AWS re:Inforce

JUNE 13 - 14, 2023 | ANAHEIM, CA

NIS331-R1

Security inspection architectures with AWS Cloud WAN

Mehar Swarup (he/him)
Sr. Solutions Architect
AWS

Pratik R. Mankad (he/him)
Sr. Network Specialist Solutions Architect
AWS

Expectations and rules of engagement

This is a chalk talk, so don’t hesitate to ask questions!

Since this is a 300-level chalk talk, we assume an associate-level solutions architect knowledge of Amazon Web Services (AWS services, VPCs, multi-VPC networking, inspection and hybrid architectures)

We’ll be available after the session to answer any additional questions and discuss further

Agenda

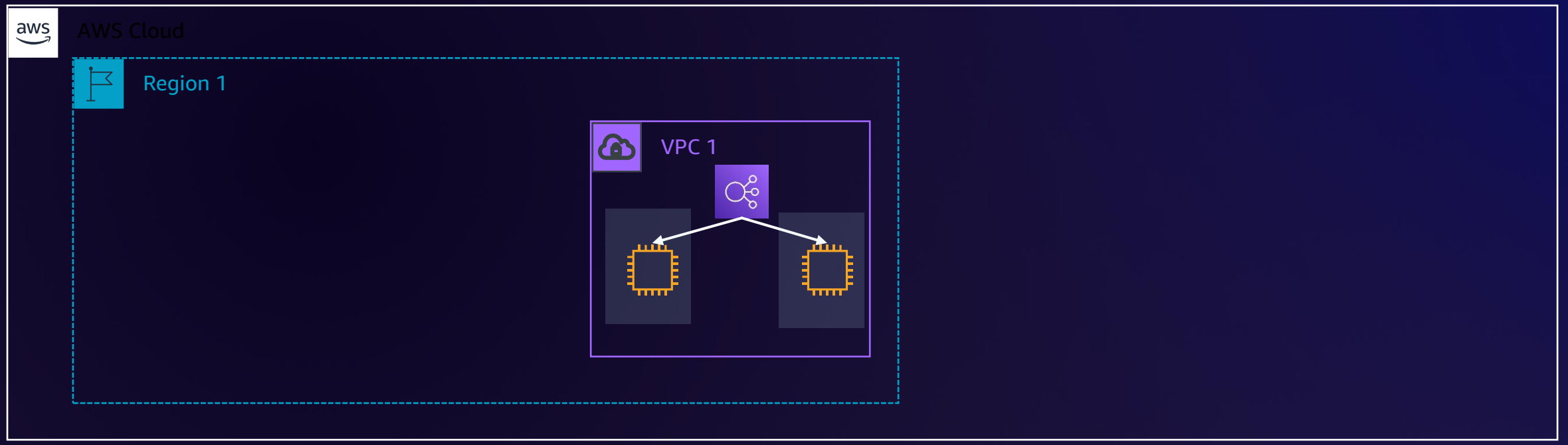
Traffic inspection patterns

Challenges in building a secure global network

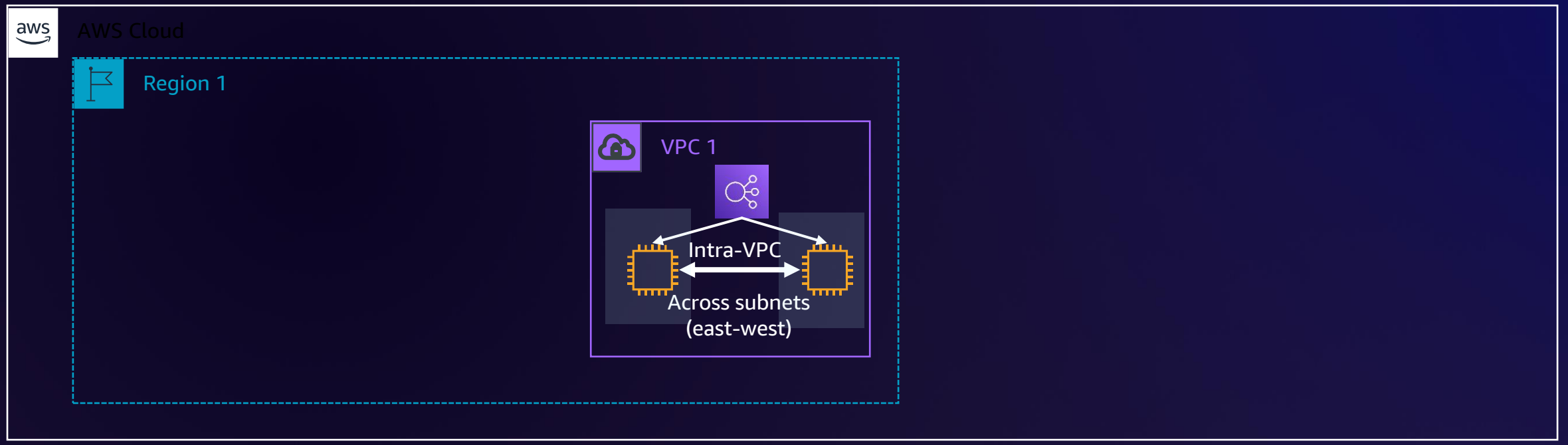
Development of AWS Cloud WAN

Walk through building inspection architecture

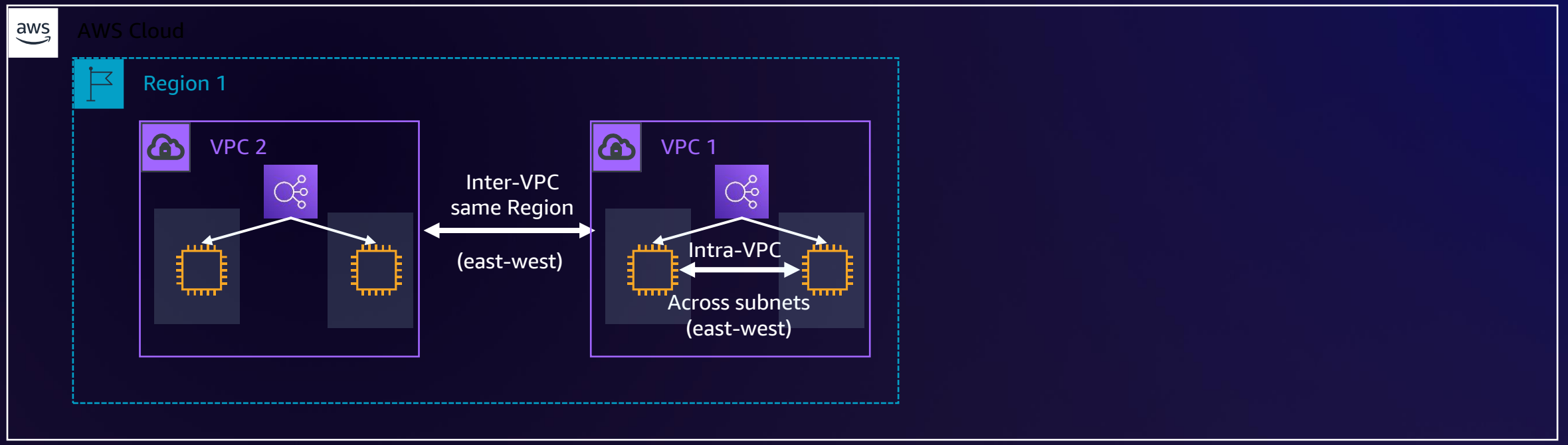
Traffic inspection patterns



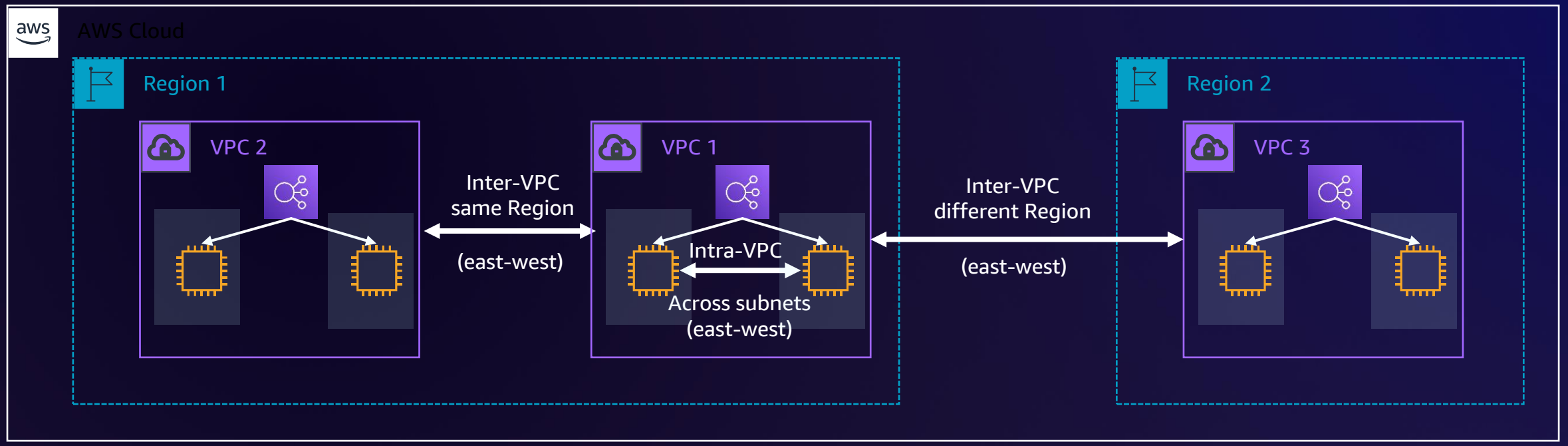
Traffic inspection patterns



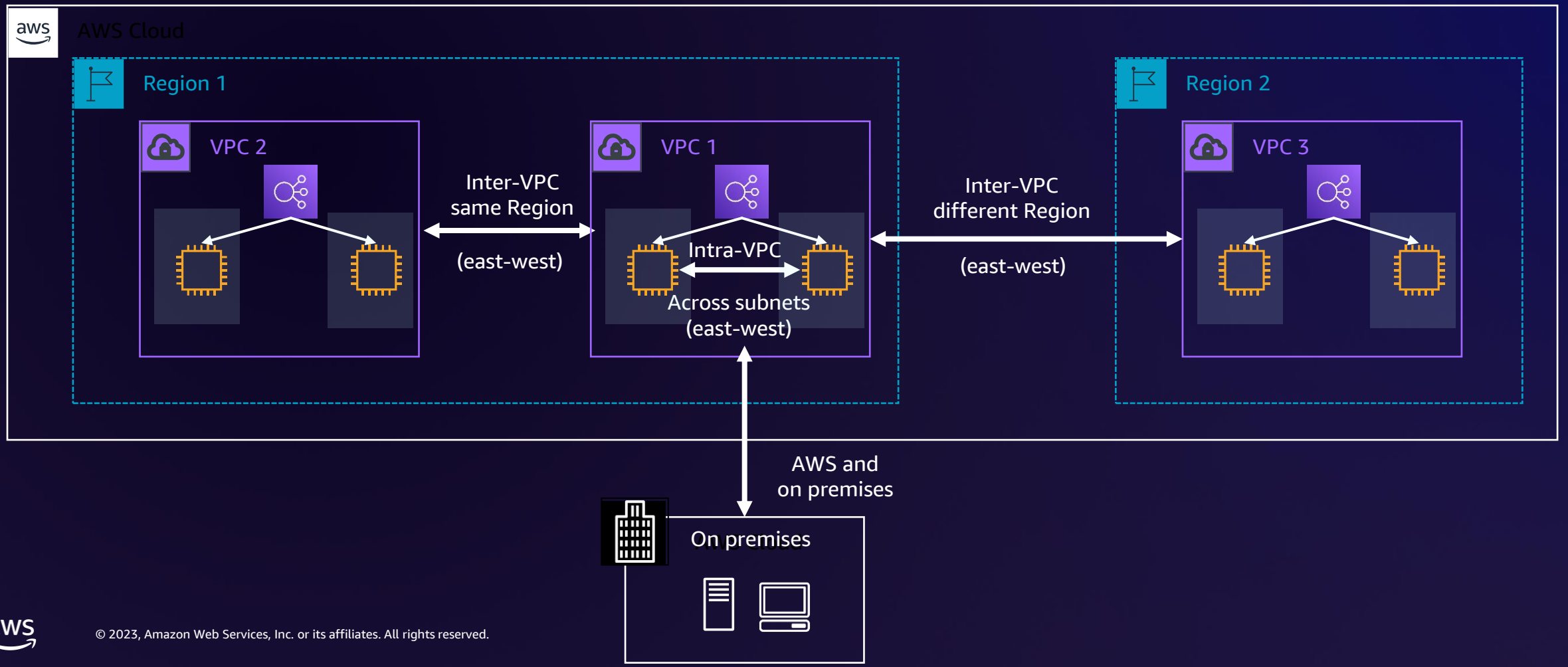
Traffic inspection patterns



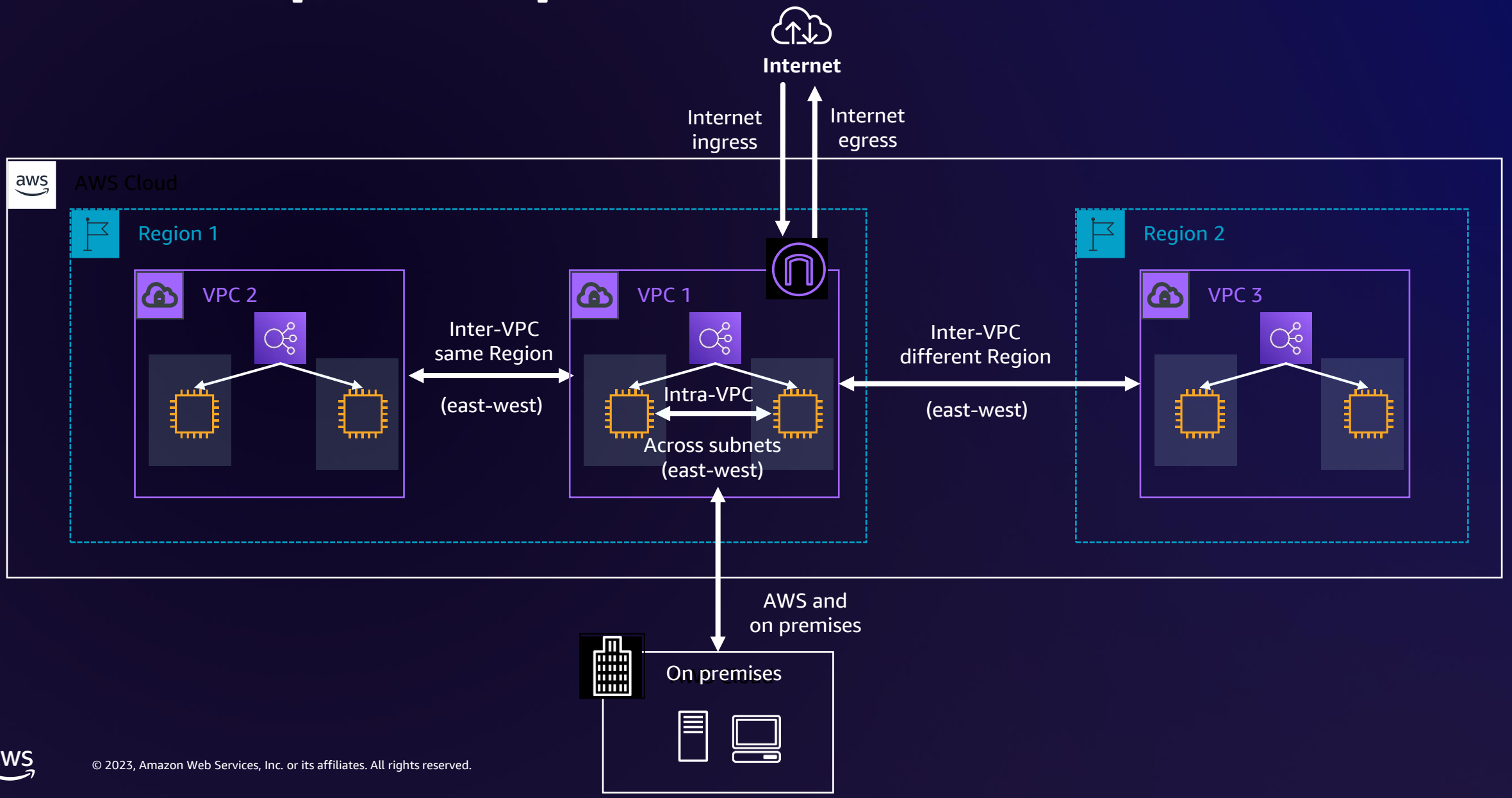
Traffic inspection patterns



Traffic inspection patterns



Traffic inspection patterns



A story of meeting needs

Alice

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1

A story of meeting needs

Alice

People who want things

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1

A story of meeting needs

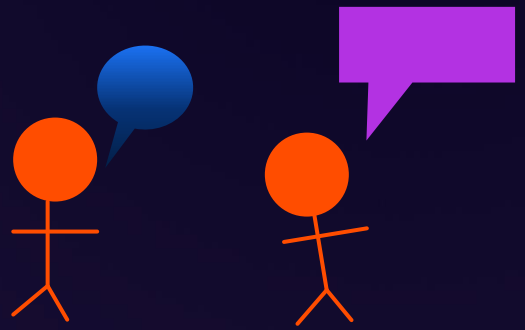
Alice

People who want things

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1

A story of meeting needs

Alice

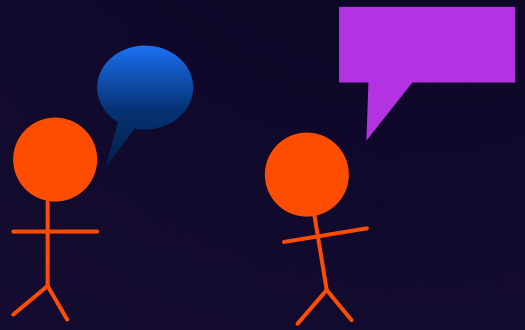


People who want things

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1

A story of meeting needs

Alice

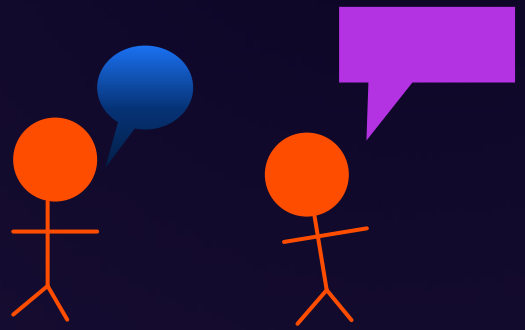


People who want things

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1

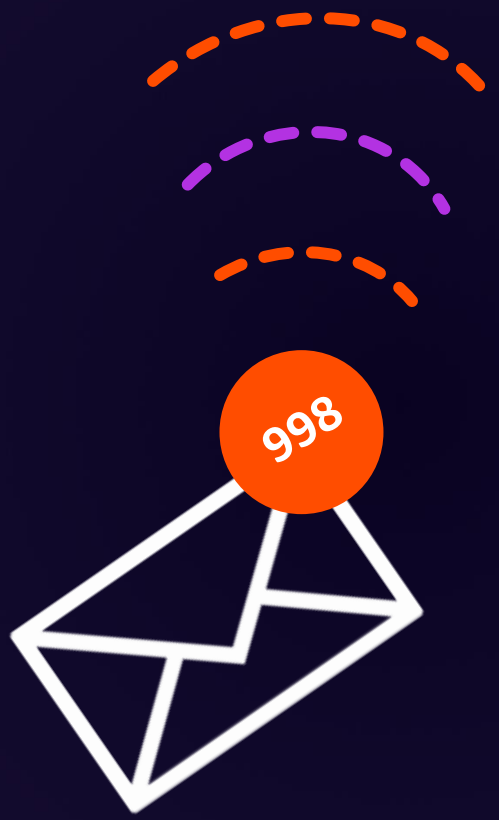
A story of meeting needs

Alice



People who want things

1. AnyCompany
2. Alice – Network Security Architect
3. Two data centers
4. AWS presence us-east-1



Alice gets an email from the security team

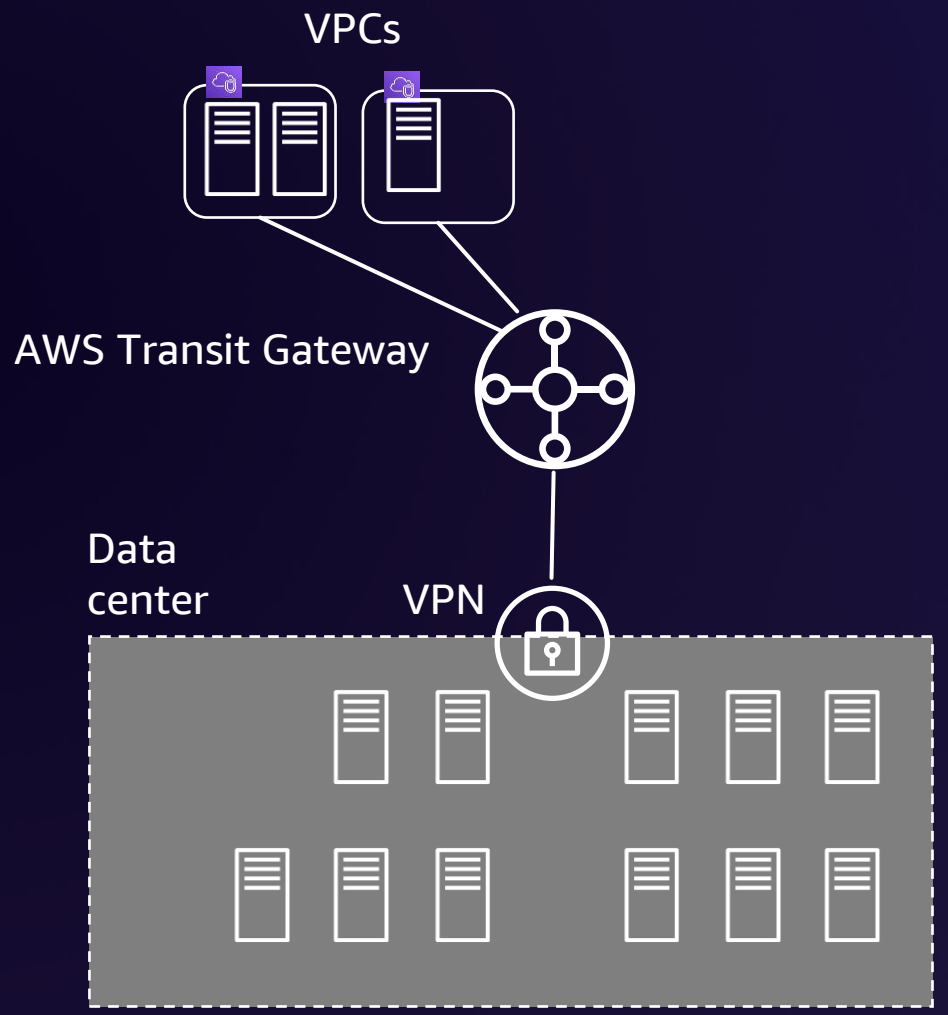
The security team found unidentified traffic from the dev environment to production environment. Alice's manager wants her to design an architecture for traffic inspection to bolster security posture of AnyCompany.

Security inspection requirements

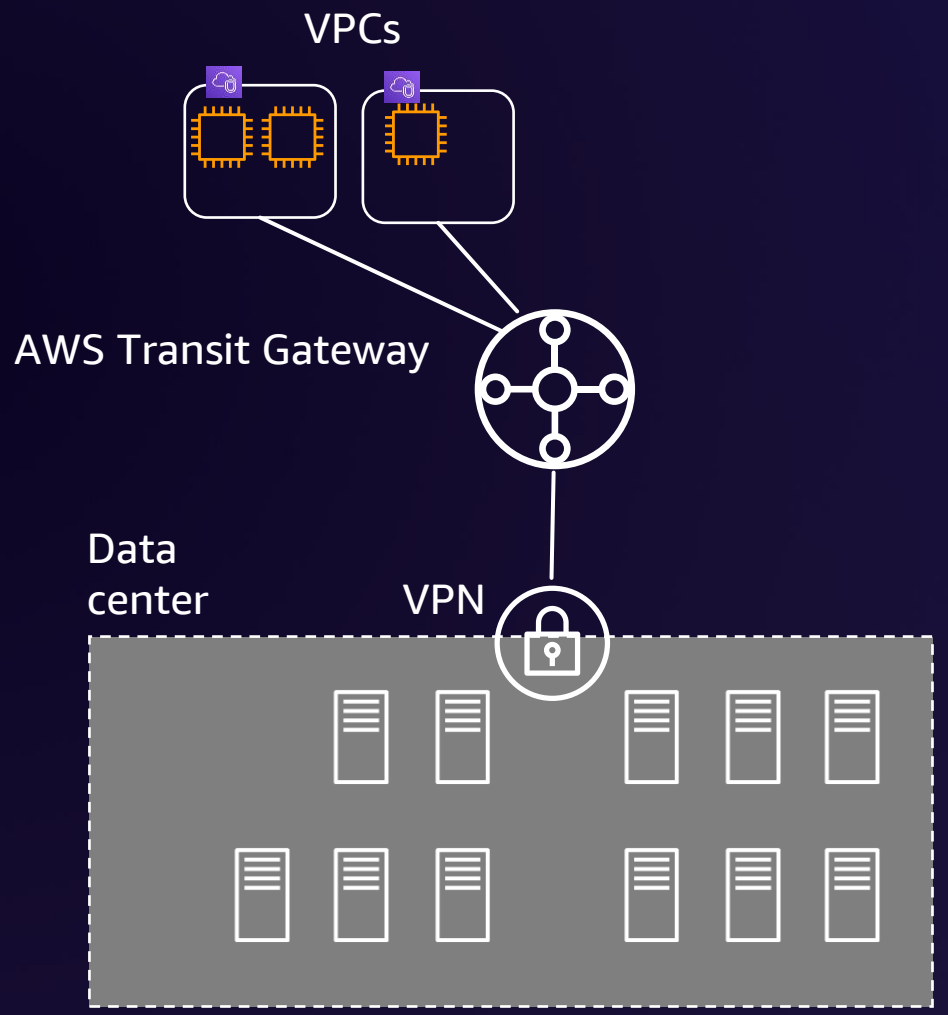
	Production	Development	Hybrid	Inspection
Production				
Development				
Hybrid				
Inspection				

1. Production segment isolated
2. East-west traffic inspection
3. North-south traffic inspection
4. Hybrid traffic inspection
5. Future-proof design
6. Automation
7. Visibility and control

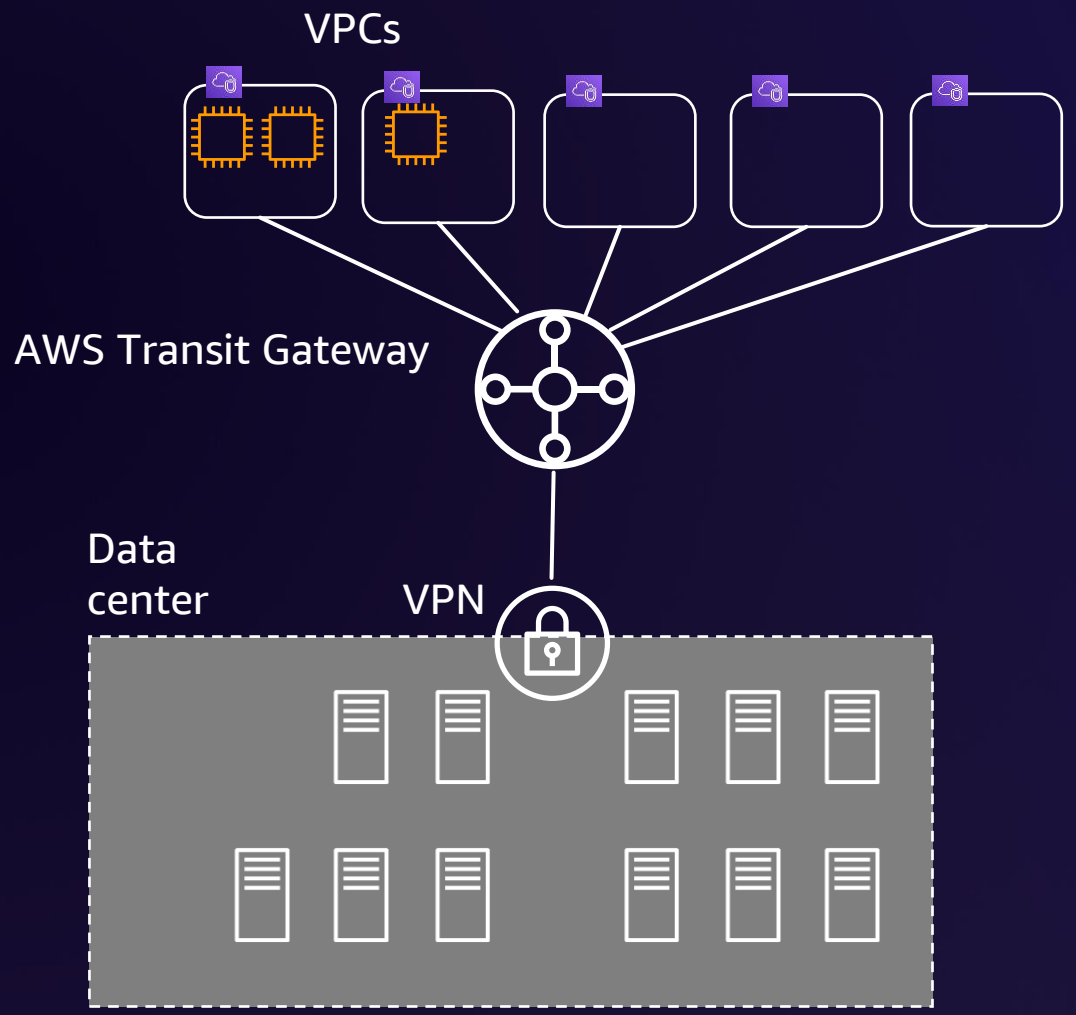
Challenges in building a secure global network



Challenges in building a secure global network



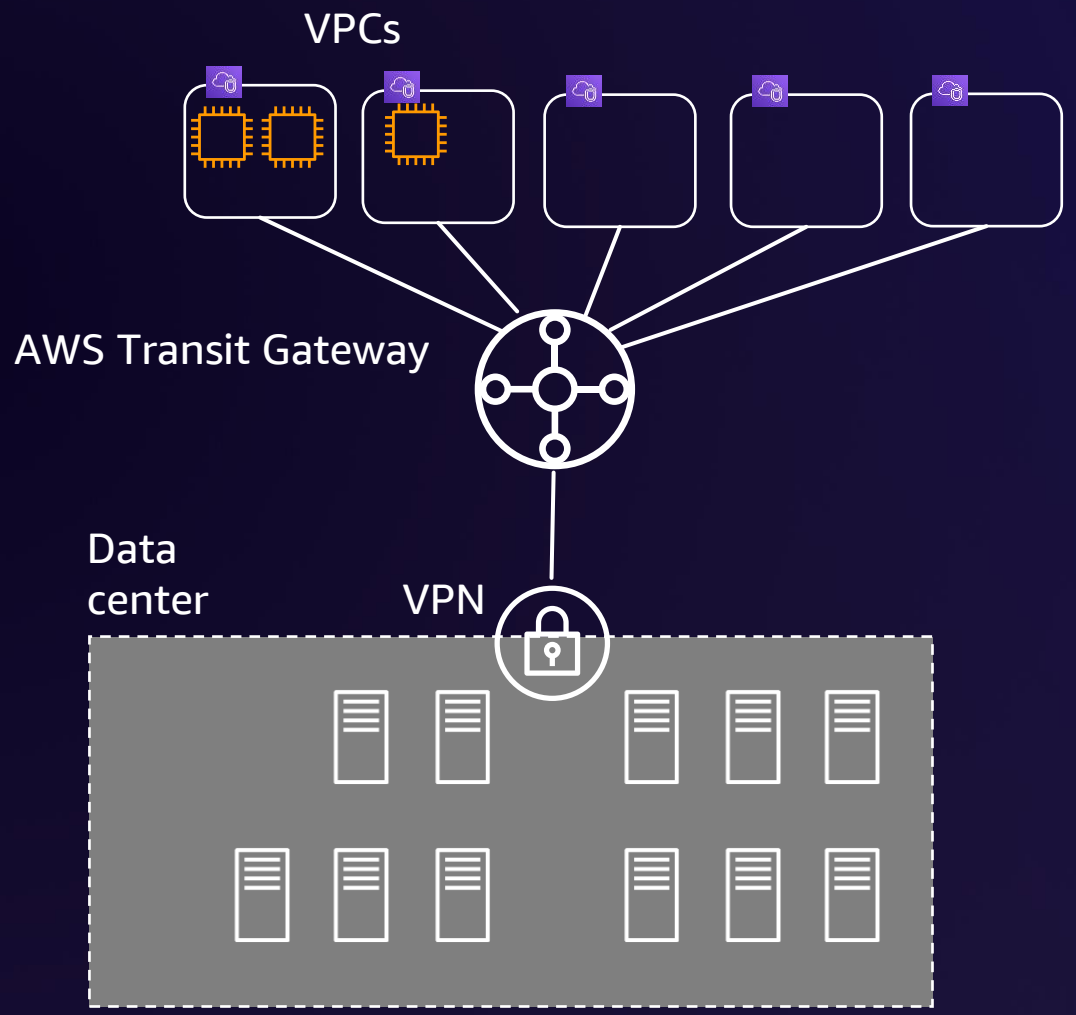
Challenges in building a secure global network



