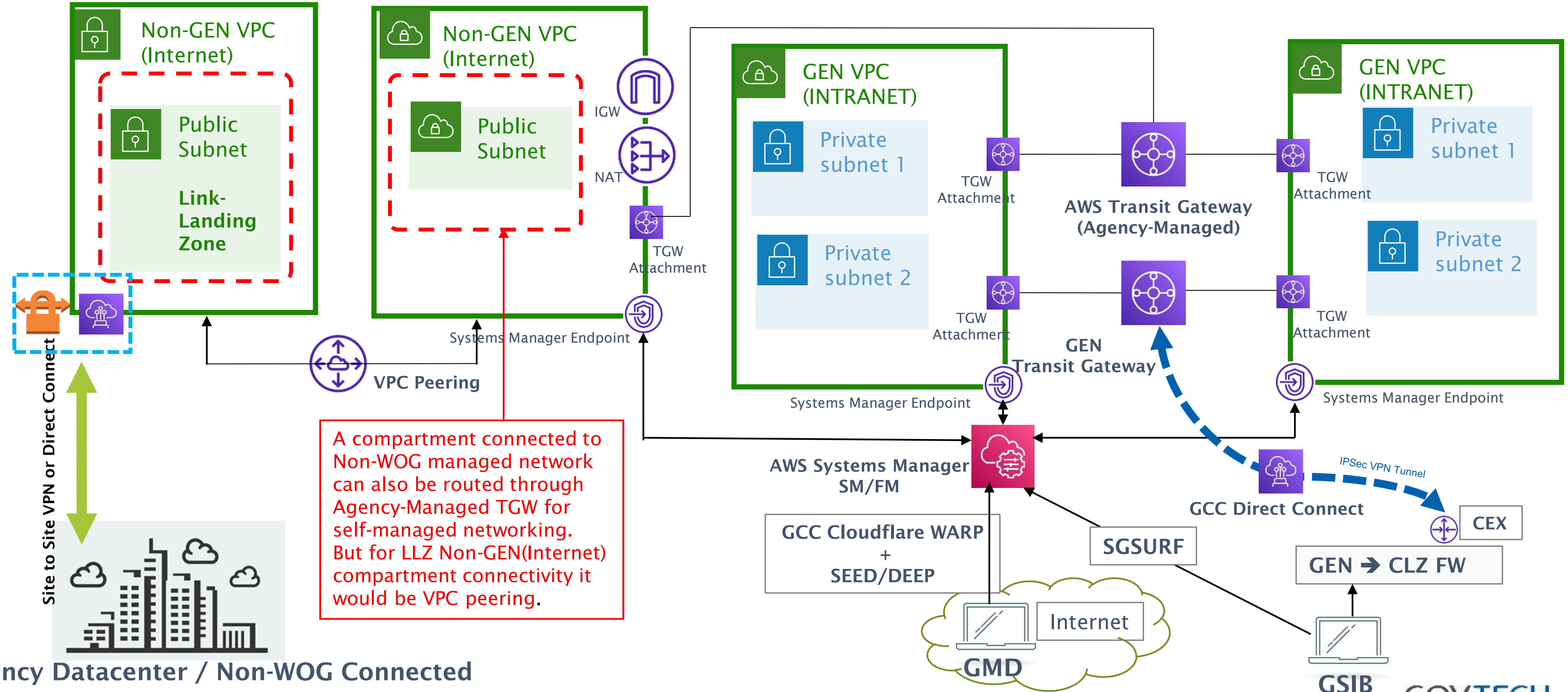
GCC Centrally managed

Once a compartment needs to tap on GCC Common Services, all aspects of Networking will need to be managed Centrally (similar to that of GEN-Routable compartment)

Between GCC Common Services and Agencies' GCC 2.0 New compartments (GEN Routable[INTRANET] and Non-GEN Routable[Internet] compartments)

Routing Scenario 5

Between GCC 2.0 AWS New Compartment (with Agency-self-managed Site to Site IPSec VPN/Direct Connect/Express Route) and GCC 2.0 provisioned Non-GEN routable[Internet] compartments)



A compartment connected to Non-WOG managed network can also be routed through Agency-Managed TGW for self-managed networking. But for LLZ Non-GEN(Internet) compartment connectivity it would be VPC peering.

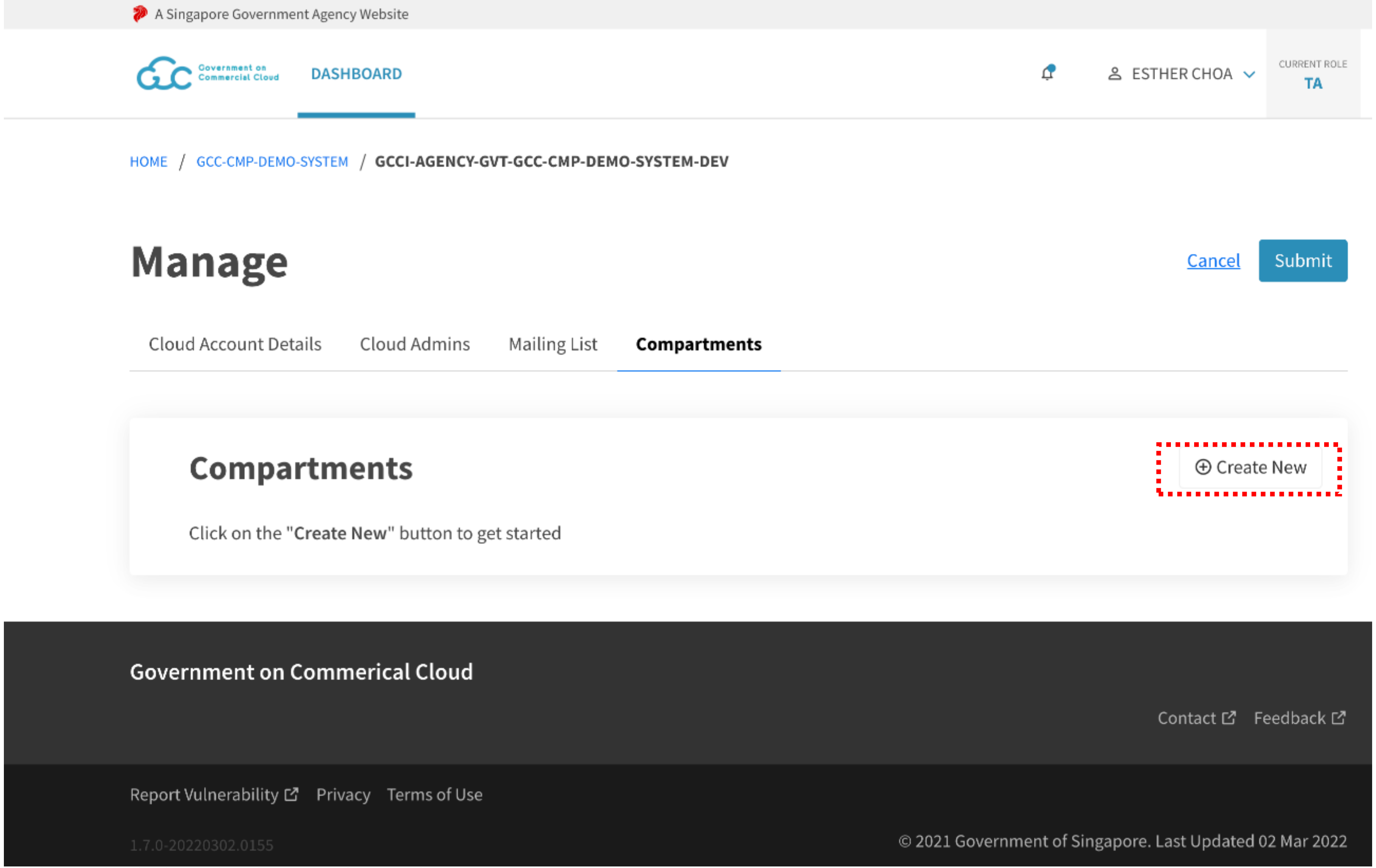
IP Address Manager(GCC IPAM centrally managed) in GCC 2.0 for AWS

What is new about this in GCC 2.0 as compared to GCC 1.0 ?

- GCC IPAM manages GEN Routable[INTRANET] and Non-GEN Routable[Internet] compartments CIDRs/IP address ranges namely 10.0.0.0/8 and 100.64.0.0/10
- Each compartment will be assigned one Gateway and Workload CIDR by default
- GCC 2.0 uses separate unique ranges e 10.x.x.x/16 & 100.x.x.x/16, these ranges are non-overlapping between GCC 1.0 and 2.0
- Standard CIDR ranges offered by CMP:
  - GEN Routable[INTRANET] → /27, /26 and /25
  - Non-GEN Routable[Internet] → /27, /26, /25 and /24
- Customised CIDR prefixes include /23, /22 & /21, Agencies have to raise Support Request (SR) on WOG ITSM (final approval will be done in the same SR)
- The migrated compartments will still using GCC 1.0 IPAM for IP address allocation
- Agency shouldn’t assign/add additional CIDRs on their own for the compartments that had been created centrally

Agency managed IPAM will be cover in future workshops when its applicable

GCC 2.0 CMP for GEN Routable(INTRANET) compartment provisioning (1/4)



A Singapore Government Agency Website

HOME / GCC-CMP-DEMO-SYSTEM / GCCI-AGENCY-GVT-GCC-CMP-DEMO-SYSTEM-DEV

Manage

Compartments

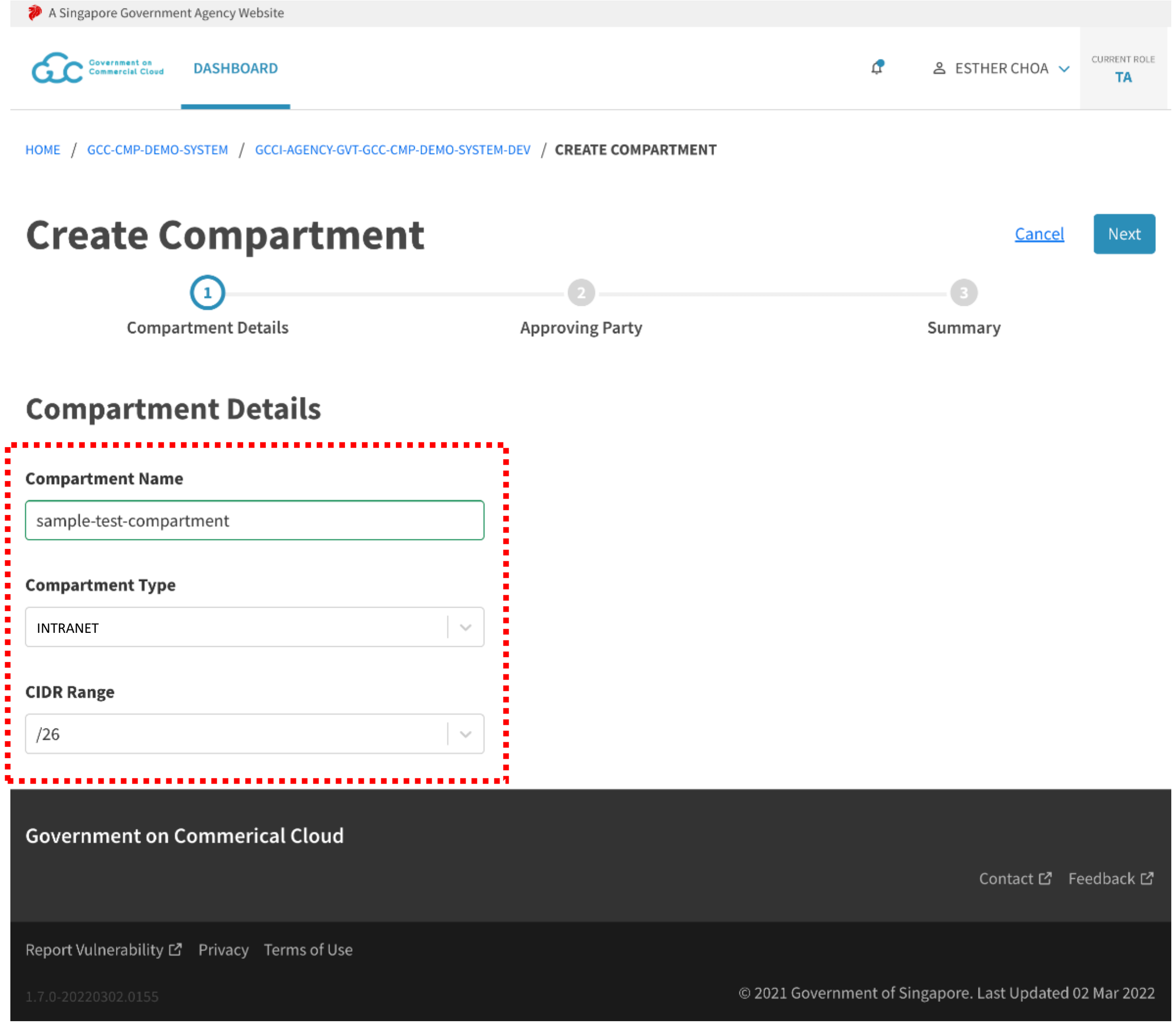
Click on the "**Create New**" button to get started