Challenges in building a secure global network

Network requirements

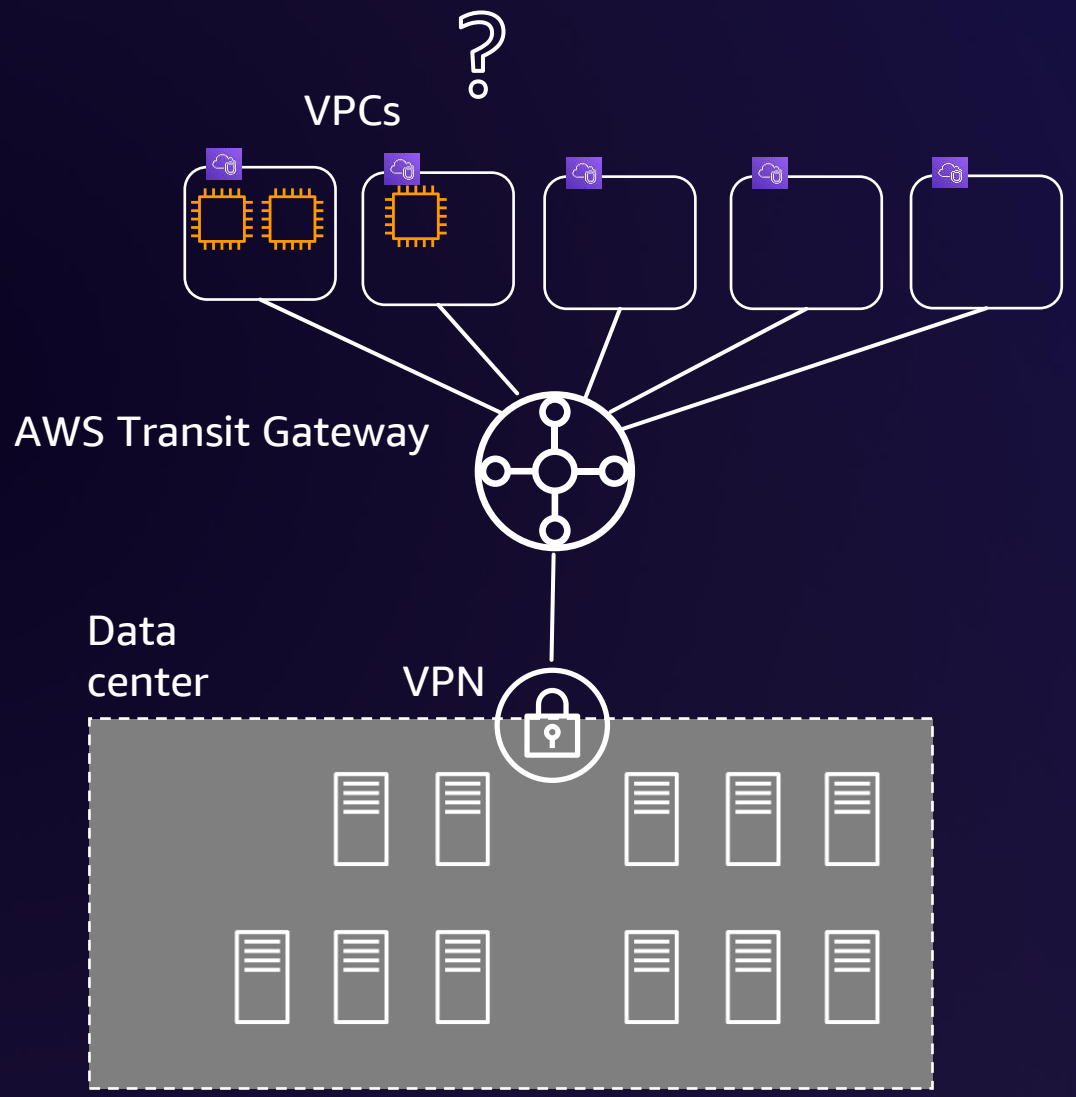
- Automation



Challenges in building a secure global network

Network requirements

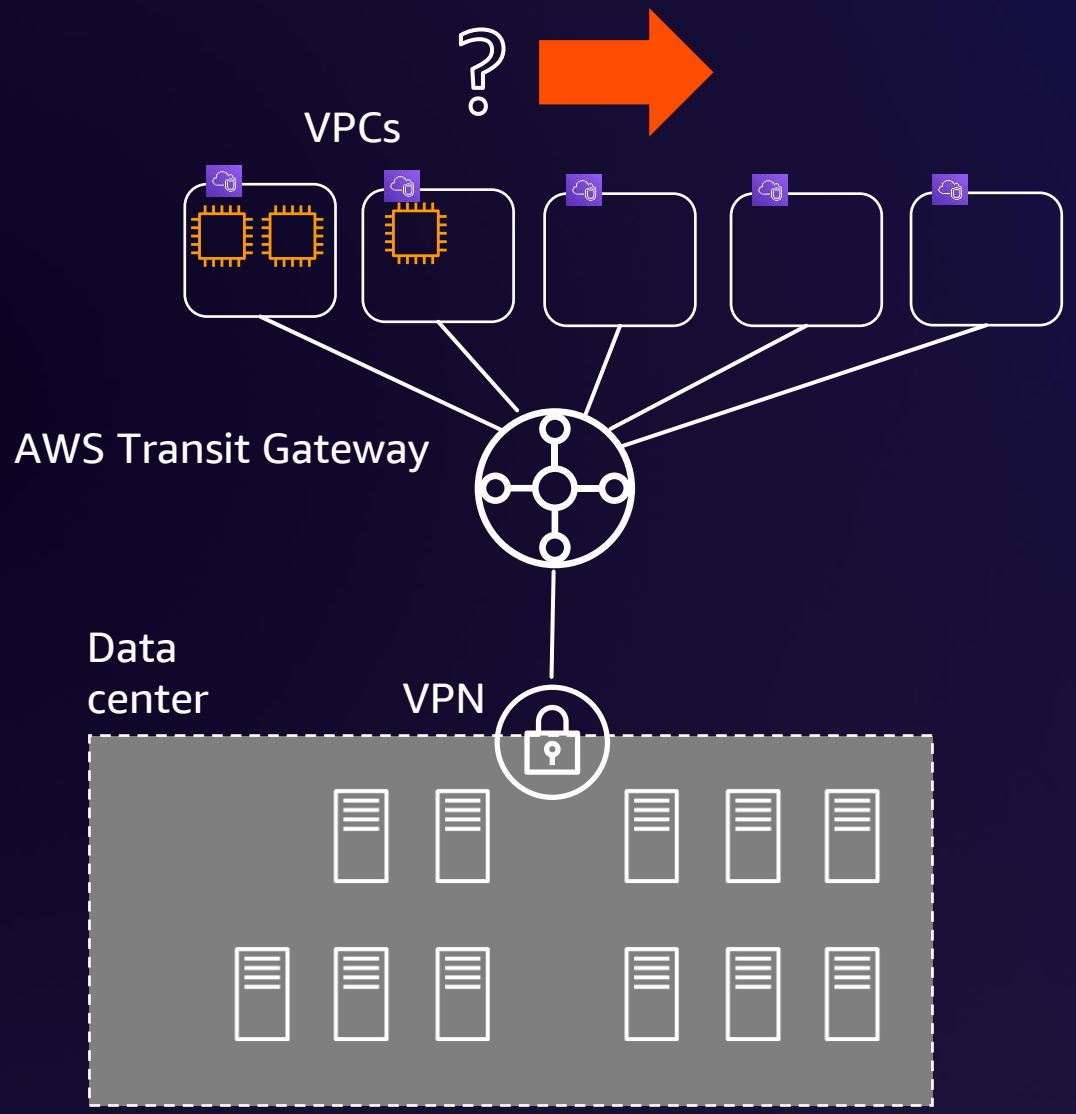
- Automation



Challenges in building a secure global network

Network requirements

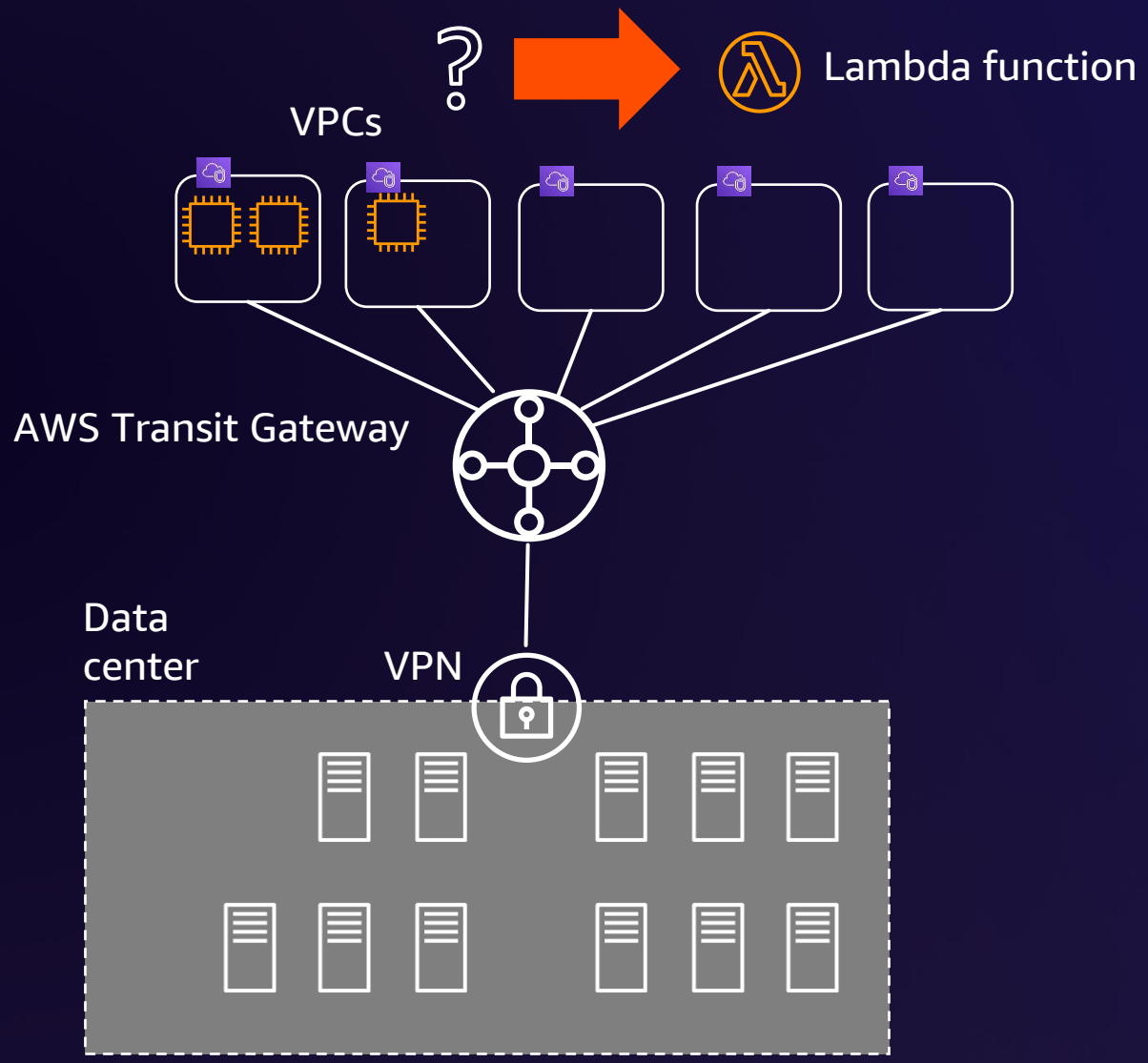
- Automation



Challenges in building a secure global network

Network requirements

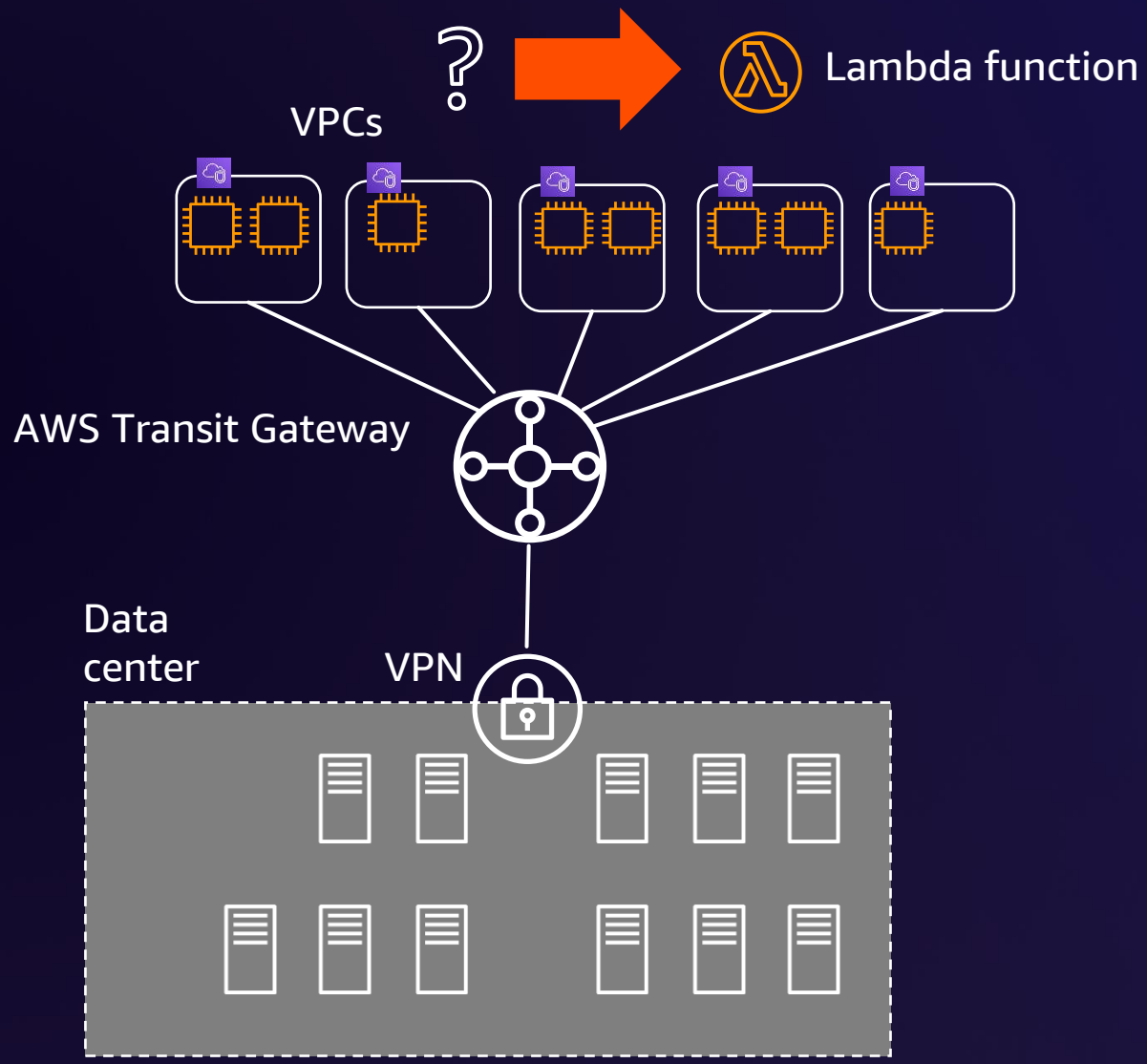
- Automation



Challenges in building a secure global network

Network requirements

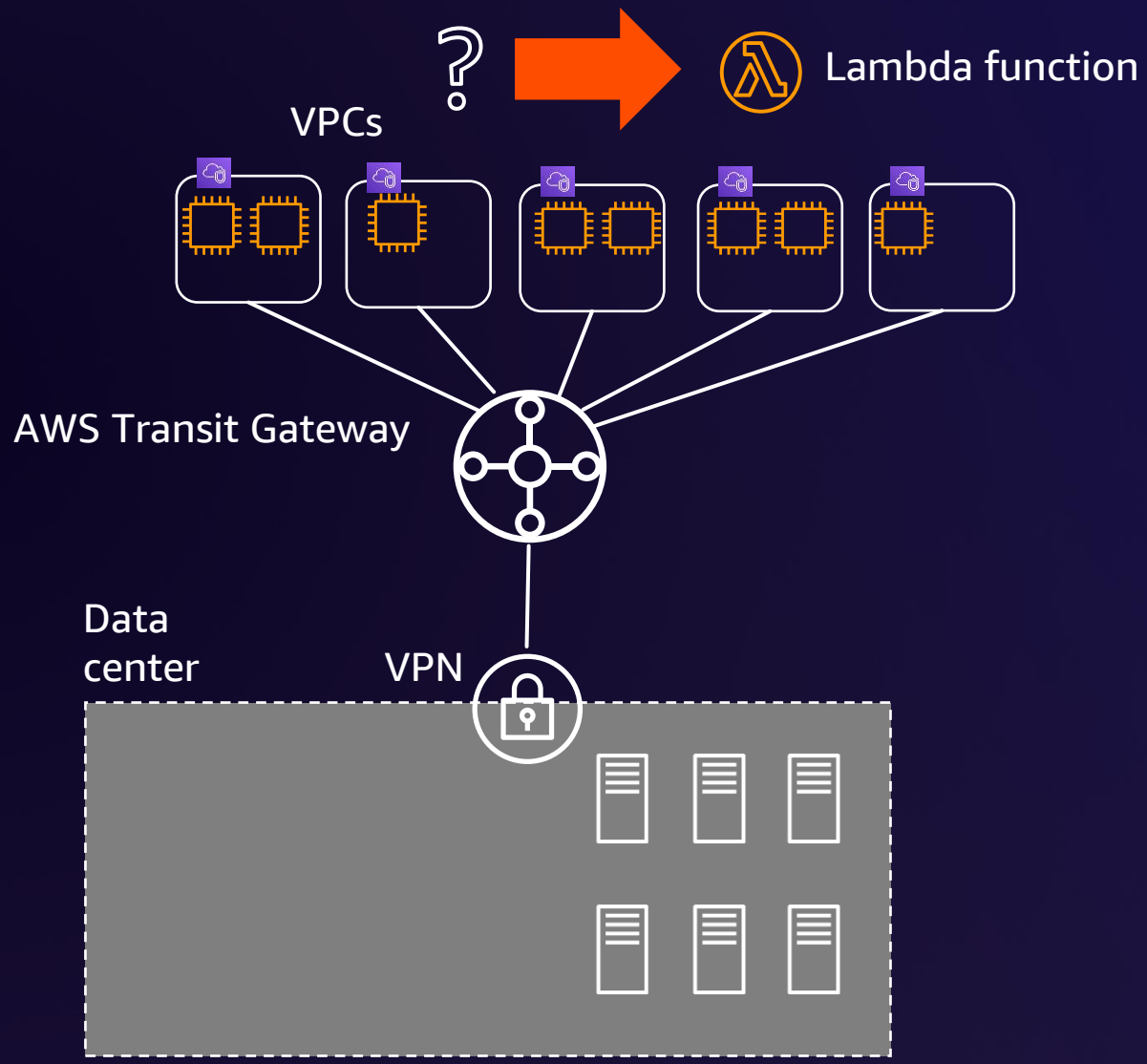
- Automation



Challenges in building a secure global network

Network requirements

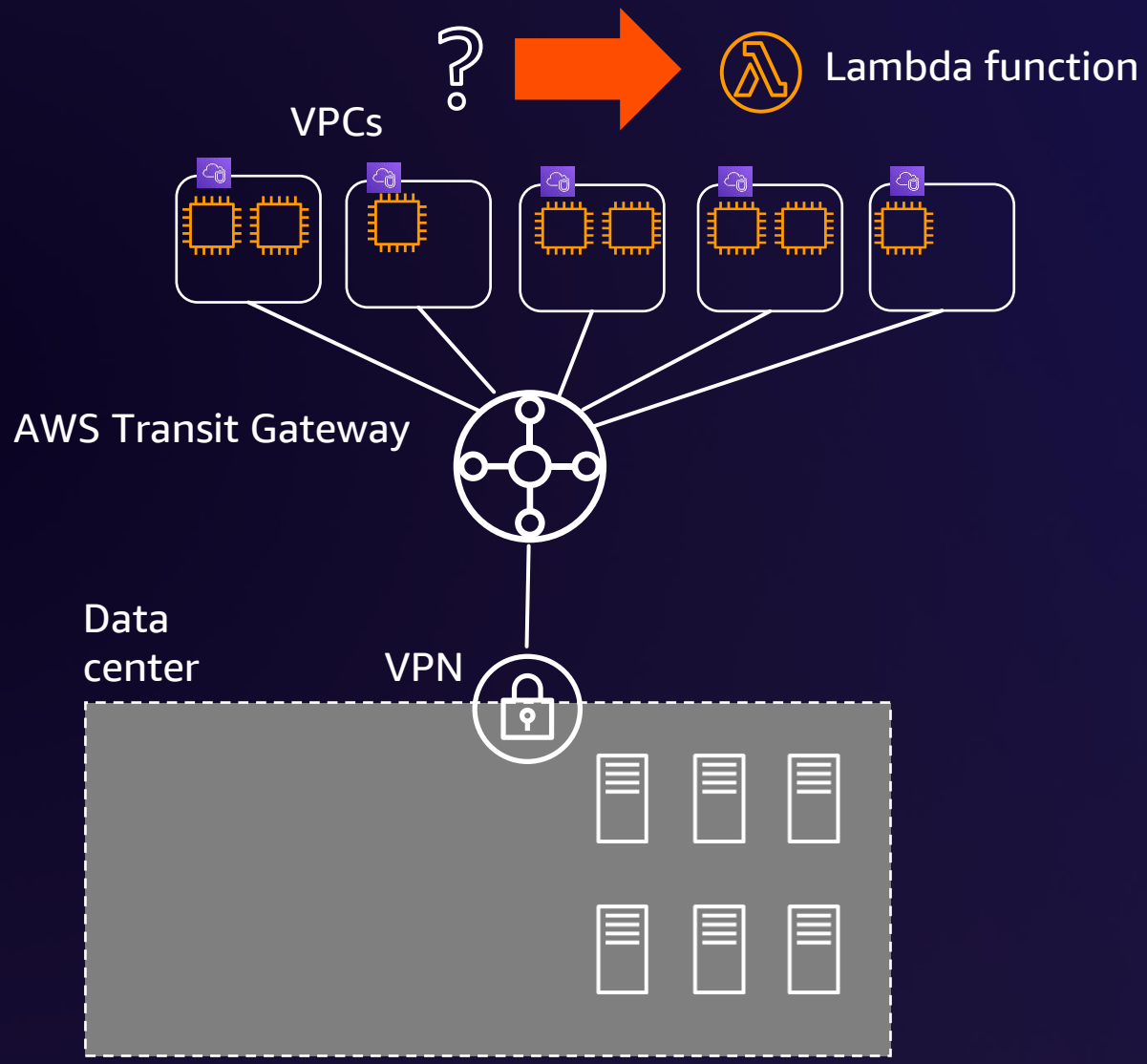
- Automation



Challenges in building a secure global network

Network requirements

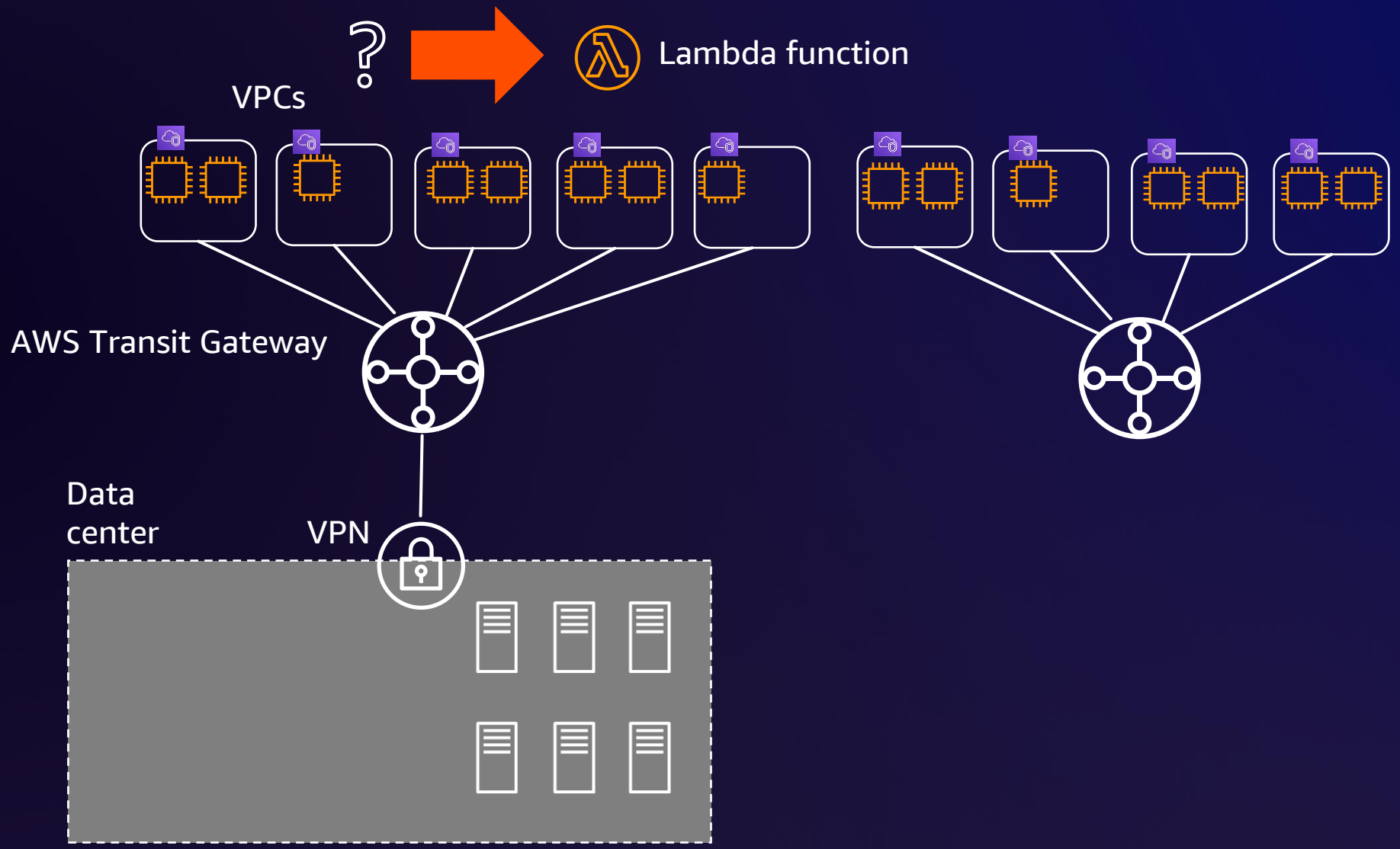
- Automation
- Multi-Region



Challenges in building a secure global network

Network requirements

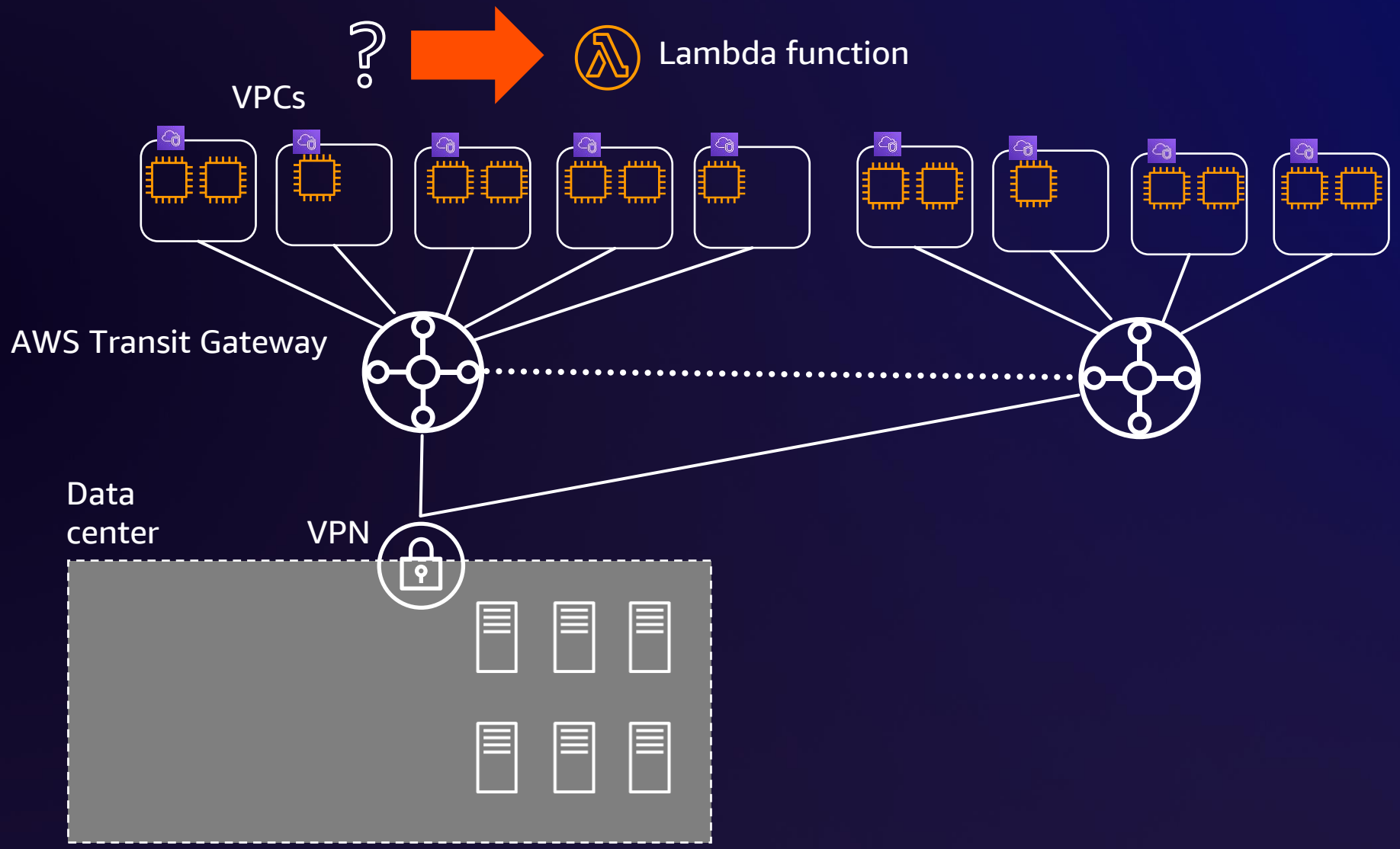
- Automation
- Multi-Region



Challenges in building a secure global network

Network requirements

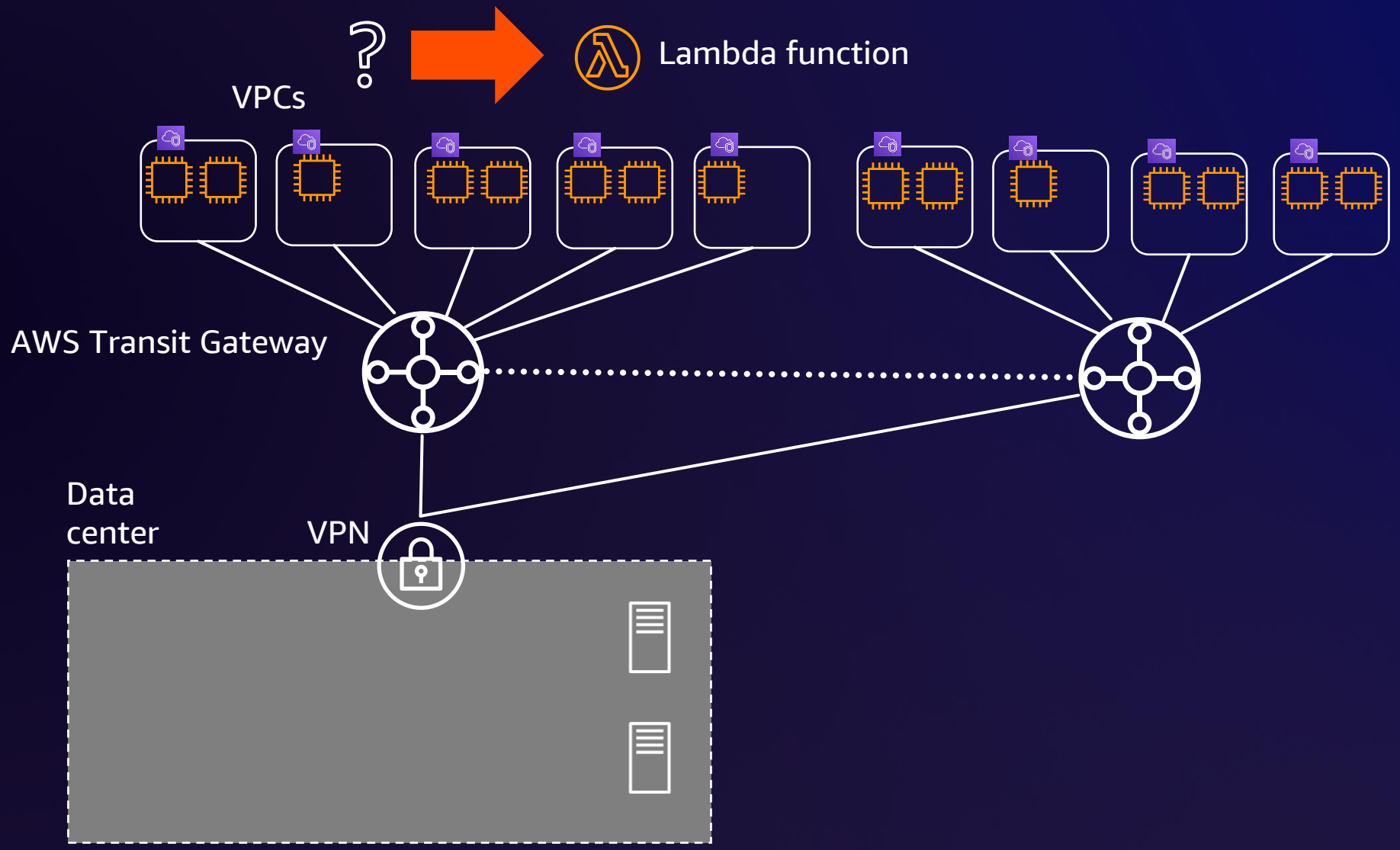
- Automation
- Multi-Region



Challenges in building a secure global network

Network requirements

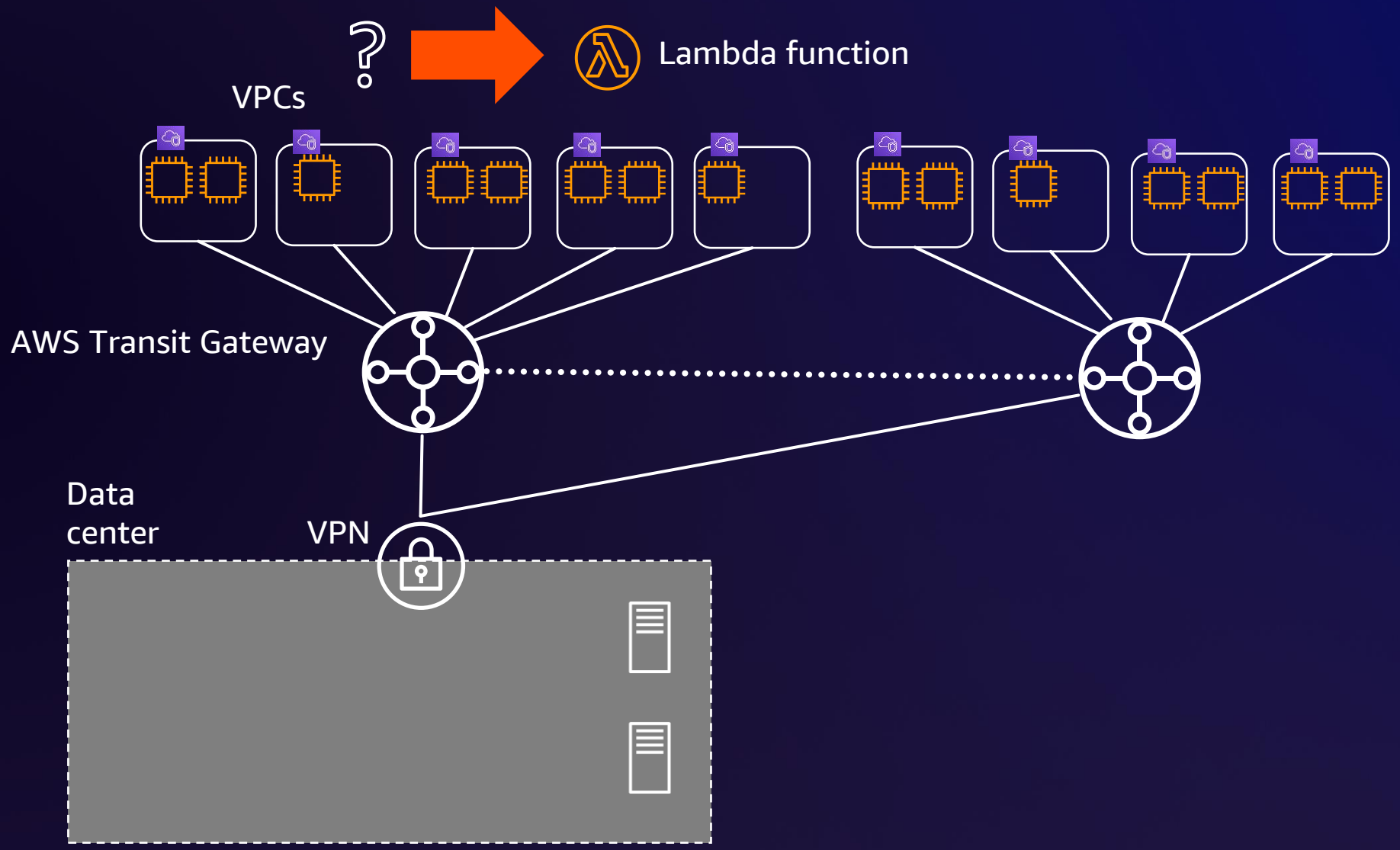
- Automation
- Multi-Region



Challenges in building a secure global network

Network requirements

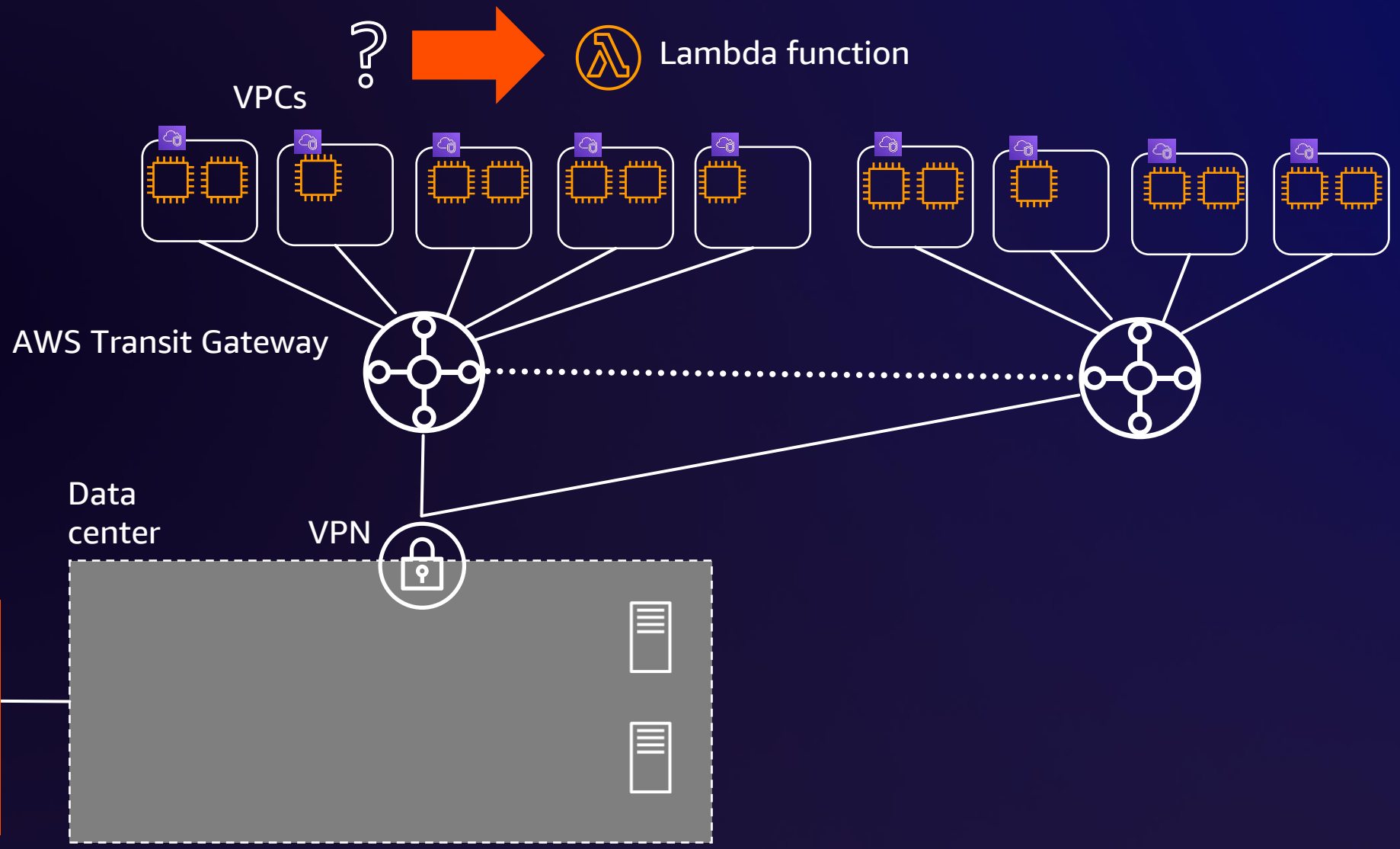
- Automation
- Multi-Region
- Security



Challenges in building a secure global network

Network requirements

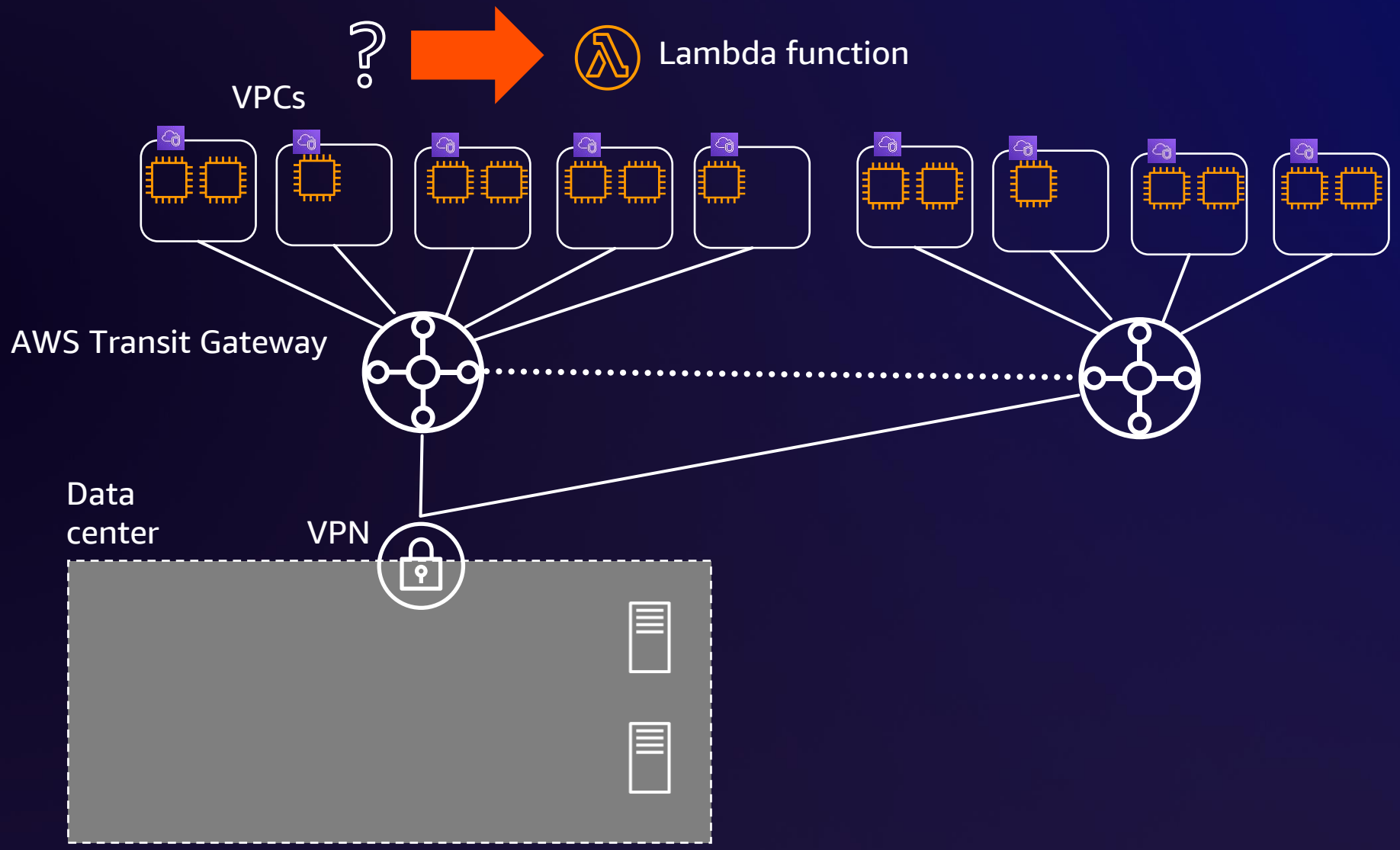
- Automation
- Multi-Region
- Security



Challenges in building a secure global network

Network requirements

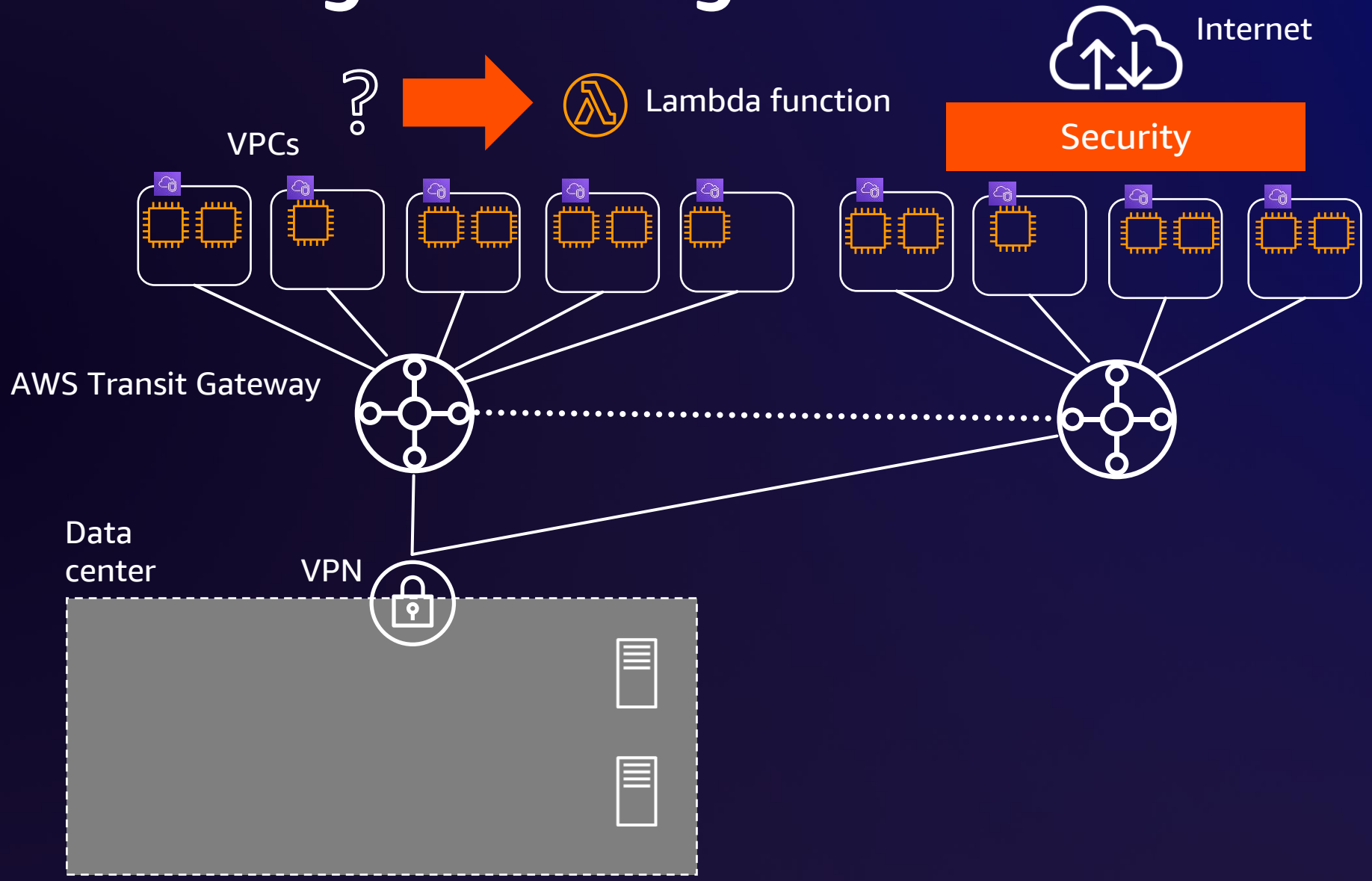
- Automation
- Multi-Region
- Security



Challenges in building a secure global network

Network requirements

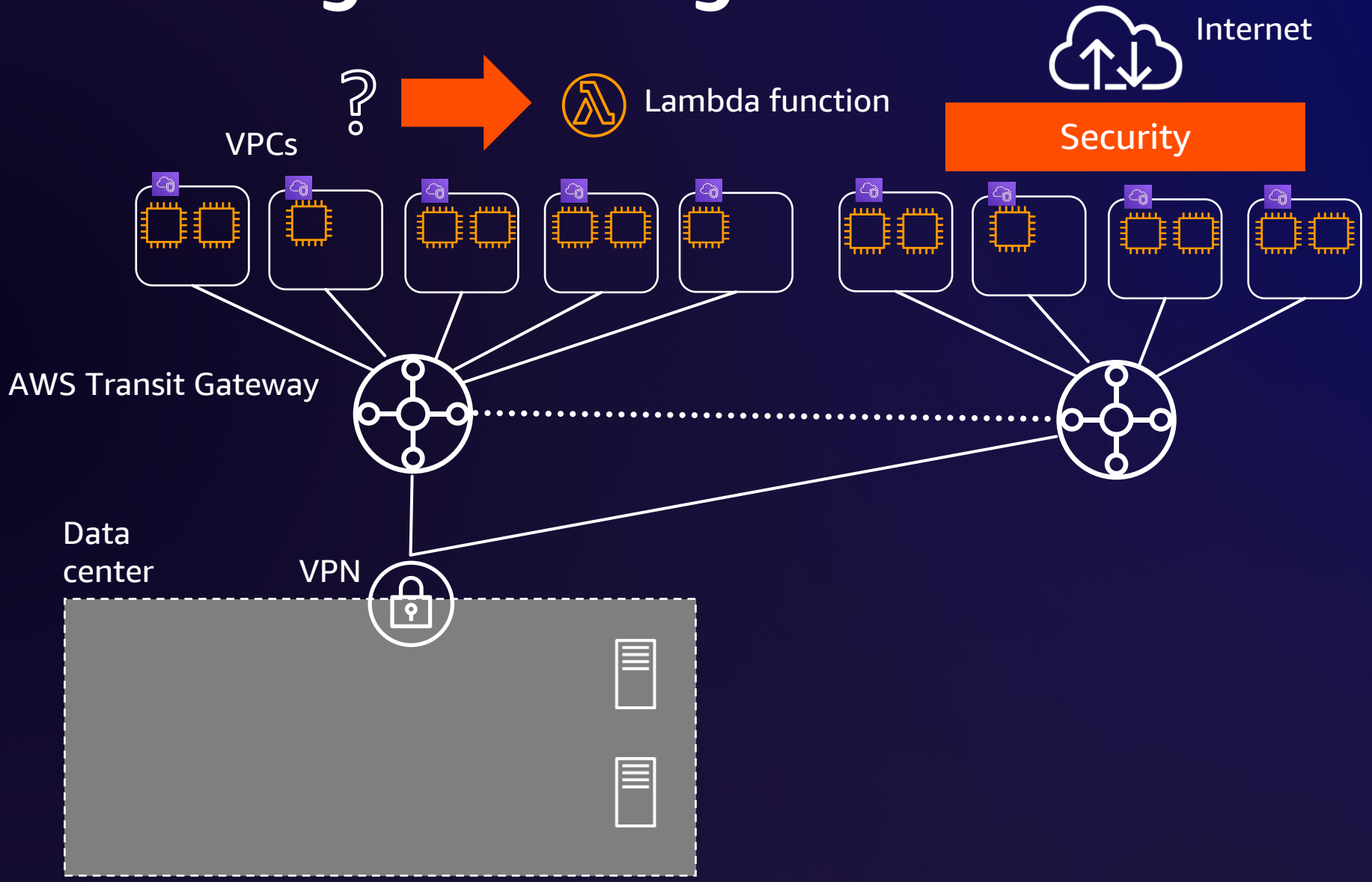
- Automation
- Multi-Region
- Security



Challenges in building a secure global network

Network requirements

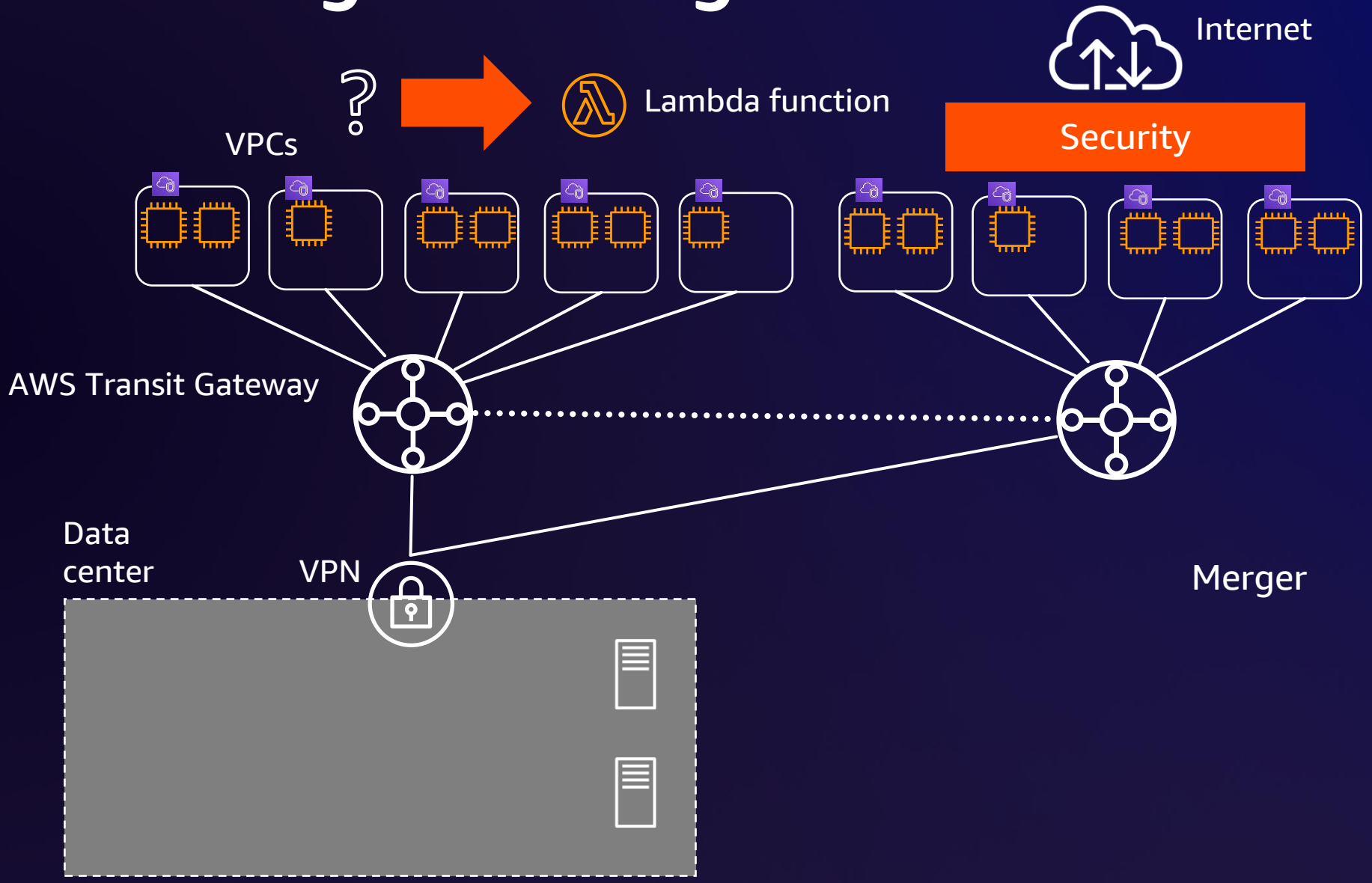
- Automation
- Multi-Region
- Security
- Extensibility



Challenges in building a secure global network

Network requirements

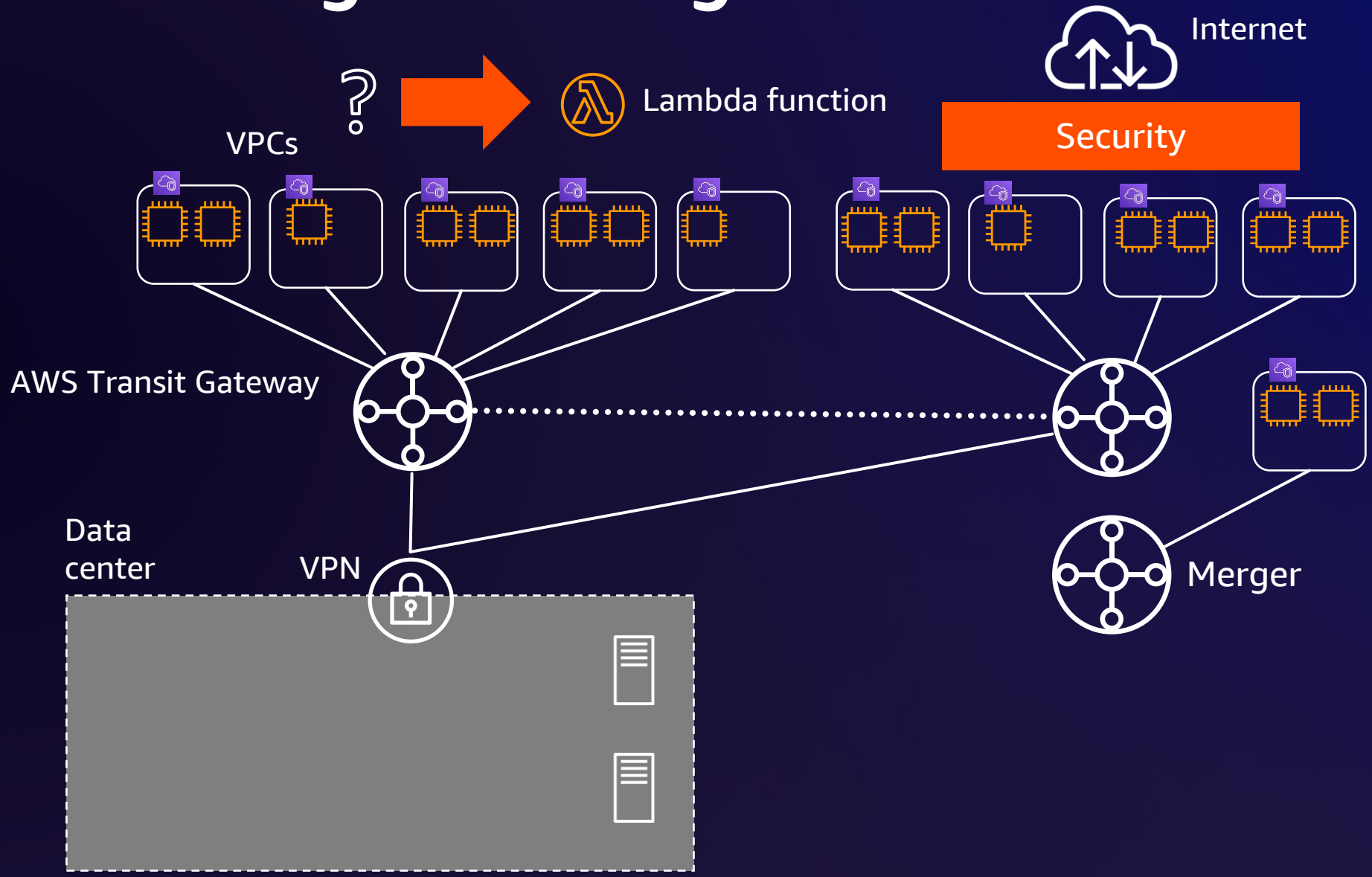
- Automation
- Multi-Region
- Security
- Extensibility



Challenges in building a secure global network

Network requirements

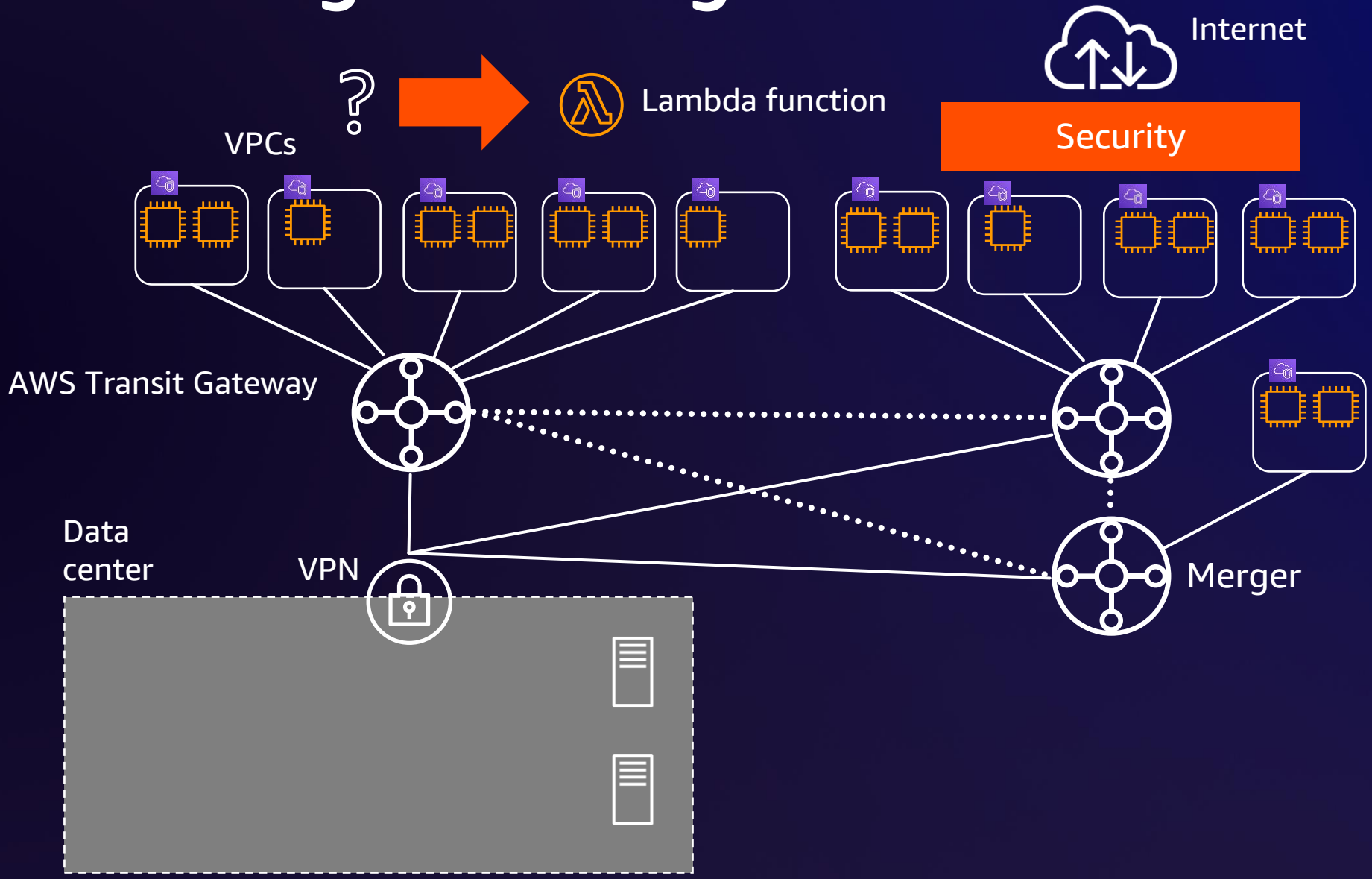
- Automation
- Multi-Region
- Security
- Extensibility



Challenges in building a secure global network

Network requirements

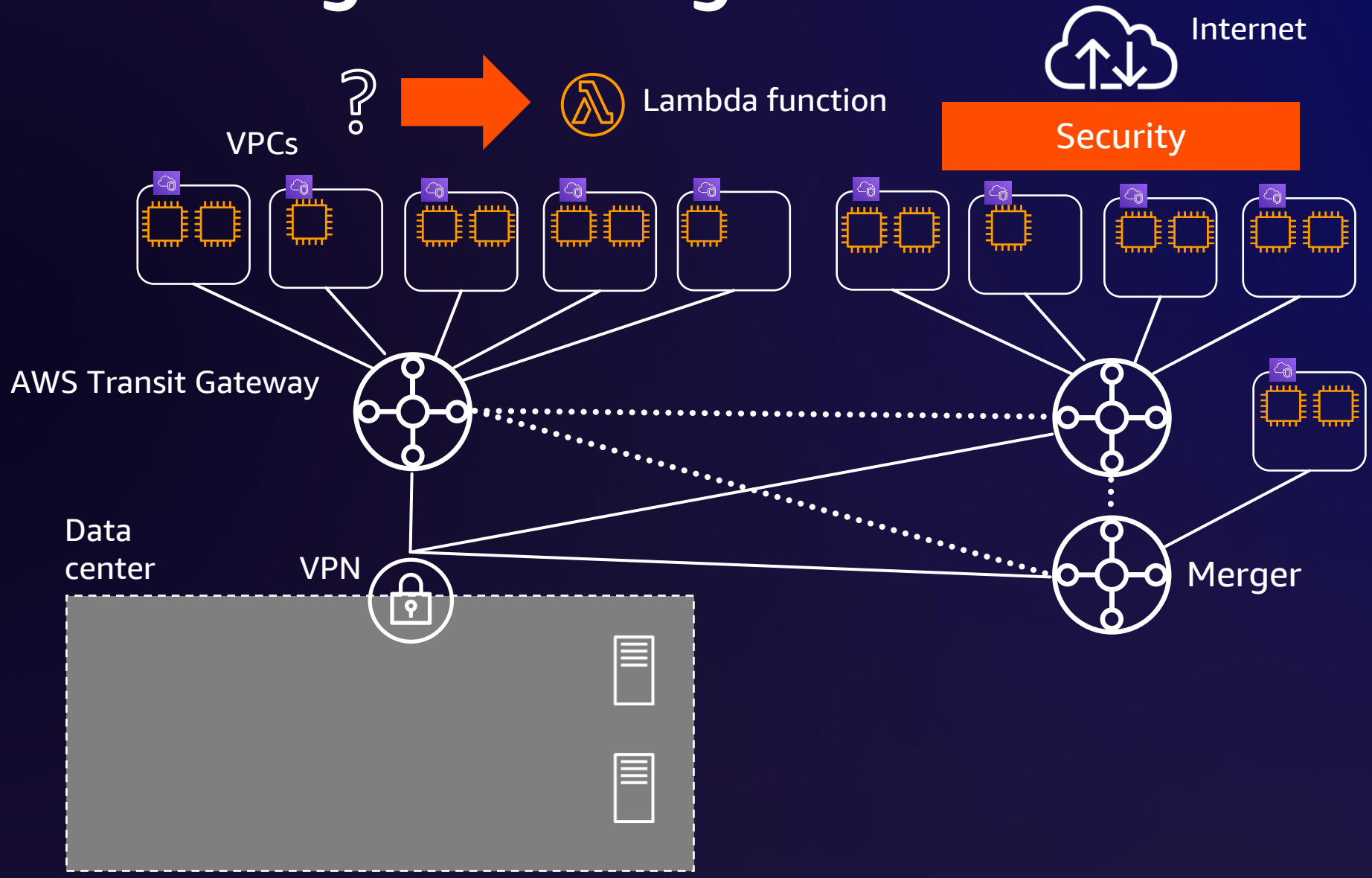
- Automation
- Multi-Region
- Security
- Extensibility



Challenges in building a secure global network

Network requirements

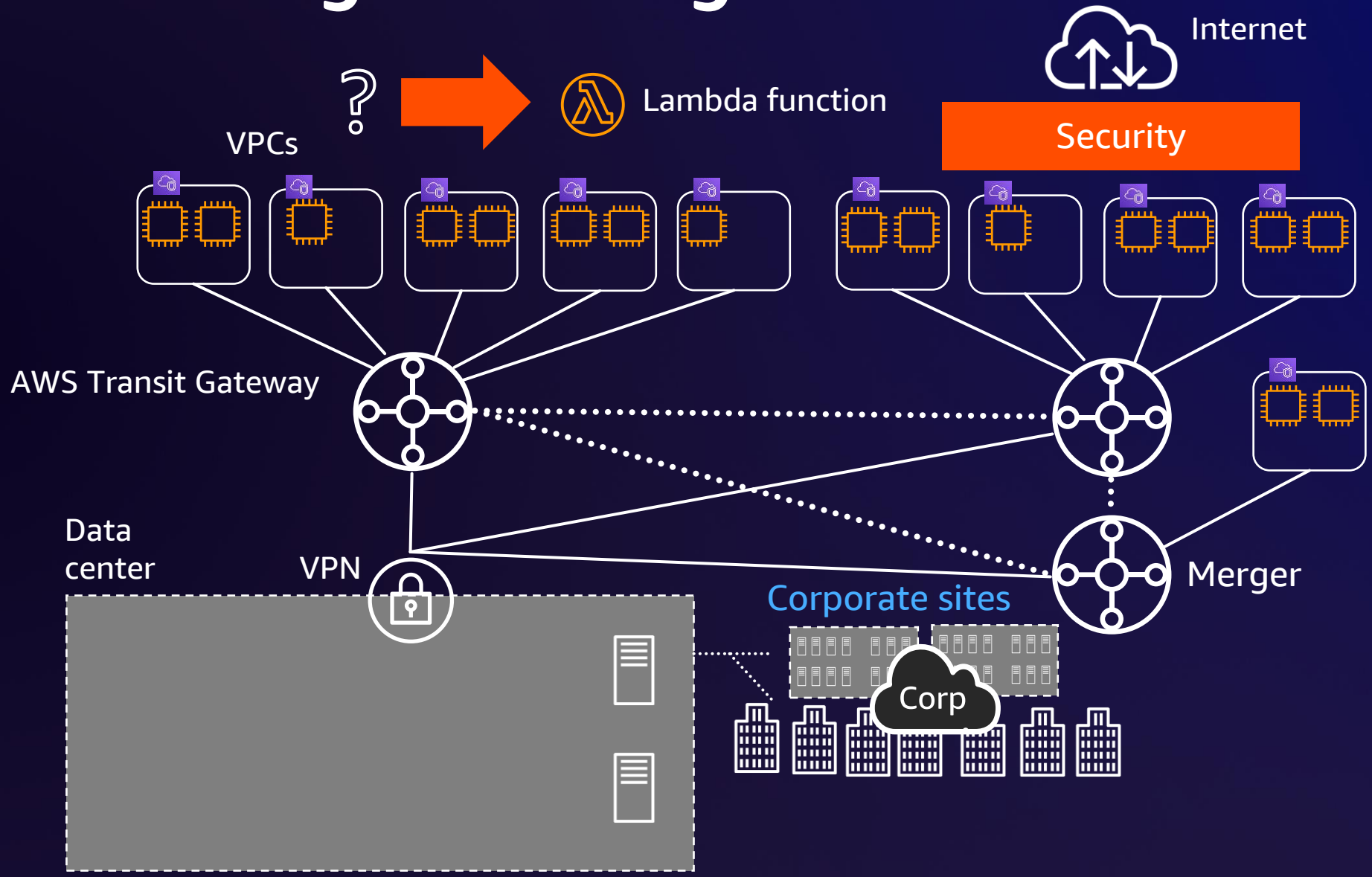
- Automation
- Multi-Region
- Security
- Extensibility
- WAN



Challenges in building a secure global network

Network requirements

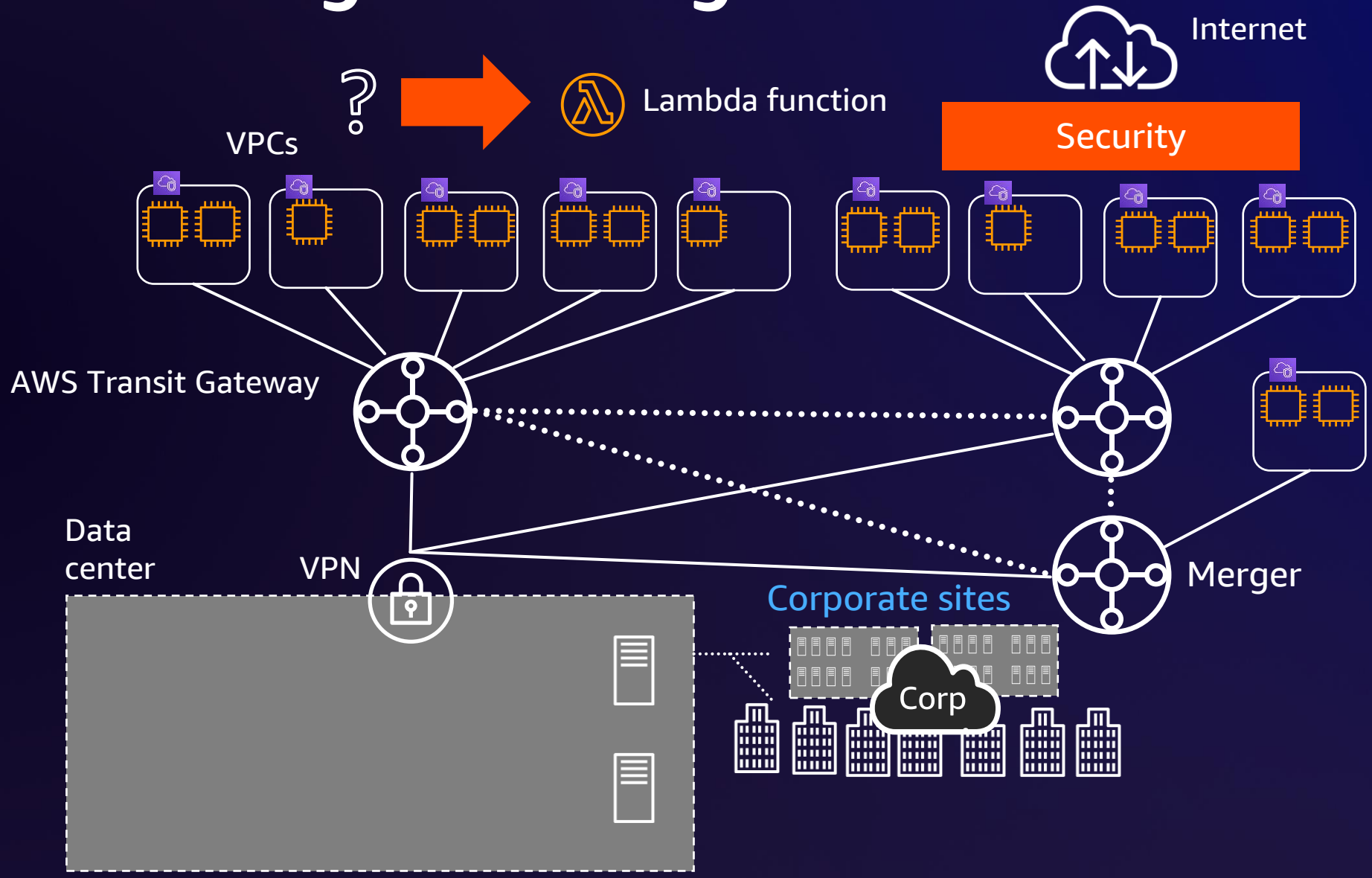
- Automation
- Multi-Region
- Security
- Extensibility
- WAN



Challenges in building a secure global network

Network requirements

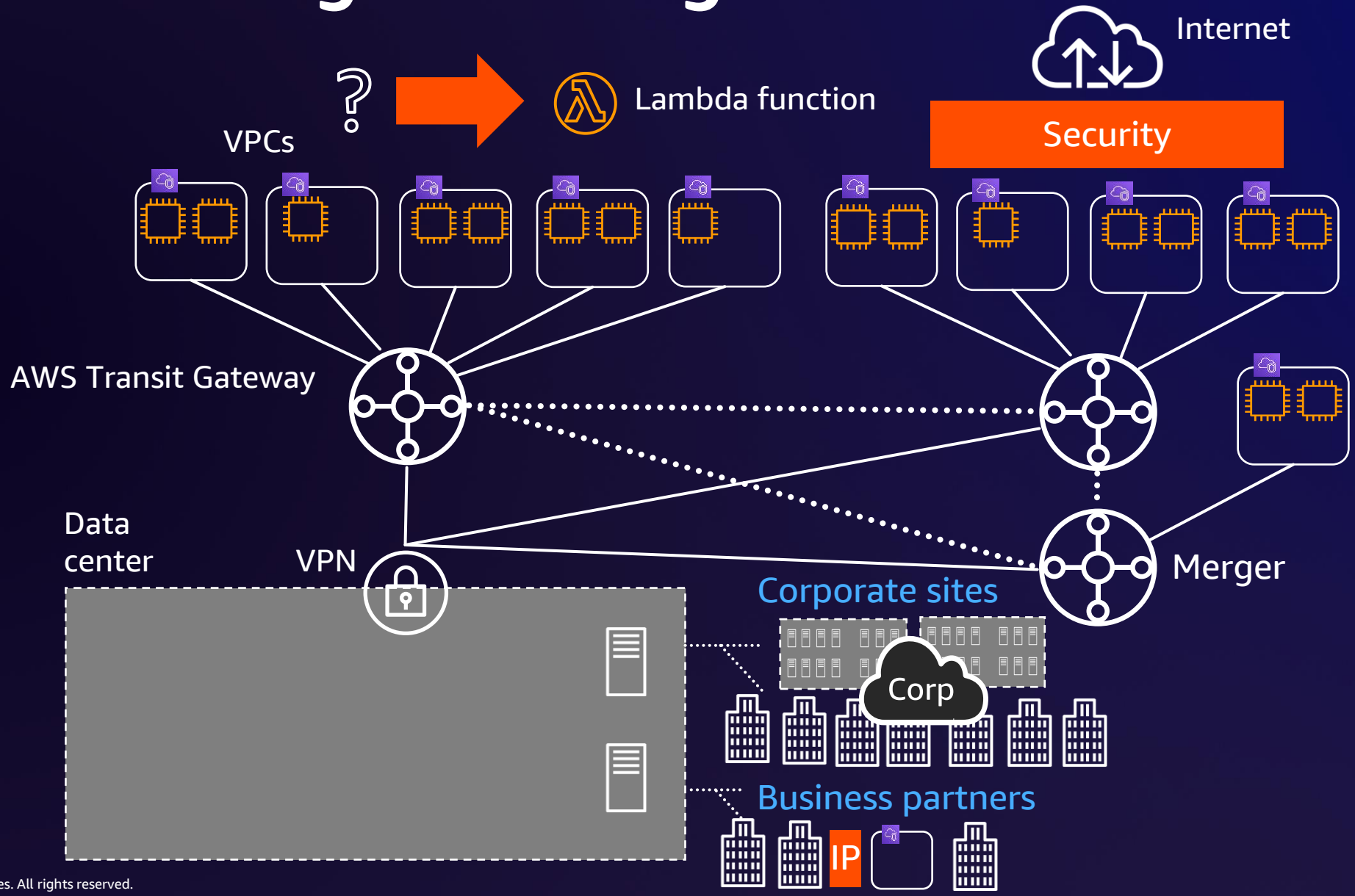
- Automation
- Multi-Region
- Security
- Extensibility
- WAN
- Extranets



Challenges in building a secure global network

Network requirements

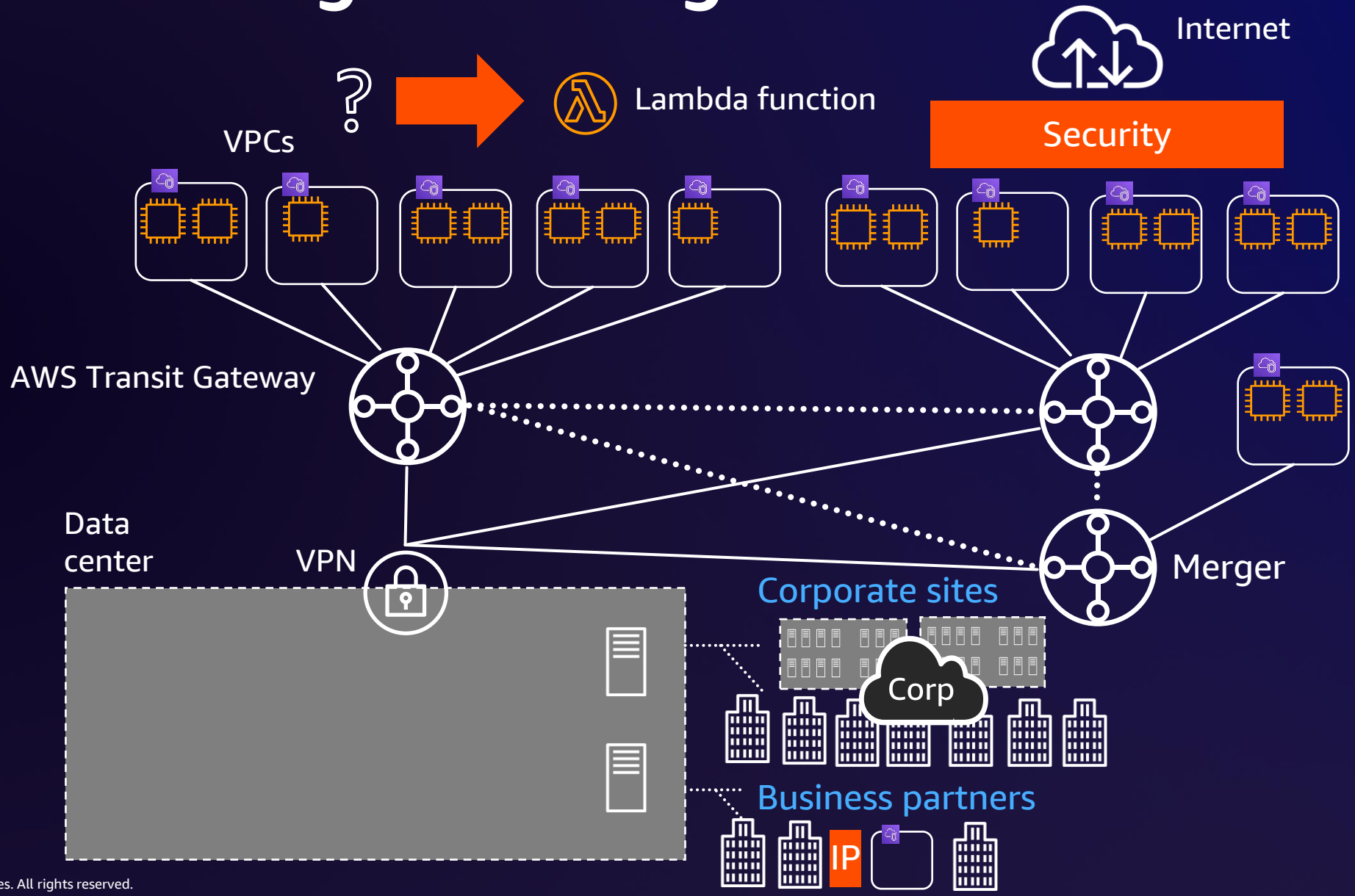
- Automation
- Multi-Region
- Security
- Extensibility
- WAN
- Extranets



Challenges in building a secure global network

Network requirements

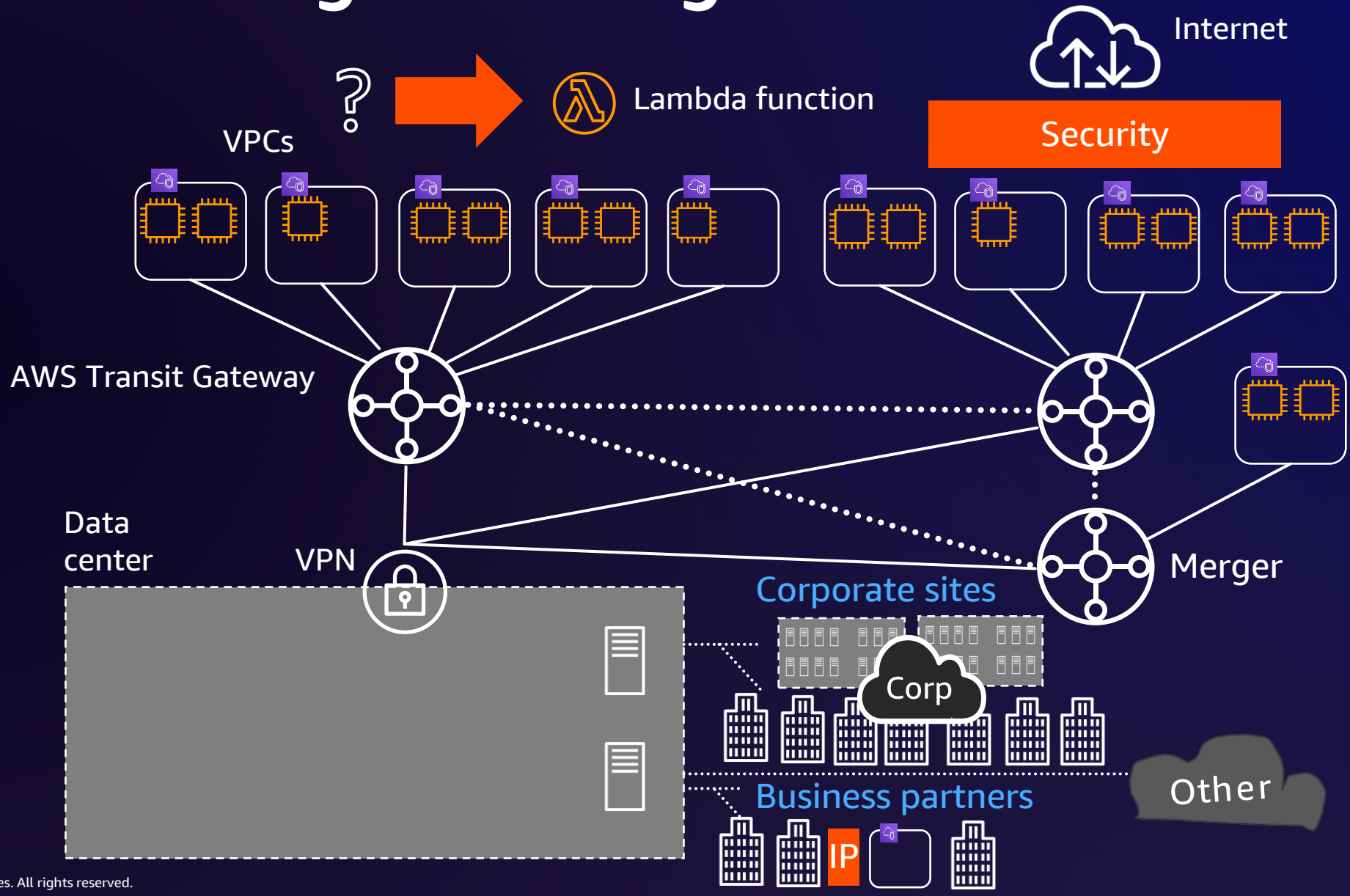
- Automation
- Multi-Region
- Security
- Extensibility
- WAN
- Extranets
- Other



Challenges in building a secure global network

Network requirements

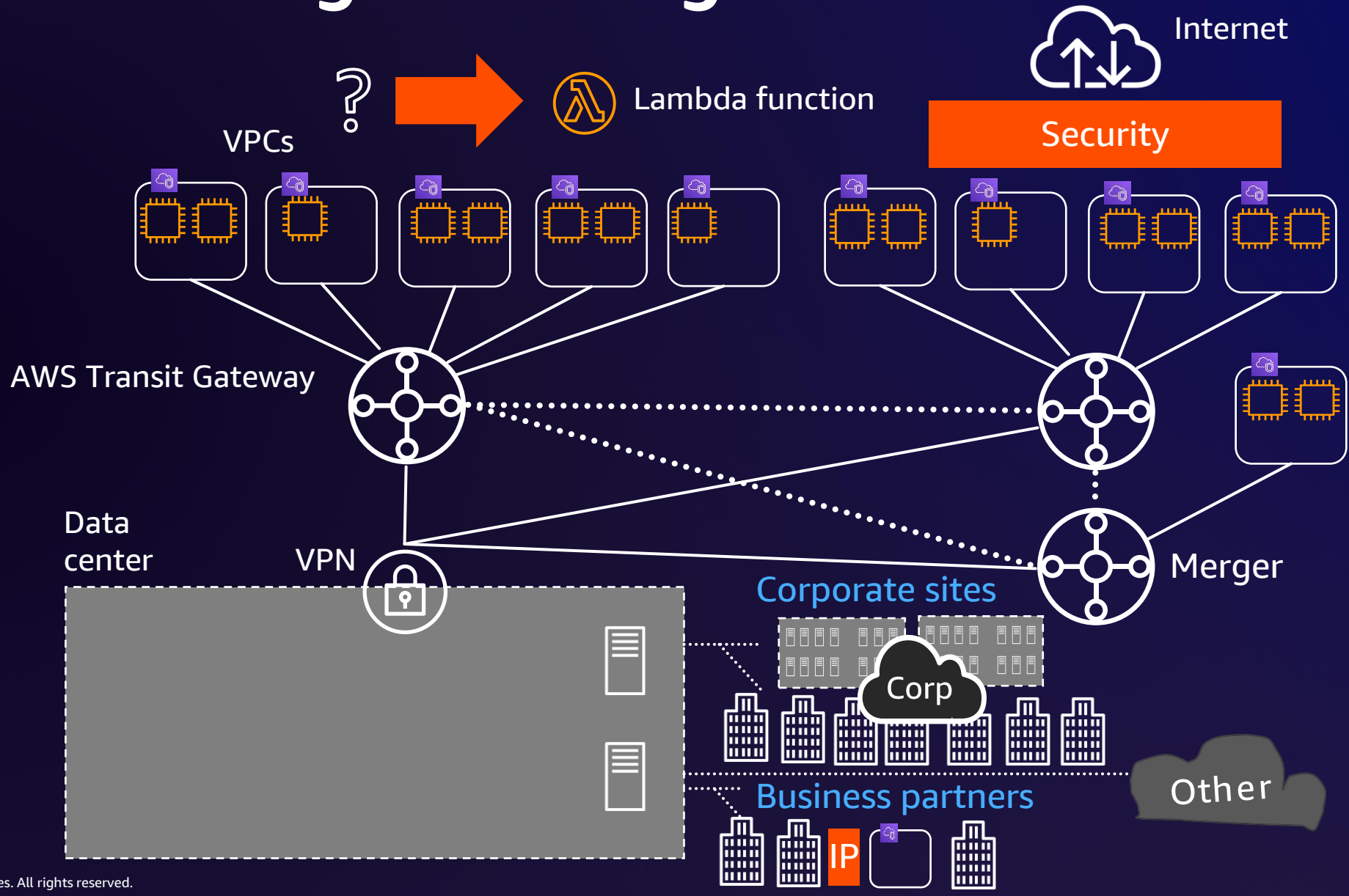
- Automation
- Multi-Region
- Security
- Extensibility
- WAN
- Extranets
- Other



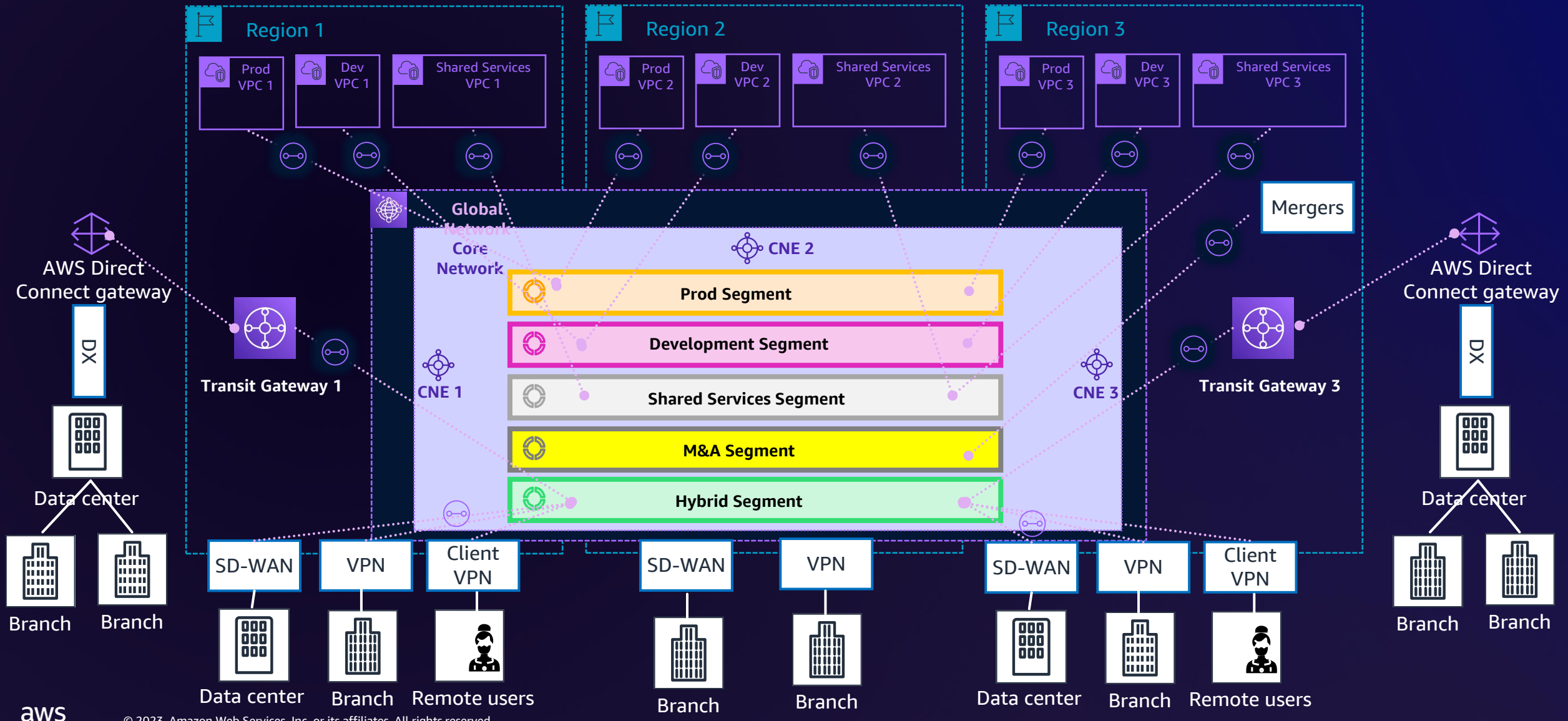
Challenges in building a secure global network