Government on Commerical Cloud

1.7.0-20220302.0155

© 2021 Government of Singapore. Last Updated 02 Mar 2022

GCC 2.0 CMP for GEN Routable(INTRANET) compartment provisioning (2/4)



A Singapore Government Agency Website

HOME / GCC-CMP-DEMO-SYSTEM / GCCI-AGENCY-GVT-GCC-CMP-DEMO-SYSTEM-DEV / CREATE COMPARTMENT

Create Compartment

Compartment Details

Compartment Name: sample-test-compartment

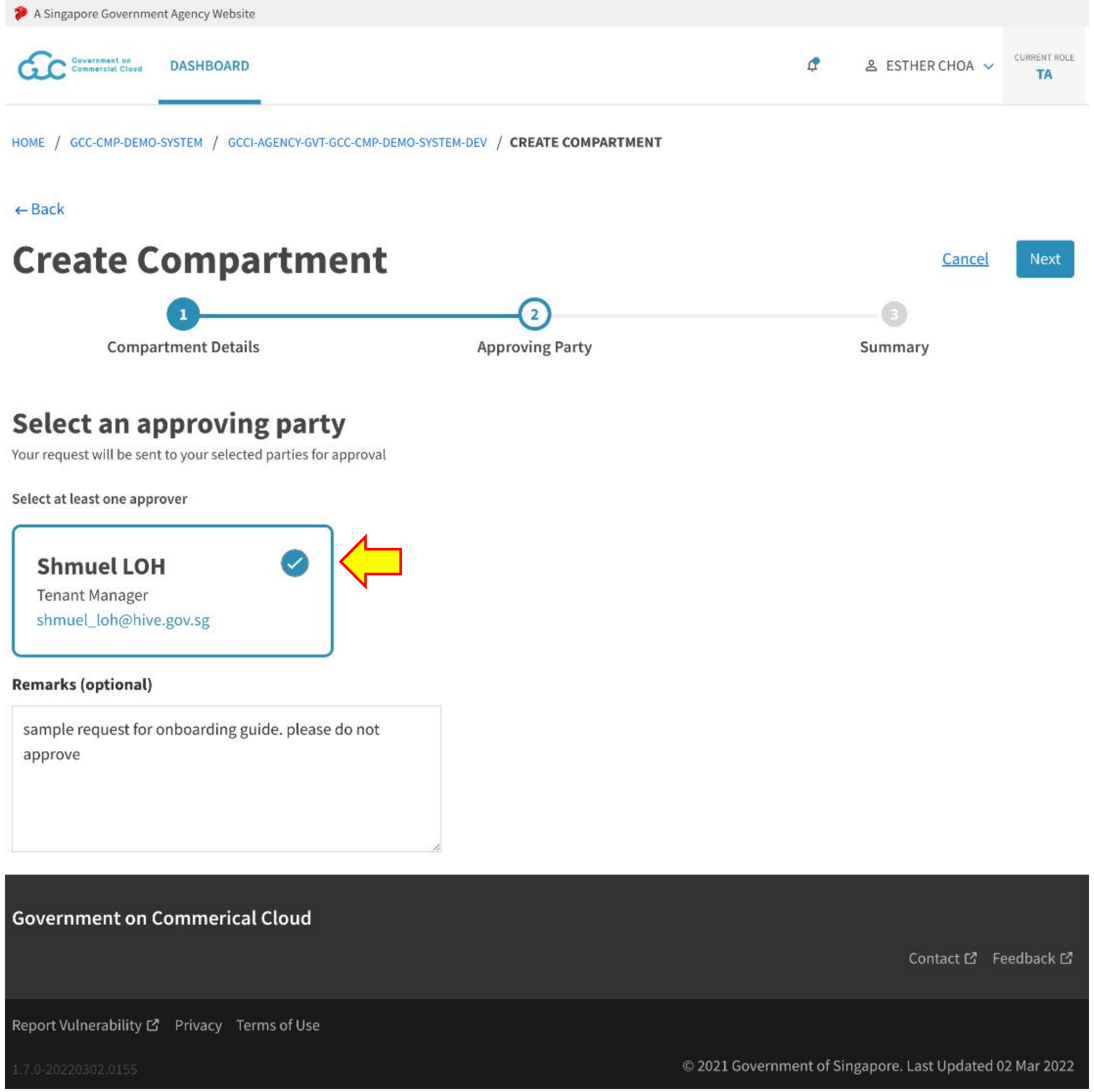
Compartment Type: INTRANET

CIDR Range: /26

Government on Commerical Cloud

1.7.0-20220302.0155

© 2021 Government of Singapore. Last Updated 02 Mar 2022



A Singapore Government Agency Website

HOME / GCC-CMP-DEMO-SYSTEM / GCCI-AGENCY-GVT-GCC-CMP-DEMO-SYSTEM-DEV / CREATE COMPARTMENT

← Back

Create Compartment

Select an approving party

Your request will be sent to your selected parties for approval

Select at least one approver

☑ **Shmuel LOH**
Tenant Manager
shmuel_loh@hive.gov.sg

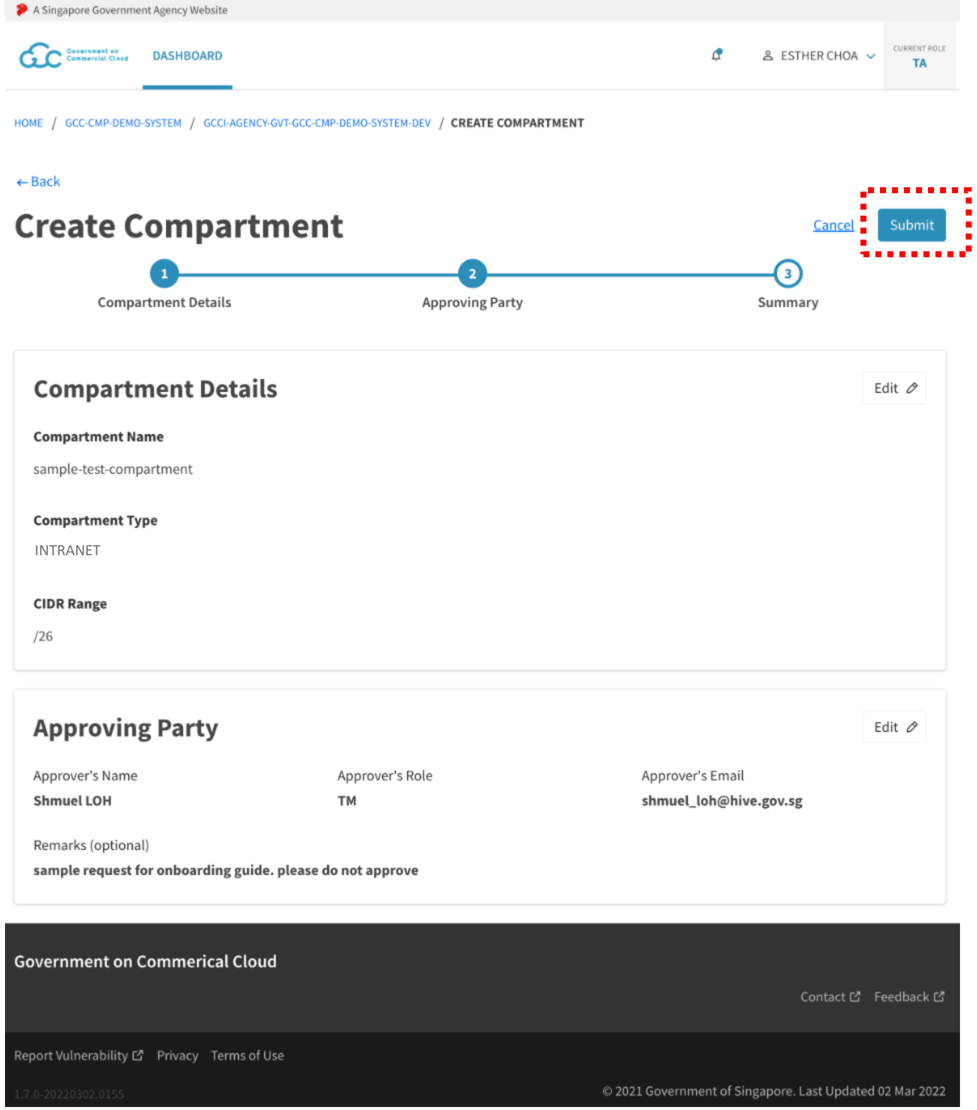
Remarks (optional): sample request for onboarding guide. please do not approve

Government on Commerical Cloud

1.7.0-20220302.0155

© 2021 Government of Singapore. Last Updated 02 Mar 2022

GCC 2.0 CMP for GEN Routable(INTRANET) compartment provisioning (3/4)



A Singapore Government Agency Website

DASHBOARD   ESTHER CHOA   CURRENT ROLE TA

HOME / GCC-CMP-DEMO-SYSTEM / GCCI-AGENCY-GVT-GCC-CMP-DEMO-SYSTEM-DEV / CREATE COMPARTMENT

← Back

Create Compartment   Cancel   Submit

1 Compartment Details — 2 Approving Party — 3 Summary

Compartment Details   Edit

Compartment Name
sample-test-compartment

Compartment Type
INTRANET

CIDR Range
/26

Approving Party   Edit

Approver's Name	Approver's Role	Approver's Email
Shmuel LOH	**TM**	**shmuel_loh@hive.gov.sg**