Network requirements

- Automation
- Multi-Region
- Security
- Extensibility
- WAN
- Extranets
- Other

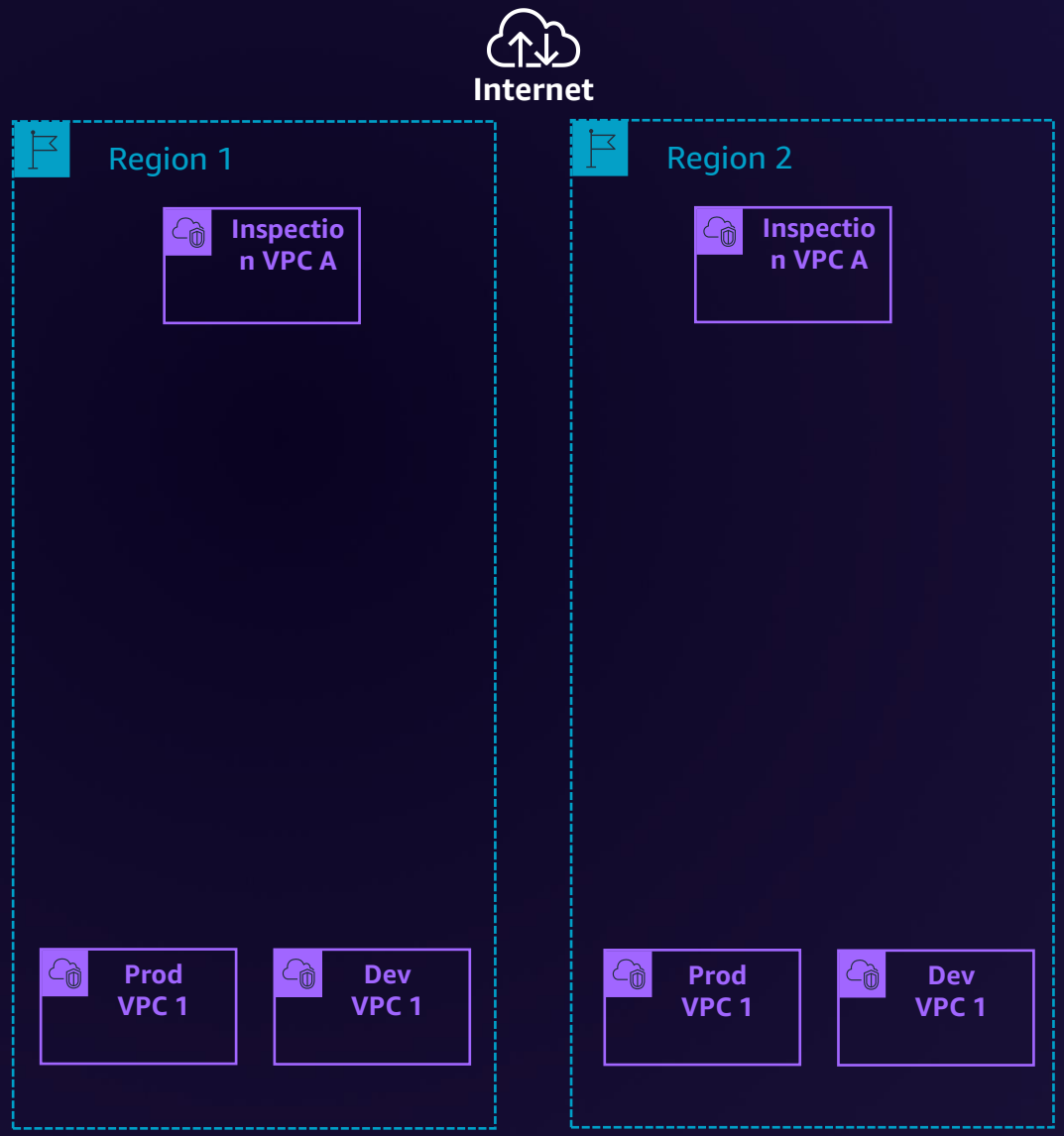


Building with AWS Cloud WAN

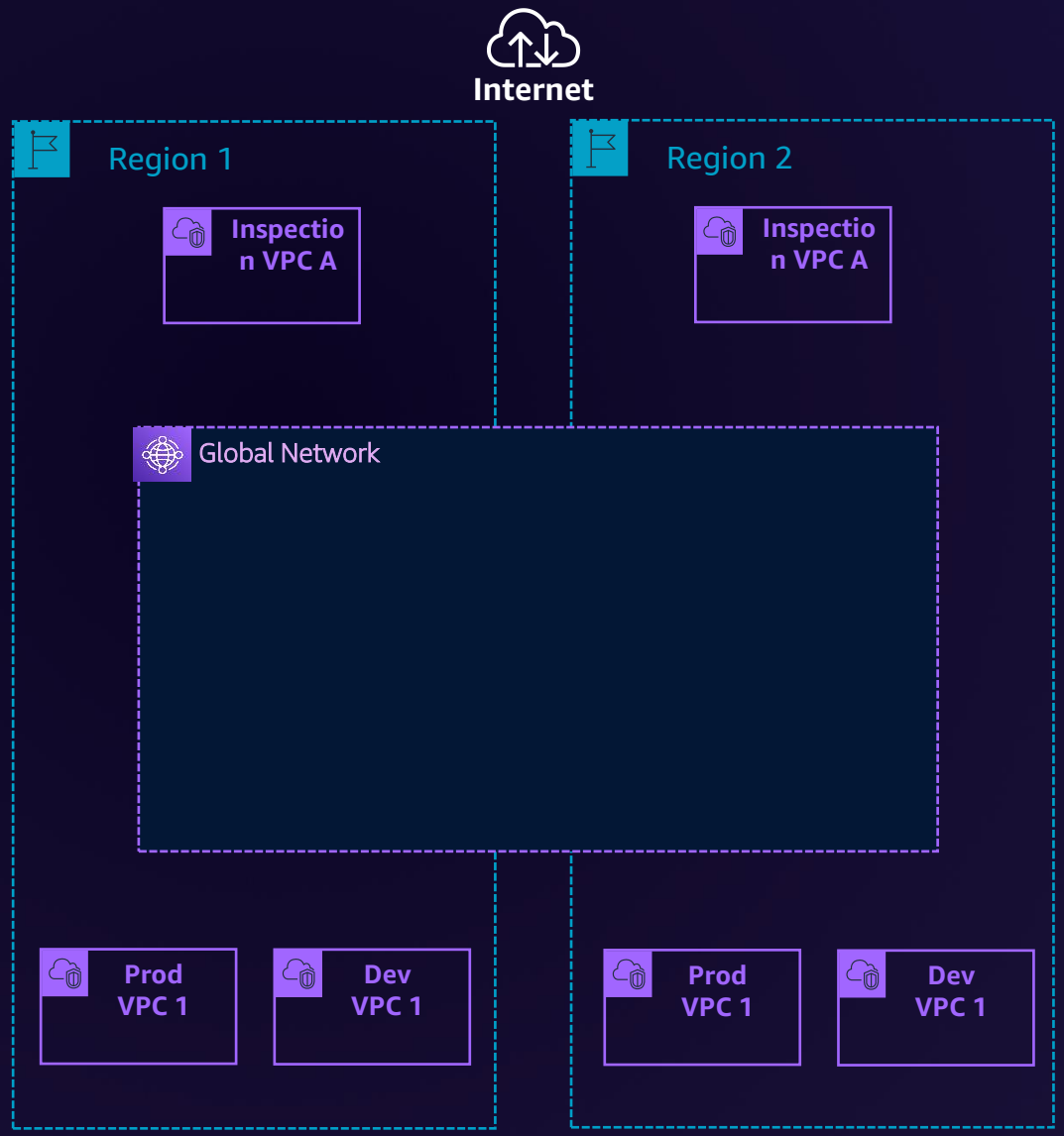


Egress inspection architecture

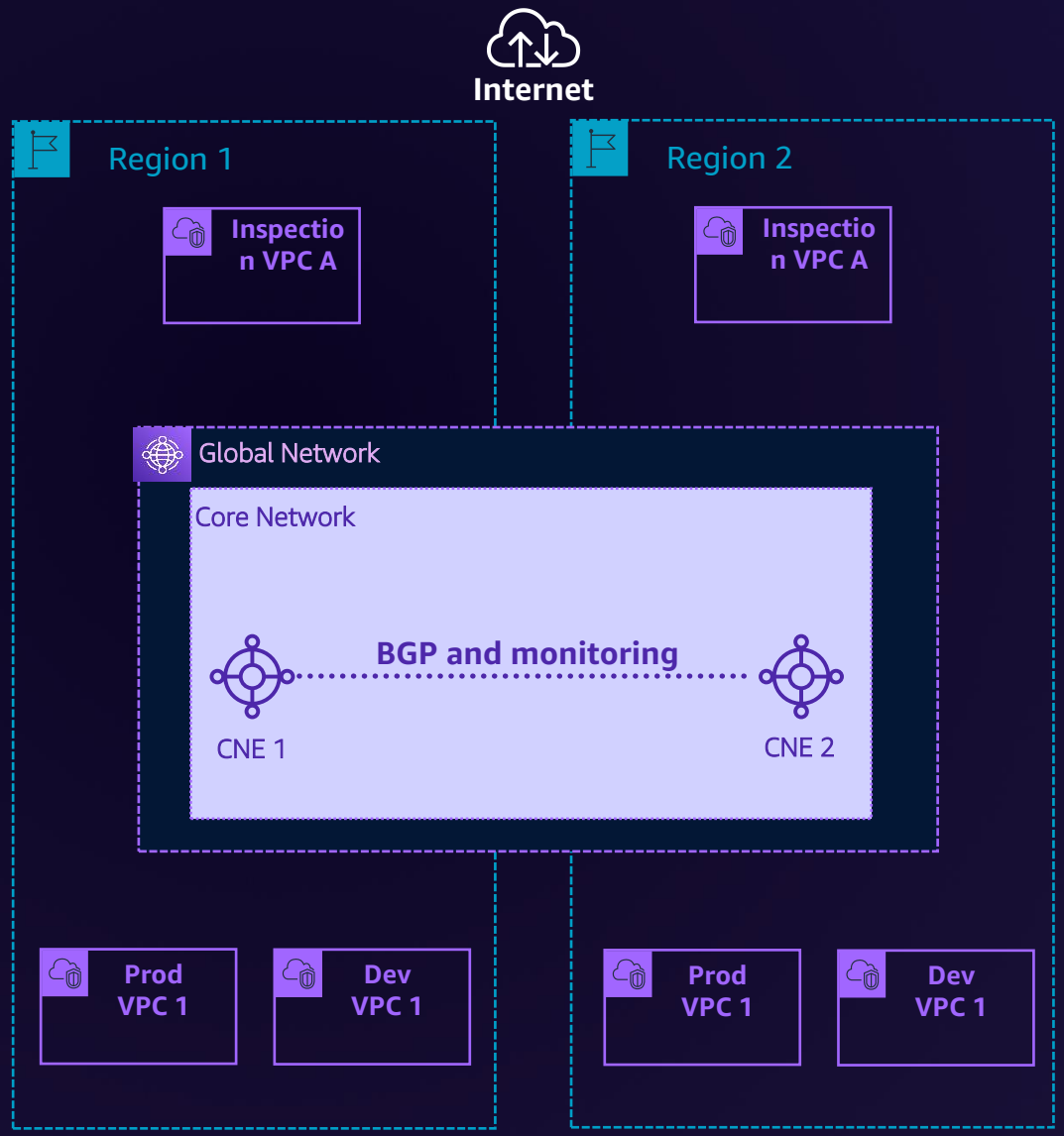
Egress inspection architecture



Egress inspection architecture

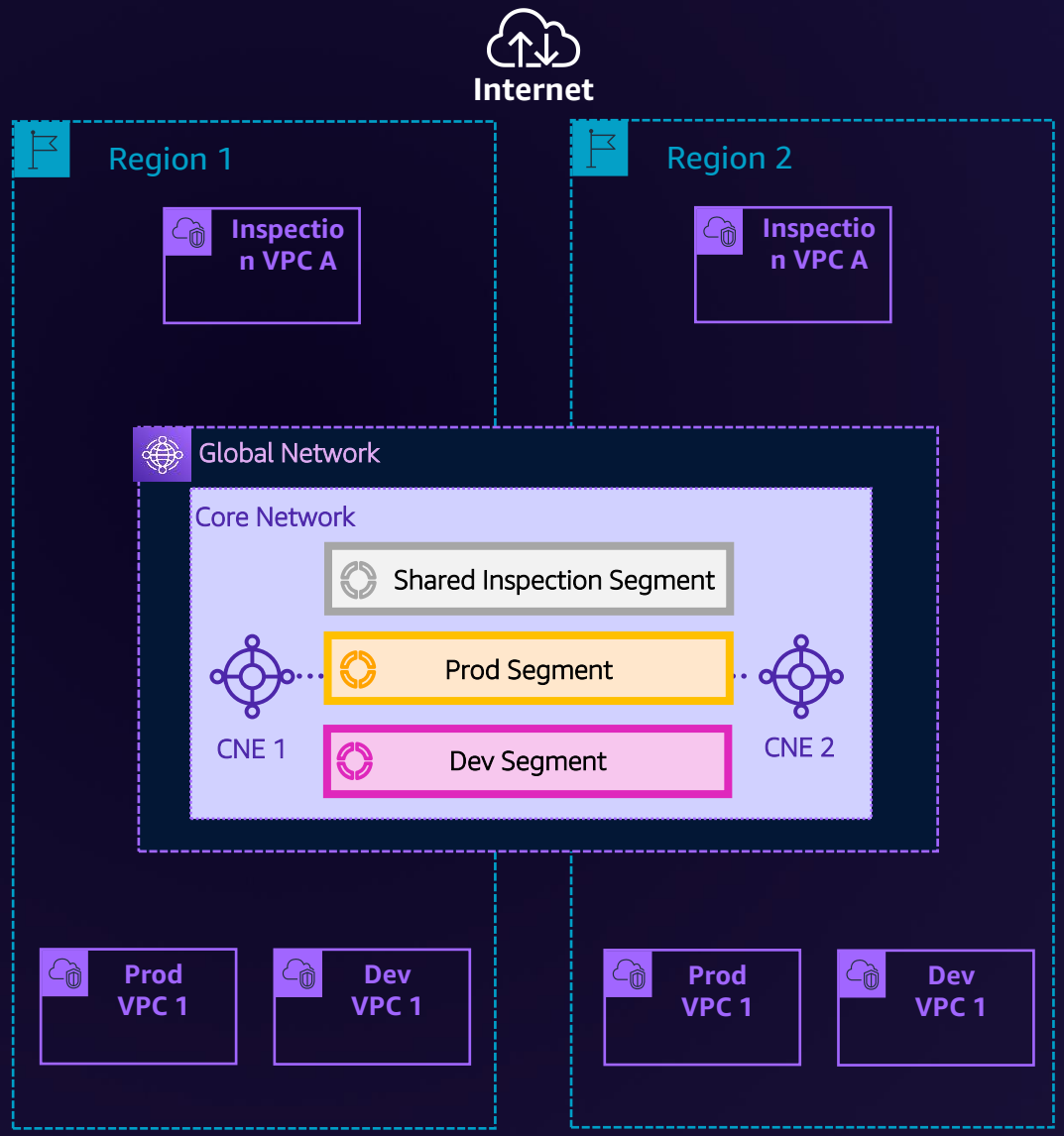


Egress inspection architecture



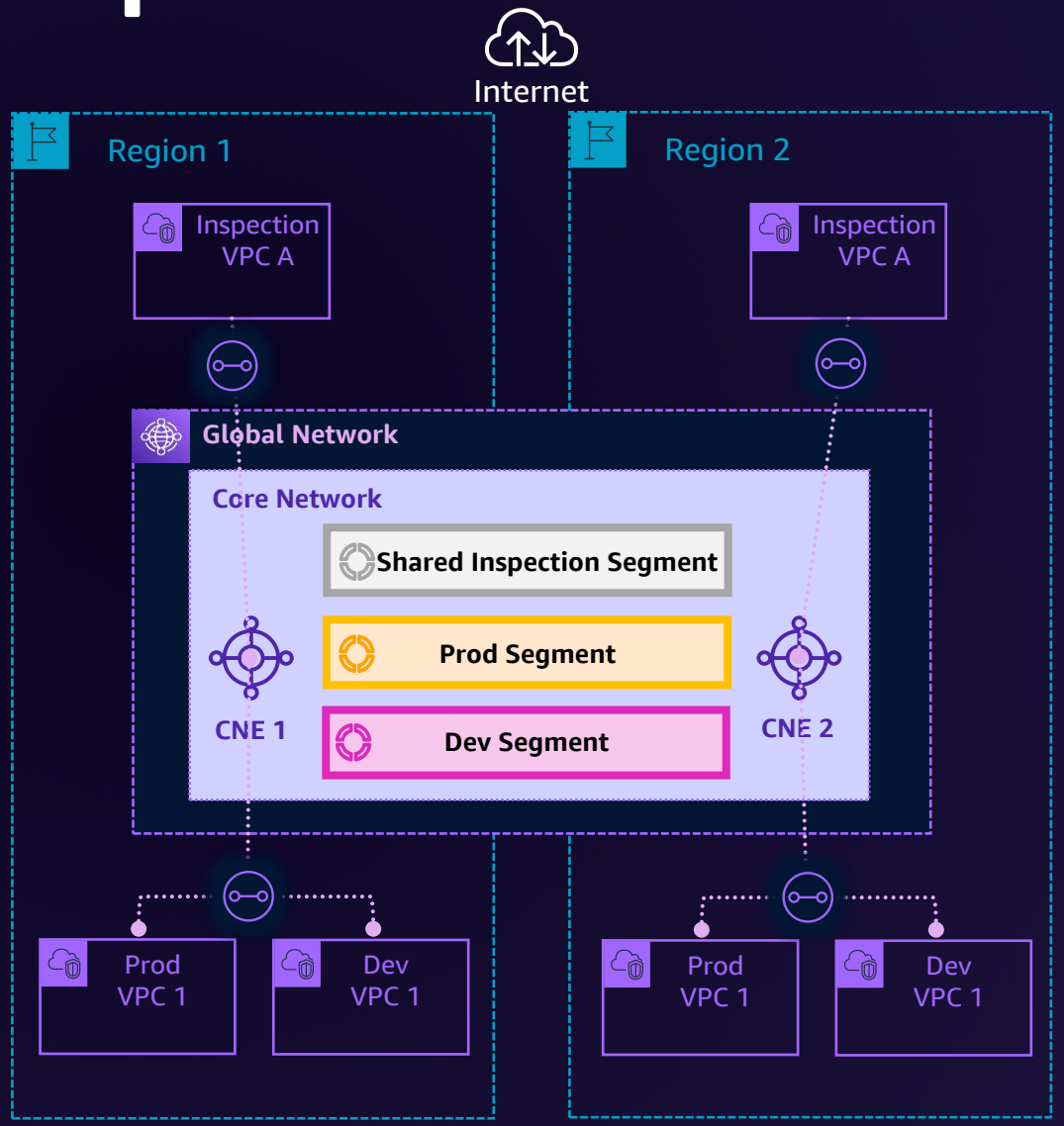

```
"core-network-configuration": {
    "vpn-ecmp-support": true,
    "asn-ranges": [
        "64512-65534"
    ],
    "edge-locations": [
        {
            "location": "us-east-1"
        },
        {
            "location": "us-west-2"
        }
    ]
}
```

Egress inspection architecture

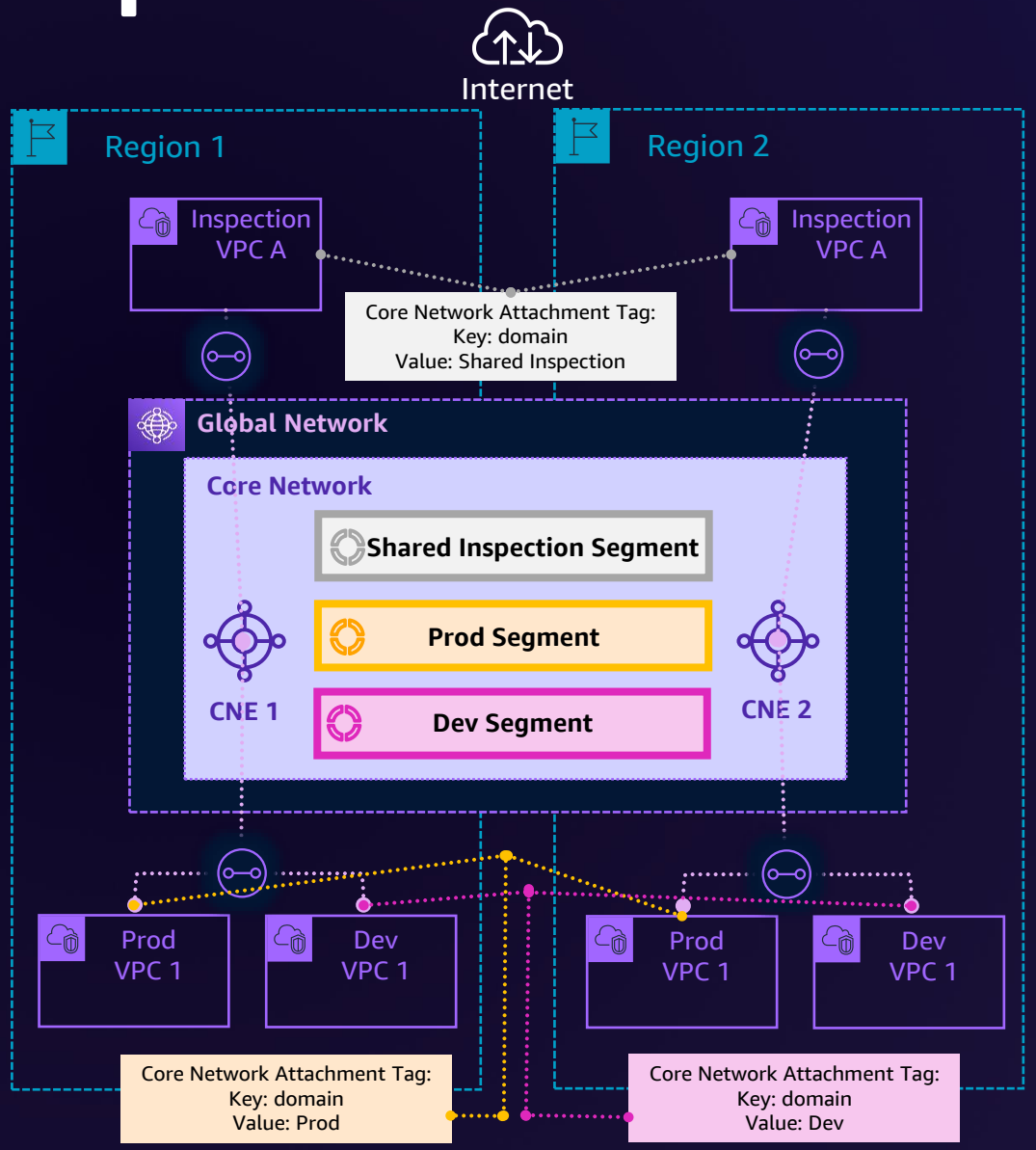



```
"core-network-configuration": {
    "vpn-ecmp-support": true,
    "asn-ranges": [
        "64512-65534"
    ],
    "edge-locations": [
        {
            "location": "us-east-1"
        },
        {
            "location": "us-west-2"
        }
    ]
},
"segments": [
    {
        "name": "Prod",
        "require-attachment-acceptance": false,
    },
    {
        "name": "Dev",
        "require-attachment-acceptance": false
    },
    {
        "name": "Shared Inspection
        "require-attachment-acceptance": false
    }
]
```

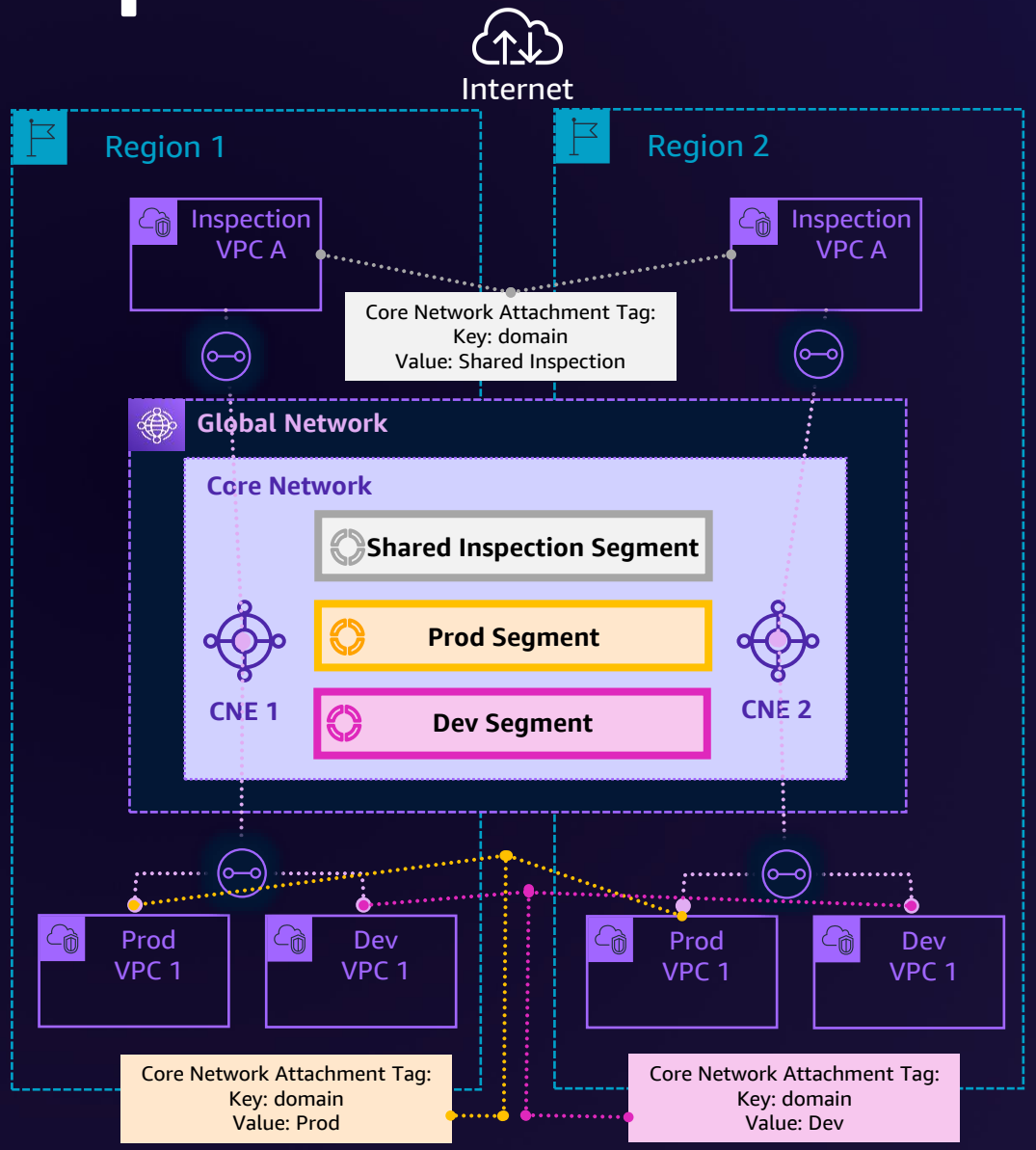
Egress inspection architecture



Egress inspection architecture

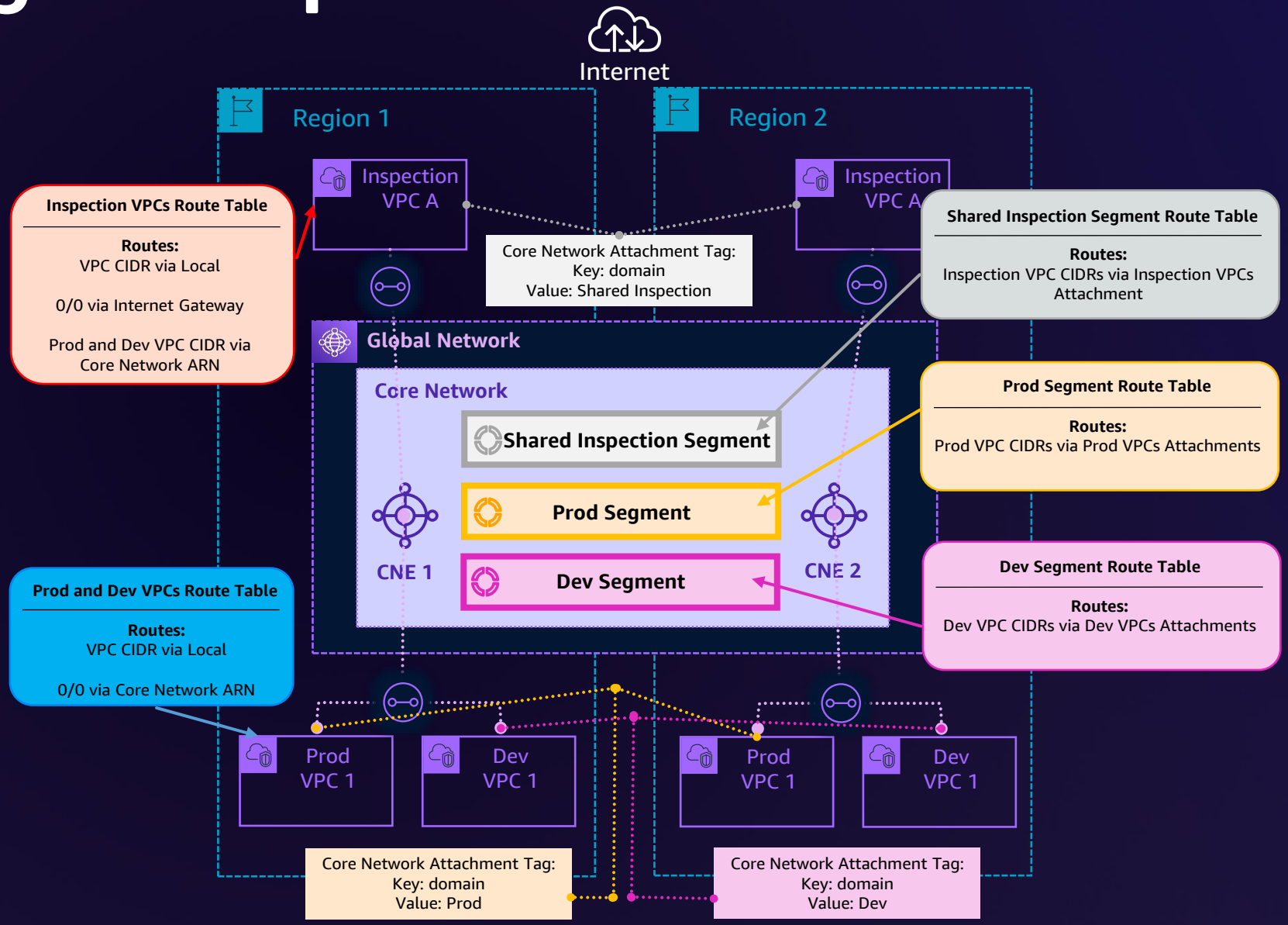


Egress inspection architecture



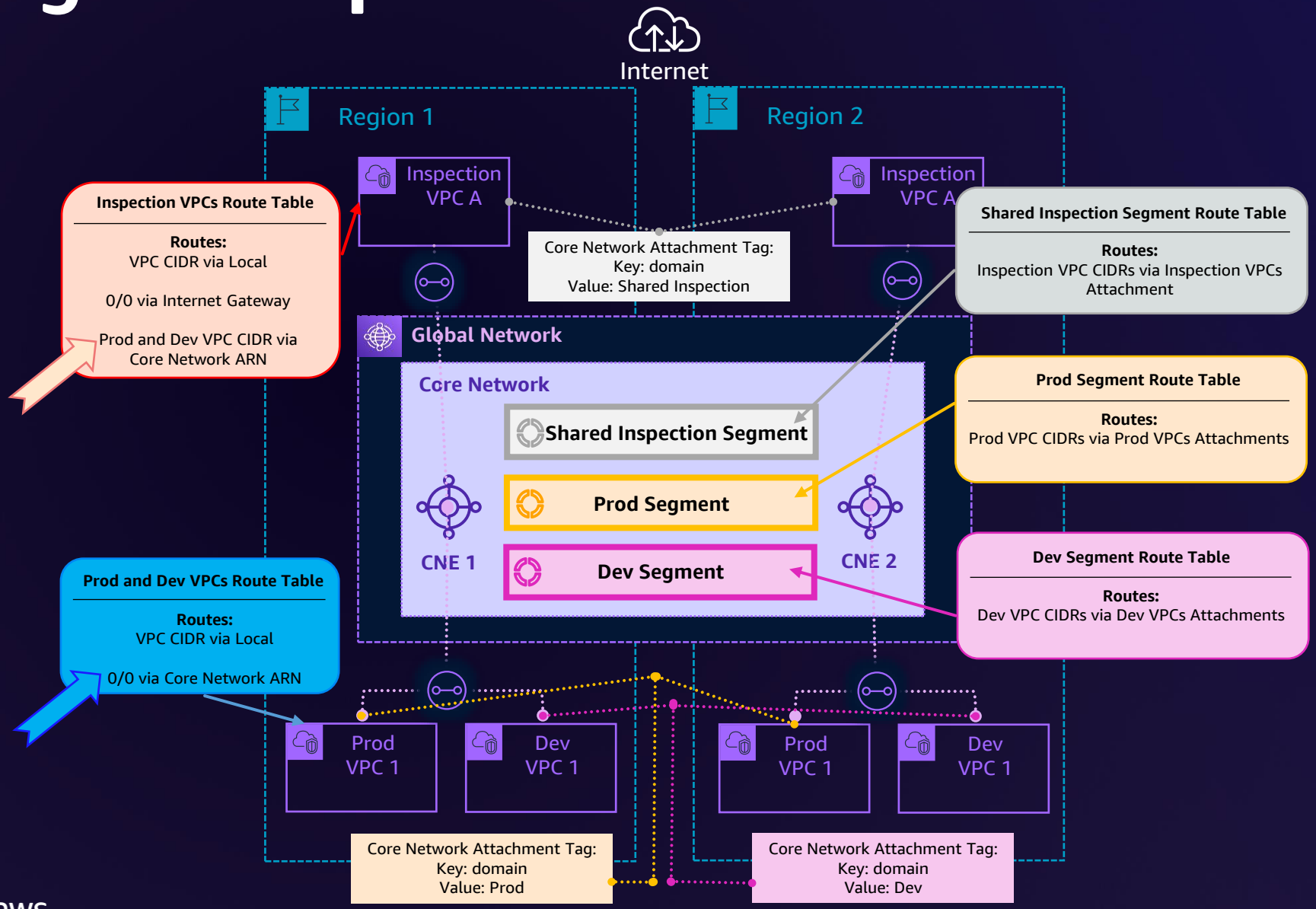

```
"attachment-policies": [
    {
        "rule-number": 100,
        "condition-logic": "or",
        "conditions": [
            {
                "type": "tag-exists",
                "key": "Segment",
            }
        ],
        "action": {
        "association-method": "tag",
        "tag-value-of-key": "Segment"
        }
    }
]
```

Egress inspection architecture



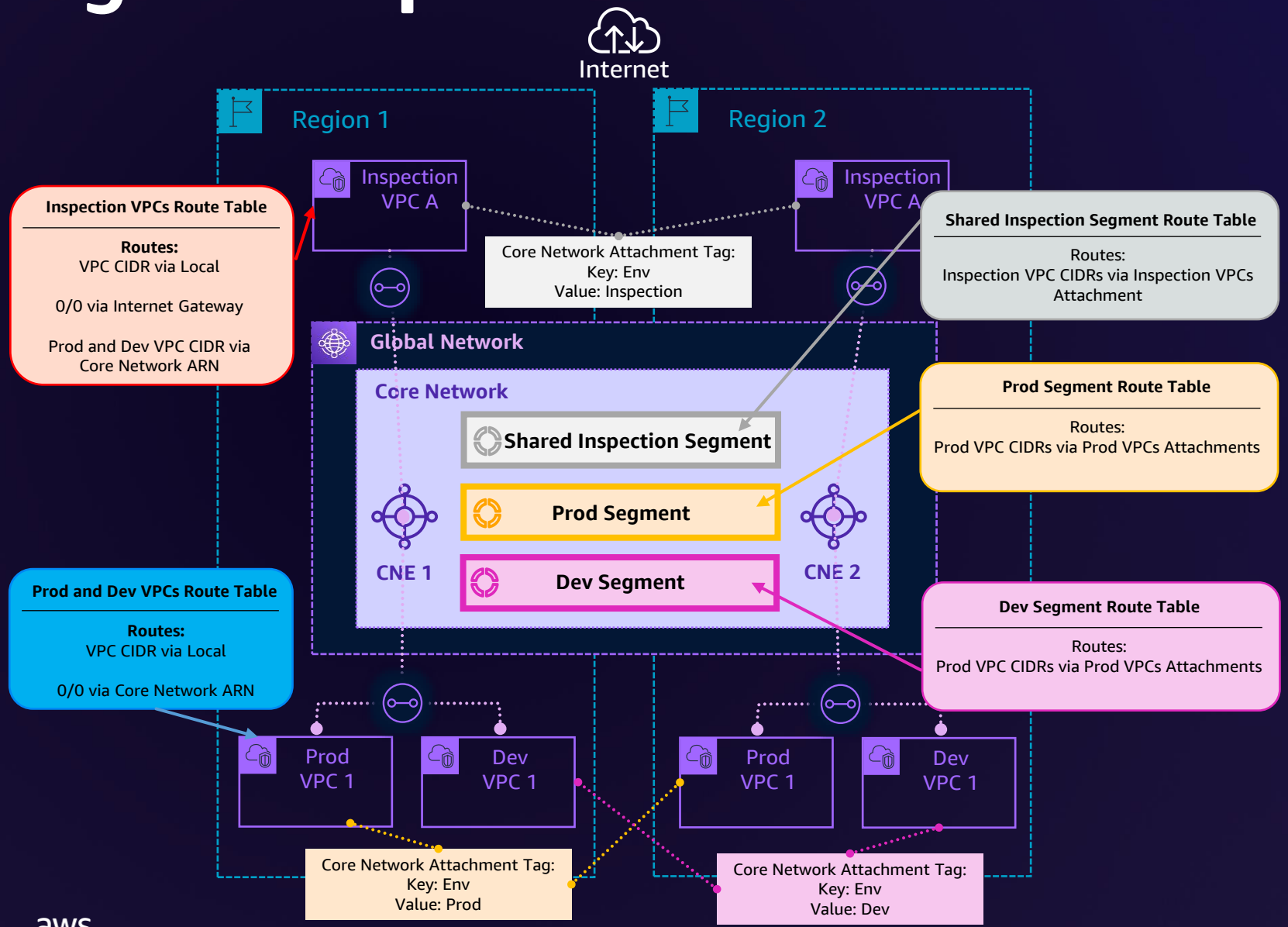

```
"attachment-policies": [
    {
        "rule-number": 100,
        "condition-logic": "or",
        "conditions": [
            {
                "type": "tag-exists",
                "key": "Segment",
            }
        ],
        "action": {
        "association-method": "tag",
        "tag-value-of-key": "Segment"
        }
    }
]
```

Egress inspection architecture



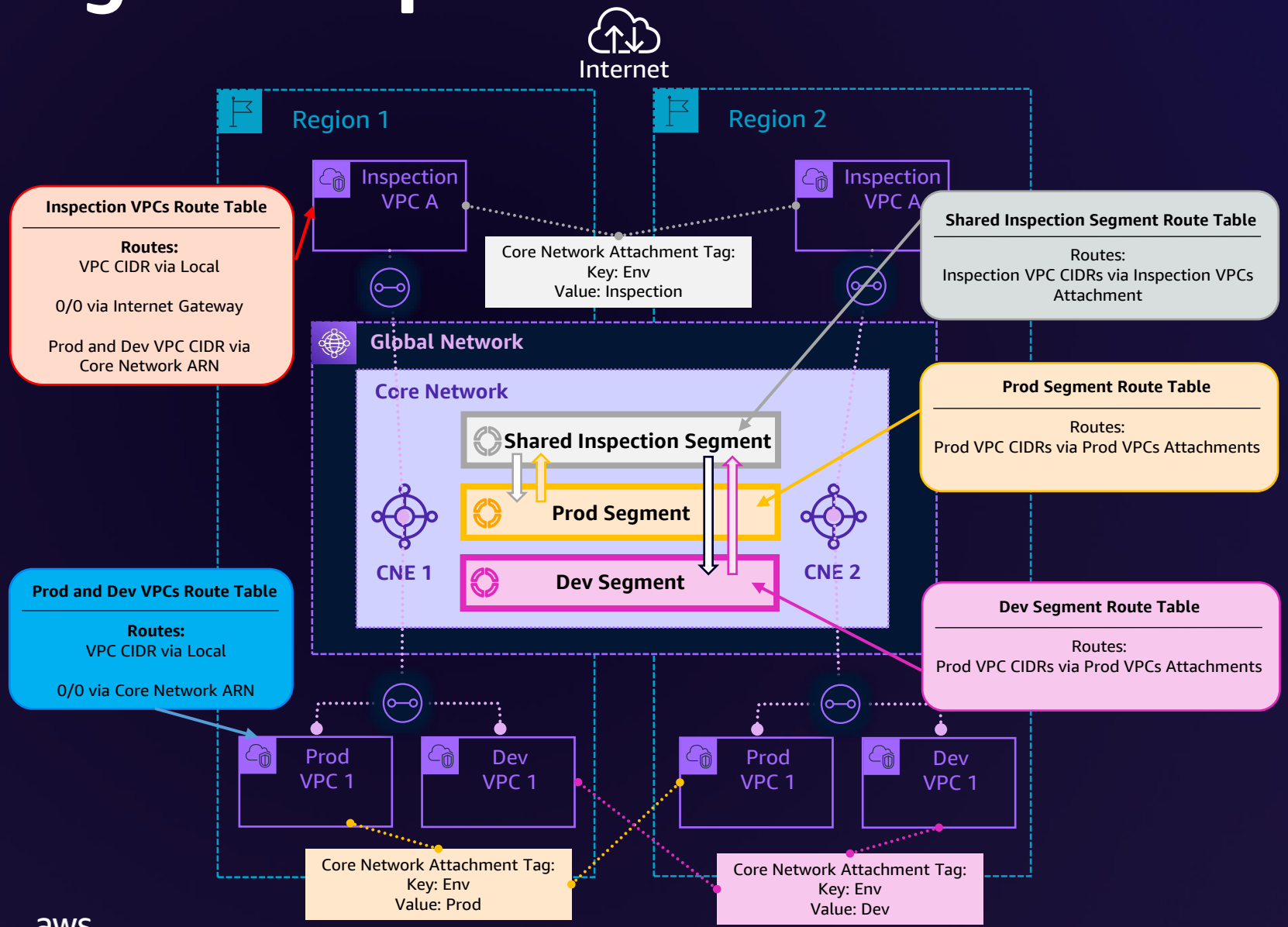

```
"attachment-policies": [
  {
    "rule-number": 100,
    "condition-logic": "or",
    "conditions": [
      {
        "type": "tag-exists",
        "key": "Segment",
      }
    ],
    "action": {
    "association-method": "tag",
    "tag-value-of-key": "Segment"
    }
  }
]
```

Egress inspection architecture



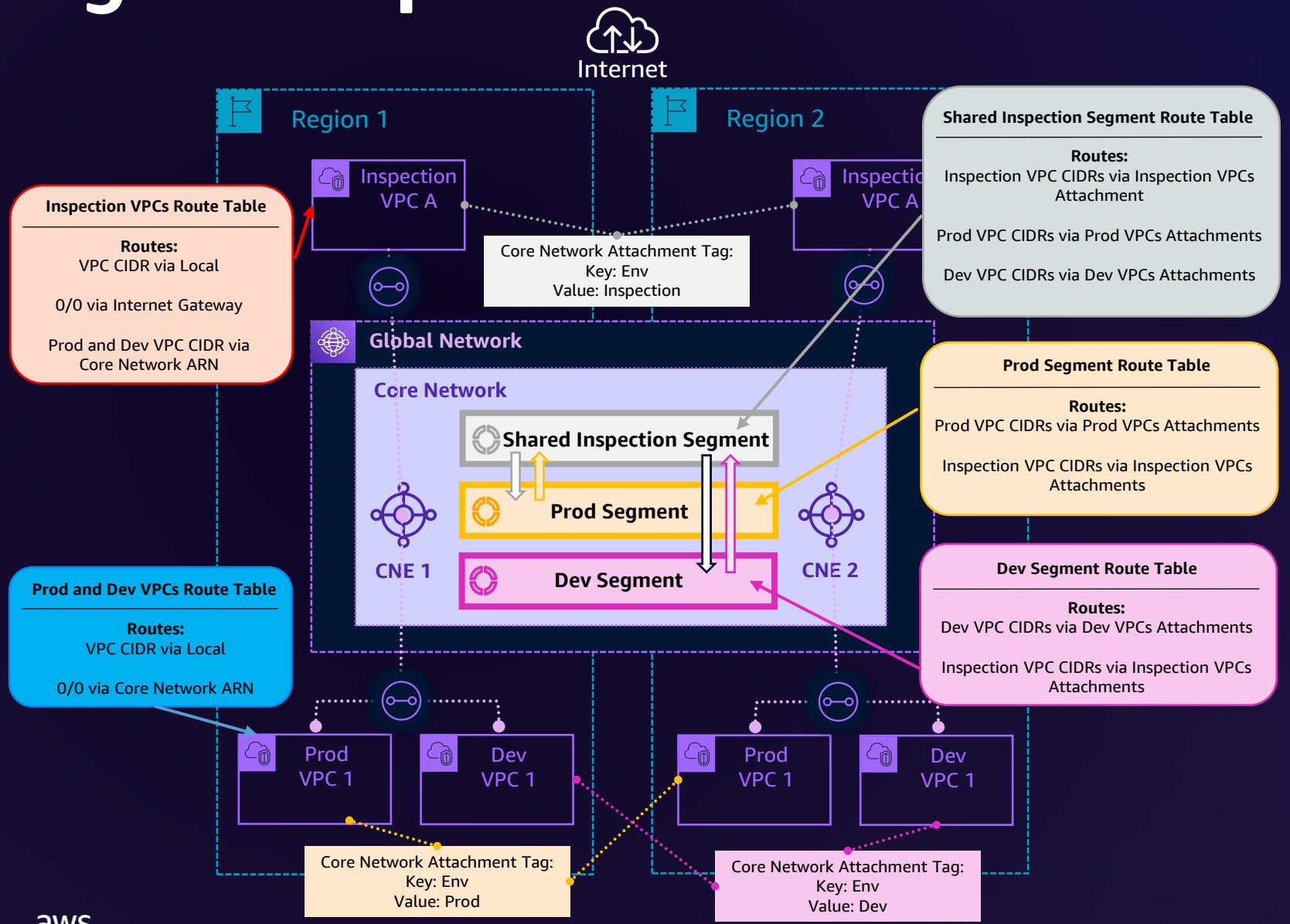

```
"attachment-policies": [
    {
        "rule-number": 100,
        "condition-logic": "or",
        "conditions": [
            {
                "type": "tag-exists",
                "key": "Segment",
            }
        ],
        "action": {
        "association-method": "tag",
        "tag-value-of-key": "Segment"
        }
    }
],
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    }
]
```

Egress inspection architecture




```
"attachment-policies": [
    {
        "rule-number": 100,
        "condition-logic": "or",
        "conditions": [
            {
                "type": "tag-exists",
                "key": "Segment",
            }
        ],
        "action": {
        "association-method": "tag",
        "tag-value-of-key": "Segment"
        }
    }
],
"segment-actions": [
  {
    "action": "share",
    "mode": "attachment-route",
    "segment": "Shared Inspection",
    "share-with": "*"
  }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

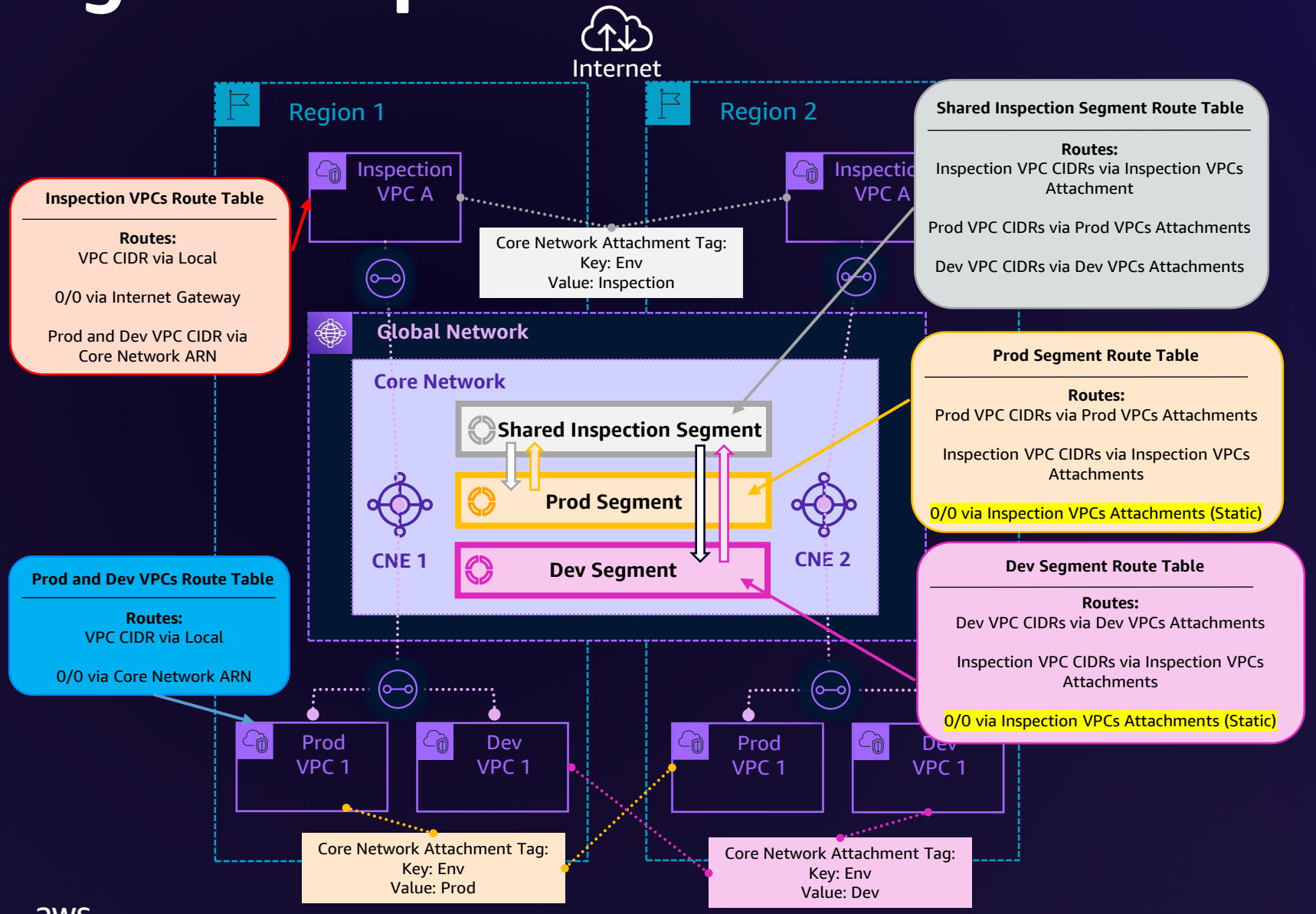
Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

```
"attachment-policies": [
    {
        "rule-number": 100,
        "condition-logic": "or",
        "conditions": [
            {
                "type": "tag-exists",
                "key": "Segment",
            }
        ],
        "action": {
        "association-method": "tag",
        "tag-value-of-key": "Segment"
        }
    }
],
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

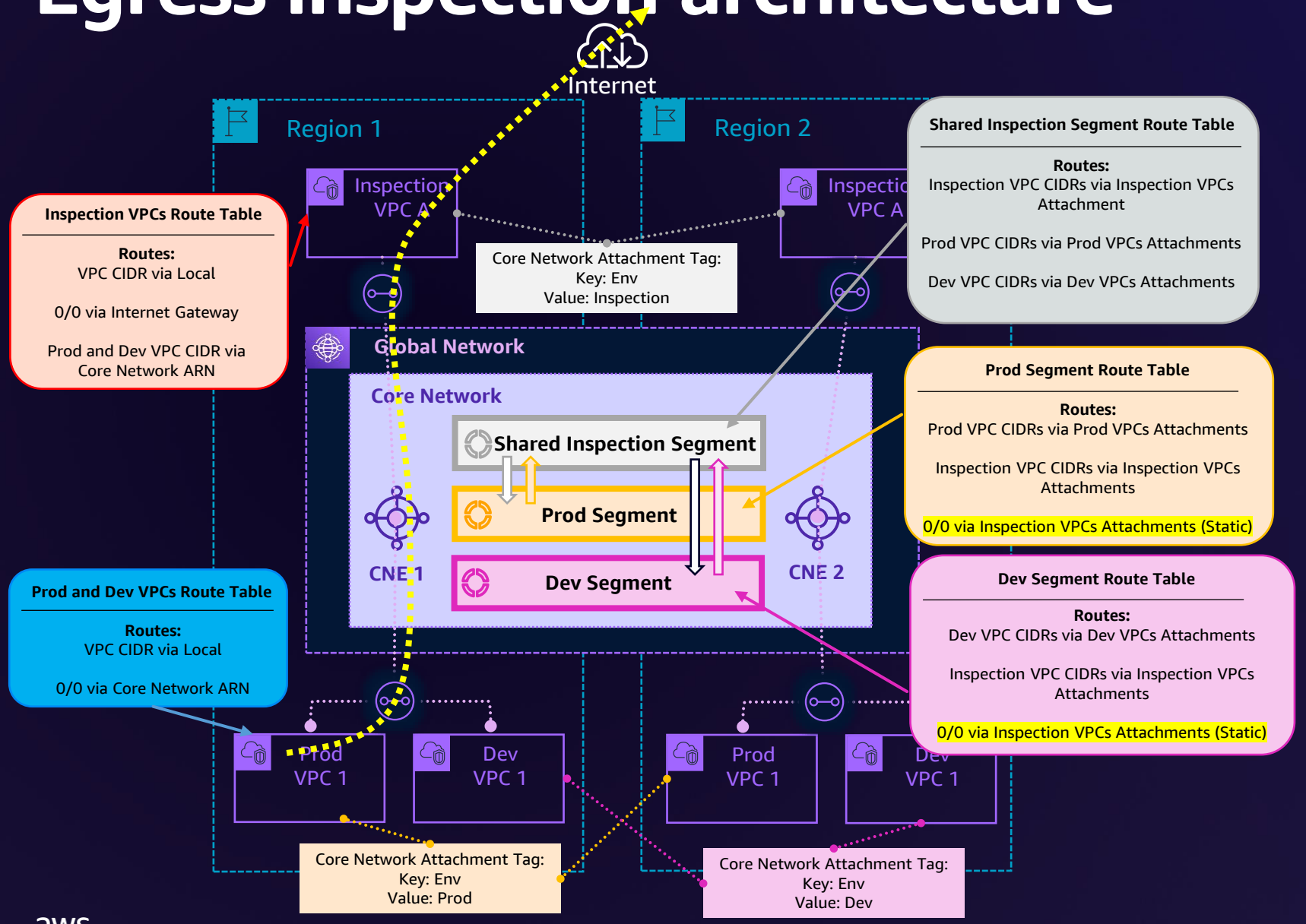
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

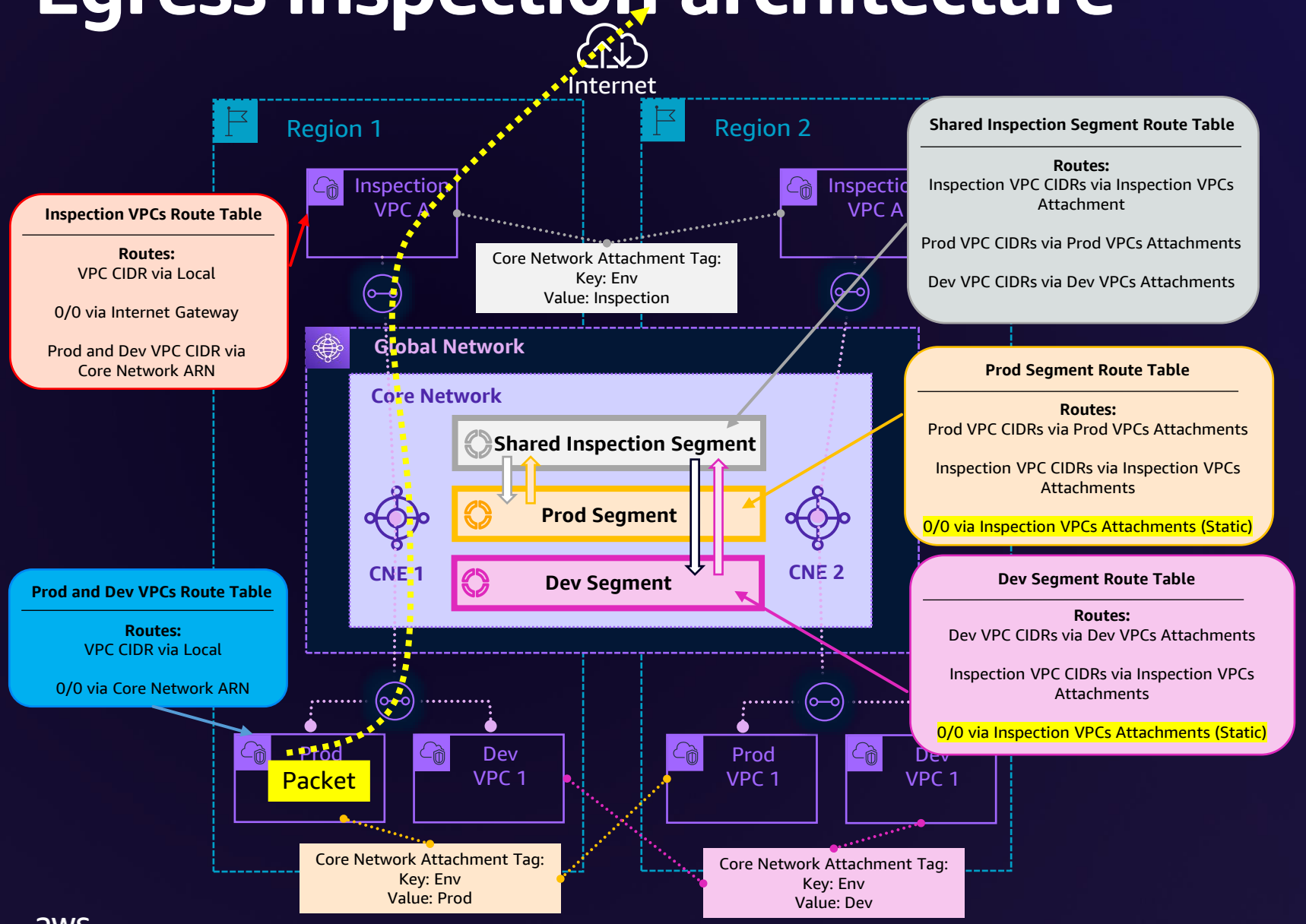
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

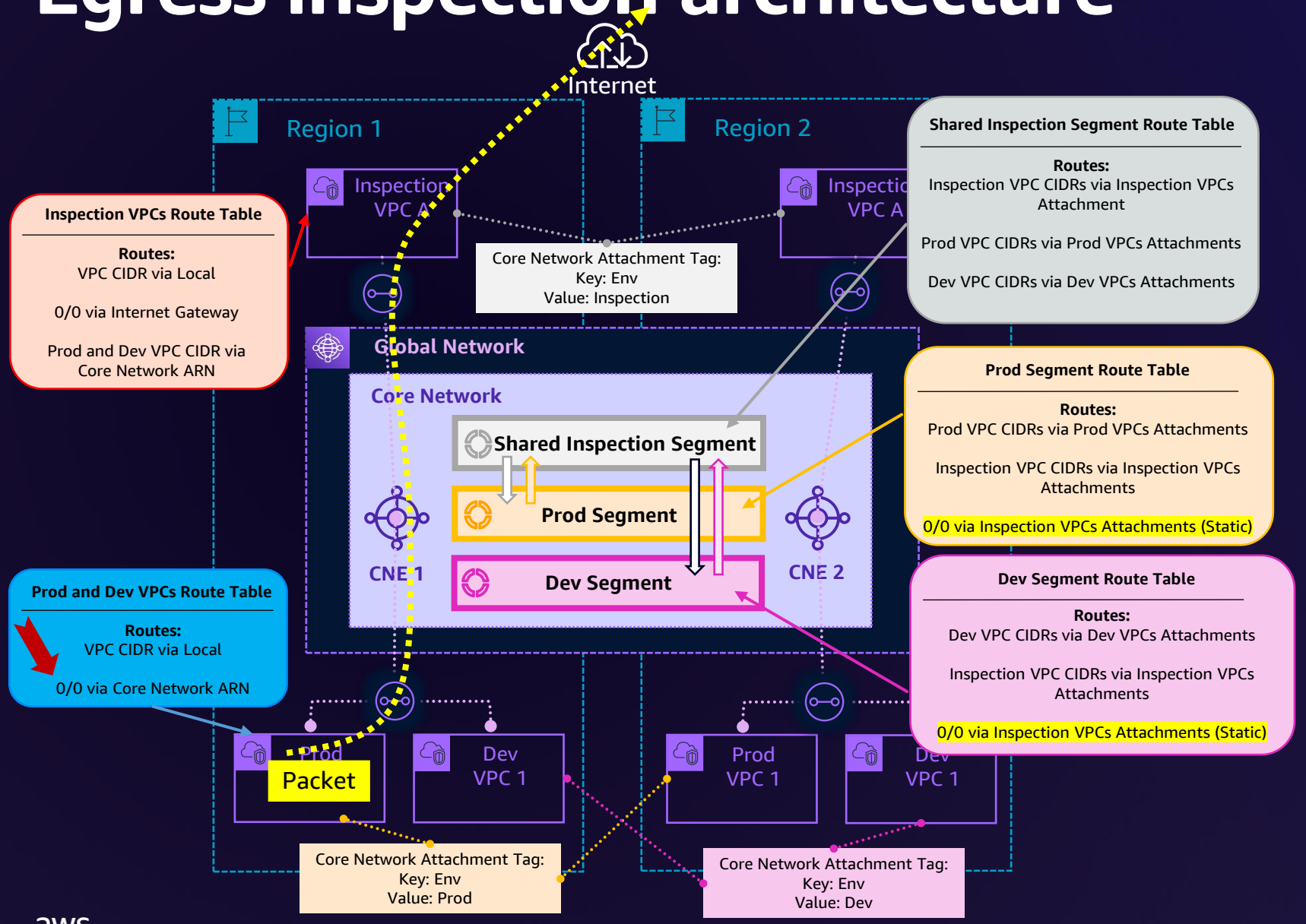
```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



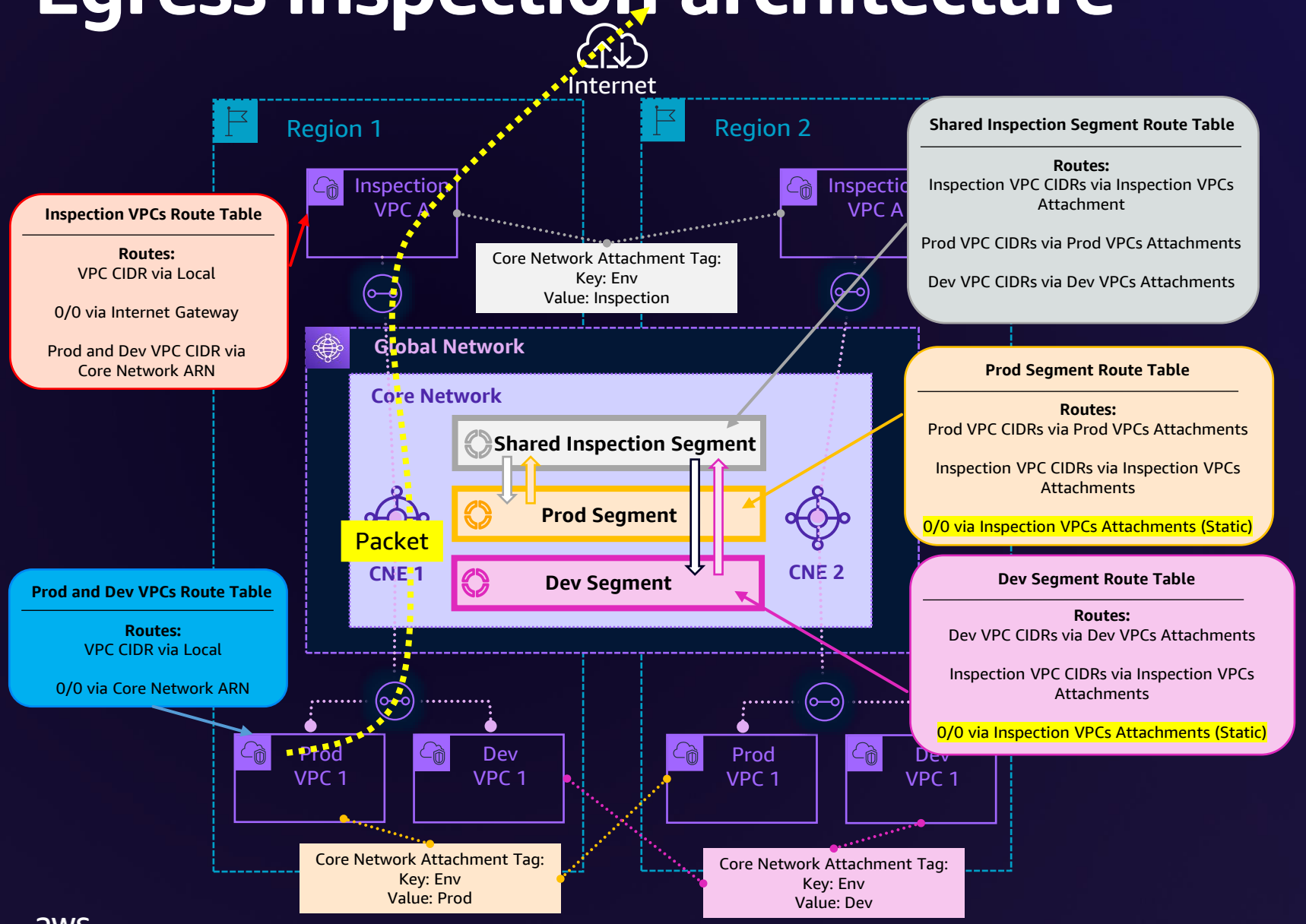

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture




```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

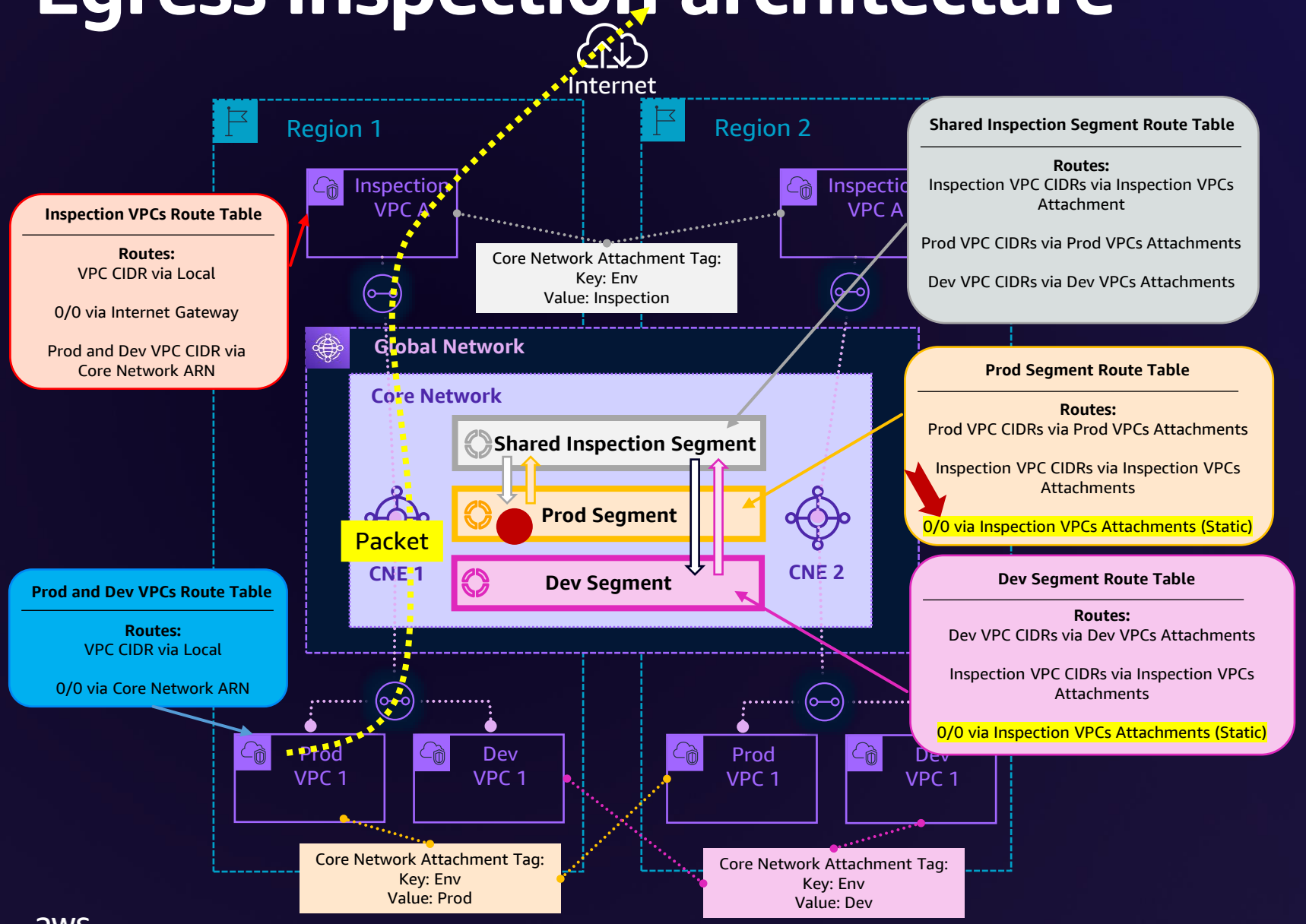
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

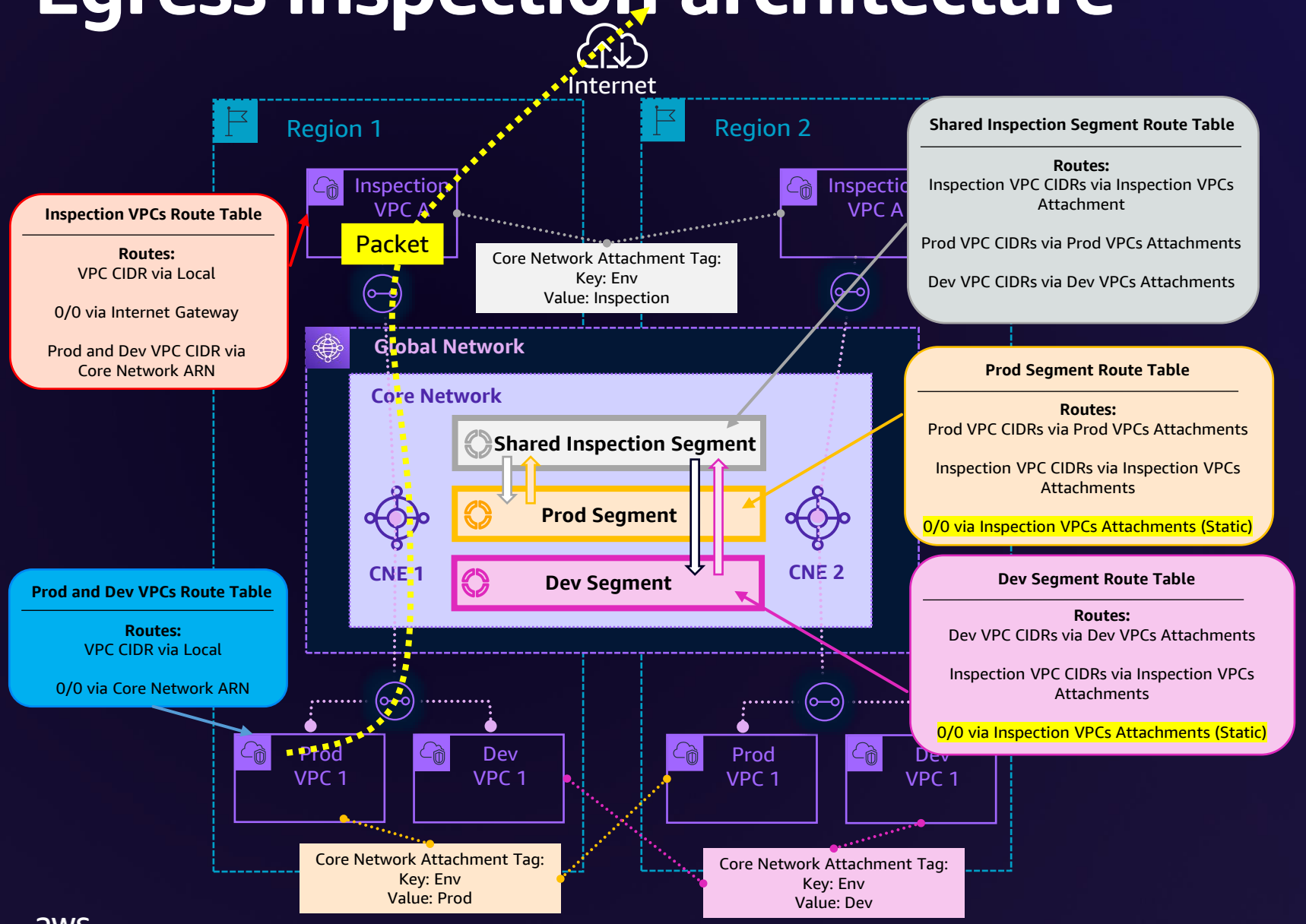
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

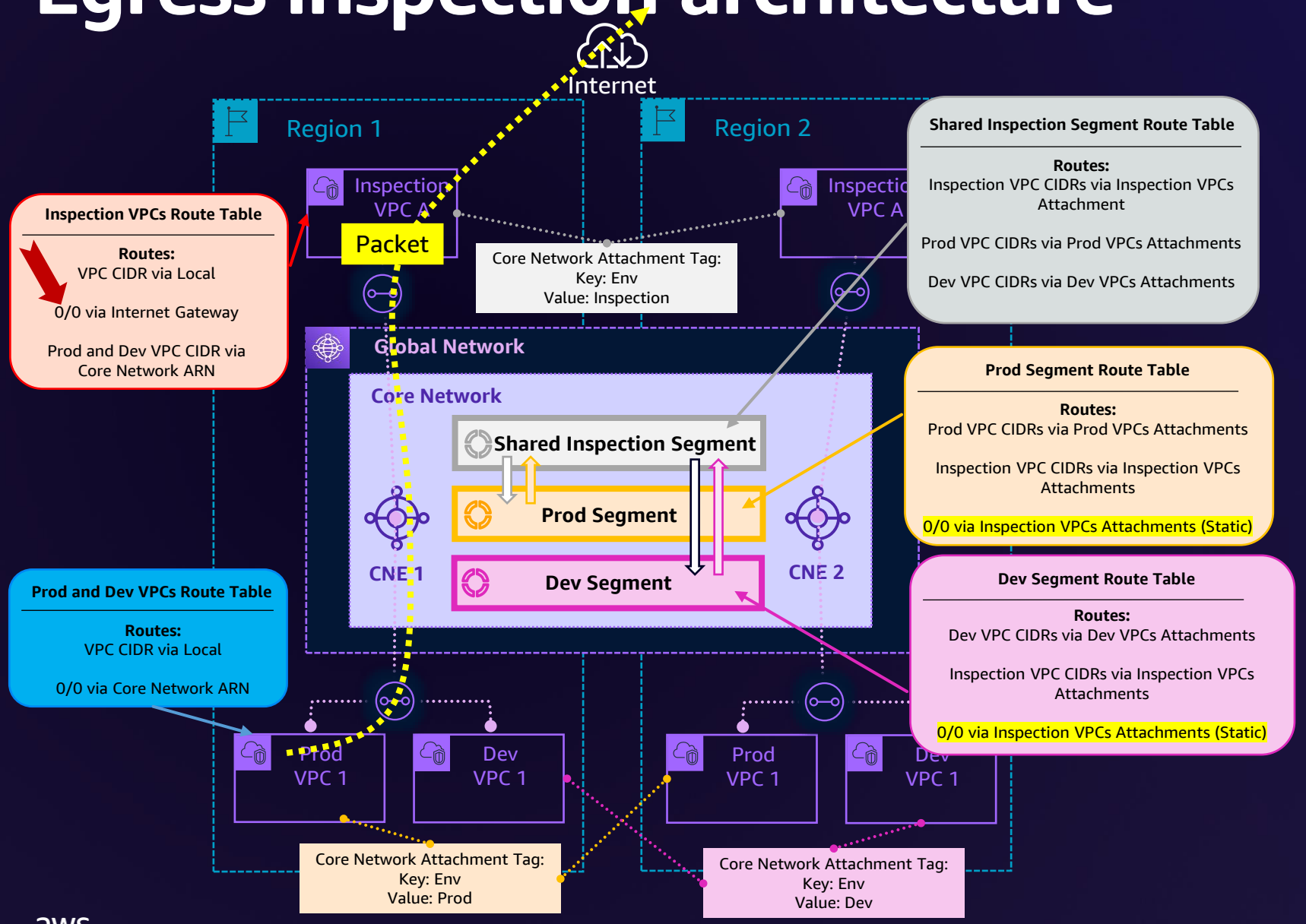
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

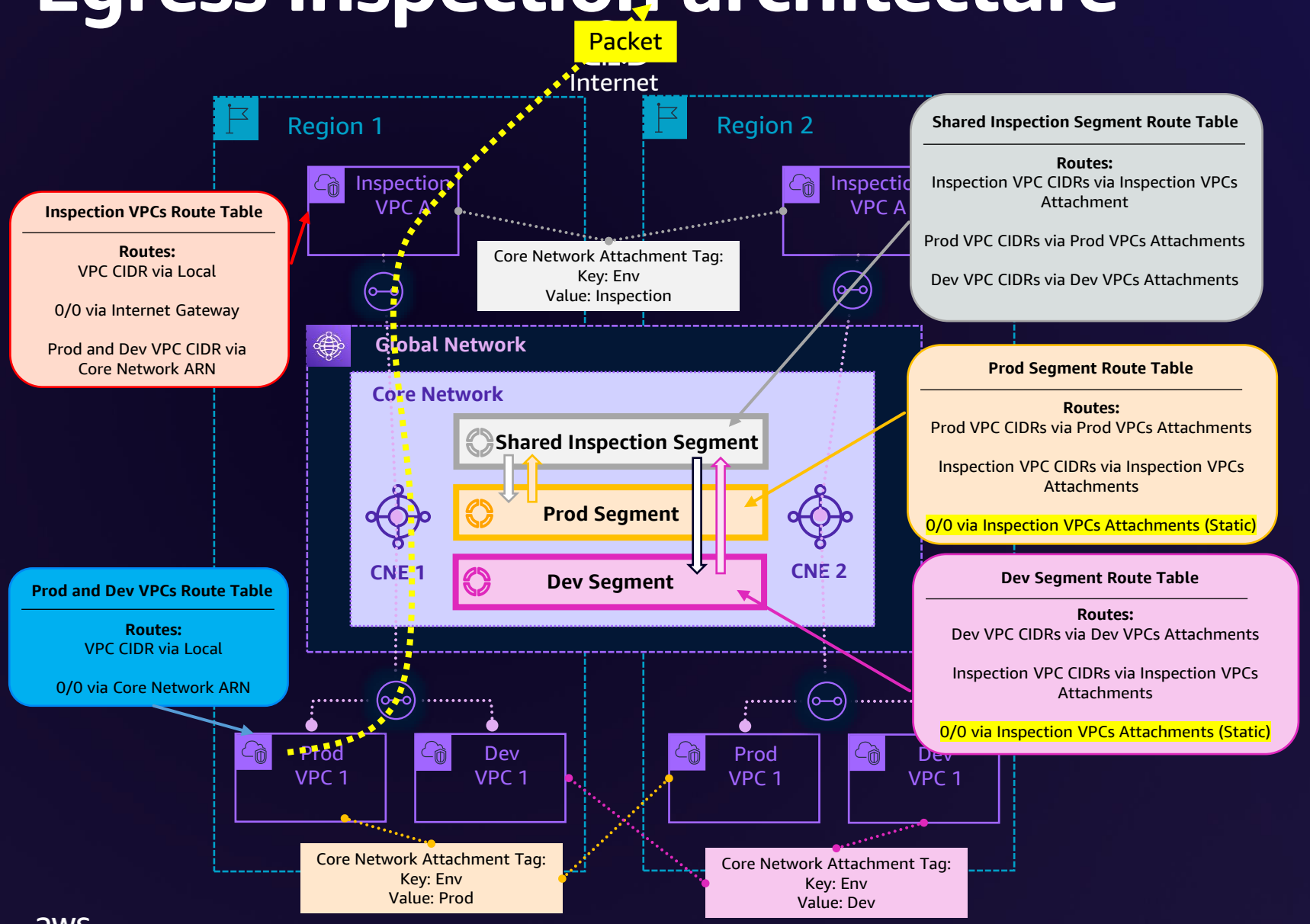
Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

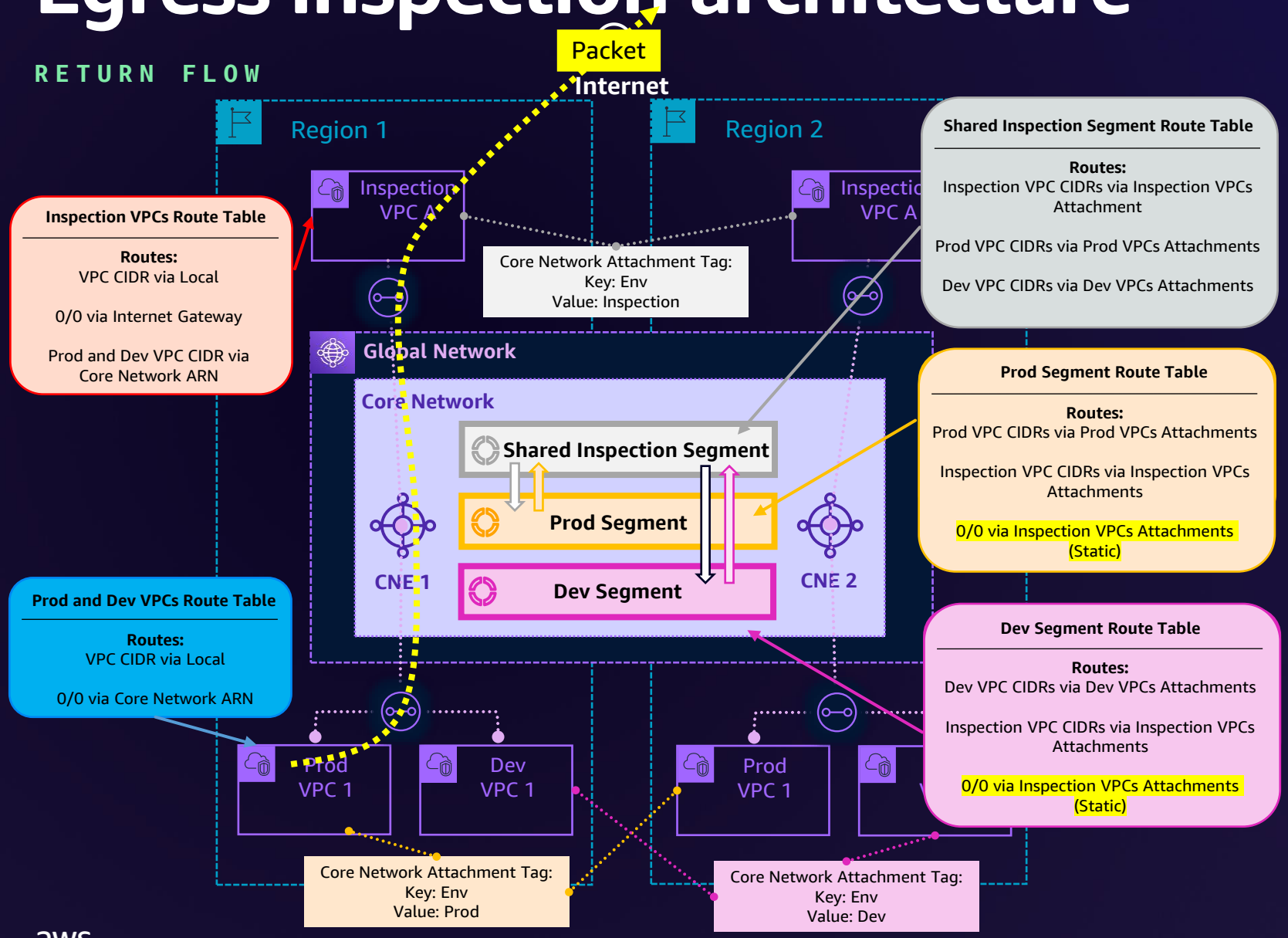
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

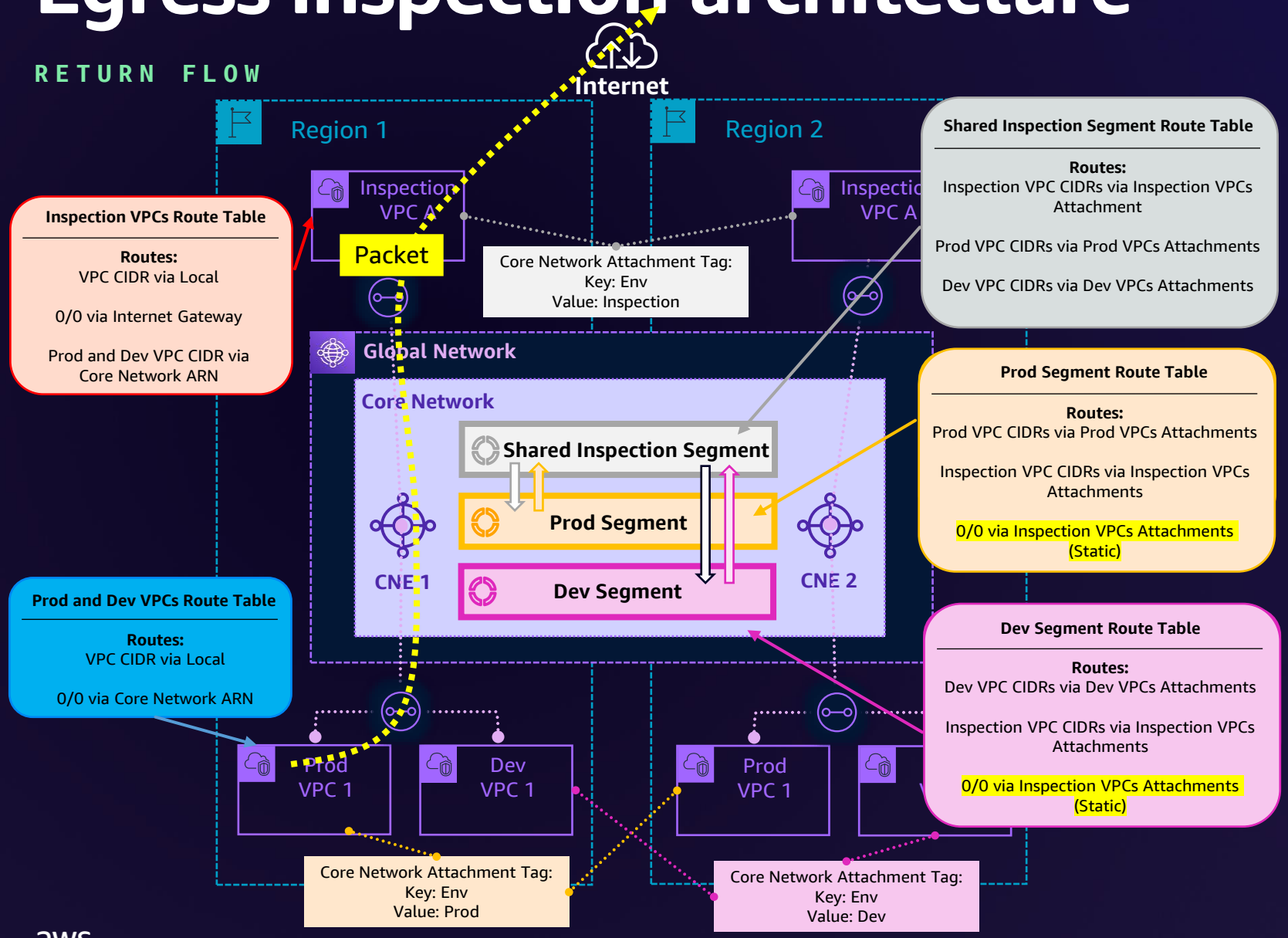
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

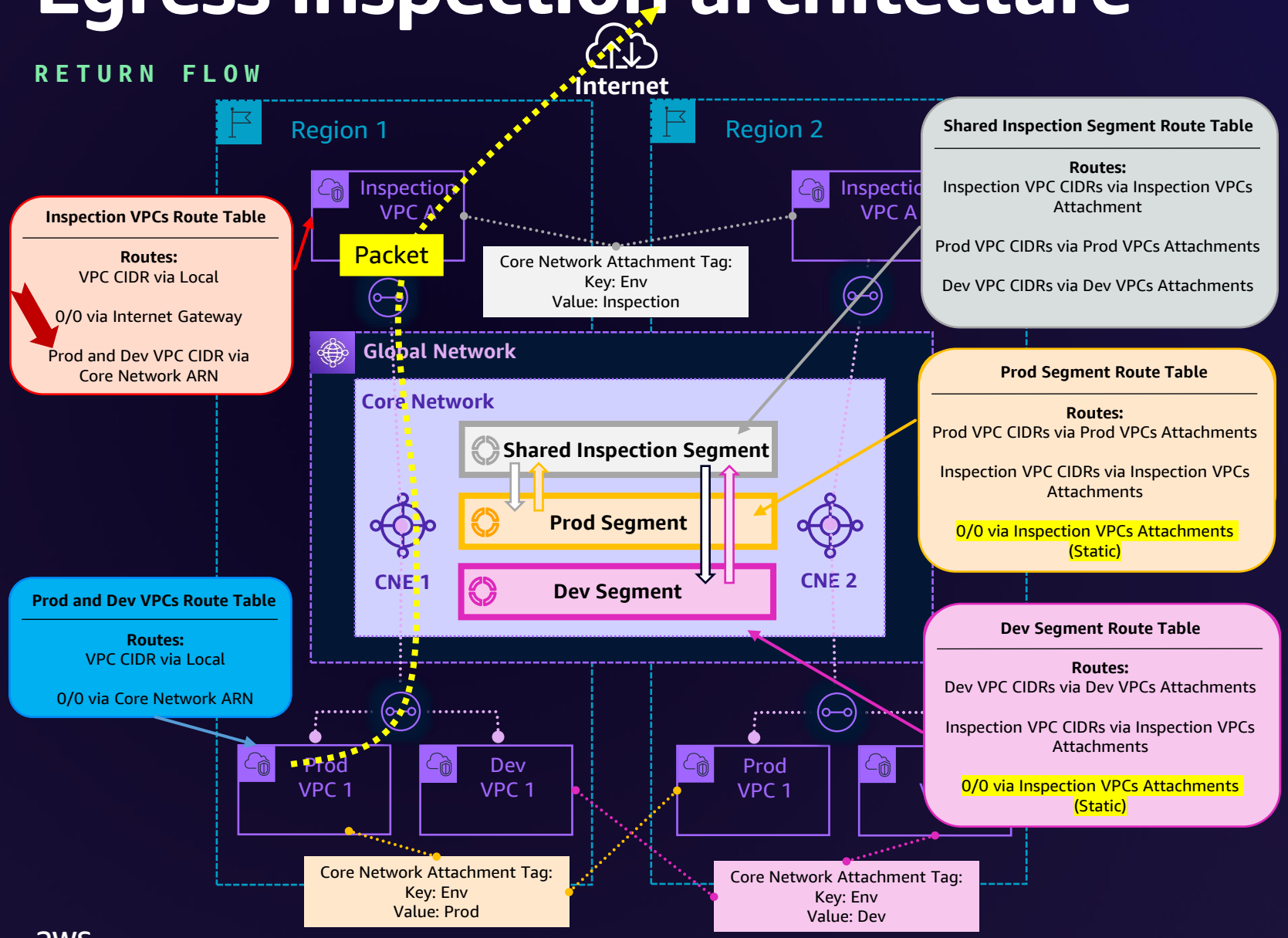
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

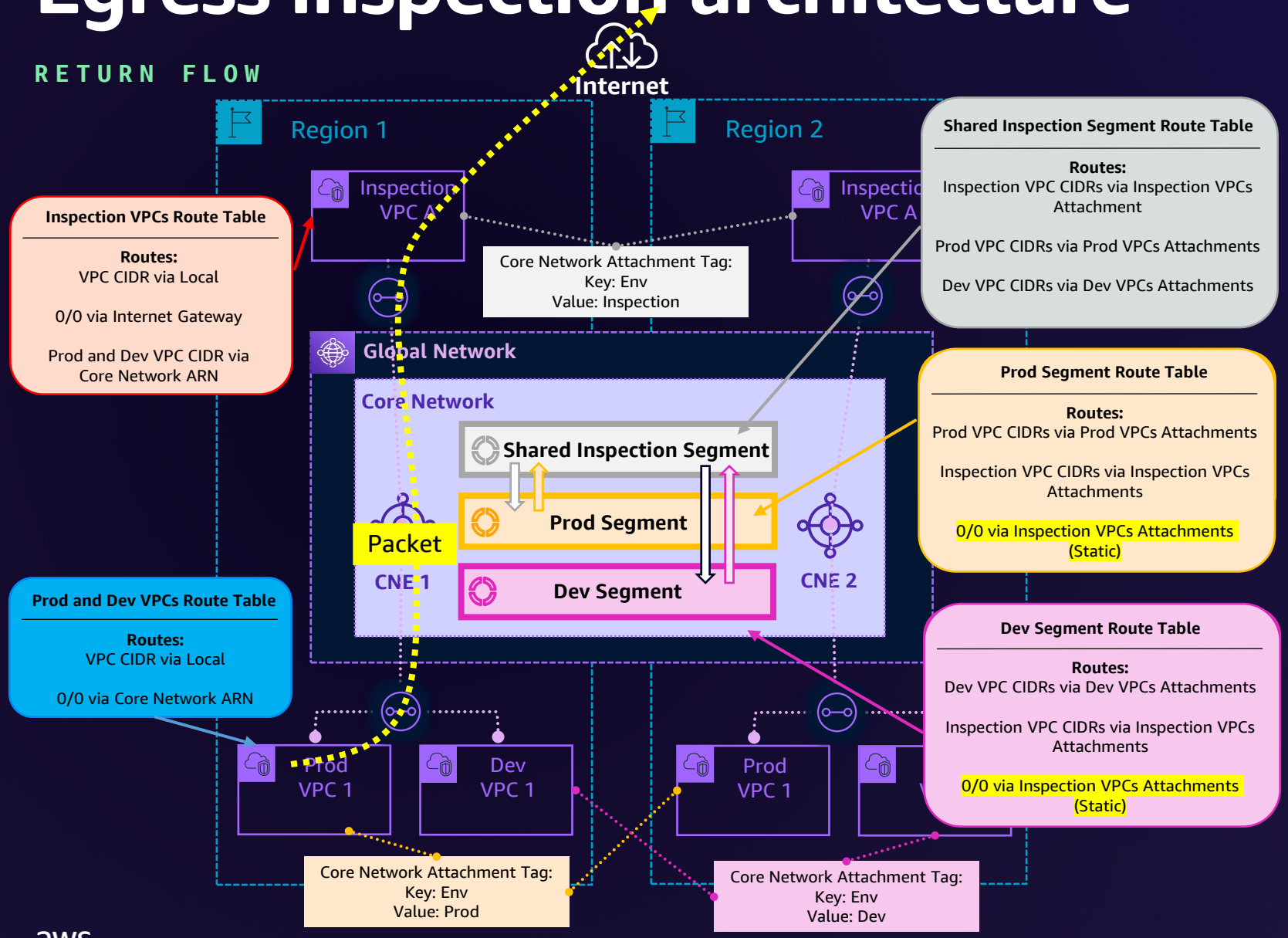
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    } ,
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
                "0.0.0.0/0"
        ],
        "destinations": [
                "inspection-vpc-a-attachment-aaaa",
                "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
                "0.0.0.0/0"
        ],
        "destinations": [
                "inspection-vpc-a-attachment-aaaa",
                "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