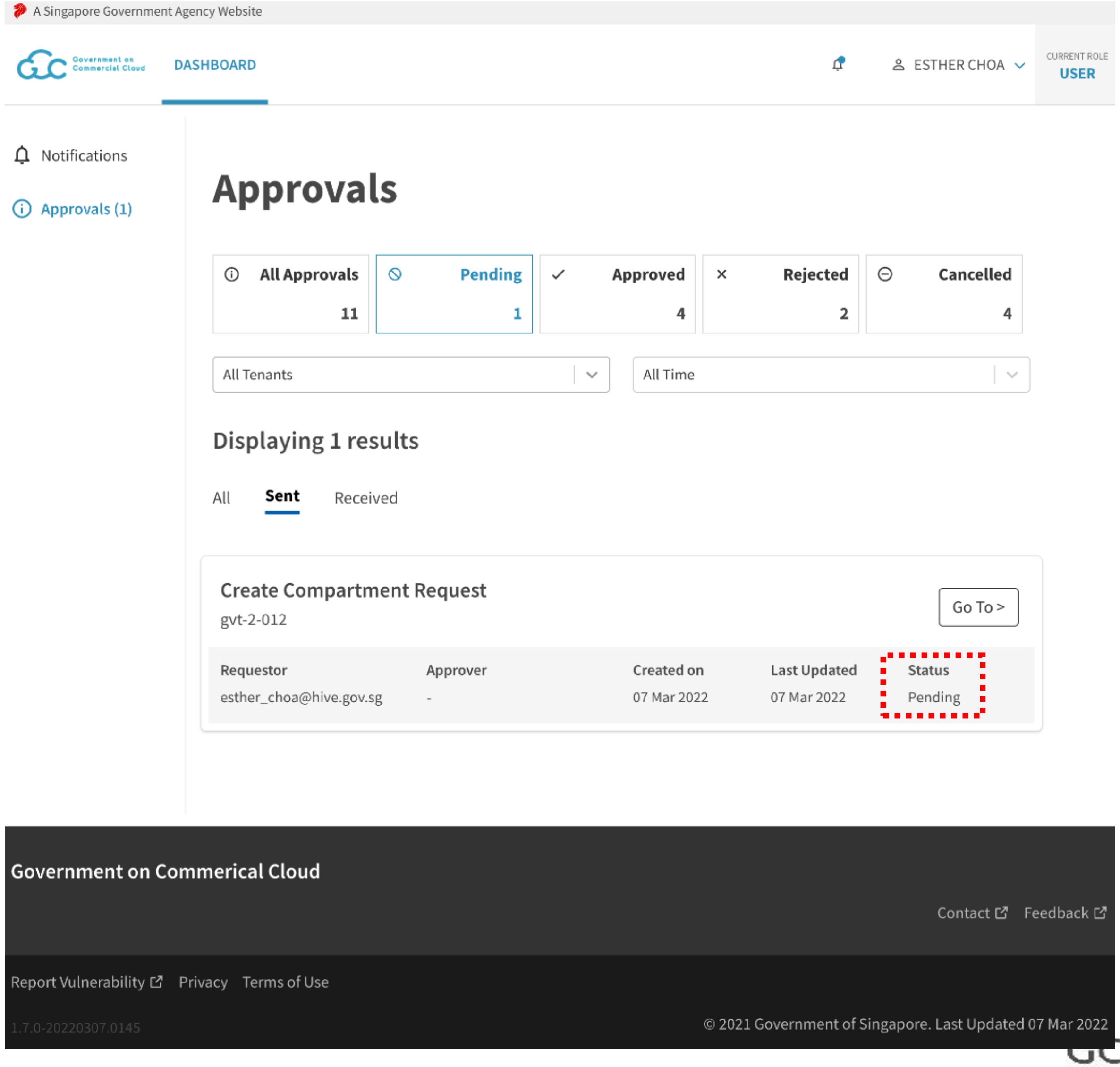
Remarks (optional)
sample request for onboarding guide. please do not approve

Government on Commerical Cloud

Contact   Feedback

Report Vulnerability   Privacy   Terms of Use

1.7.0-20220302.0155   © 2021 Government of Singapore. Last Updated 02 Mar 2022



A Singapore Government Agency Website

DASHBOARD   ESTHER CHOA   CURRENT ROLE USER

Notifications

Approvals (1)

Approvals

All Approvals	Pending	Approved	Rejected	Cancelled
11	1	4	2	4

All Tenants   All Time

Displaying 1 results

All   **Sent**   Received

Create Compartment Request
gvt-2-012   Go To >

Requestor	Approver	Created on	Last Updated	Status
esther_choa@hive.gov.sg	-	07 Mar 2022	07 Mar 2022	Pending

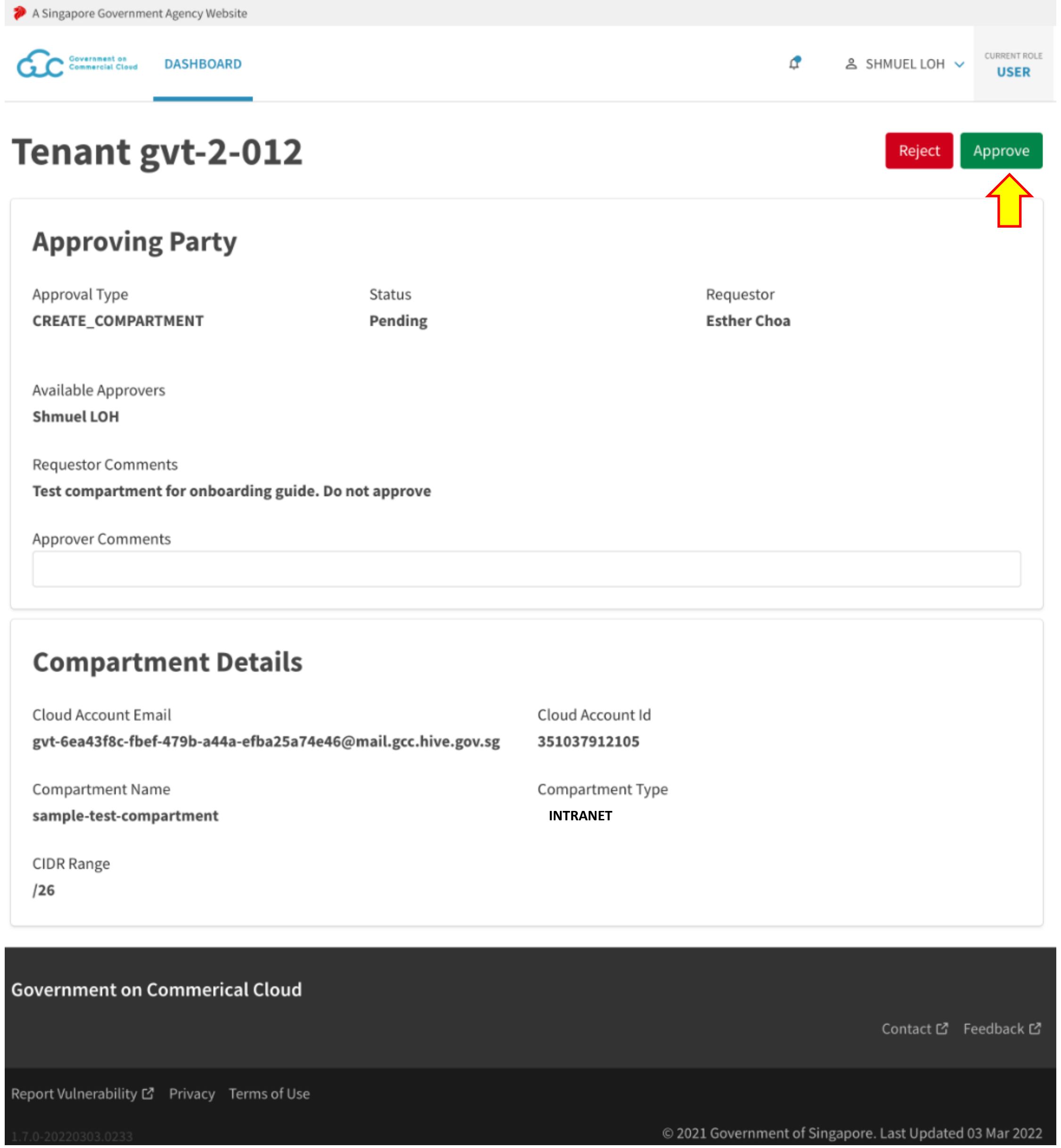
Government on Commerical Cloud

Contact   Feedback

Report Vulnerability   Privacy   Terms of Use

1.7.0-20220307.0145   © 2021 Government of Singapore. Last Updated 07 Mar 2022

GCC 2.0 CMP for GEN Routable(INTRANET) compartment provisioning (4/4)



A Singapore Government Agency Website

DASHBOARD

SHMUEL LOH

CURRENT ROLE
USER

Tenant gvt-2-012

Reject Approve

Approving Party

Approval Type
CREATE_COMPARTMENT

Status
Pending

Requestor
Esther Choa

Available Approvers
Shmuel LOH

Requestor Comments
Test compartment for onboarding guide. Do not approve

Approver Comments

Compartment Details

Cloud Account Email
gvt-6ea43f8c-fbef-479b-a44a-efba25a74e46@mail.gcc.hive.gov.sg

Cloud Account Id
351037912105

Compartment Name
sample-test-compartment

Compartment Type
INTRANET

CIDR Range
/26

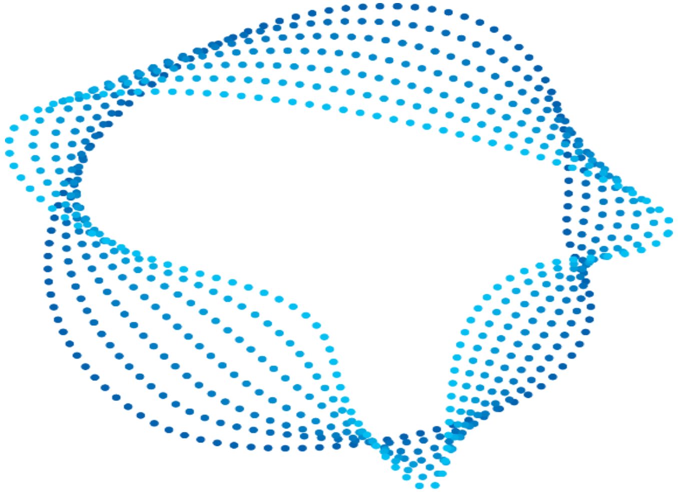
Government on Commerical Cloud

Contact Feedback

Report Vulnerability Privacy Terms of Use

1.7.0-20220303.0233

© 2021 Government of Singapore. Last Updated 03 Mar 2022



Frequently Asked Questions (FAQs)

FAQs

- Can Agency managed compartment connect to Common Services TGW or GEN TGW ?

  No, unfortunately Agency managed compartments can't connect to Common Services TGW or GEN TGW. Agencies needs to provision GEN Routable(INTRANET) or Non-GEN Routable(Internet) compartments from GCC 2.0 CMP which default includes GCC Common Services CIDR.

- Can Agency attach Non-GEN routable IPs as secondary or subsequent CIDRs to GEN Routable(INTRANET) compartment to conserve GEN routable IPs ?

  Yes, Agencies are encouraged to leverage on Non-GEN routable IPs if the workloads don't need to connect back to GEN(On-prem).

- How is the lifecycle of migrated compartments from GCC 1.0 managed ?

  Migrated compartments' lifecycle will be covered in future migration workshops. It will likely be migrated 'As-Is'.

- Are Agencies able to use AWS IPAM in their accounts ?

  AWS IPAM is on our feature roadmap, we will announce to Agencies in a future workshop on how would the deployment be done & rolled out.

Agency Managed AWS
Transit Gateway (TGW)

1. Overview

Agency managed AWS Transit Gateway (TGW) in GCC 2.0

What is new about this in GCC 2.0 as compared to GCC 1.0 ?