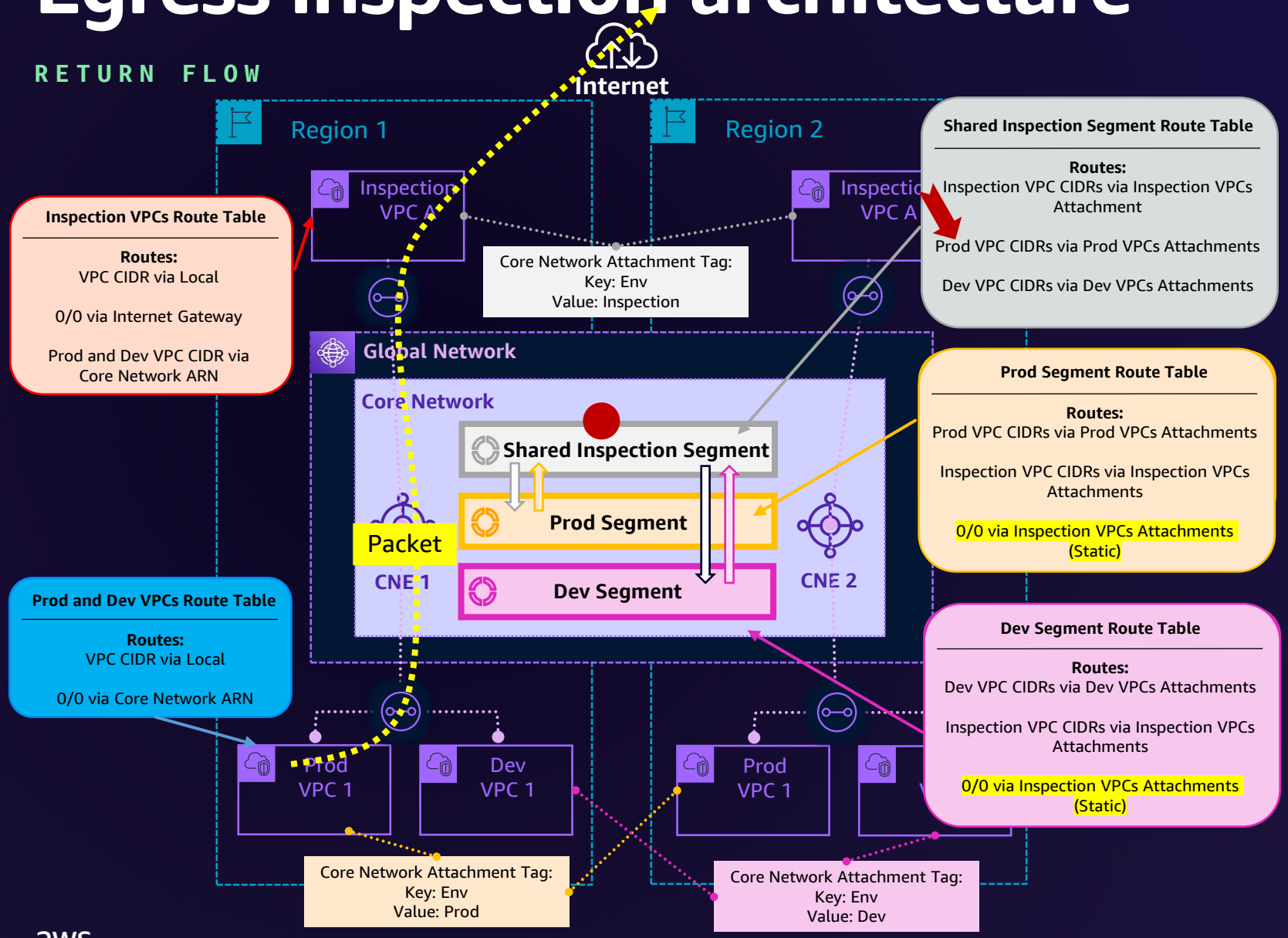
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Shared Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

Dev VPC CIDRs via Dev VPCs Attachments

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

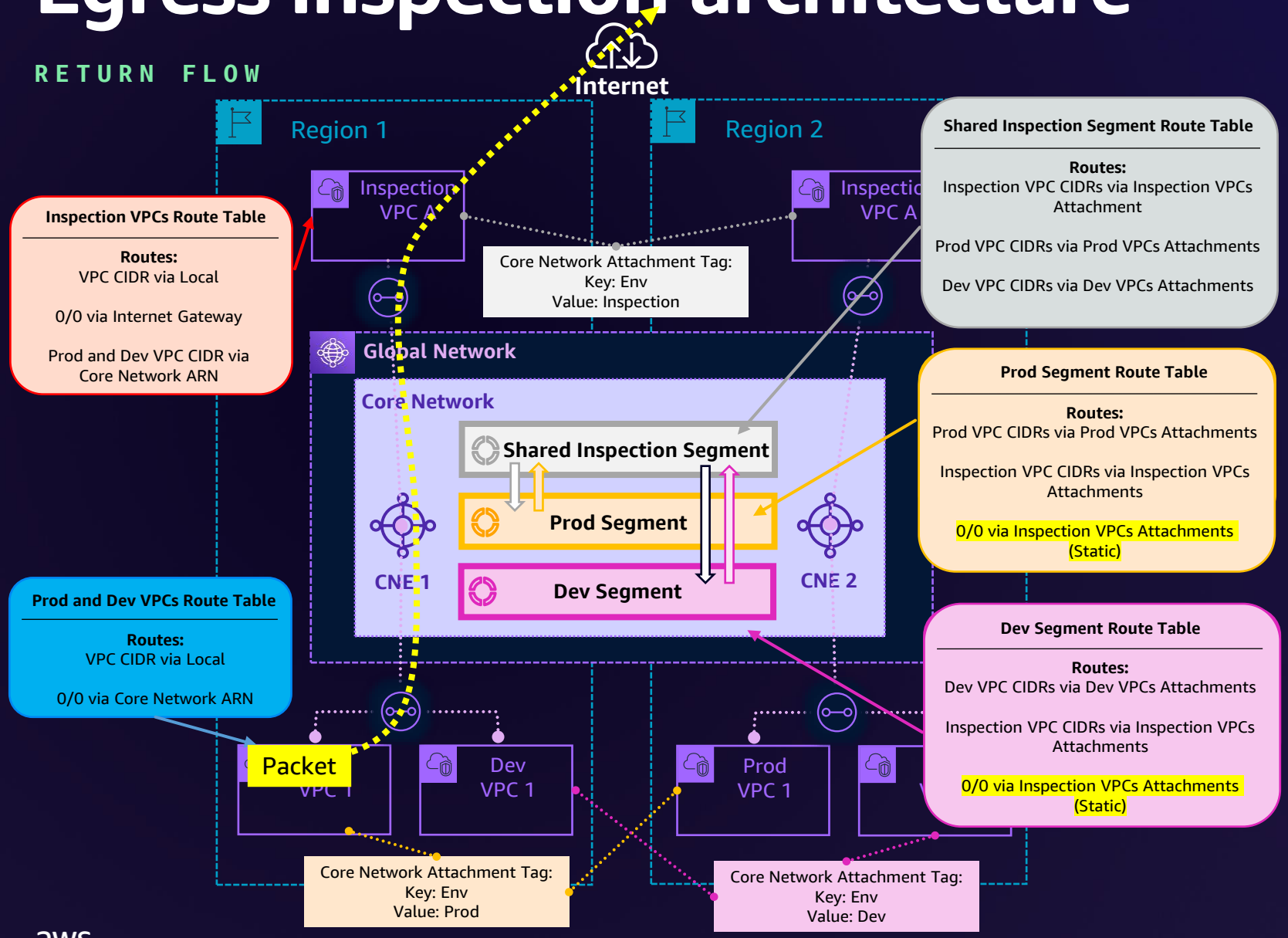
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

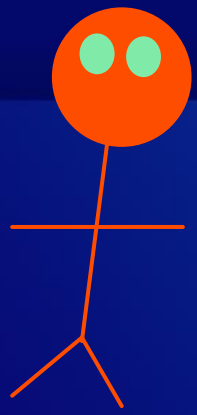
```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```

Egress inspection architecture

RETURN FLOW

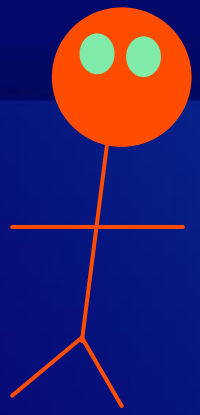