- In GCC 1.0, Agency is now able to create and manage Transit Gateway (TGW) for their compartments from the AWS Console, **<u>except</u>** for the following operations :-
  - Create TGW Attachment
  - Accept TGW Attachment
  - Share TGW

- In GCC 2.0 will be able to perform all operations/configurations related to Agency managed Transit Gateway(TGW)

- For Agency managed TGW it would be possible to connect to other network components/services e.g VPC, TGW(Intra region), Direct Connect & Site to Site IPsec VPN, note these are Agency managed as well

- We would like to further share the best practices for AWS Transit Gateway in the following slides …

AWS Transit Gateway – Key Features and Benefits

- Fully managed and highly available
- Scales to support thousands of VPCs across accounts
- Hybrid connectivity via Direct Connect, VPN
- Simplified management and network visibility
- Ability to peer TGW with other TGW (intra-region peering)
  - New feature, available since Re:Invent 2021

AWS Transit Gateway – Use Cases

Interconnecting Geographically Dispersed On-Premise and VPC resources

- Customer with multiple VPCs
- Build applications that span a large number of VPCs
- Share network services (DNS, Active Directory, Firewall, IDS)
- Reduce management overhead

Edge Consolidation

- Share a common VPN or Direct Connect Gateway (DXGW) across VPCs
- Reduce time to connect on-premises resources to multiple VPCs
- No additional customer network changes required when adding a VPC to AWS Transit Gateway

Digital security and threat intelligence

- Shared VPC hosts security tools
- AWS Network Firewall, Third Party Firewall with Gateway Load Balancer (GWLB), Web application Firewall (WAF), etc
- Scales out over native AWS Services

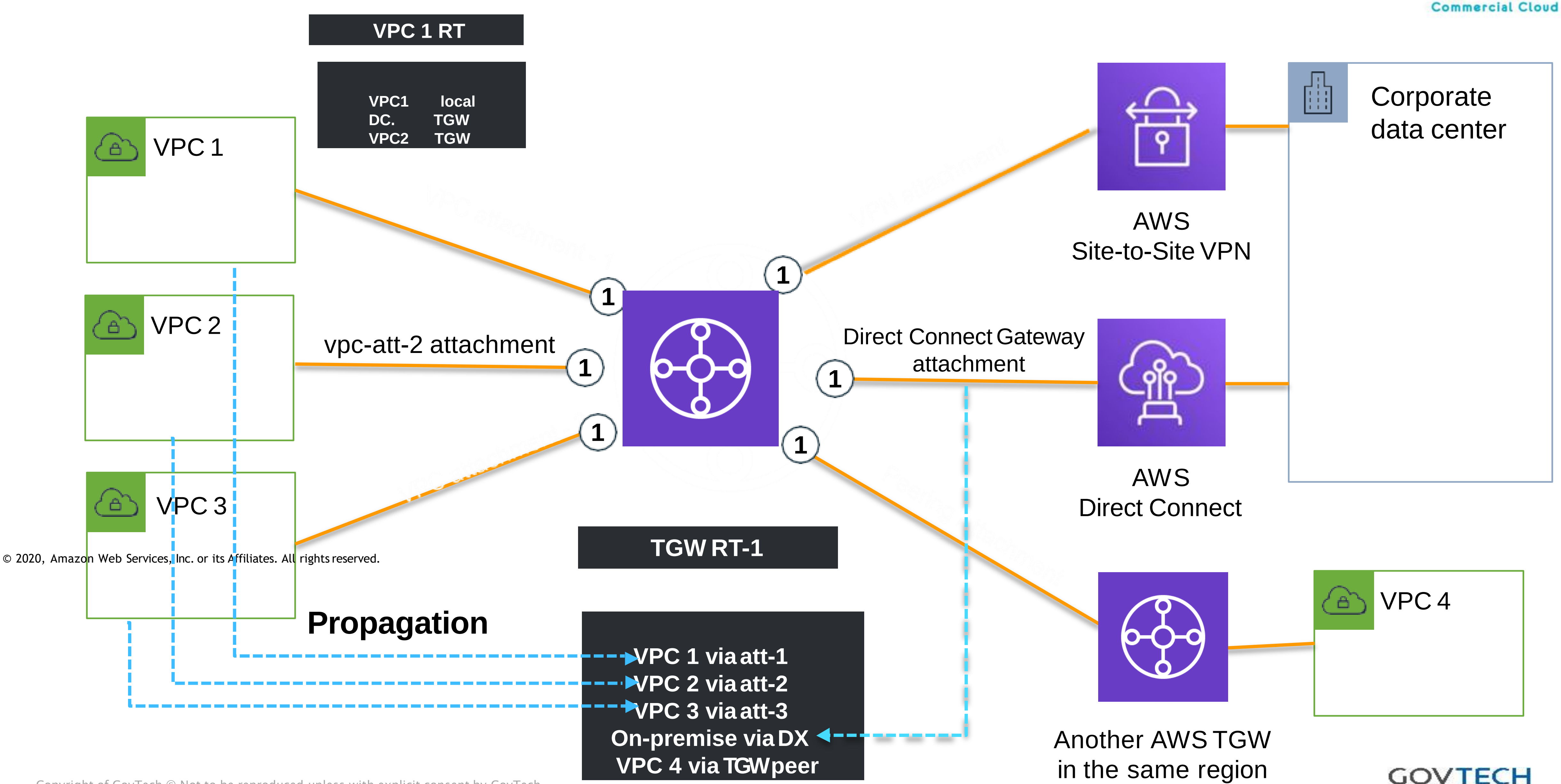
Interconnecting Multicast Based Applications

- Enable Media Distribution and Financial Applications migration to AWS Cloud
- Clustering use-cases

AWS Transit Gateway Components

- Attachment types = VPN, VPC, DX Gateway and peering to another TGW
- TGW route table = To indicate next hop based on packet destination IP -> target of the routes would be TGW attachments
- TGW association = Maps an attachment to a route table [1 attachment is associated with exactly 1 route table]
- TGW route propagation = Routes can be static routes (TGW peering attachments) or propagated via BGP (VPN, DX Gateway attachments)

AWS Transit Gateway Routing



VPC 1 RT

VPC1	local
DC.	TGW
VPC2	TGW

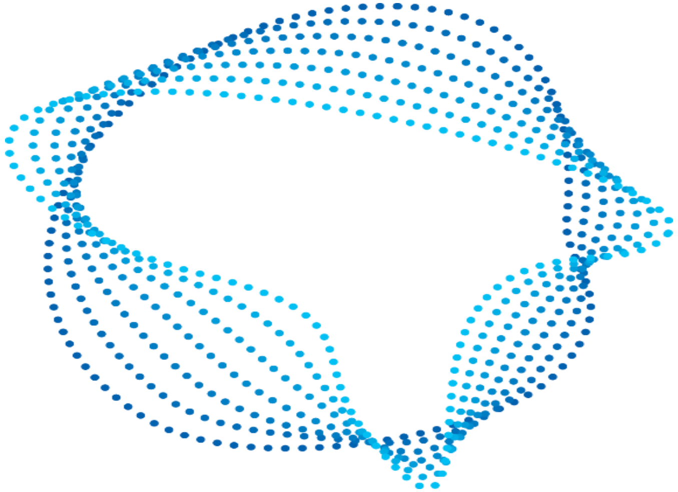
TGW RT-1

VPC 1 via att-1
VPC 2 via att-2
VPC 3 via att-3
On-premise via DX
VPC 4 via TGW peer

AWS Transit Gateway Route Evaluation Order

- TGW routes are evaluated in the following order:
  - The most specific route for the destination address
  - For routes with the same destination IP address but different targets, the route priority is:
    - → Static routes
    - → Prefix list referenced routes
    - → VPC propagated routes
    - → DX GW propagated routes
    - → Site to Site VPN propagated routes

Agency managed AWS
Transit Gateway (TGW)



2. Traffic Control Mechanisms

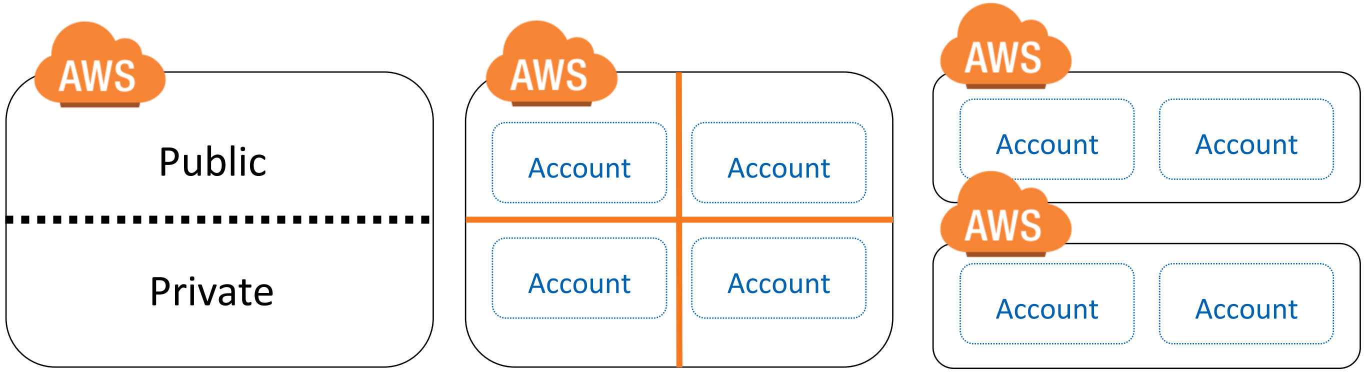
Segmentation options: Layers

Inside the account

- IAM users and roles
- Security groups

At the VPC

- Route tables
- Network ACLs
- Separate VPCs



Tenant configuration

Baseline security

IAM: Control actions and privileges inside the account between users and role

Security groups: Whitelist ports, protocols, and other security groups for network access

Tenant and infrastructure shared security line

Network security

Infrastructure configuration

Route tables: Route table policy defines what VPC resources can access on the network

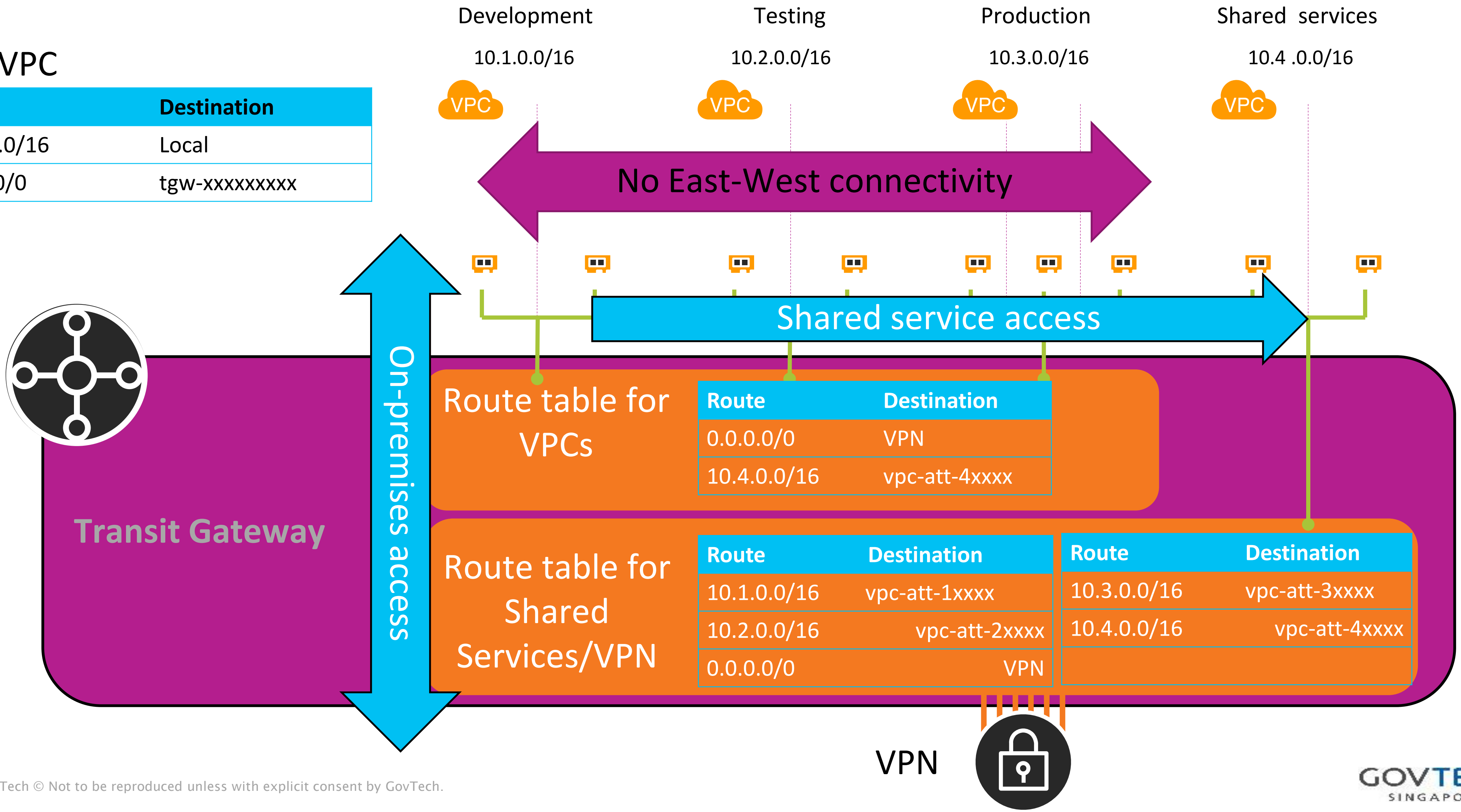
Network ACLs: Fence off access between specific subnets, ports, or destinations.