```
"segment-actions": [
    {
        "action": "share",
        "mode": "attachment-route",
        "segment": "Shared Inspection",
        "share-with": "*"
    },
    {
        "action": "create-route",
        "segment": "Prod",
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    },
    {
        "action": "create-route",
        "segment": "Dev"
        "destination-cidr-blocks": [
            "0.0.0.0/0"
        ],
        "destinations": [
            "inspection-vpc-a-attachment-aaaa",
            "inspection-vpc-b-attachment-bbbb "
        ]
    }
]
```



Happy Alice

A story of meeting needs



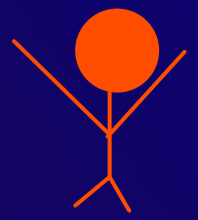
Happy Alice

A story of meeting needs

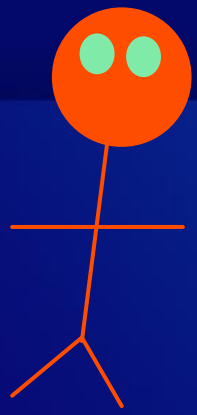
People got what they wanted

Happy Alice

A story of meeting needs

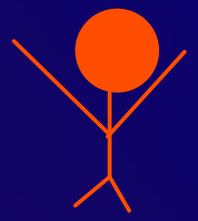


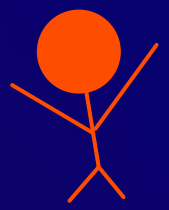
People got what they wanted



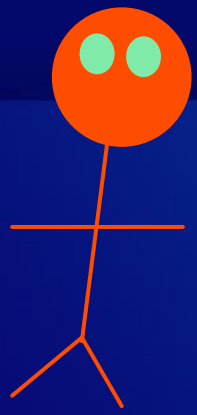
Happy Alice

A story of meeting needs



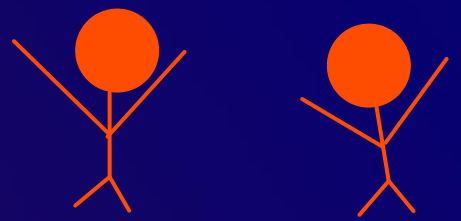


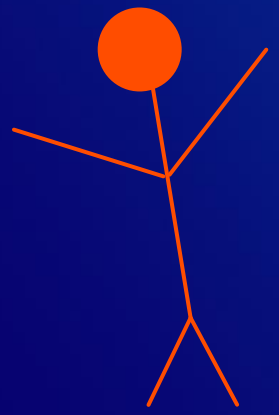
People got what they wanted



Happy Alice

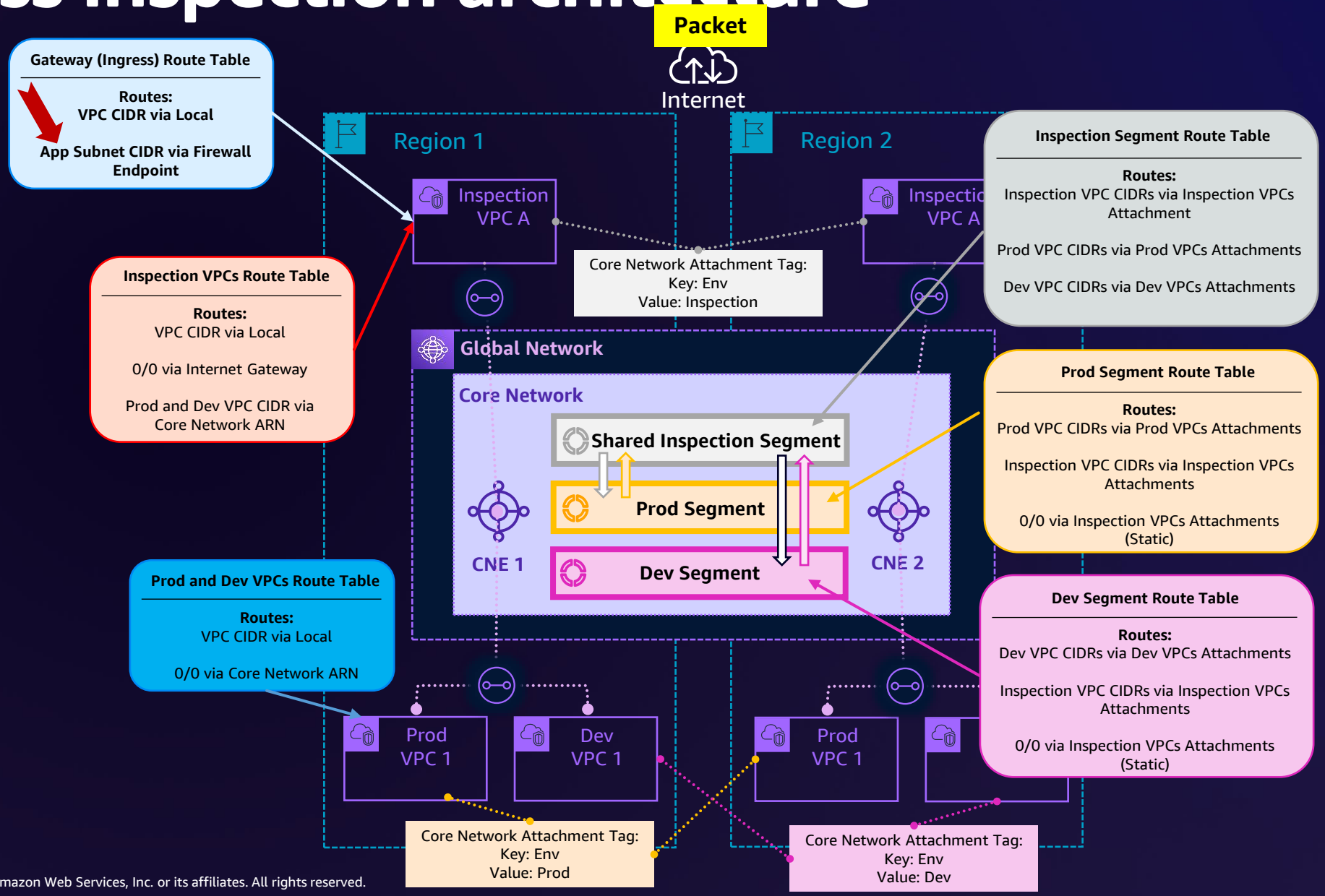
A story of meeting needs



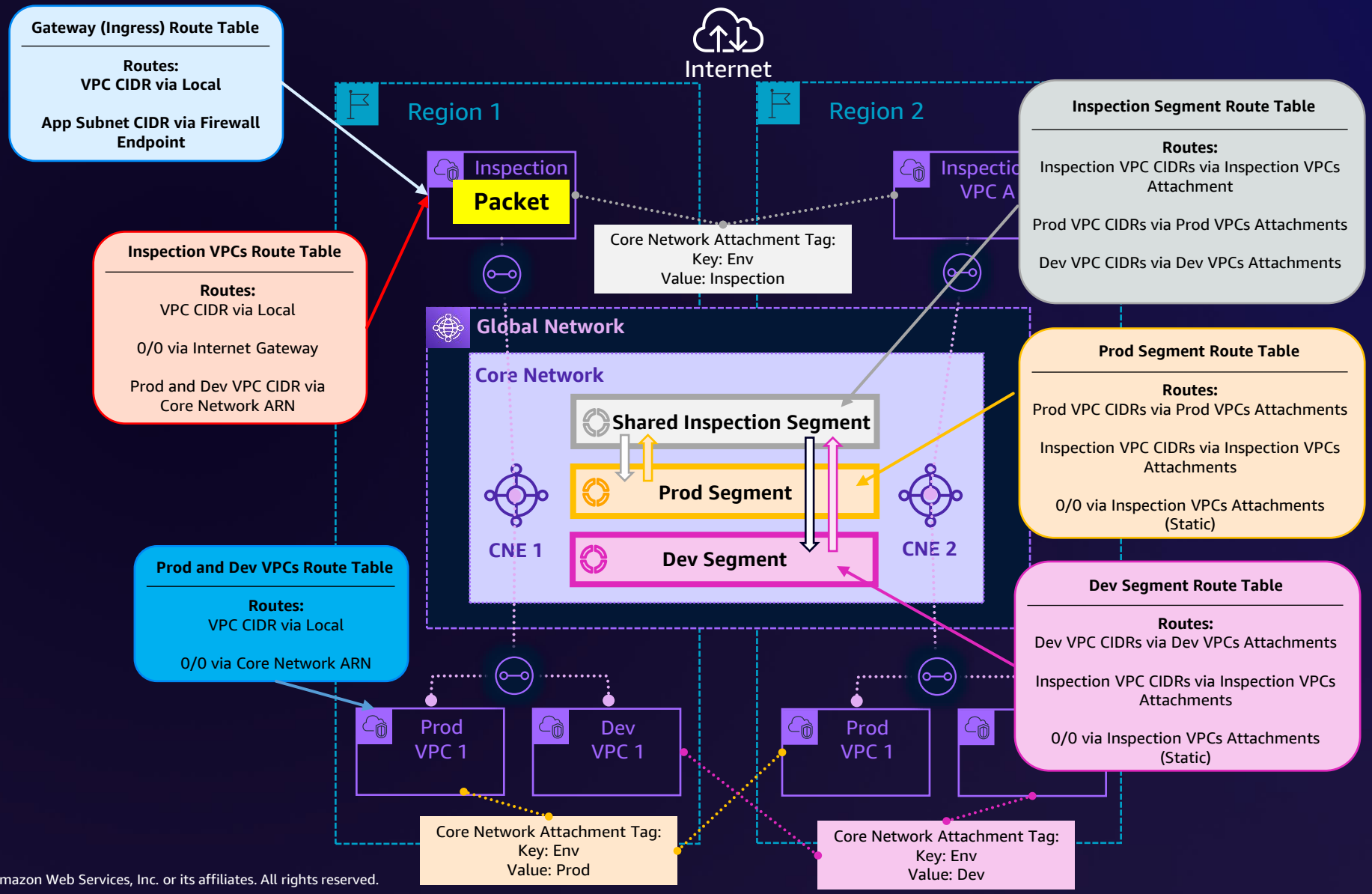


People got what they wanted

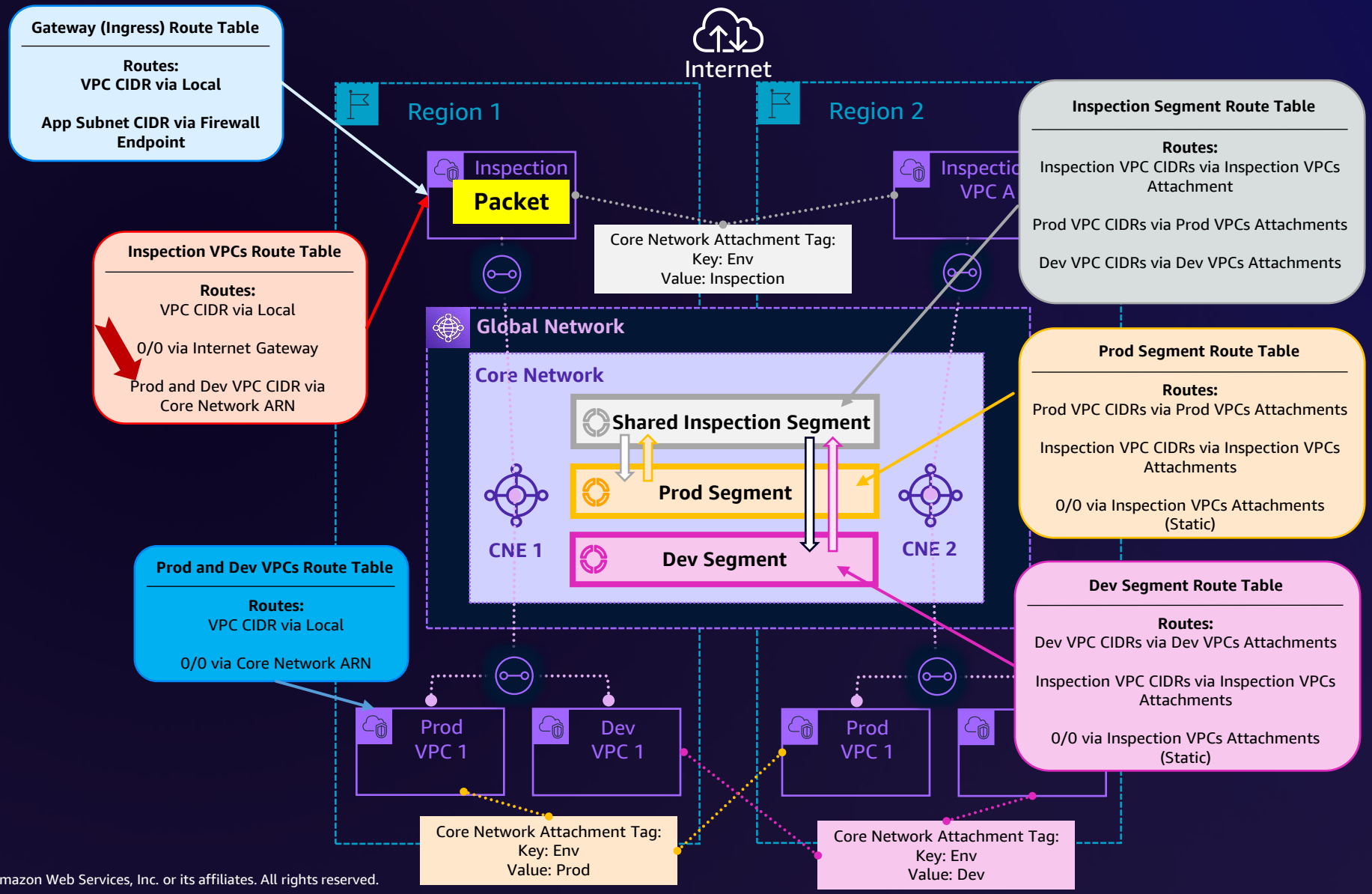
Ingress inspection architecture



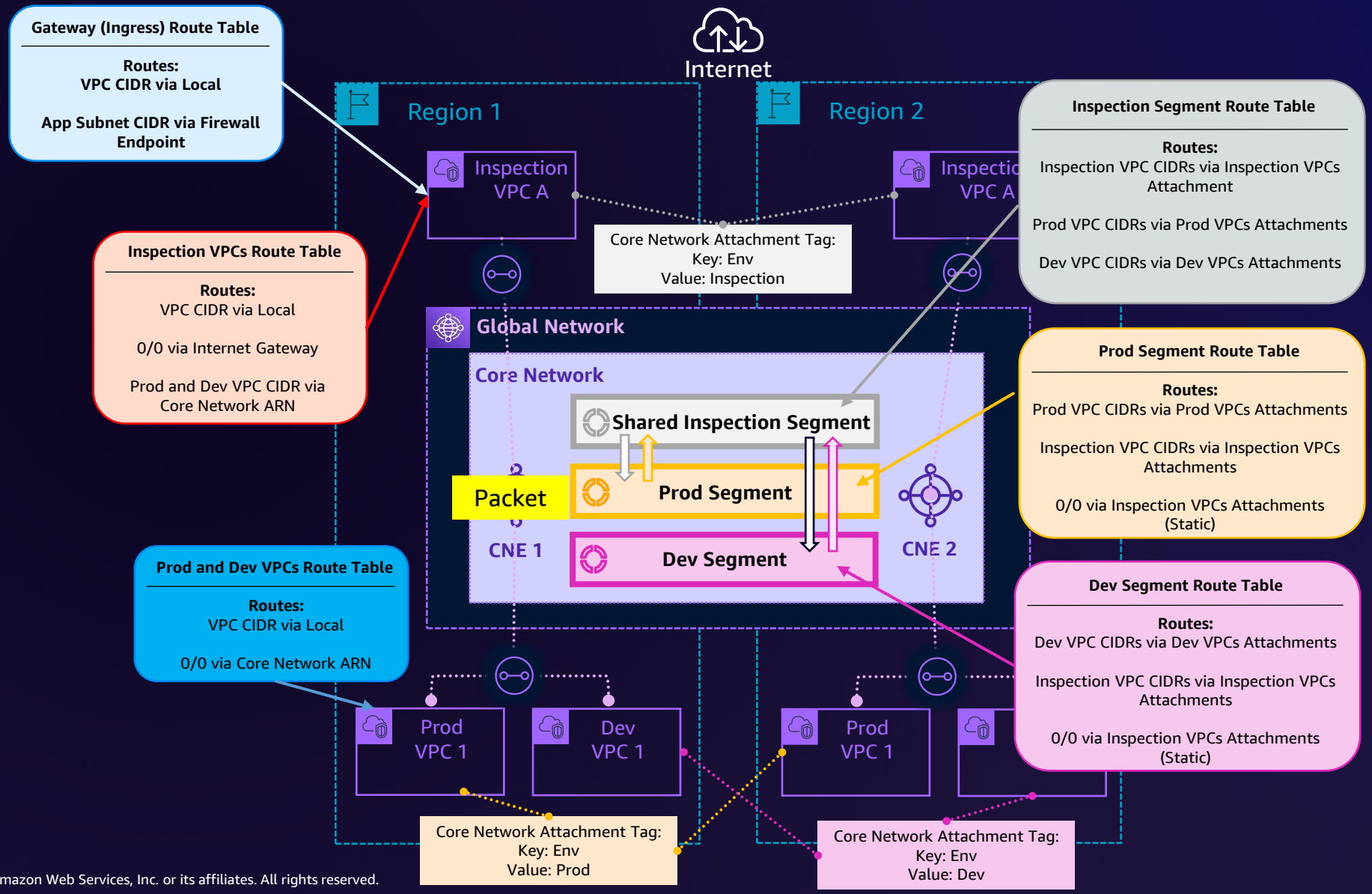
Ingress inspection architecture



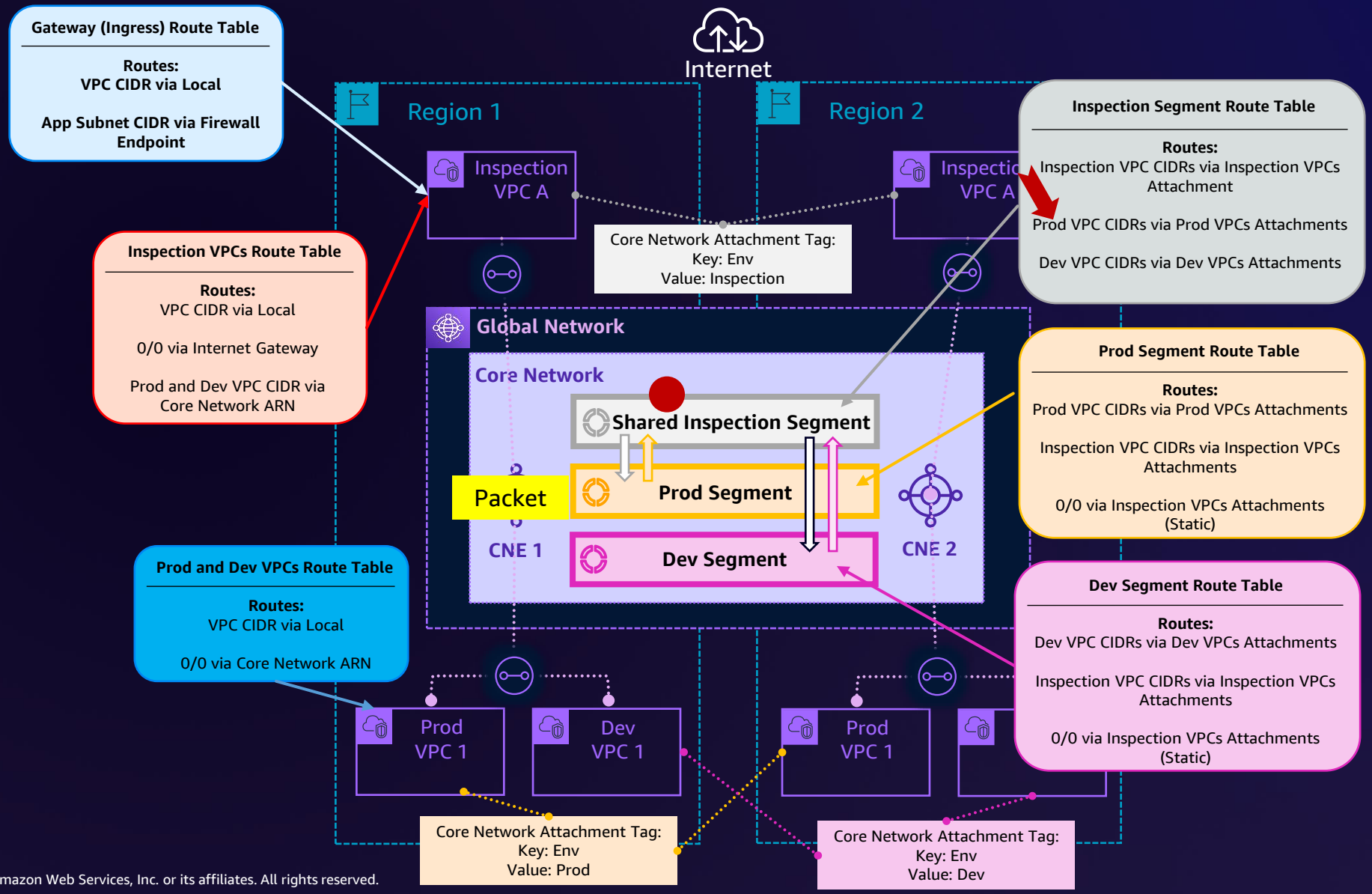
Ingress inspection architecture



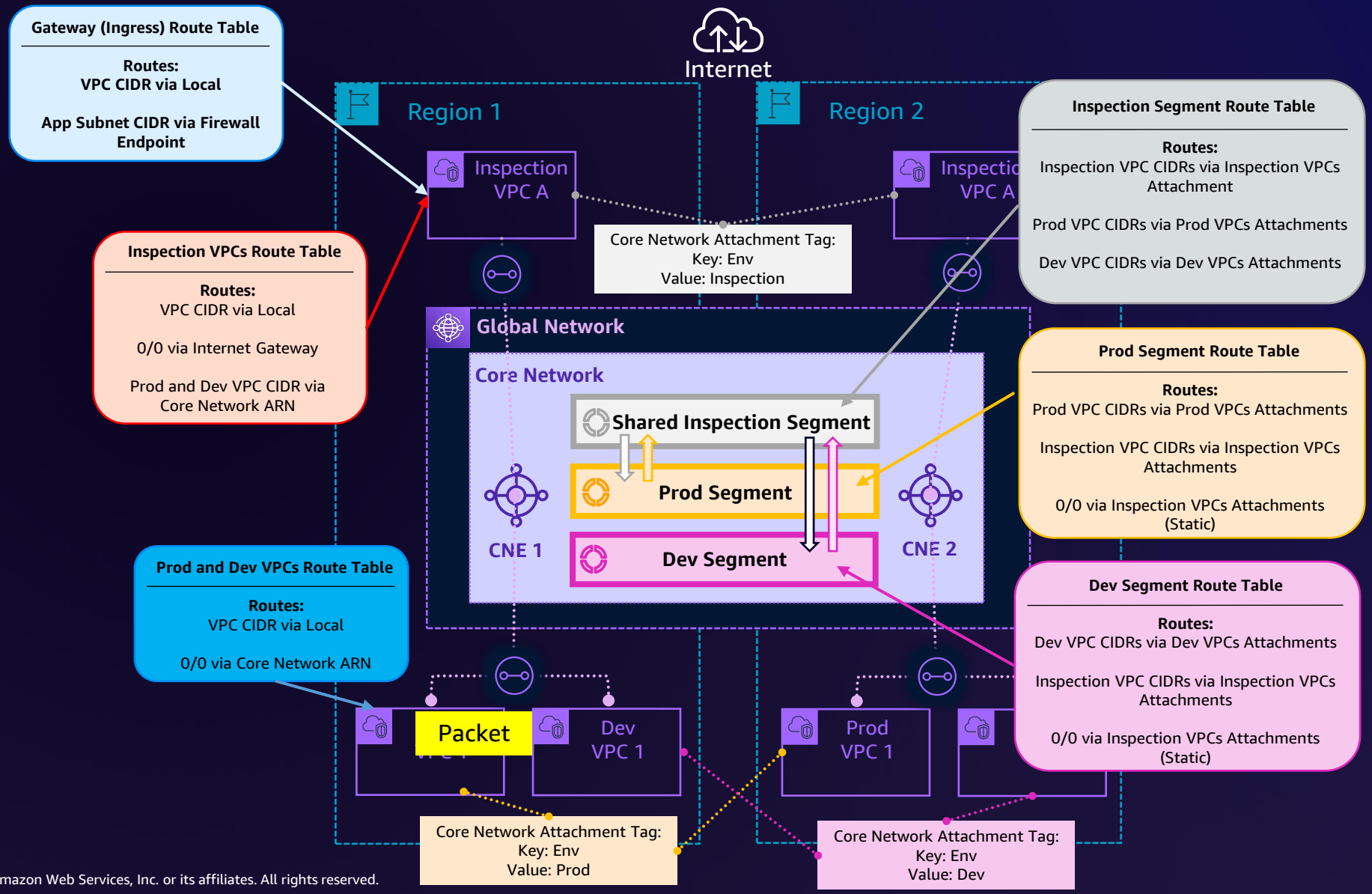
Ingress inspection architecture



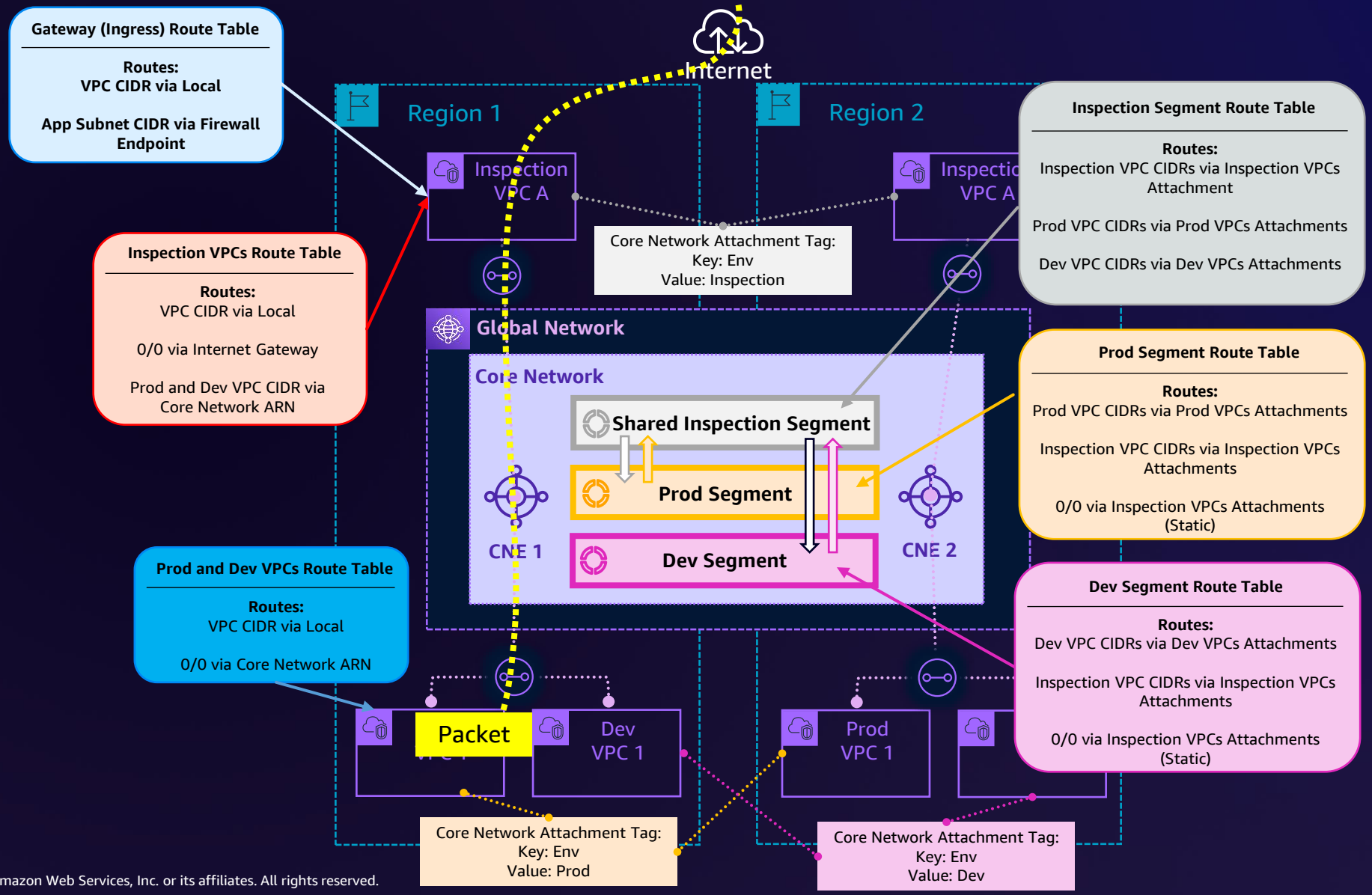
Ingress inspection architecture



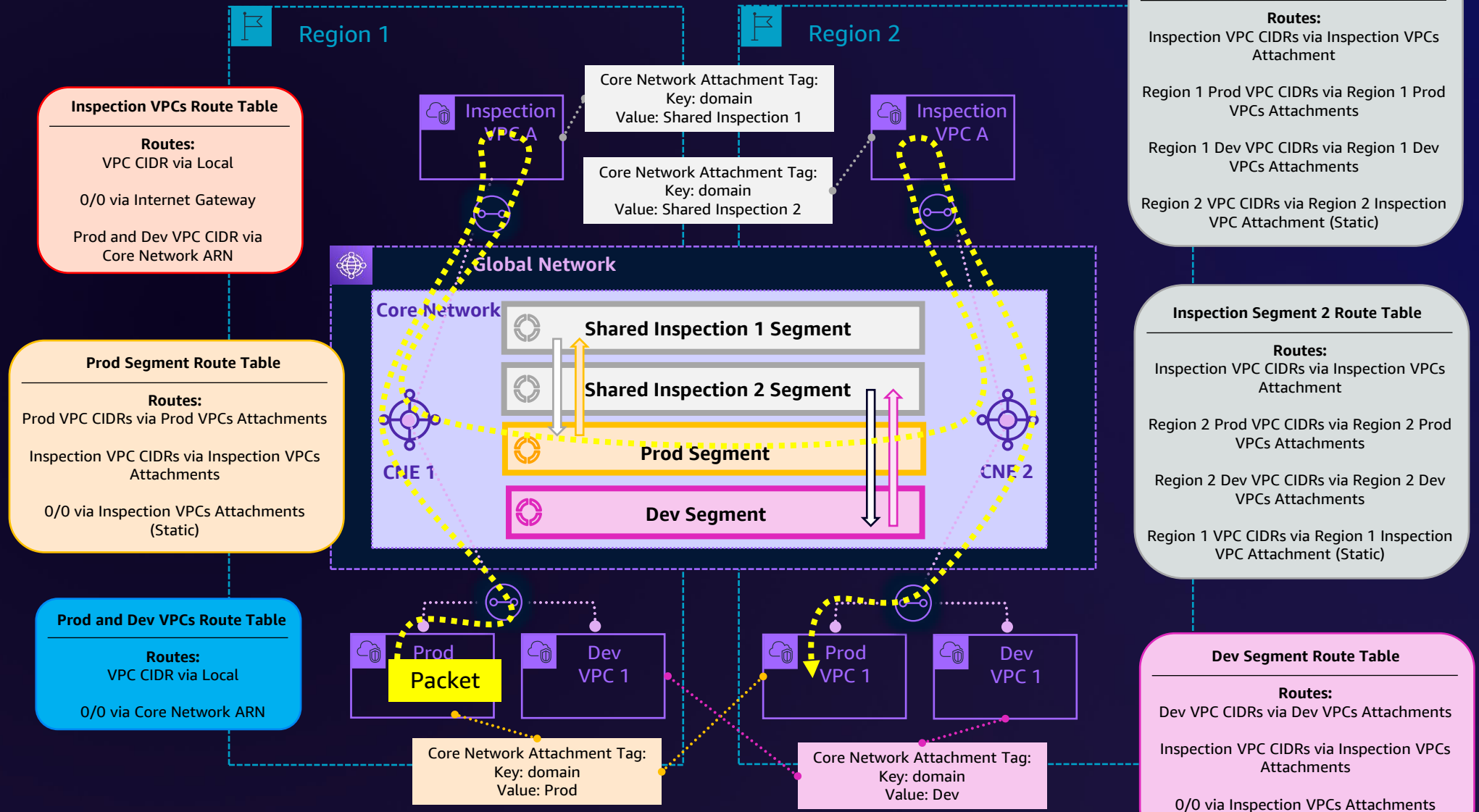
Ingress inspection architecture



Ingress inspection architecture



VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

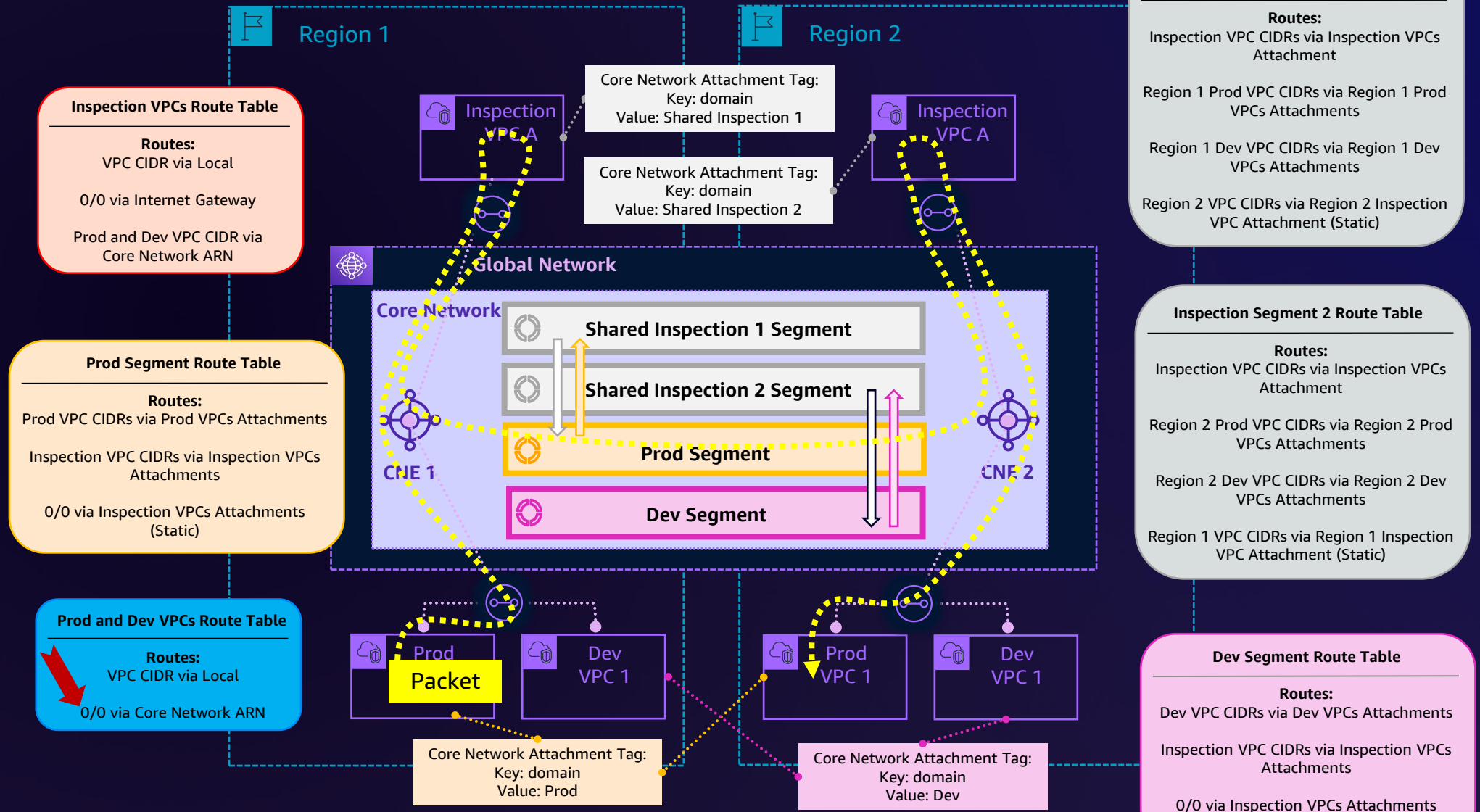
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

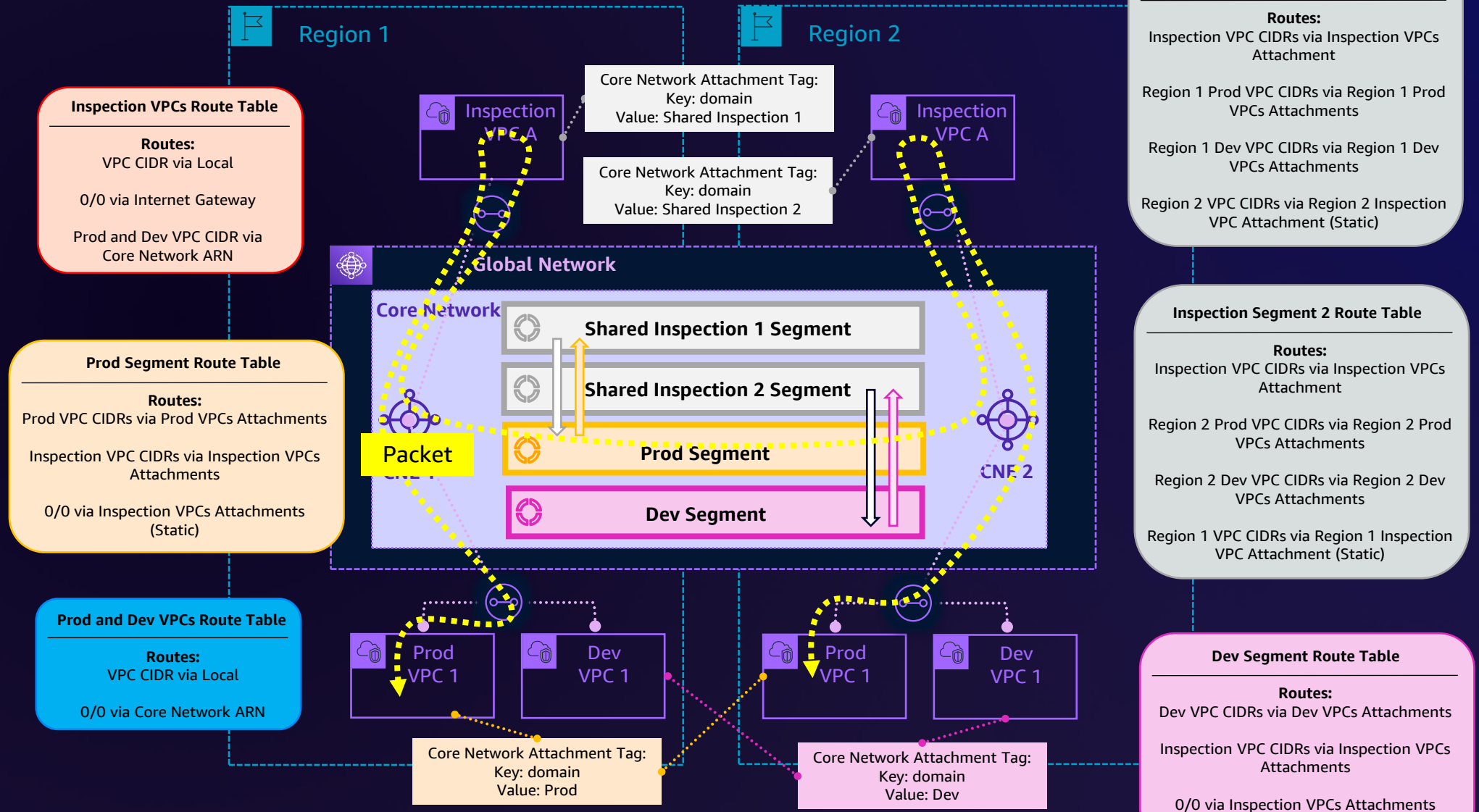
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

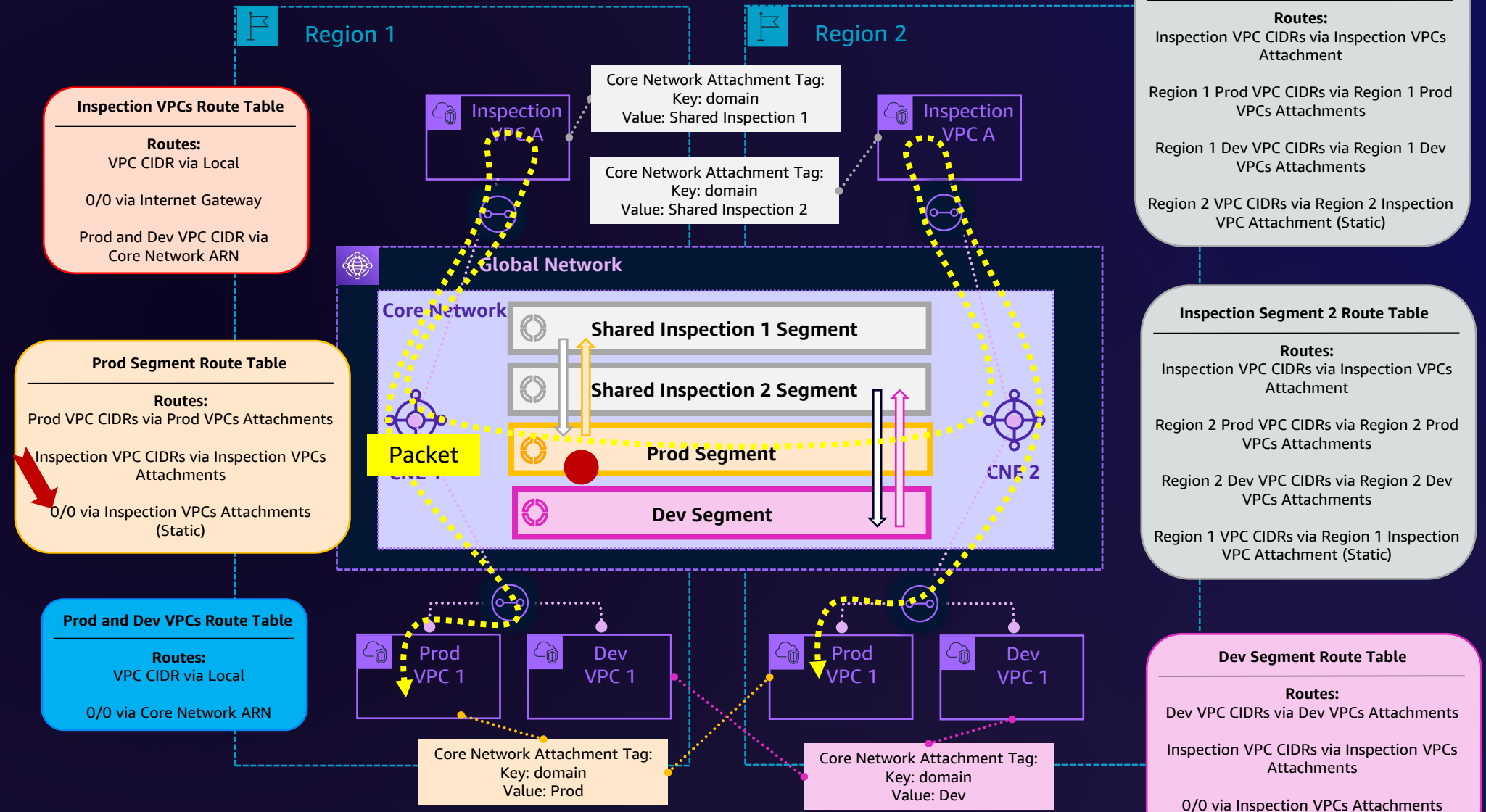
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

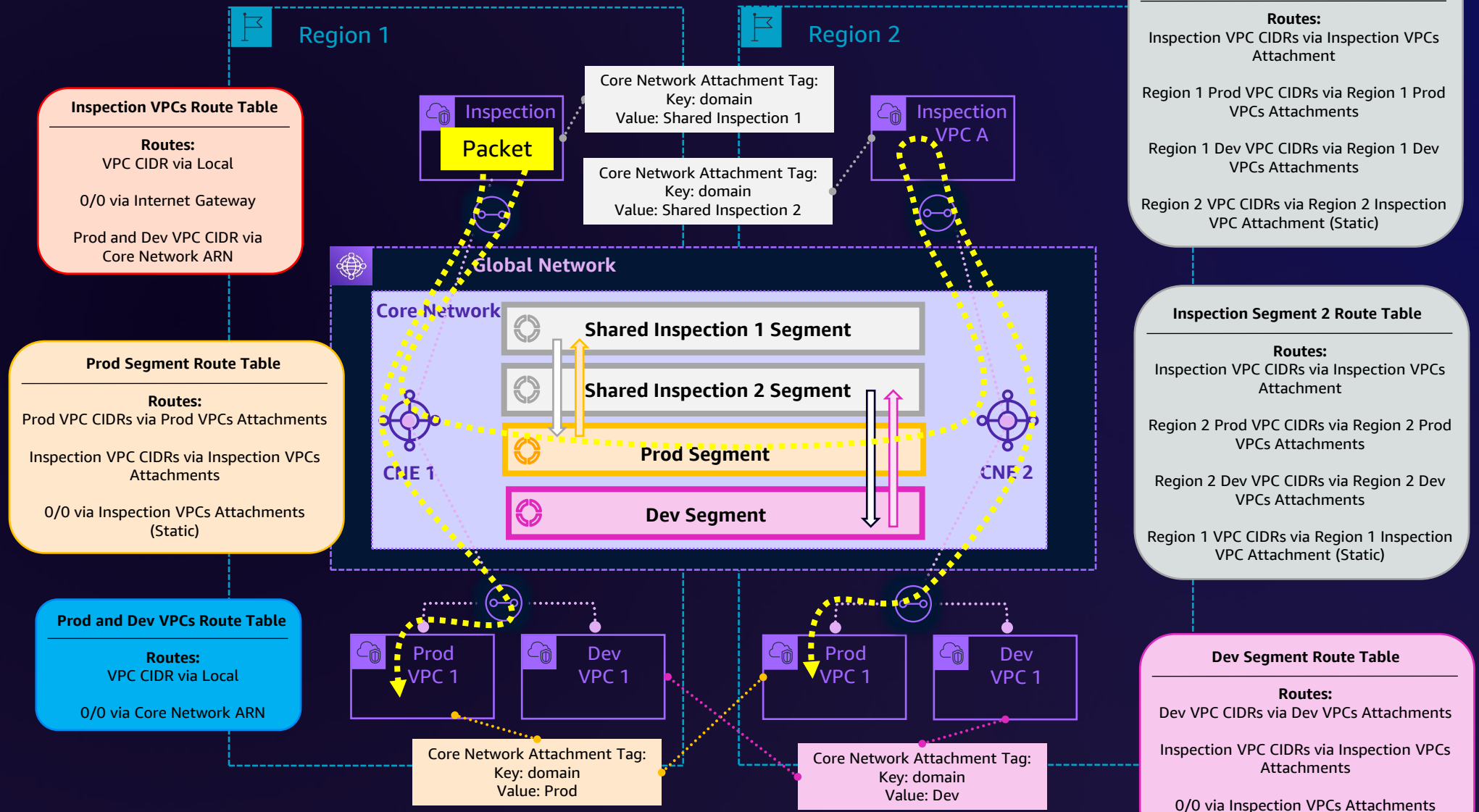
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

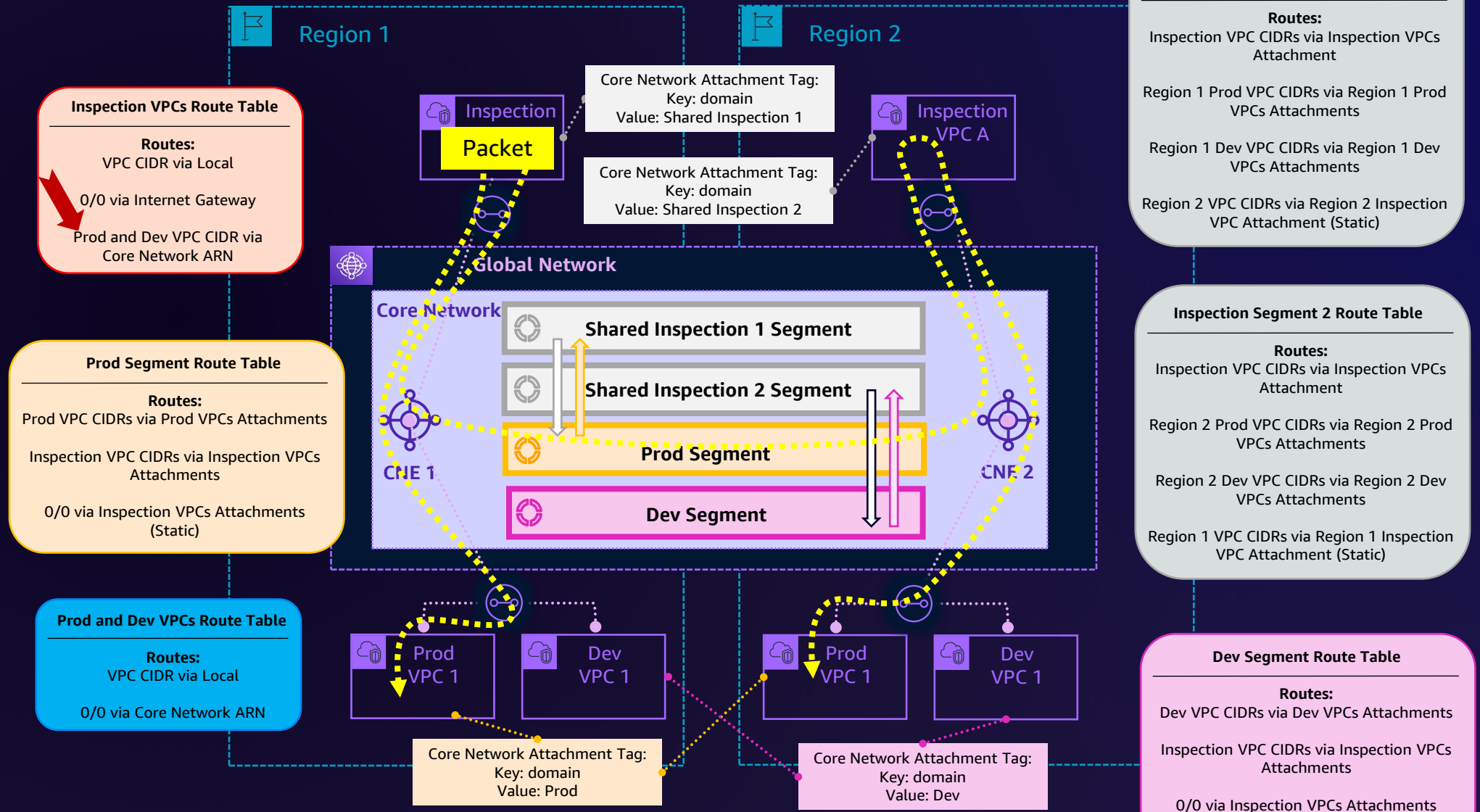
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

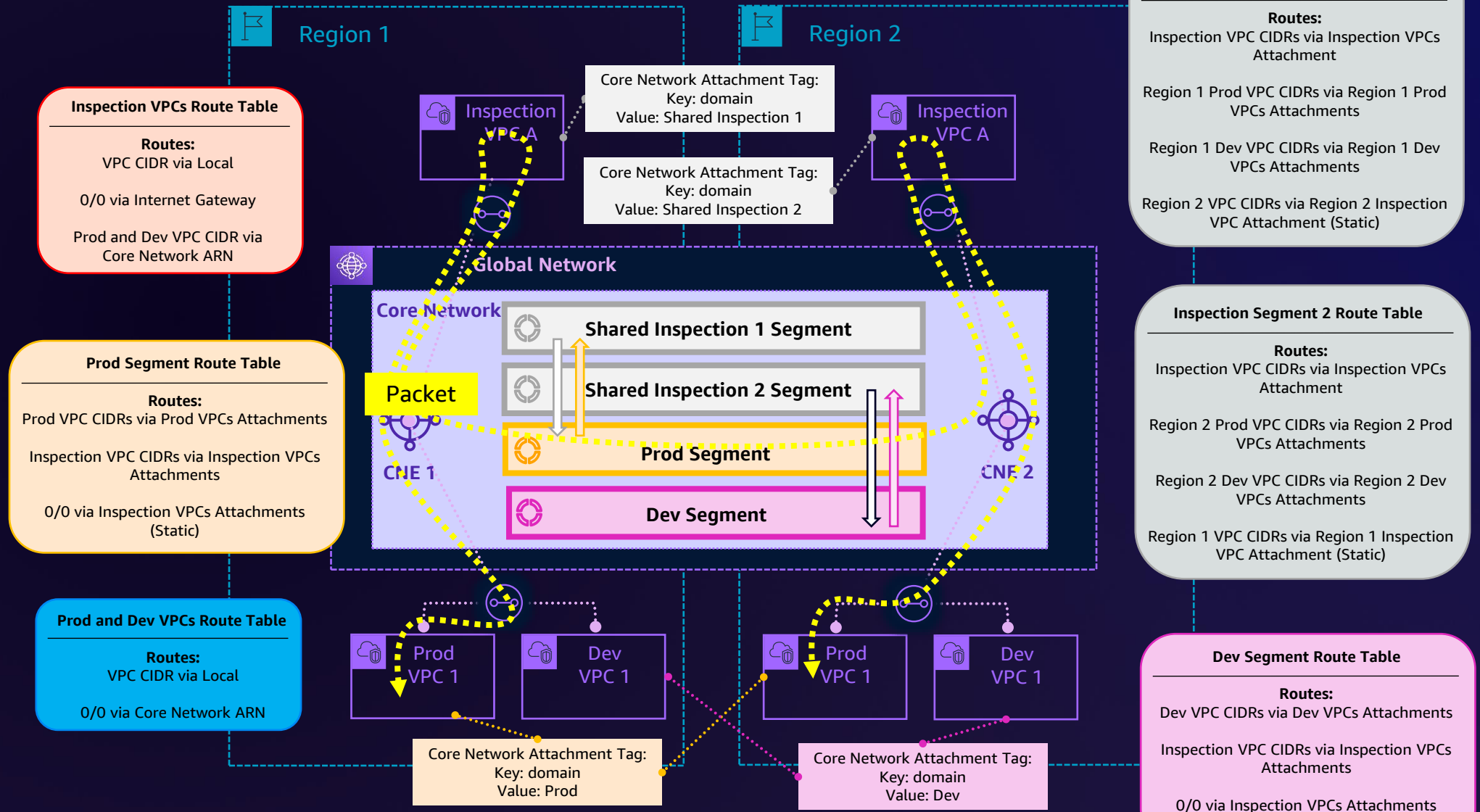
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

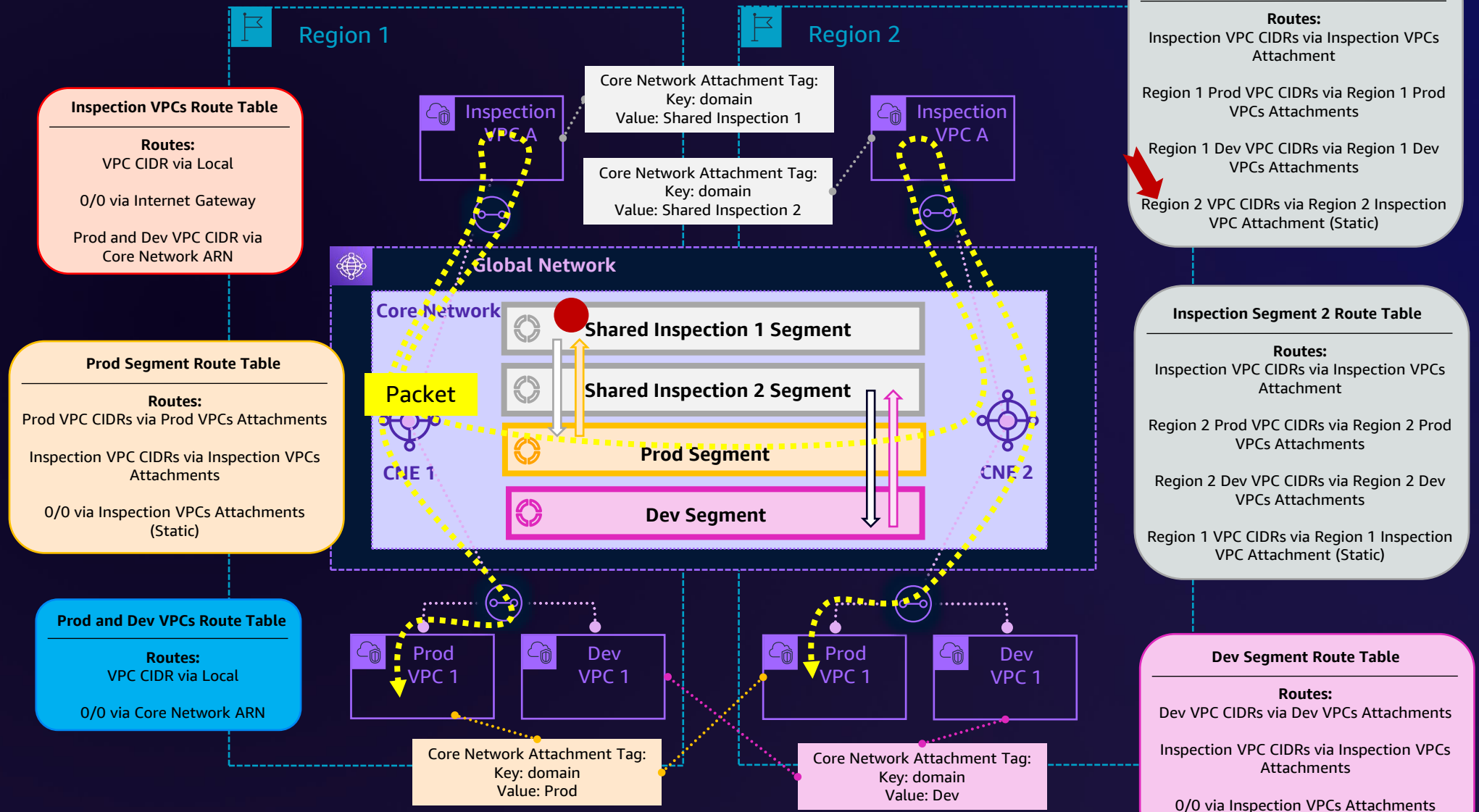
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

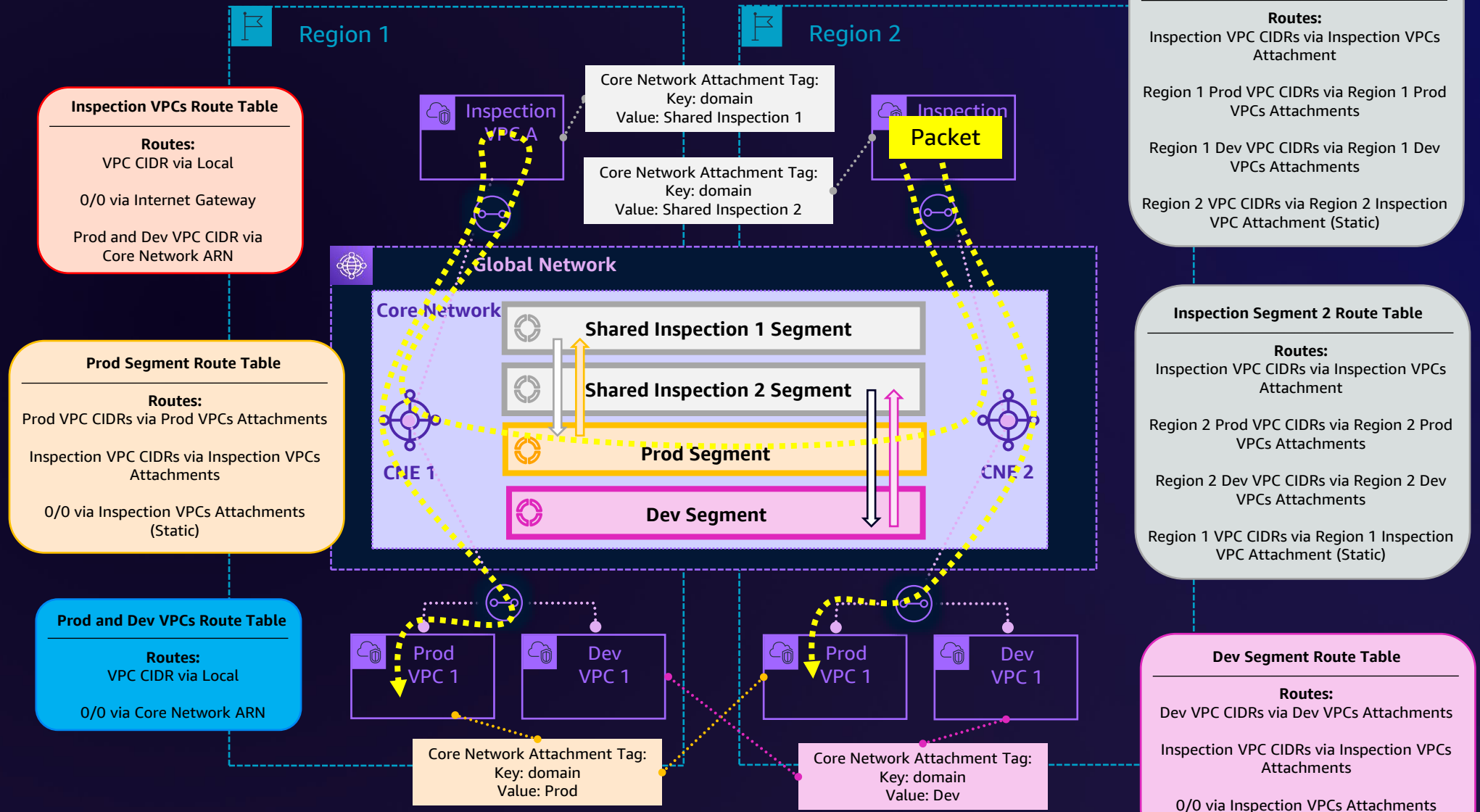
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

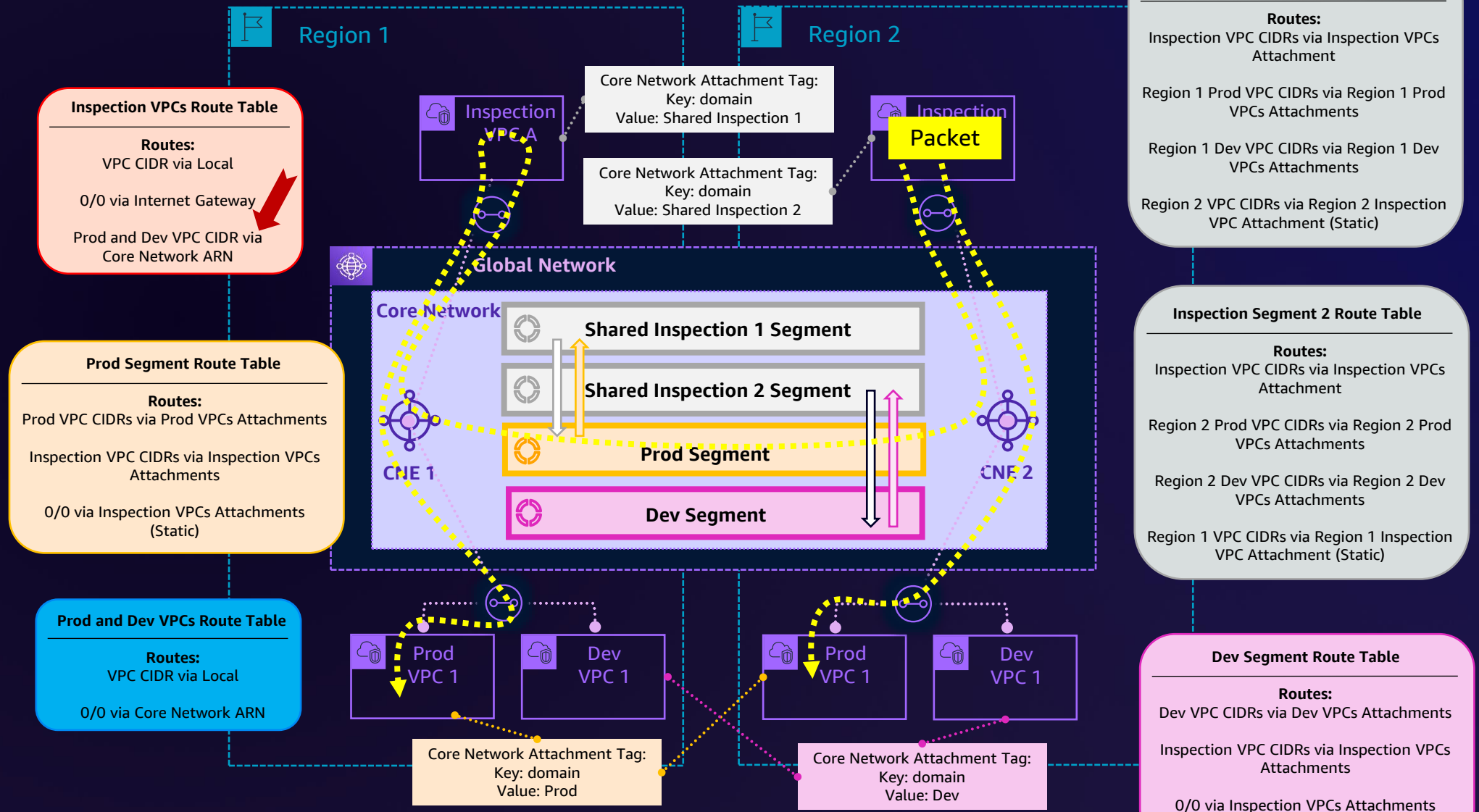
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

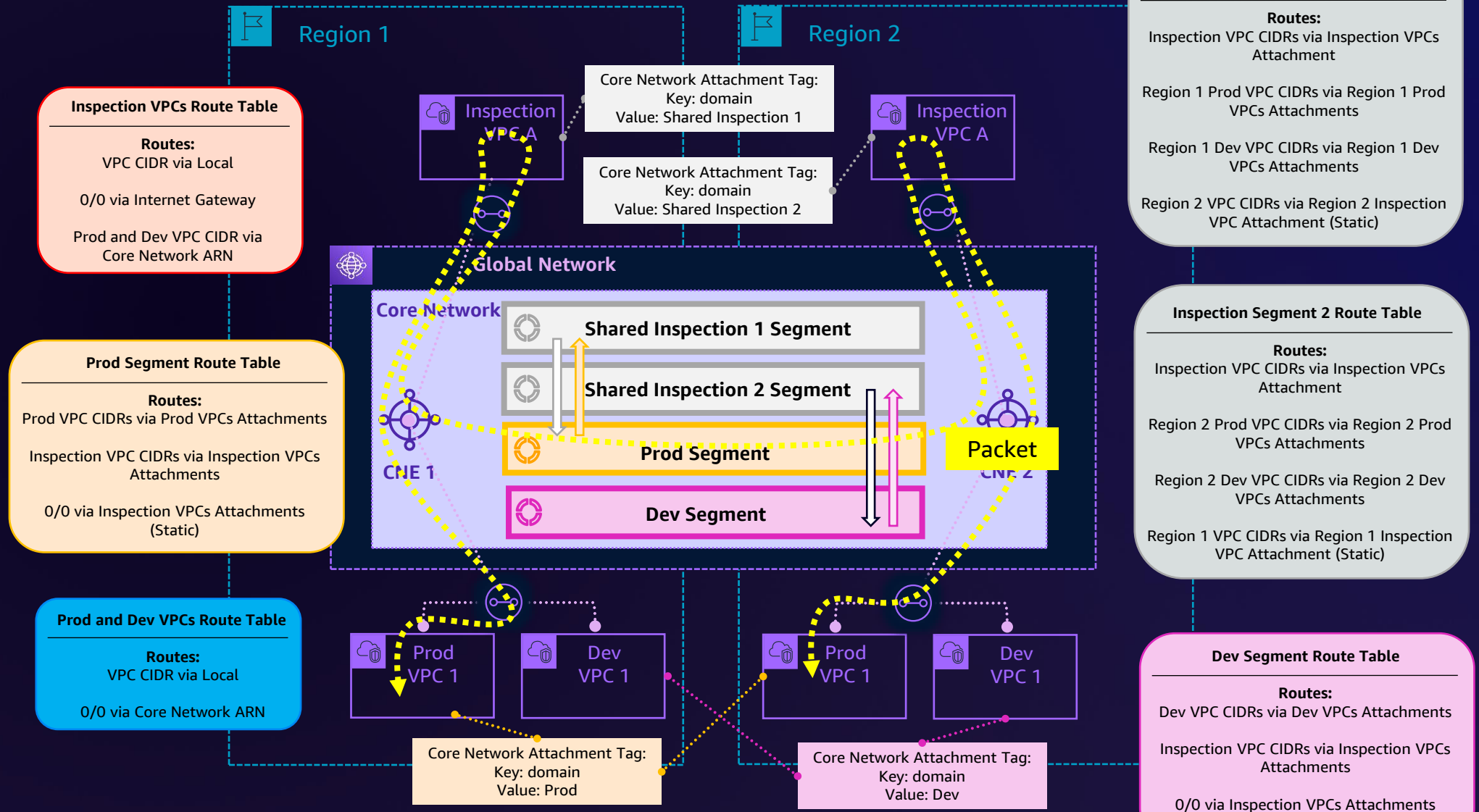
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

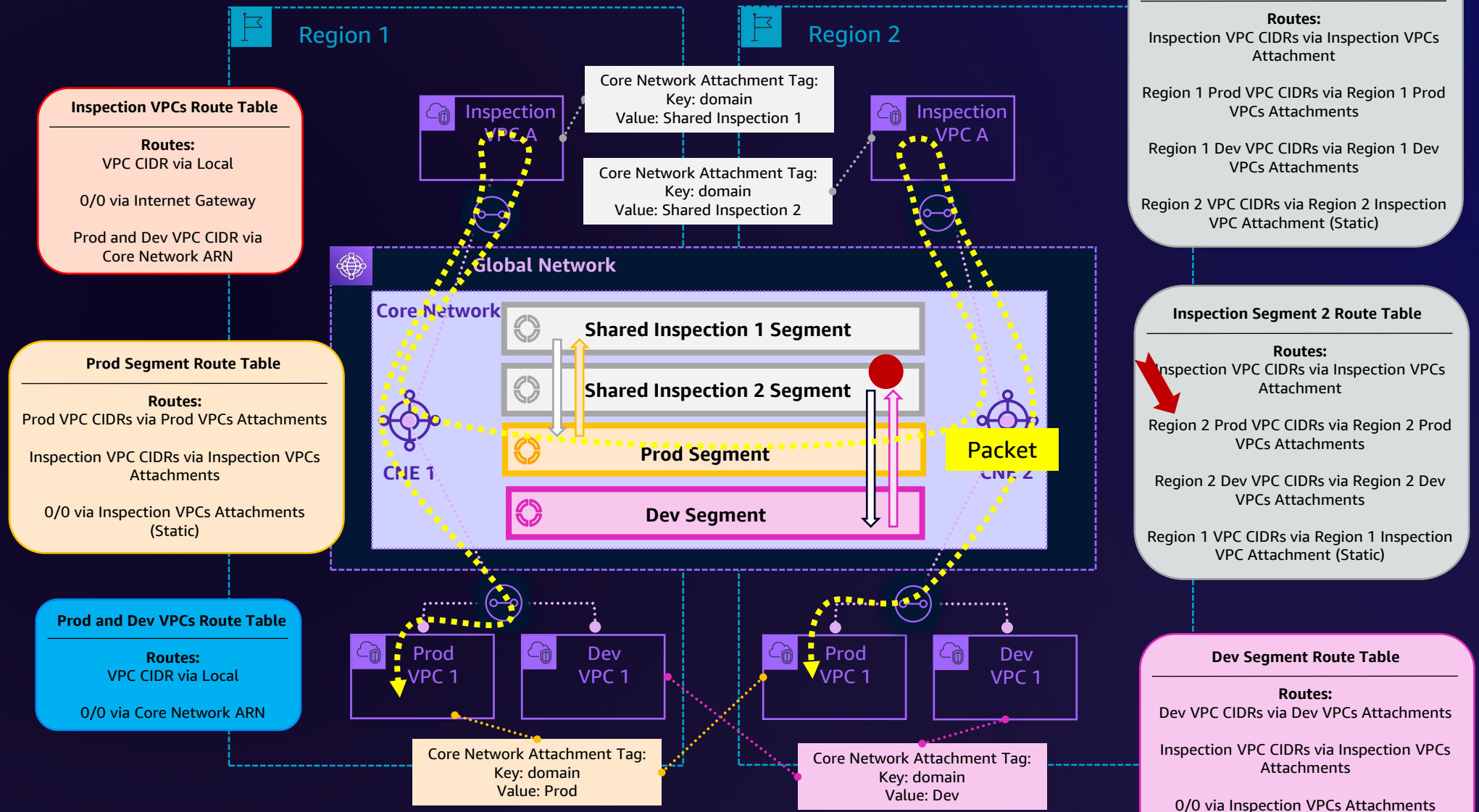
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

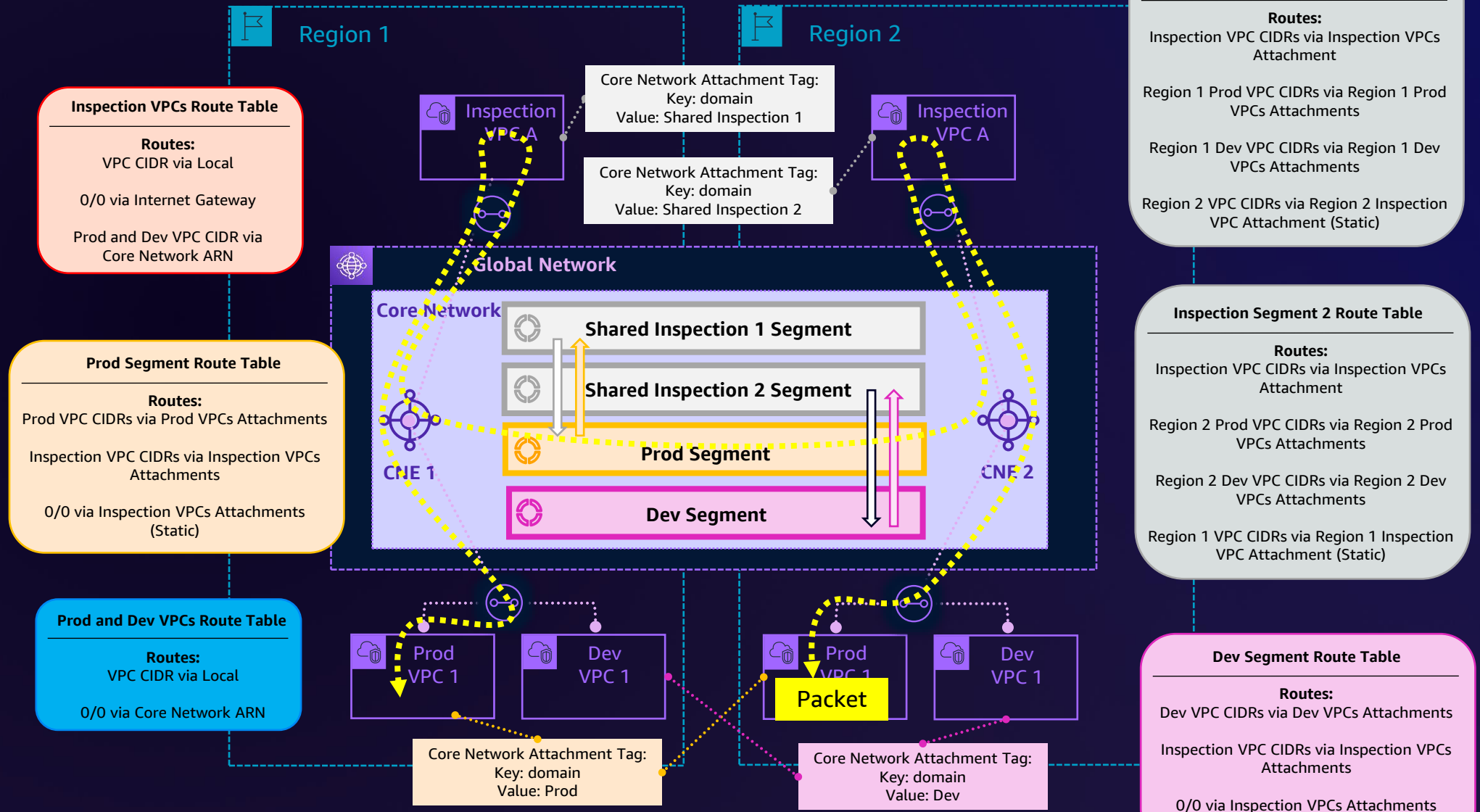
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-VPC inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Inspection Segment 1 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 1 Prod VPC CIDRs via Region 1 Prod VPCs Attachments

Region 1 Dev VPC CIDRs via Region 1 Dev VPCs Attachments

Region 2 VPC CIDRs via Region 2 Inspection VPC Attachment (Static)

Inspection Segment 2 Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Region 2 Prod VPC CIDRs via Region 2 Prod VPCs Attachments

Region 2 Dev VPC CIDRs via Region 2 Dev VPCs Attachments

Region 1 VPC CIDRs via Region 1 Inspection VPC Attachment (Static)

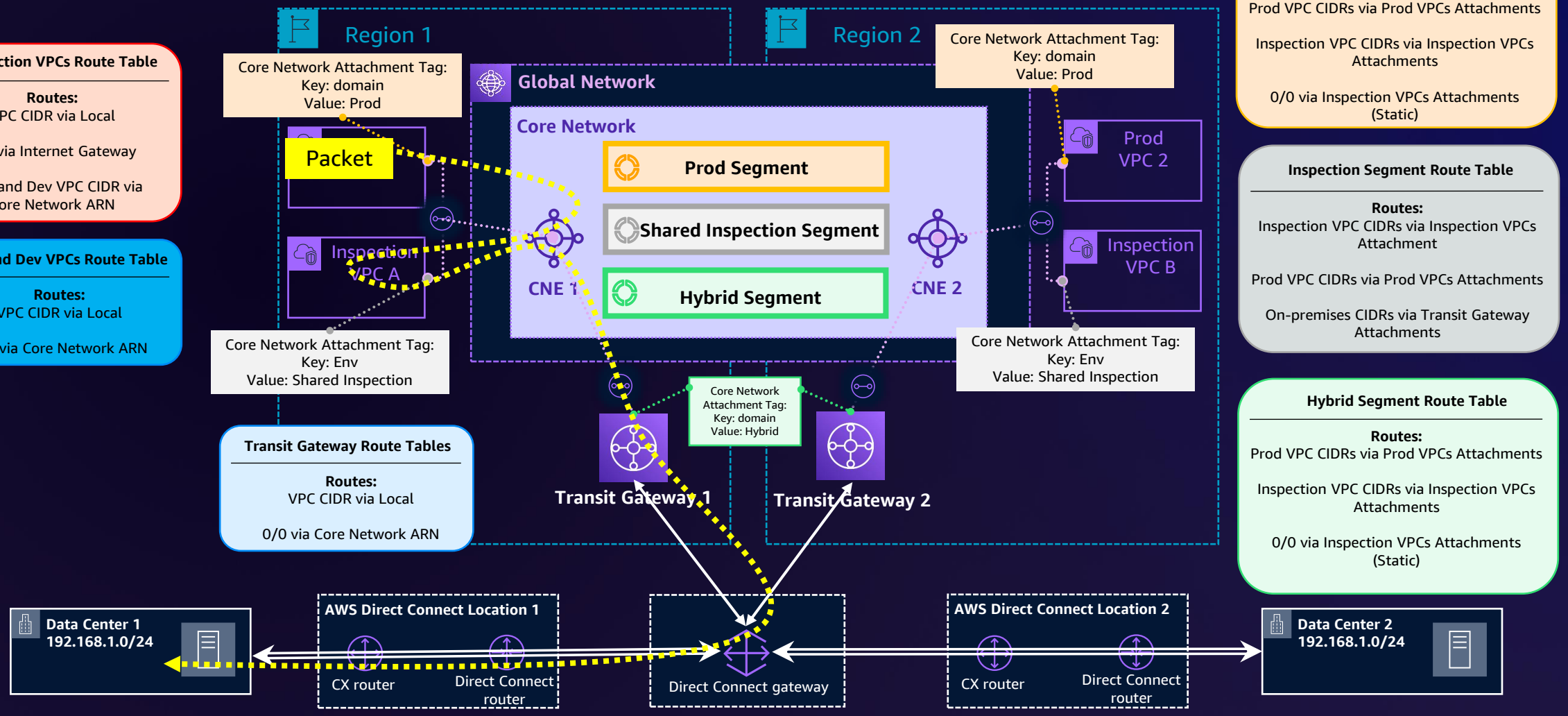
Dev Segment Route Table

Routes:
Dev VPC CIDRs via Dev VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

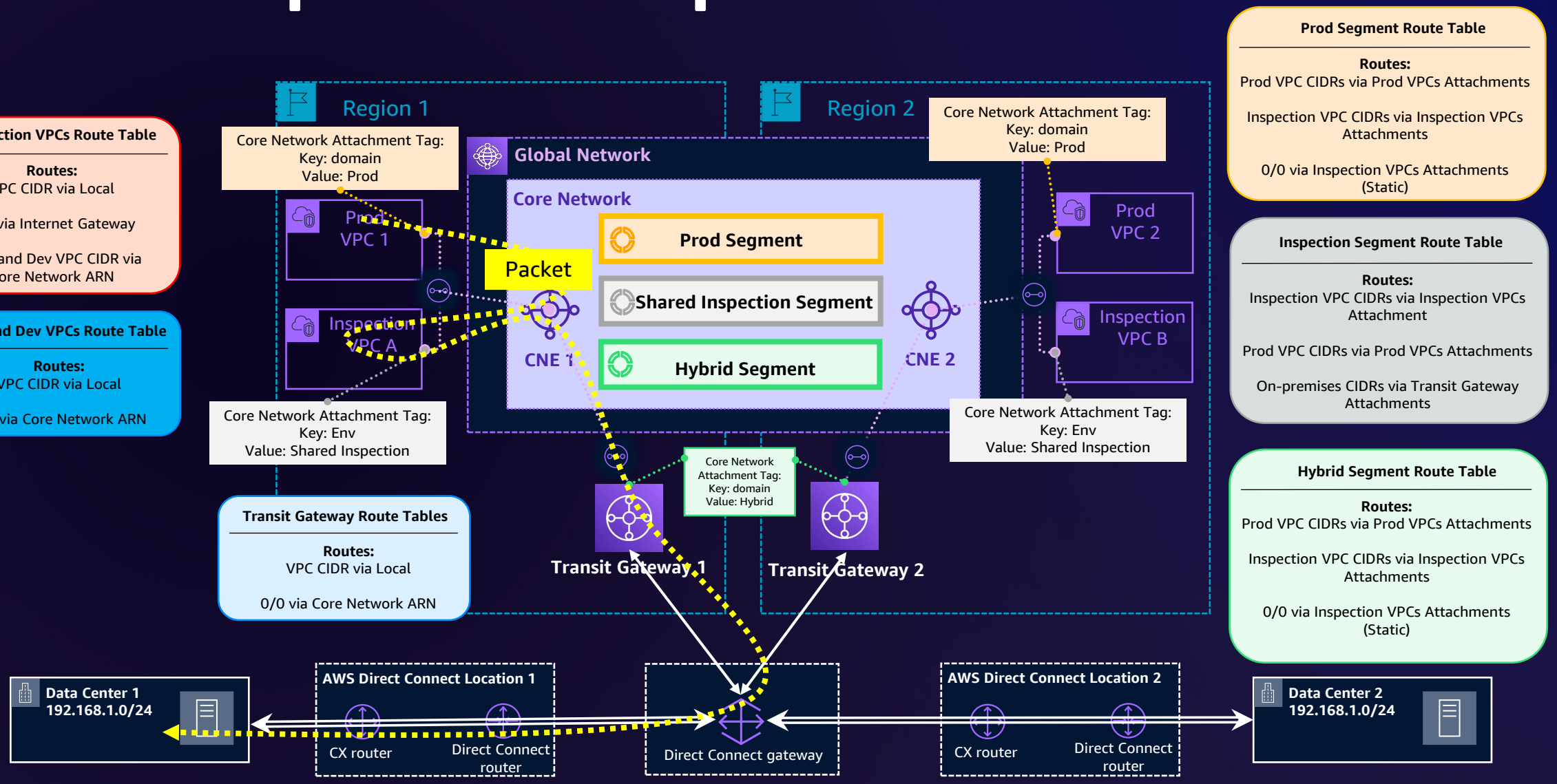
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

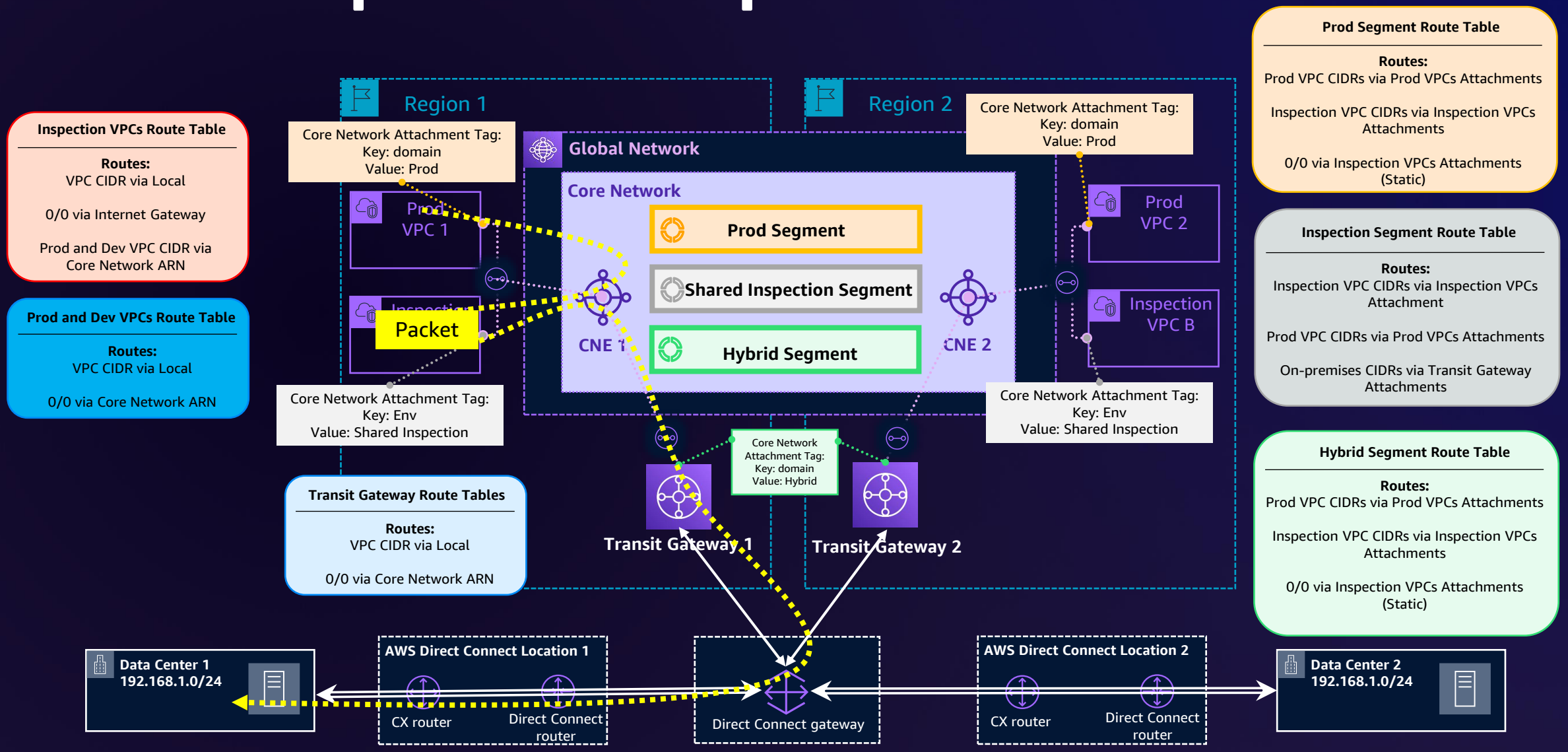
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

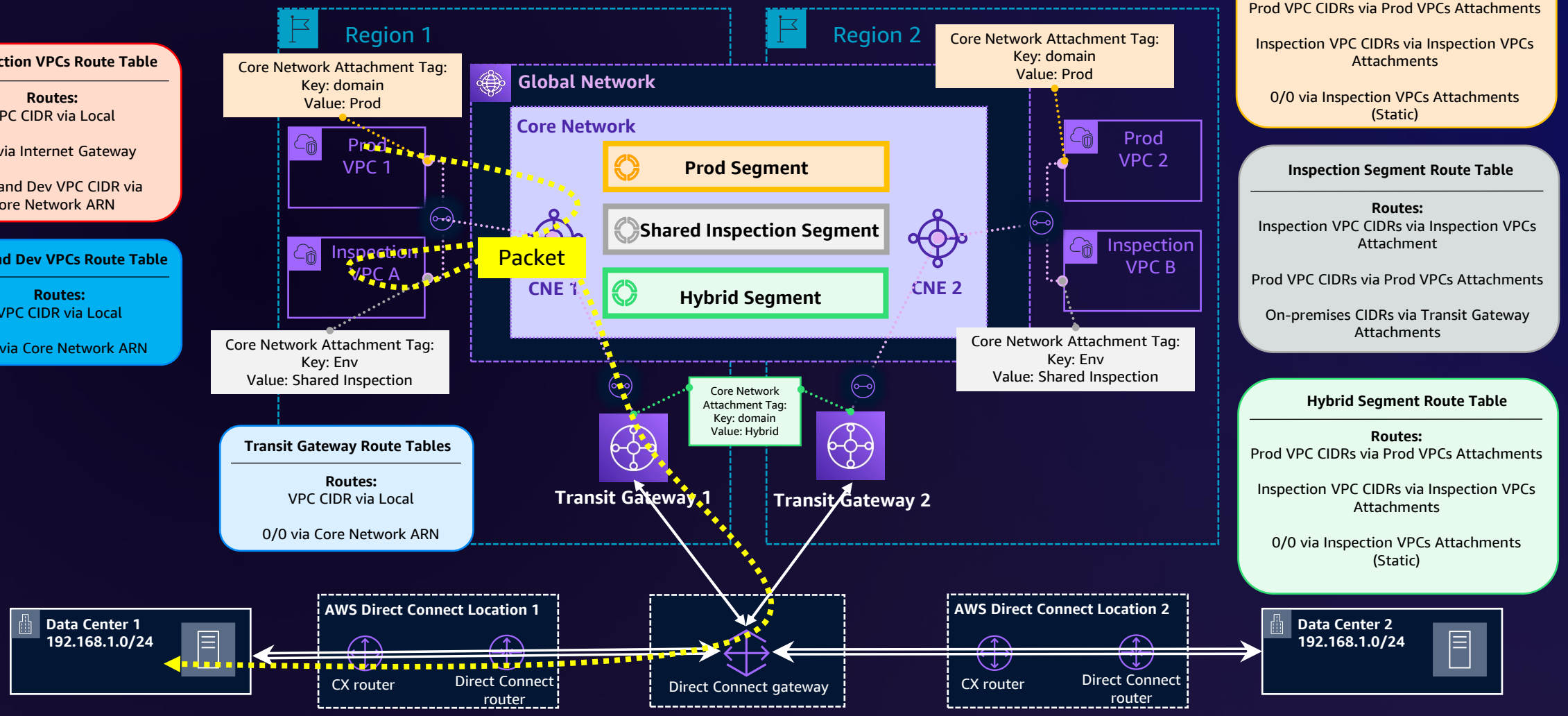
Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

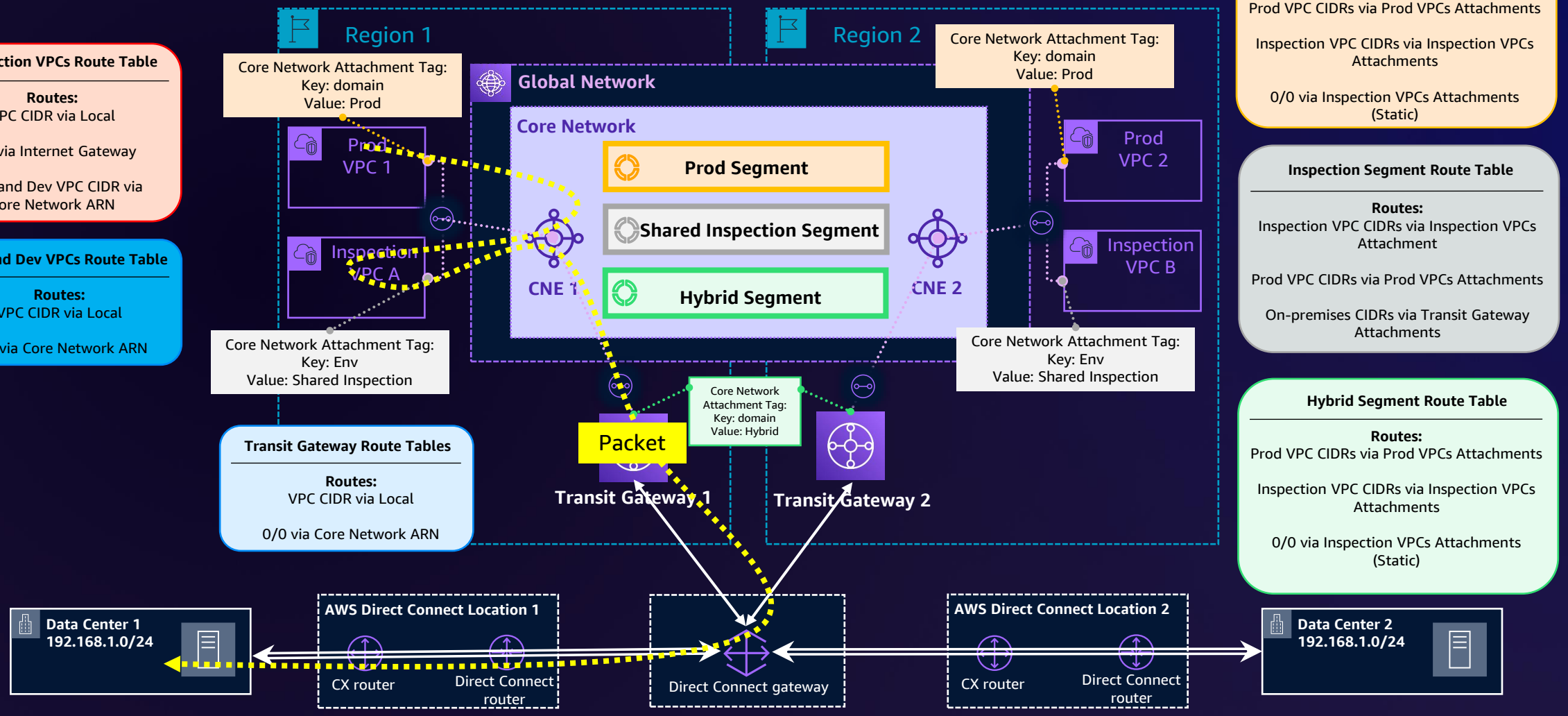
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

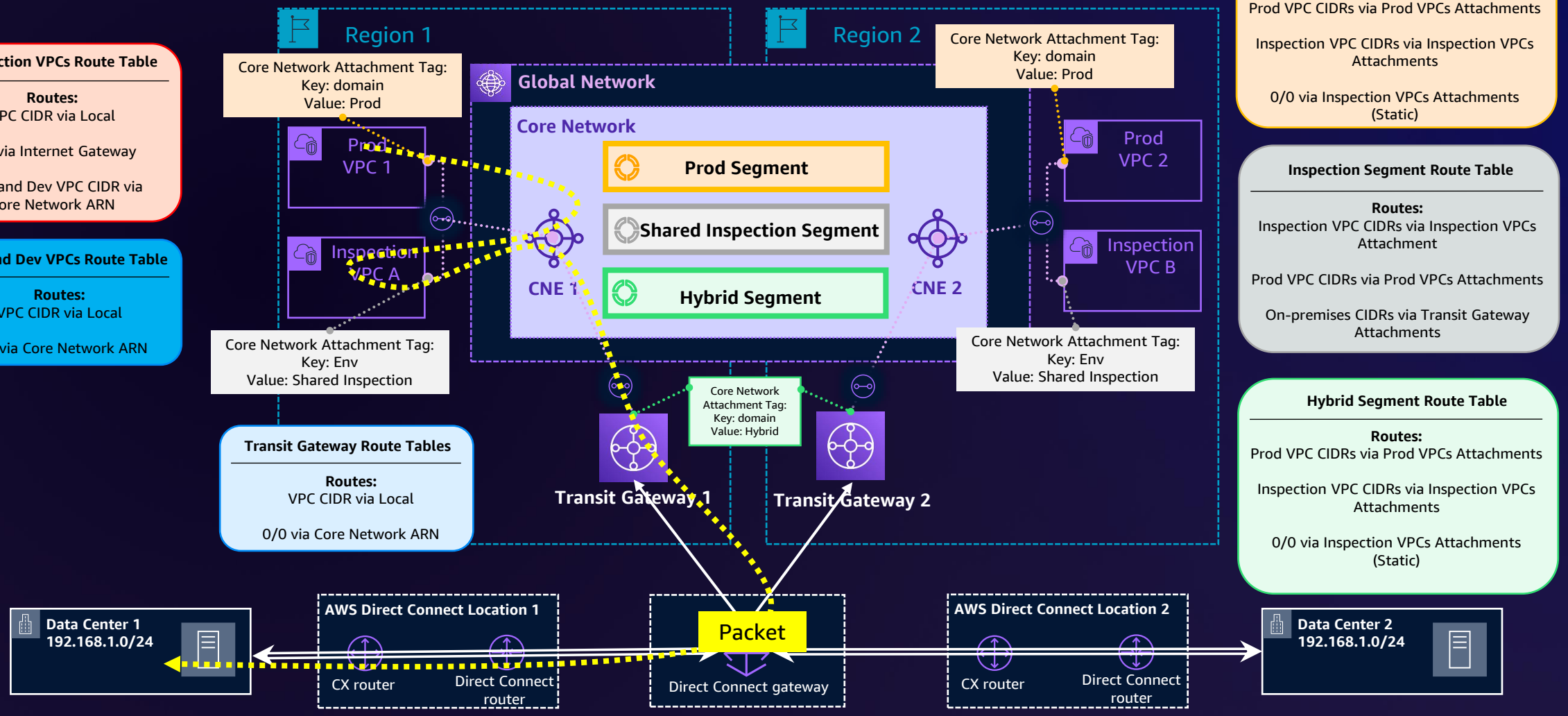
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

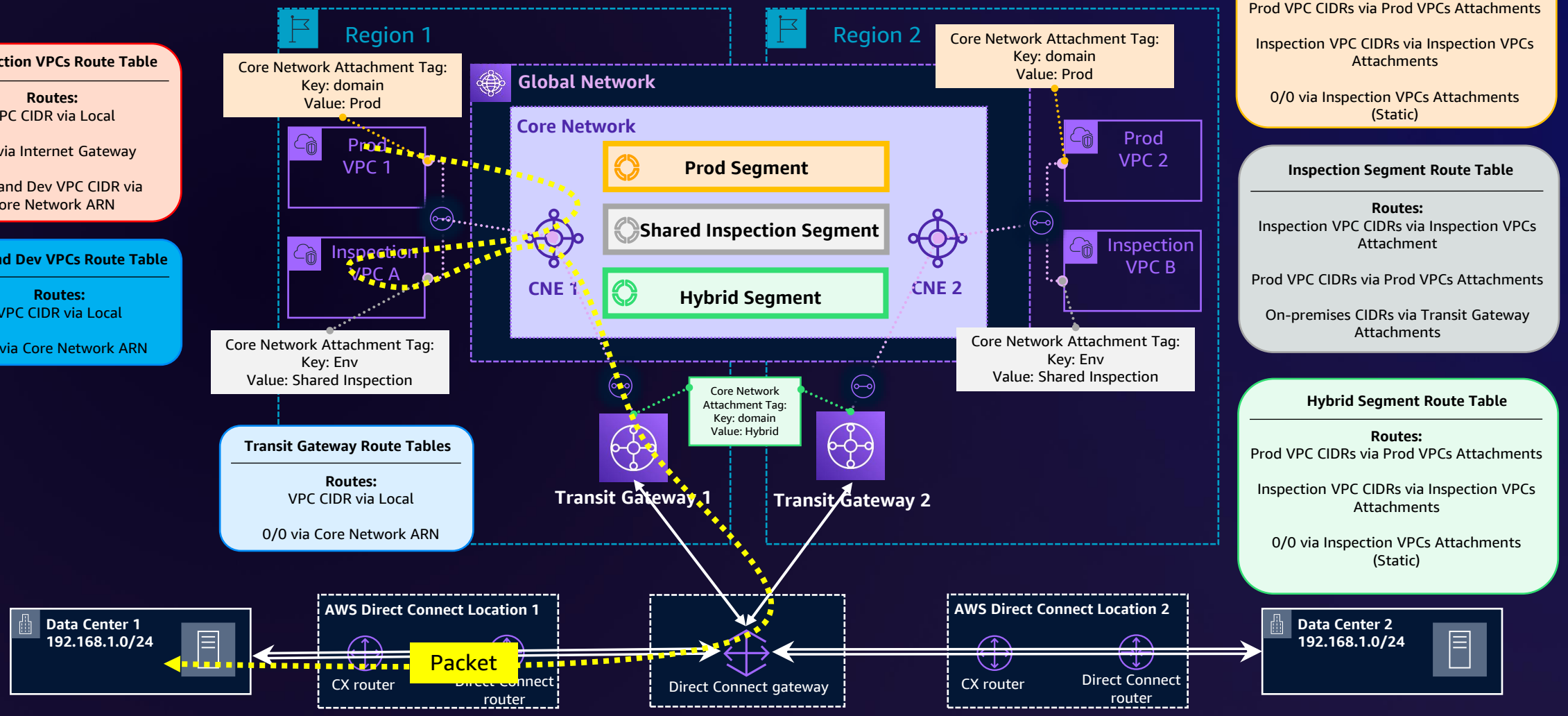
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

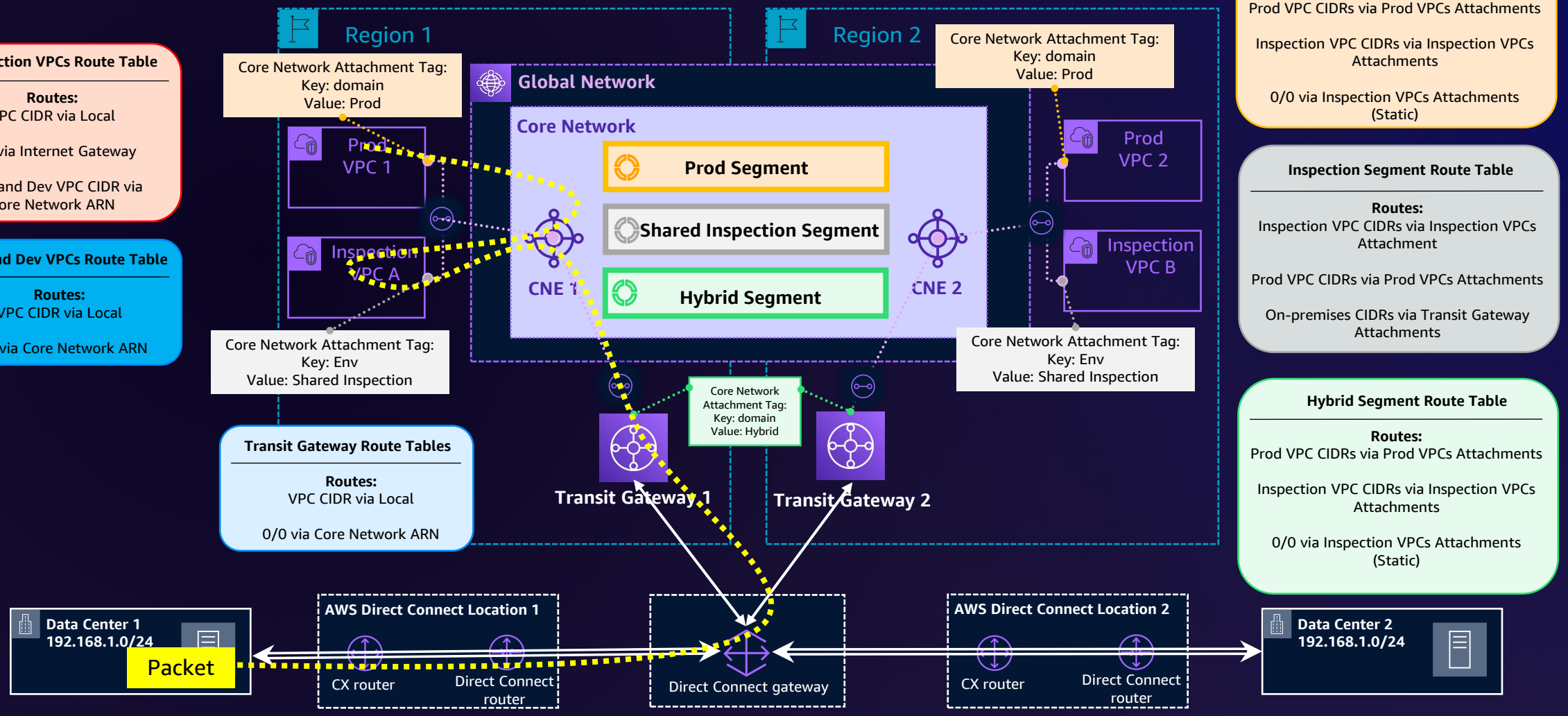
Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

VPC-to-on-premises inspection architecture



Inspection VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Internet Gateway

Prod and Dev VPC CIDR via Core Network ARN

Prod and Dev VPCs Route Table