Separate VPCs: Full separation from other tenants.

Transit Gateway Route Domains

Per VPC

Route	Destination
10.x.0.0/16	Local
0.0.0.0/0	tgw-xxxxxxxxx



Route table for VPCs

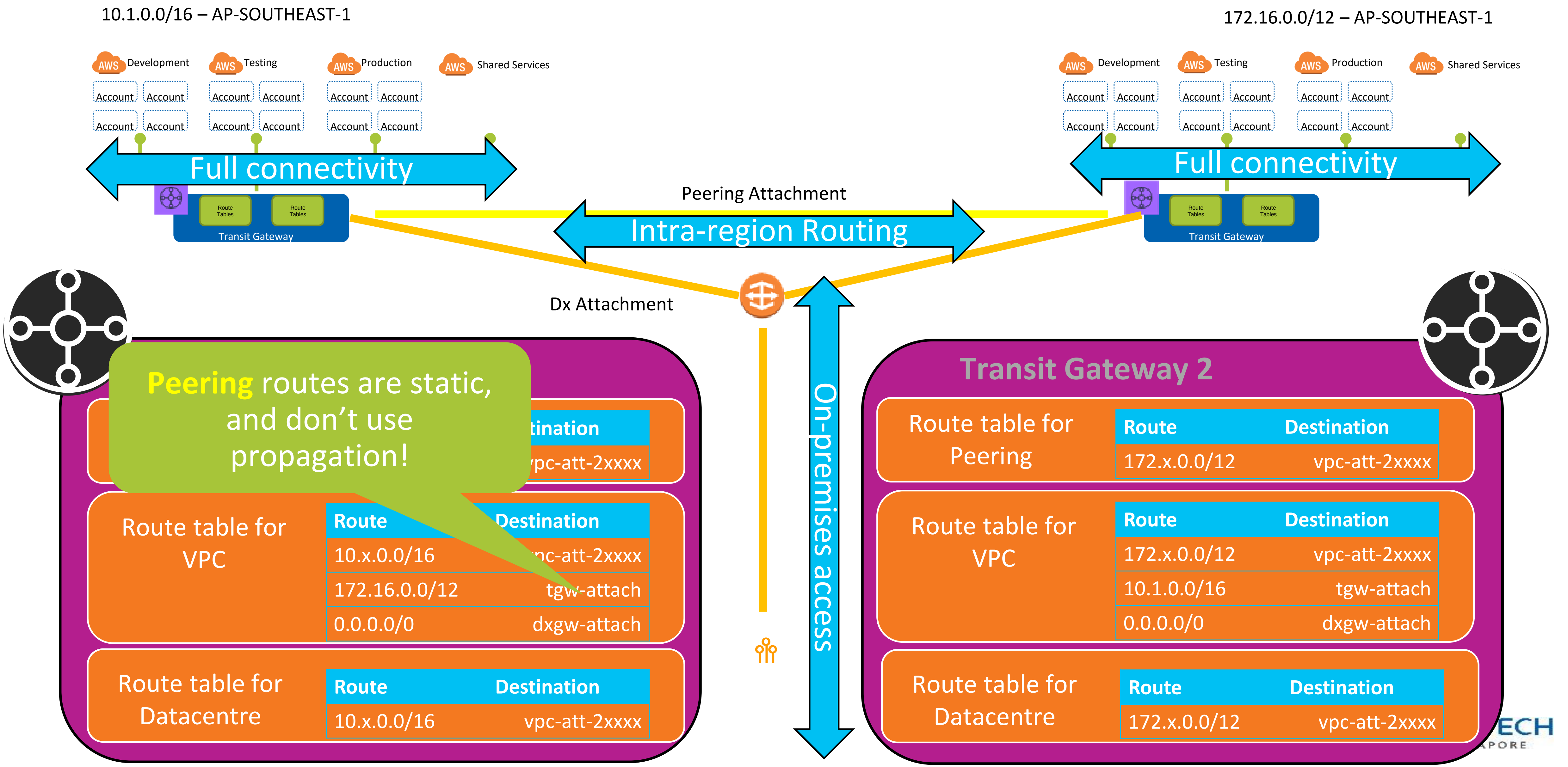
Route	Destination
0.0.0.0/0	VPN
10.4.0.0/16	vpc-att-4xxxx

Route table for Shared Services/VPN

Route	Destination
10.1.0.0/16	vpc-att-1xxxx
10.2.0.0/16	vpc-att-2xxxx
0.0.0.0/0	VPN

Route	Destination
10.3.0.0/16	vpc-att-3xxxx
10.4.0.0/16	vpc-att-4xxxx

Transit Gateway Intra-Region Peering



Peering routes are static, and don't use propagation!

	tination
	vpc-att-2xxxx

Route table for VPC

Route	Destination
10.x.0.0/16	pc-att-2xxxx
172.16.0.0/12	tgw-attach
0.0.0.0/0	dxgw-attach

Route table for Datacentre

Route	Destination
10.x.0.0/16	vpc-att-2xxxx

Transit Gateway 2

Route table for Peering

Route	Destination
172.x.0.0/12	vpc-att-2xxxx

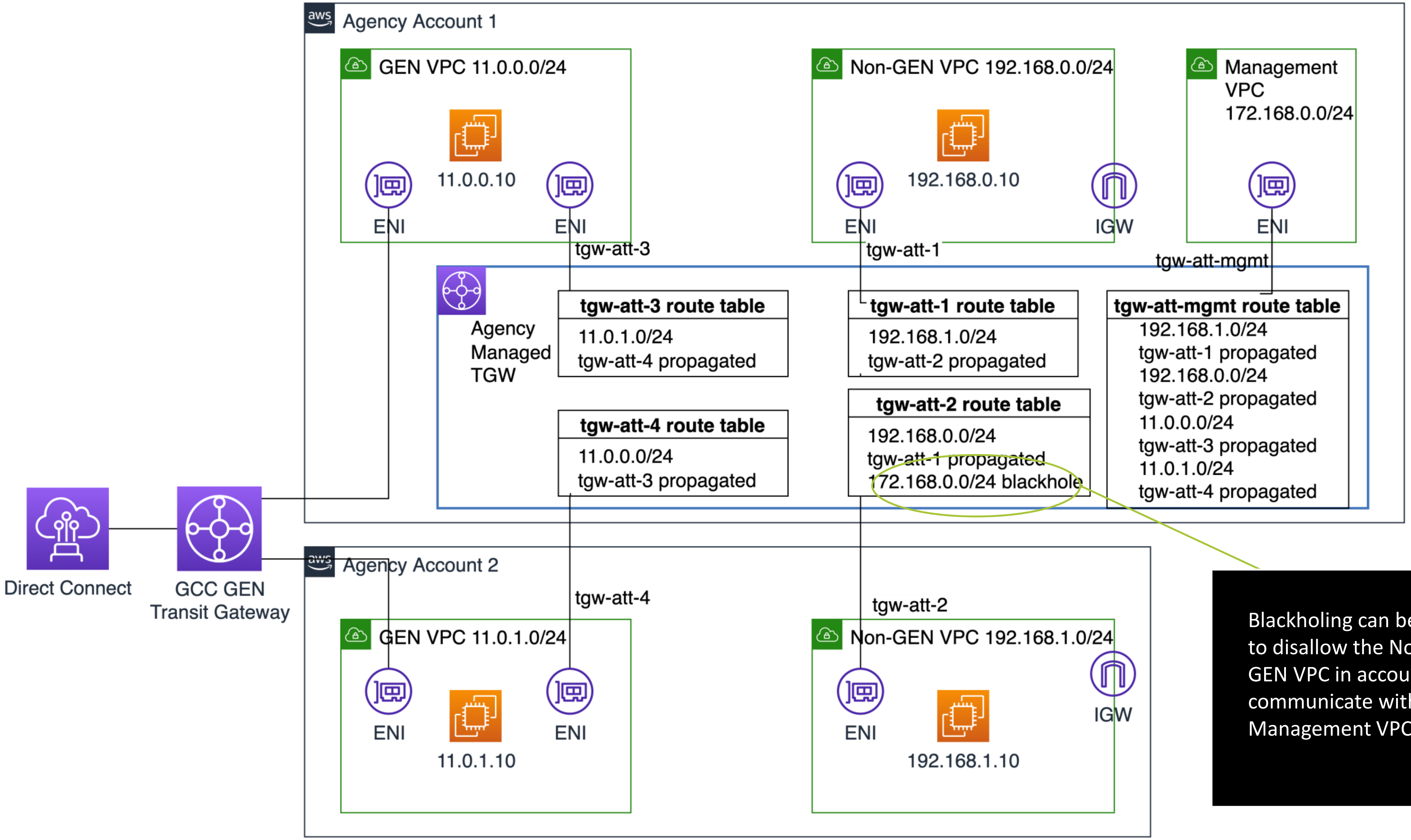
Route table for VPC

Route	Destination
172.x.0.0/12	vpc-att-2xxxx
10.1.0.0/16	tgw-attach
0.0.0.0/0	dxgw-attach

Route table for Datacentre

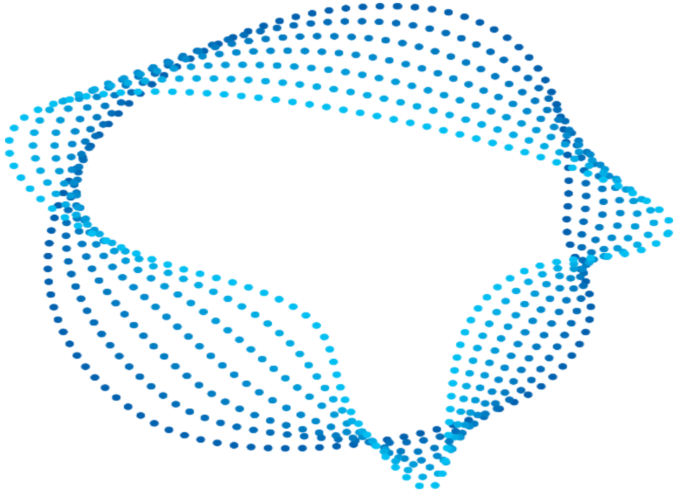
Route	Destination
172.x.0.0/12	vpc-att-2xxxx

Agency-Managed TGW Setup Example



Blackholing can be used to disallow the Non-GEN VPC in account 2 to communicate with Management VPC

Agency managed AWS Transit Gateway (TGW)



2. Best Practices & Service Limits

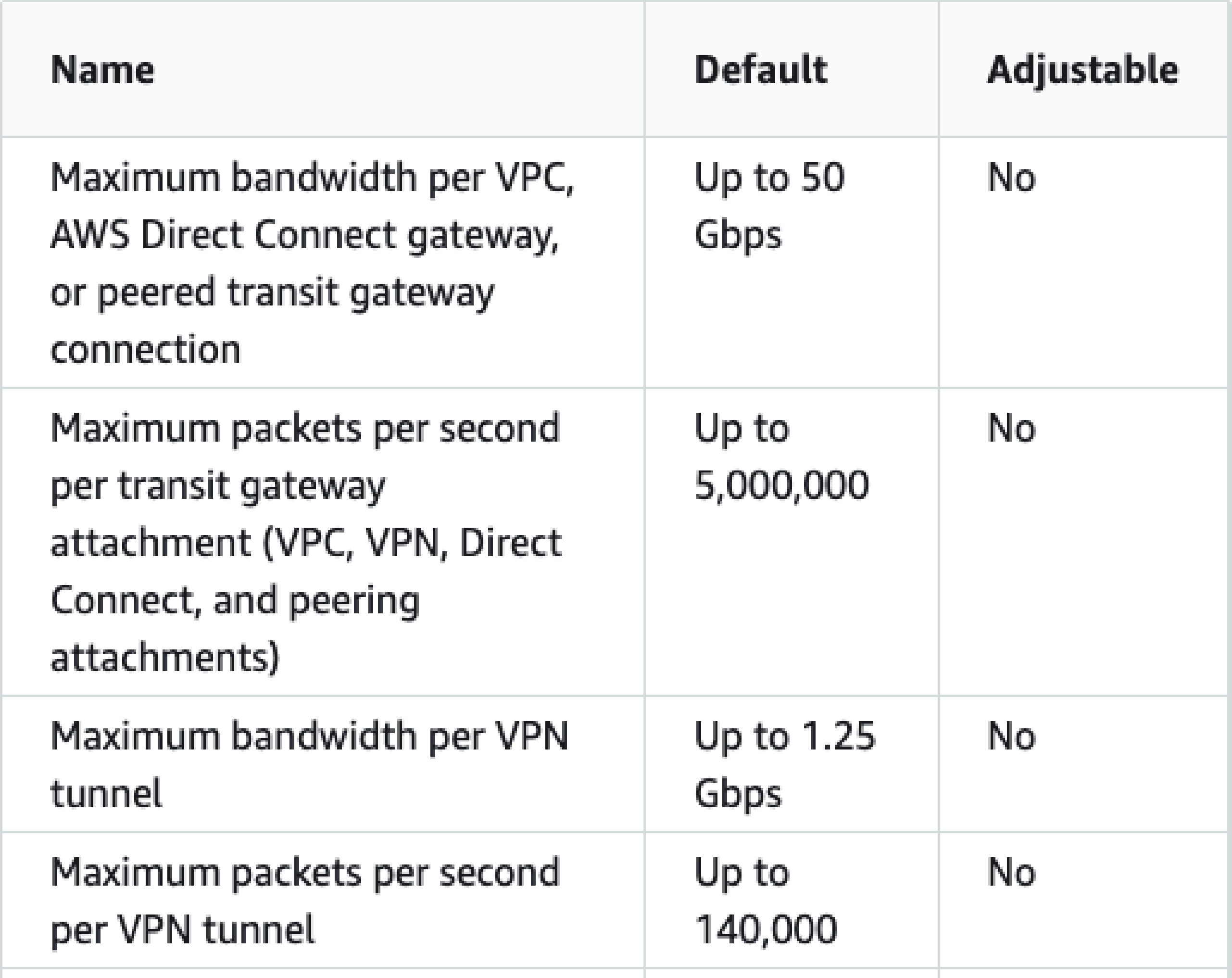
AWS Transit Gateway Best Practices

- Use separate subnets for TGW VPC attachments and your workload subnets.
- When migrating from VPC peering to AWS TGW, keep in mind that
  - A TGW does not support security group referencing
  - A MTU size mismatch between VPC peering and TGW might result in packet drops -> Update both VPCs at the same time to avoid jumbo packets dropping.
  - No need to provision additional TGW for HA, since TGW are highly available by design.

Service Limits

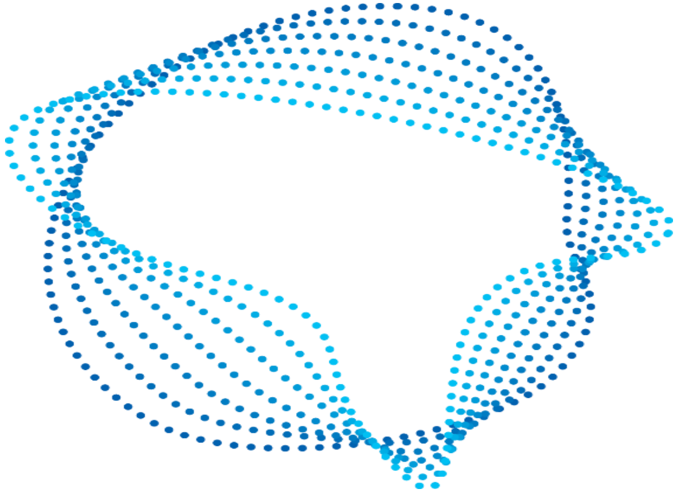
- Up to 5 TGW per AWS account – adjustable quota
- Up to 5 TGW per VPC – adjustable quota
- Up to 20 TGW route tables per TGW – adjustable quota
- Up to 10000 static routes per TGW – adjustable quota
- Up to 5000 attachments per TGW – adjustable quota
- Up to 50 peering attachments per TGW – adjustable quota
- Up to 20 DX GW per TGW – not adjustable
- Up to 3 TGW per DX GW – not adjustable

Service Limits - Bandwidth



Name	Default	Adjustable
Maximum bandwidth per VPC, AWS Direct Connect gateway, or peered transit gateway connection	Up to 50 Gbps	No
Maximum packets per second per transit gateway attachment (VPC, VPN, Direct Connect, and peering attachments)	Up to 5,000,000	No
Maximum bandwidth per VPN tunnel	Up to 1.25 Gbps	No
Maximum packets per second per VPN tunnel	Up to 140,000	No

AWS Direct Connect (DX)



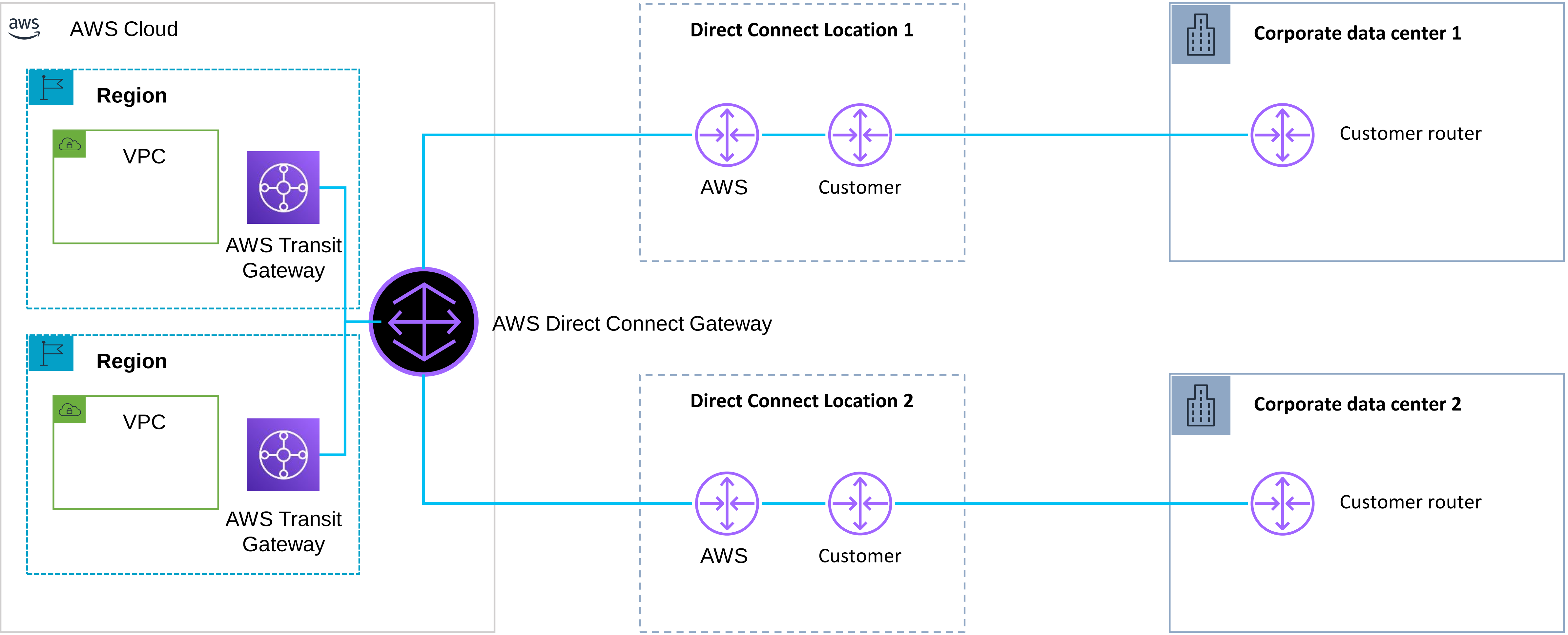
Dedicated Connection
or
Hosted Connection

AWS Direct Connect Overview

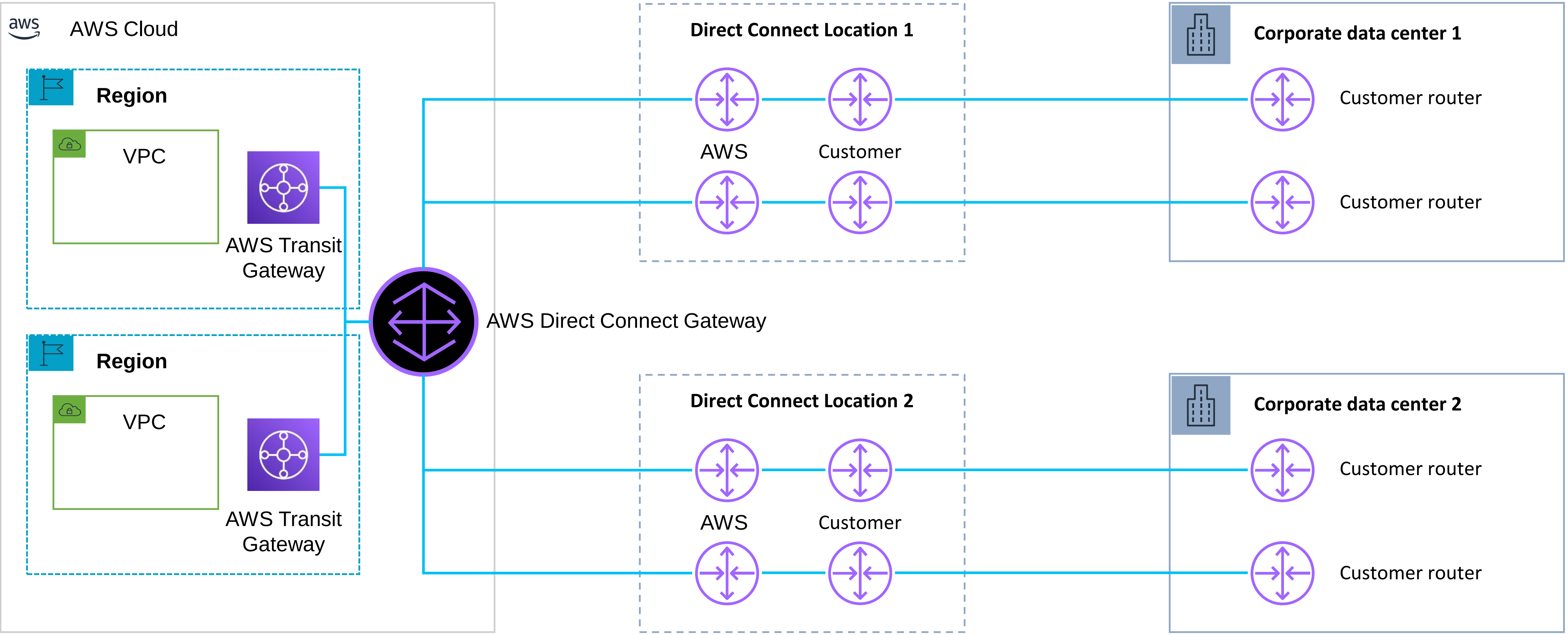
Bypass the public internet and connect directly to AWS

- Improve application performance by connecting directly to AWS, bypassing the public internet
- Speeds from 50 Mbps to 100 Gbps (200 Gbps using a LAG)
- Over 100 PoPs worldwide
- Protect data in transit with multiple encryption options, including MACsec
- May help reduce your networking costs with low data-transfer-out rates and no ingress fees
- Flexible deployment options: dedicated (by AWS) or hosted (by Partners)

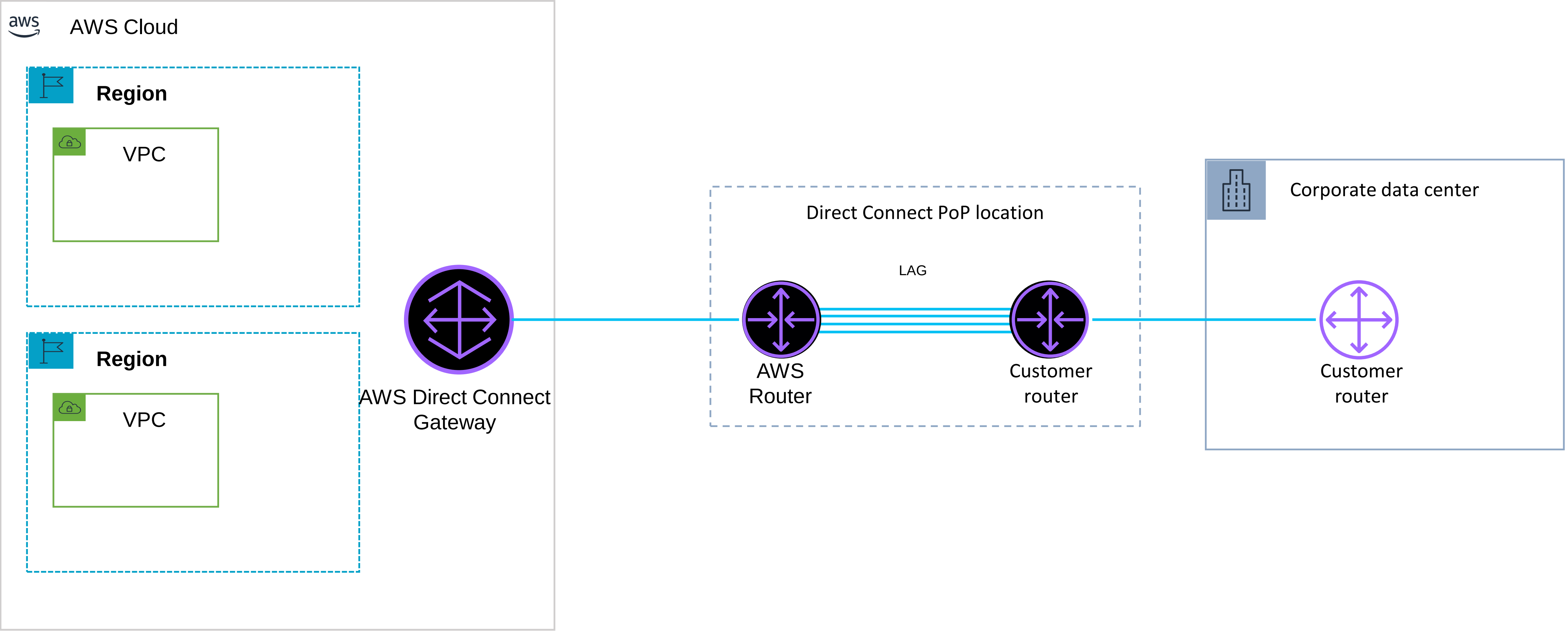
Deployment – High resiliency



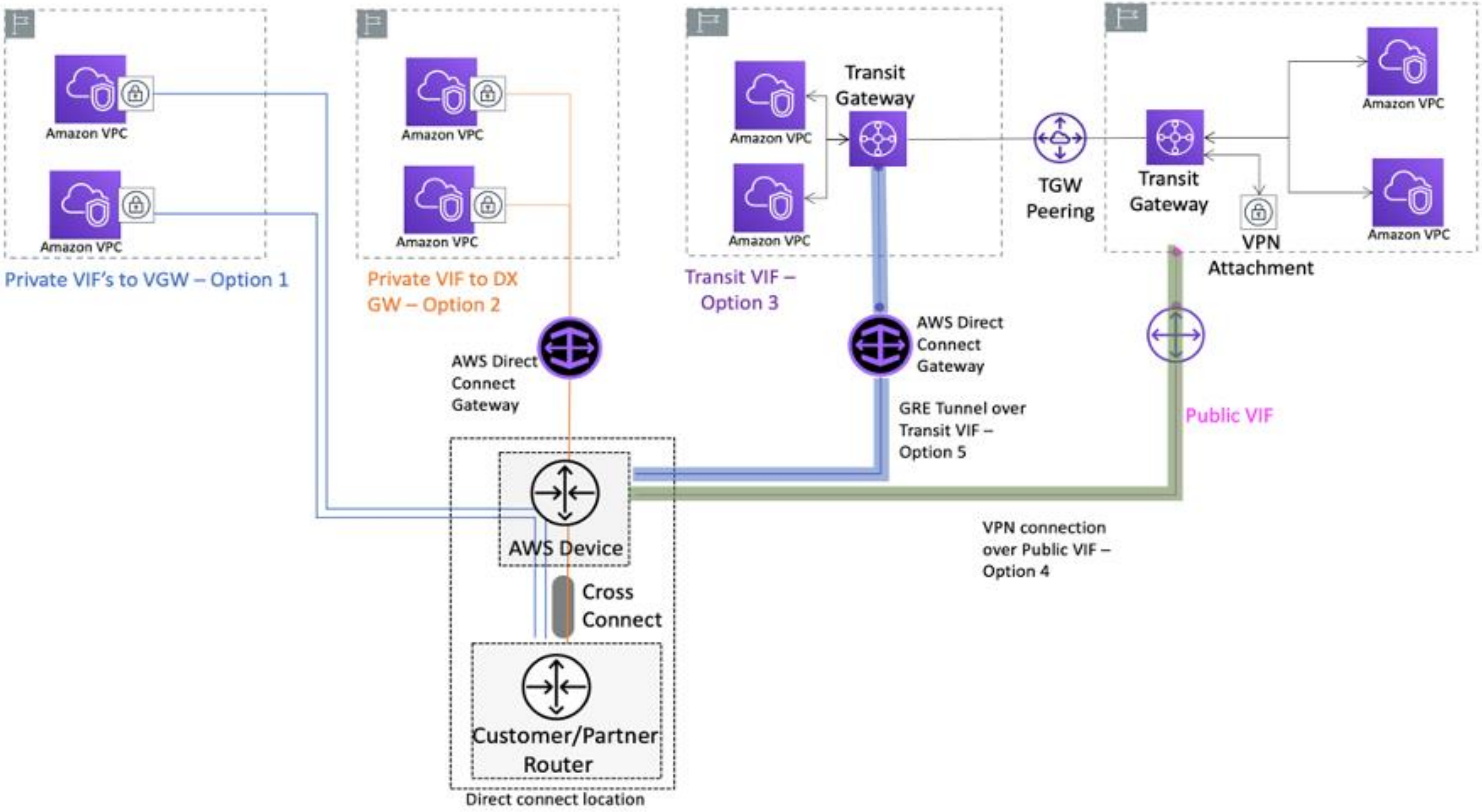
Deployment – Maximum resiliency



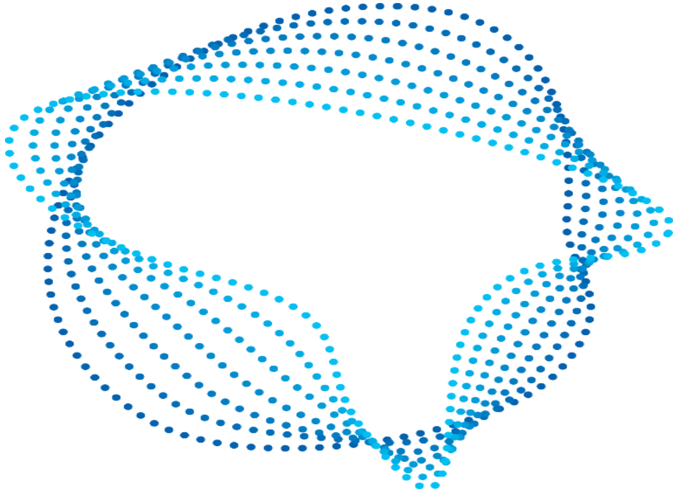
Link aggregation groups (LAGs)



DX Connectivity Options



VPN Solutions on AWS



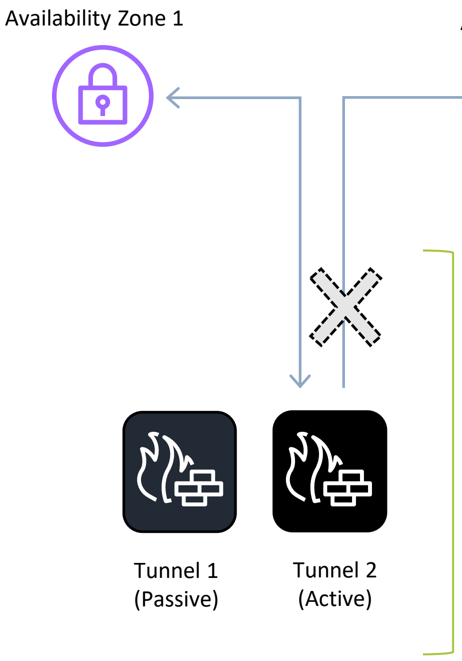
Site-to-Site (S2S) IPsec VPN

AWS Site-to-Site IPsec VPN

- Fully managed and highly available VPN termination endpoints at AWS end
- Two VPN tunnels per one VPN connection
- IPsec Site-to-Site tunnel with AES-256, SHA-2, and latest DH groups
- Support for NAT-T
- Charged per hour per VPN connection

AWS Site-to-Site IPsec VPN setup options

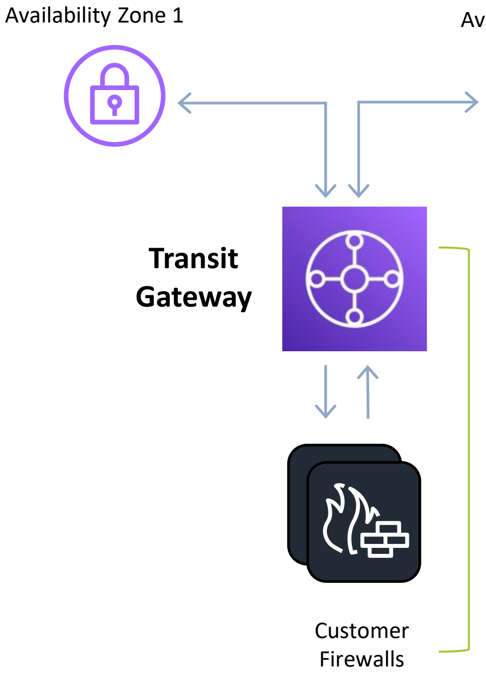
Static



Management of static routes
Passive tunnel sits idle
Manual failover

172.16.0.0
172.16.1.0
172.16.2.0

Dynamic



Higher availability
Detect failures
Load balancing (ECMP)
Fault tolerant

AWS Site-to-Site IPsec VPN Authentication

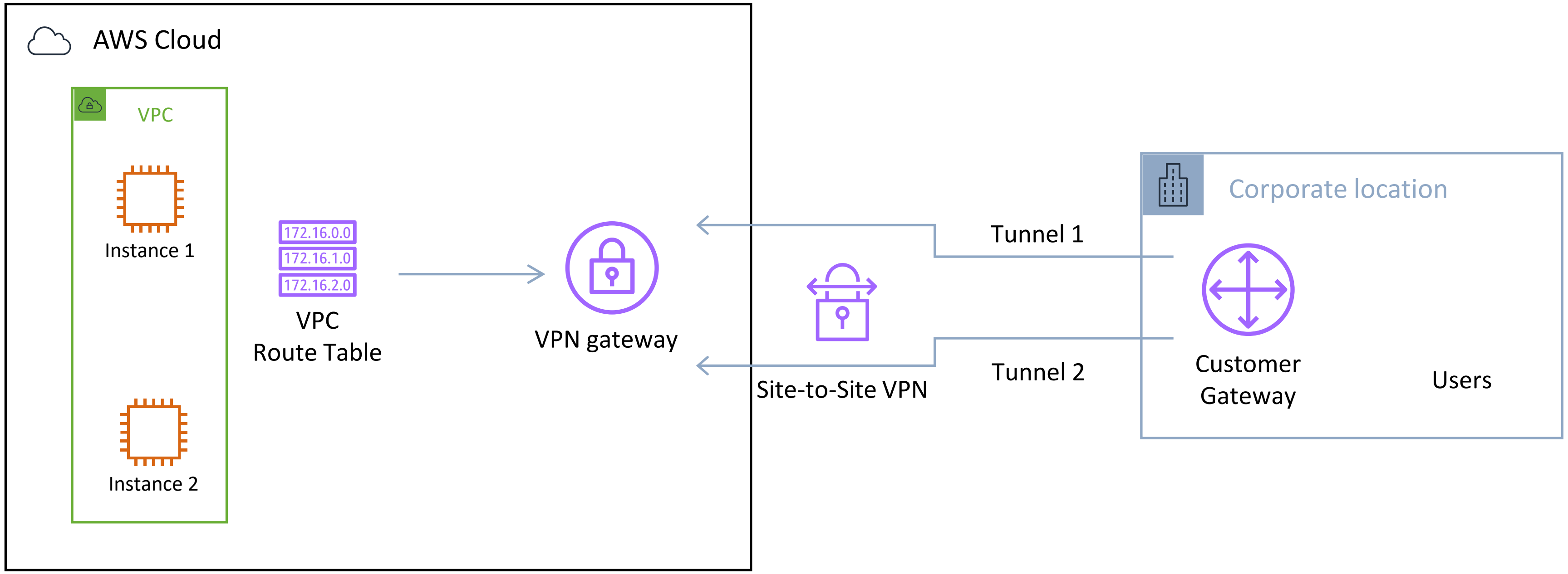
Pre Shared Keys

- Default authentication option
- Customer specified or automatically generated
- Modify existing PSK if needed

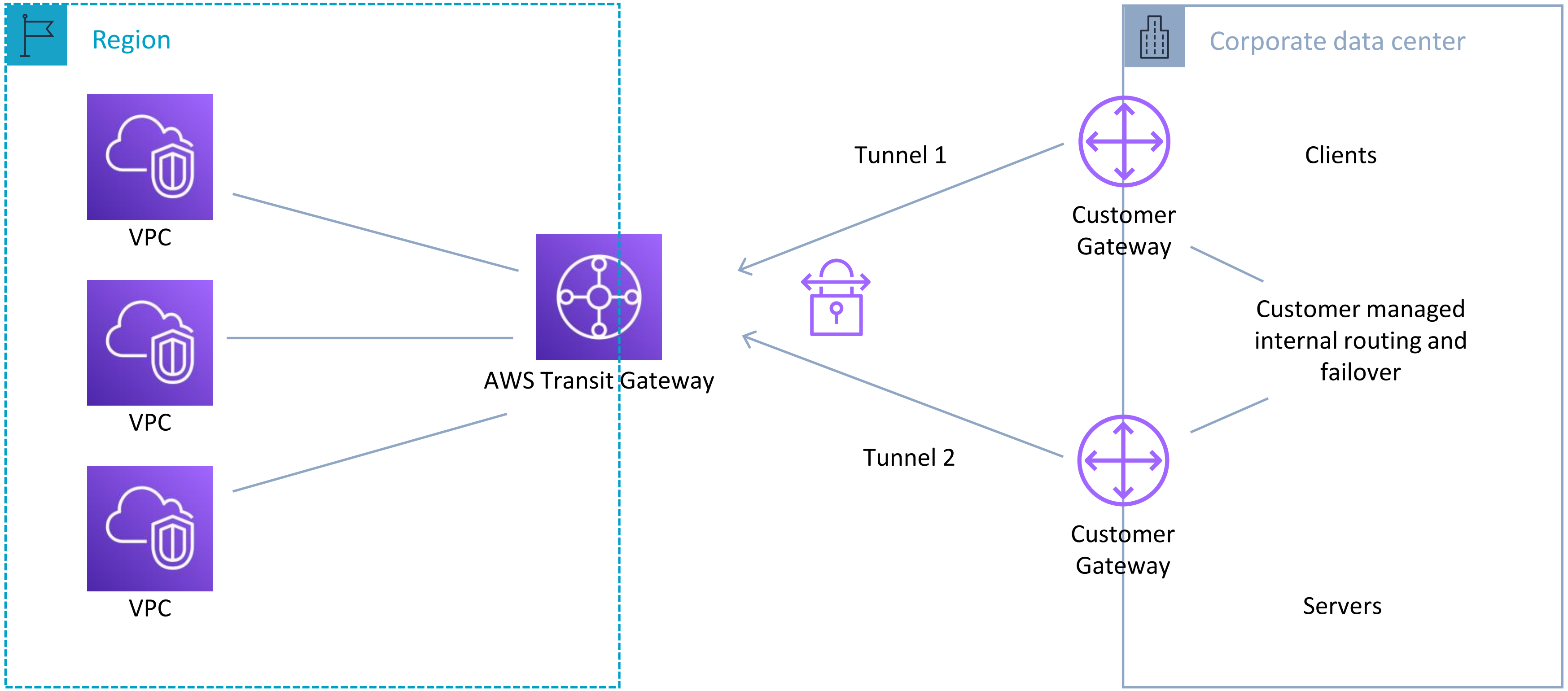
Cert Based Authentication

- Using private certs from AWS Certificate Manager Private CA
- Revoke cert on demand
- Easily change CGW IP address

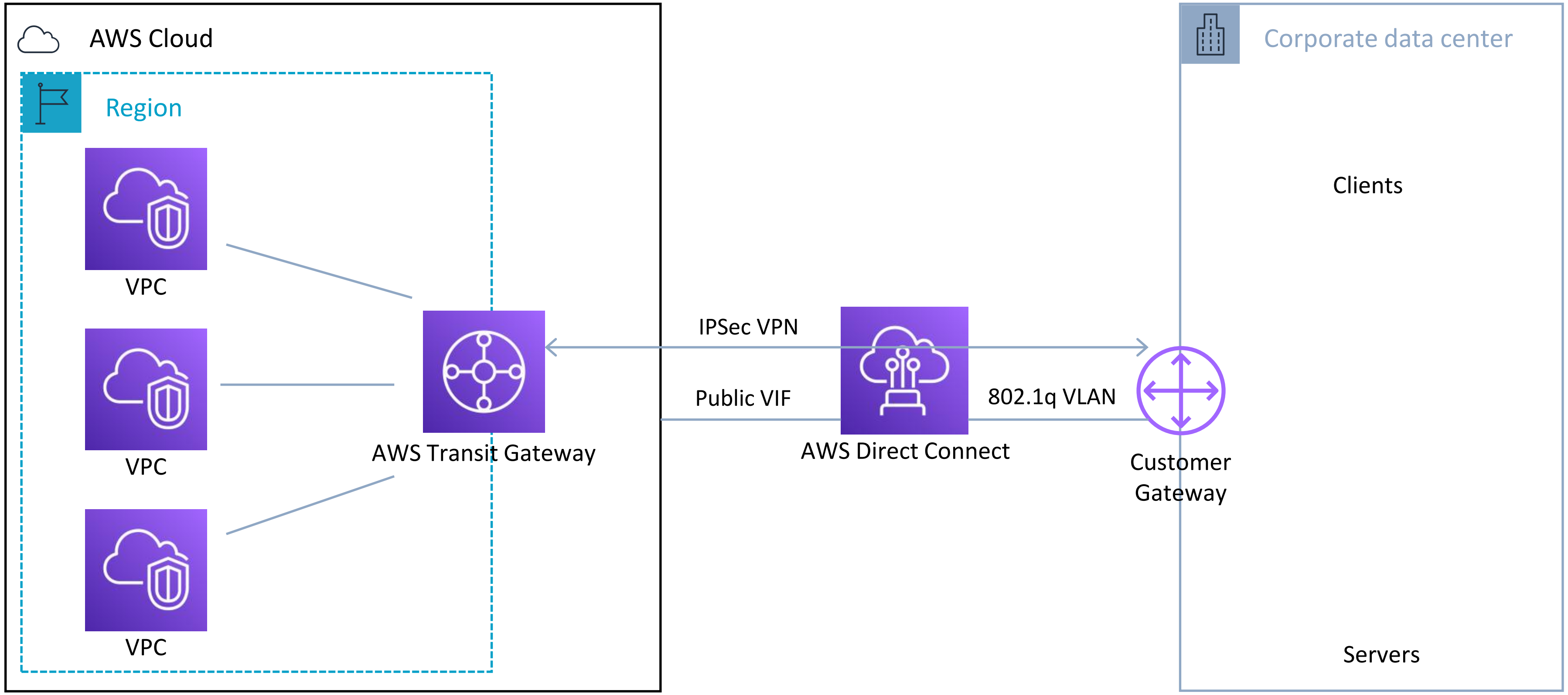
Site-to-Site IPsec VPN Setup



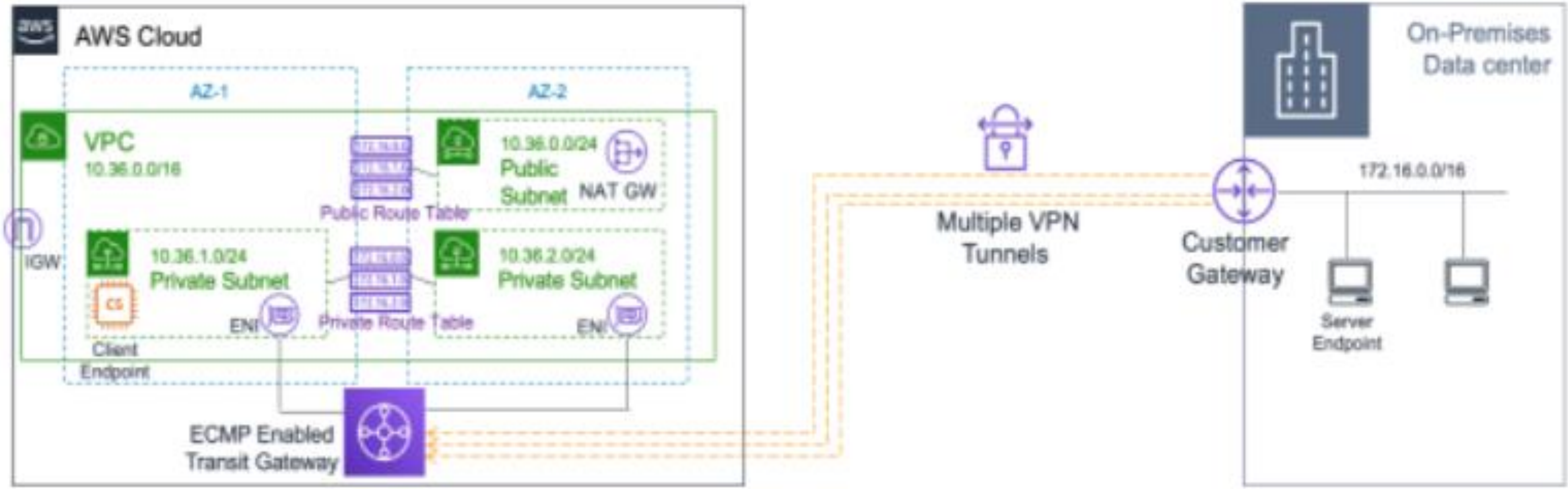
AWS TGW + Site-to-Site IPsec VPN



AWS TGW + DX + Site-to-Site IPsec VPN



Scaling VPN Throughput using AWS TGW



THANK YOU

Questions and Answers

We Want to Hear Your Feedback!

https://form.gov.sg/625cbcecf319210013fe01b3

- Let us know what went well and how we can improve.
- We want to ensure that we are bringing the right contents to you so as to help Agencies.
- If you have any questions, please reach out to us at Ask_CODEX@tech.gov.sg