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Transit Gateway Route Tables

Routes:
VPC CIDR via Local

0/0 via Core Network ARN

Prod Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Inspection Segment Route Table

Routes:
Inspection VPC CIDRs via Inspection VPCs Attachment

Prod VPC CIDRs via Prod VPCs Attachments

On-premises CIDRs via Transit Gateway Attachments

Hybrid Segment Route Table

Routes:
Prod VPC CIDRs via Prod VPCs Attachments

Inspection VPC CIDRs via Inspection VPCs Attachments

0/0 via Inspection VPCs Attachments (Static)

Thank you!

Please complete the session survey in the mobile app

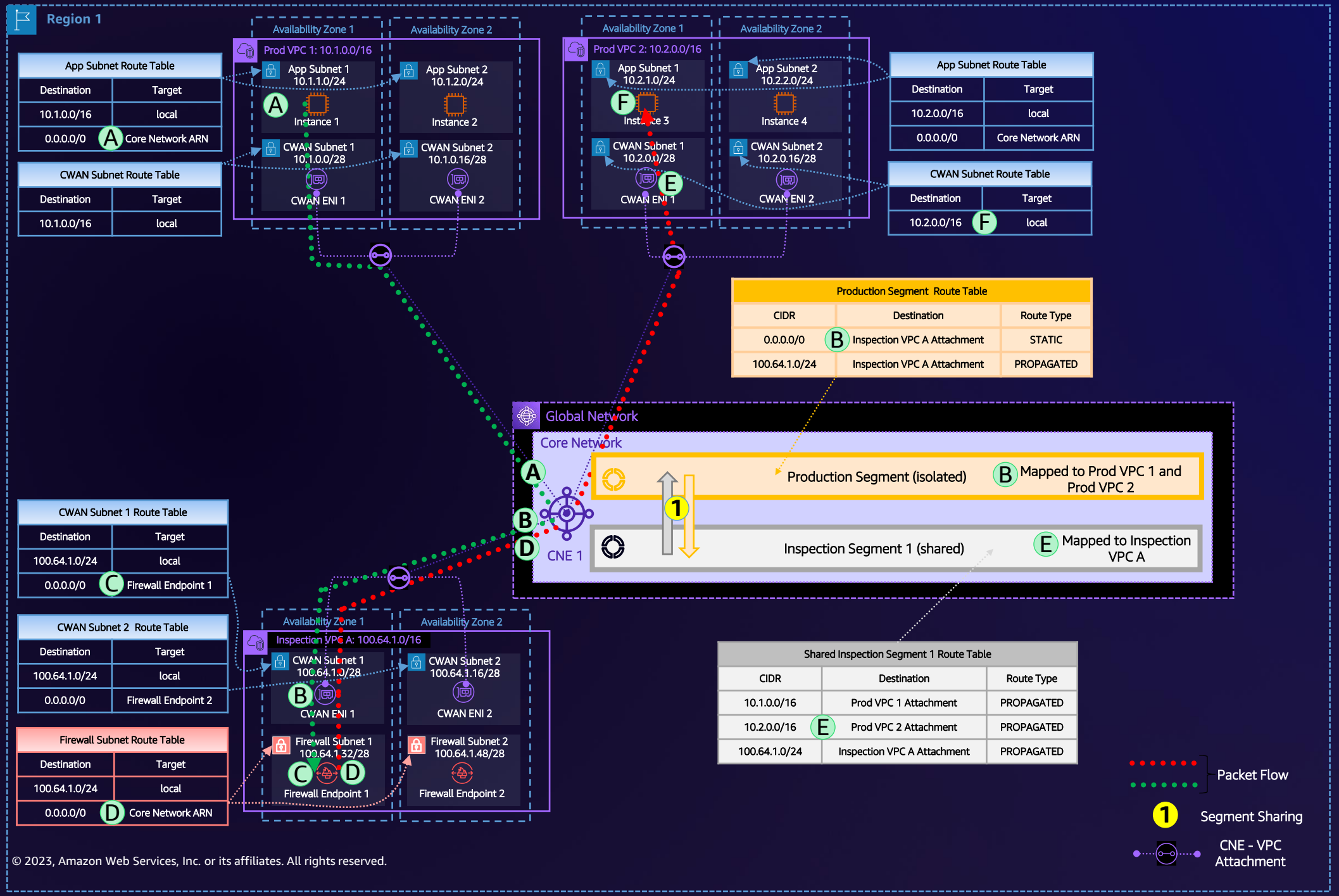
Mehar Swarup
linkedin.com/in/mehar-swarup/

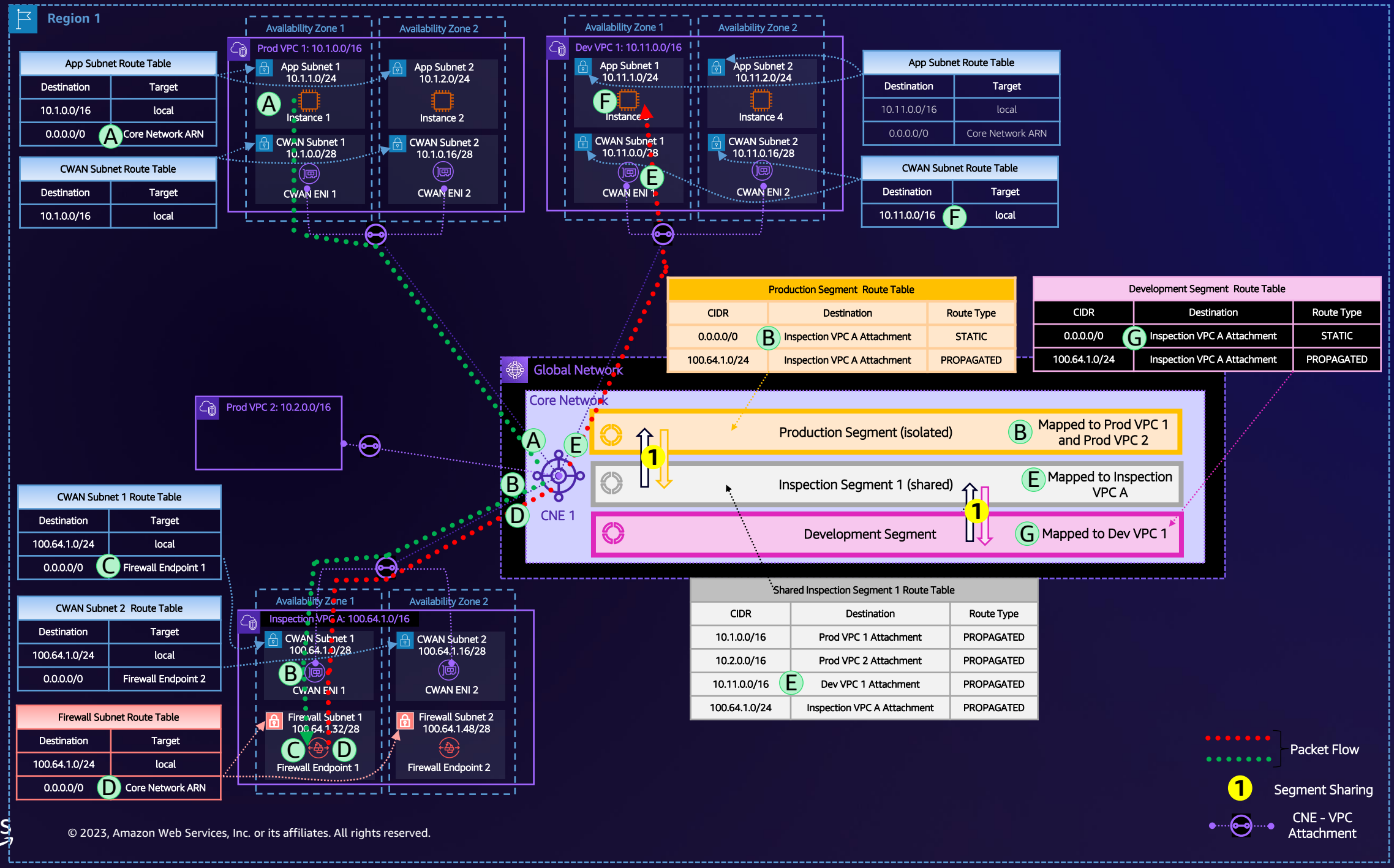
Pratik R. Mankad
linkedin.com/in/pratikrmankad/

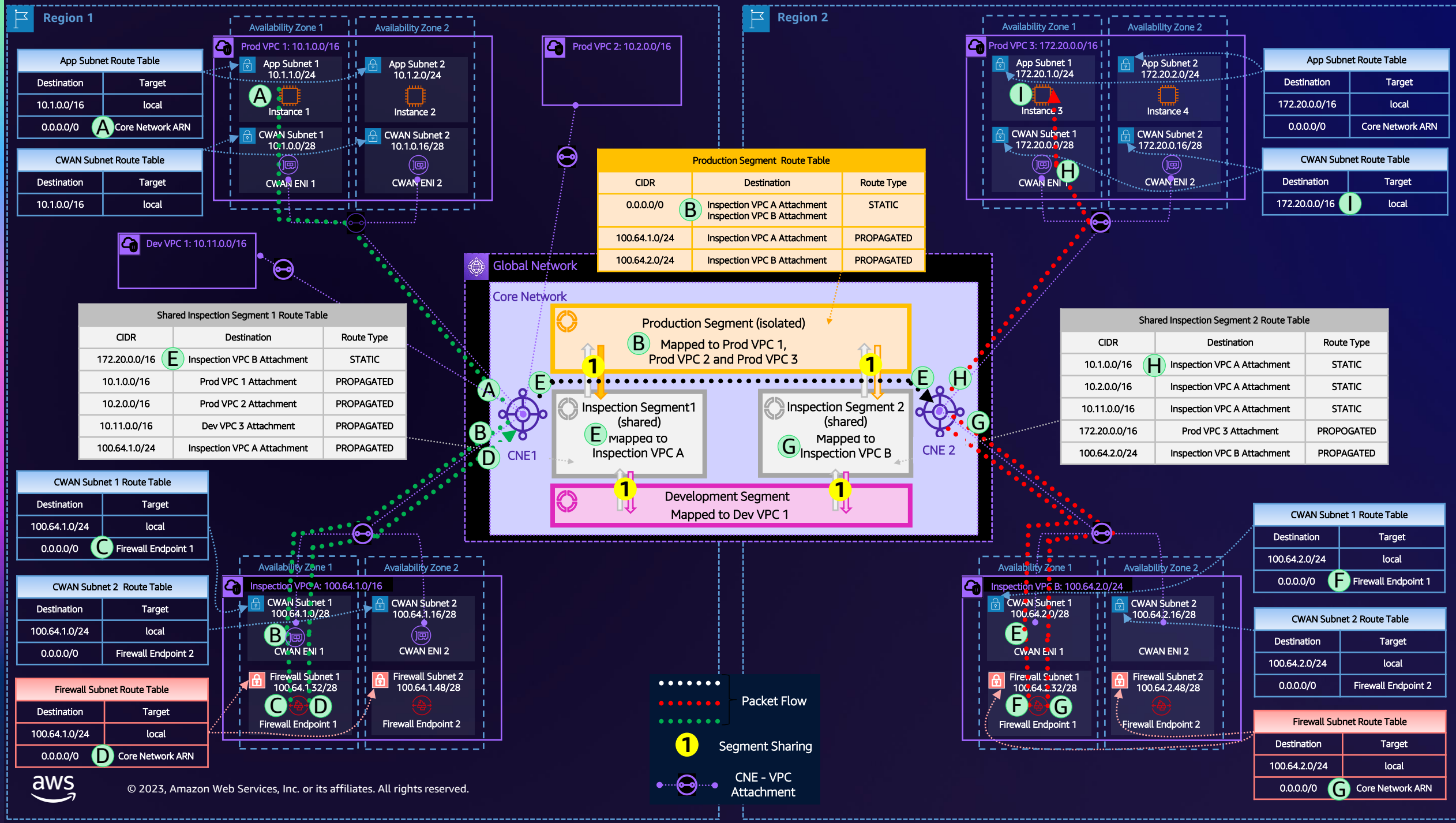
Appendix

Inspection architectures

East-west scenario







App Subnet Route Table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	A Core Network ARN

CWAN Subnet Route Table

Destination	Target
10.1.0.0/16	local

Production Segment Route Table

CIDR	Destination	Route Type
0.0.0.0/0	B Inspection VPC A Attachment, Inspection VPC B Attachment	STATIC
100.64.1.0/24	Inspection VPC A Attachment	PROPAGATED
100.64.2.0/24	Inspection VPC B Attachment	PROPAGATED

App Subnet Route Table

Destination	Target
172.20.0.0/16	local
0.0.0.0/0	Core Network ARN

CWAN Subnet Route Table

Destination	Target
172.20.0.0/16	I local

Shared Inspection Segment 1 Route Table

CIDR	Destination	Route Type
172.20.0.0/16	E Inspection VPC B Attachment	STATIC
10.1.0.0/16	Prod VPC 1 Attachment	PROPAGATED
10.2.0.0/16	Prod VPC 2 Attachment	PROPAGATED
10.11.0.0/16	Dev VPC 3 Attachment	PROPAGATED
100.64.1.0/24	Inspection VPC A Attachment	PROPAGATED

Shared Inspection Segment 2 Route Table

CIDR	Destination	Route Type
10.1.0.0/16	H Inspection VPC A Attachment	STATIC
10.2.0.0/16	Inspection VPC A Attachment	STATIC
10.11.0.0/16	Inspection VPC A Attachment	STATIC
172.20.0.0/16	Prod VPC 3 Attachment	PROPOGATED
100.64.2.0/24	Inspection VPC B Attachment	PROPAGATED

CWAN Subnet 1 Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0	C Firewall Endpoint 1

CWAN Subnet 2 Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0	Firewall Endpoint 2

Firewall Subnet Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0	D Core Network ARN

CWAN Subnet 1 Route Table

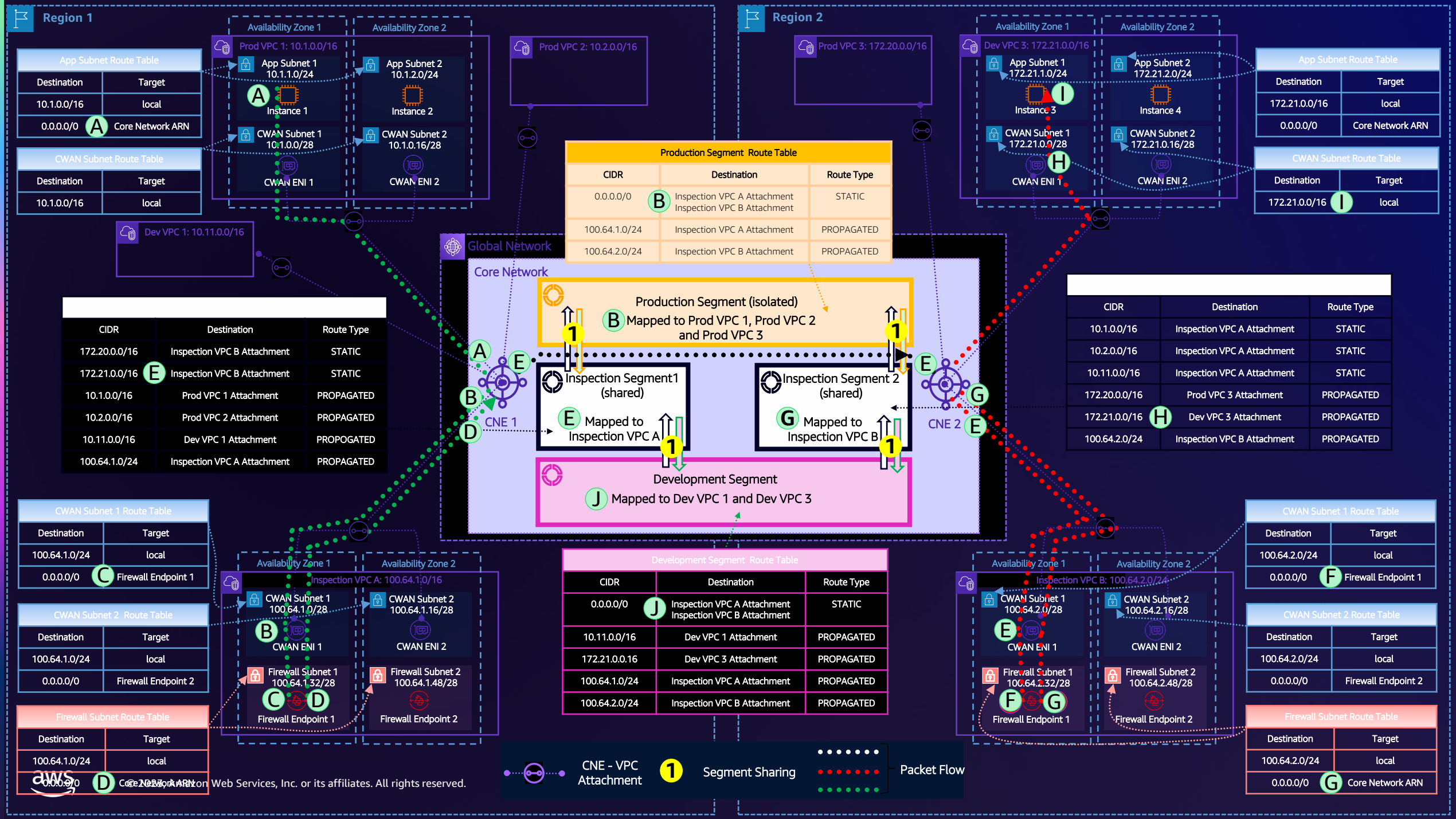
Destination	Target
100.64.2.0/24	local
0.0.0.0/0	F Firewall Endpoint 1

CWAN Subnet 2 Route Table

Destination	Target
100.64.2.0/24	local
0.0.0.0/0	Firewall Endpoint 2

Firewall Subnet Route Table

Destination	Target
100.64.2.0/24	local
0.0.0.0/0	G Core Network ARN



App Subnet Route Table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0 A	Core Network ARN

CWAN Subnet Route Table

Destination	Target
10.1.0.0/16	local

Production Segment Route Table

CIDR	Destination	Route Type
0.0.0.0/0 B	Inspection VPC A Attachment, Inspection VPC B Attachment	STATIC
100.64.1.0/24	Inspection VPC A Attachment	PROPAGATED
100.64.2.0/24	Inspection VPC B Attachment	PROPAGATED

CIDR	Destination	Route Type
172.20.0.0/16	Inspection VPC B Attachment	STATIC
172.21.0.0/16 E	Inspection VPC B Attachment	STATIC
10.1.0.0/16	Prod VPC 1 Attachment	PROPAGATED
10.2.0.0/16	Prod VPC 2 Attachment	PROPAGATED
10.11.0.0/16	Dev VPC 1 Attachment	PROPOGATED
100.64.1.0/24	Inspection VPC A Attachment	PROPAGATED

CIDR	Destination	Route Type
10.1.0.0/16	Inspection VPC A Attachment	STATIC
10.2.0.0/16	Inspection VPC A Attachment	STATIC
10.11.0.0/16	Inspection VPC A Attachment	STATIC
172.20.0.0/16	Prod VPC 3 Attachment	PROPAGATED
172.21.0.0/16 H	Dev VPC 3 Attachment	PROPAGATED
100.64.2.0/24	Inspection VPC B Attachment	PROPAGATED

App Subnet Route Table

Destination	Target
172.21.0.0/16	local
0.0.0.0/0	Core Network ARN

CWAN Subnet Route Table

Destination	Target
172.21.0.0/16 I	local

CWAN Subnet 1 Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0 C	Firewall Endpoint 1

CWAN Subnet 2 Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0	Firewall Endpoint 2

Firewall Subnet Route Table

Destination	Target
100.64.1.0/24	local
0.0.0.0/0 D	Core Network ARN

Development Segment Route Table

CIDR	Destination	Route Type
0.0.0.0/0 J	Inspection VPC A Attachment, Inspection VPC B Attachment	STATIC
10.11.0.0/16	Dev VPC 1 Attachment	PROPAGATED
172.21.0.0.16	Dev VPC 3 Attachment	PROPAGATED
100.64.1.0/24	Inspection VPC A Attachment	PROPAGATED
100.64.2.0/24	Inspection VPC B Attachment	PROPAGATED

CWAN Subnet 1 Route Table

Destination	Target
100.64.2.0/24	local
0.0.0.0/0 F	Firewall Endpoint 1

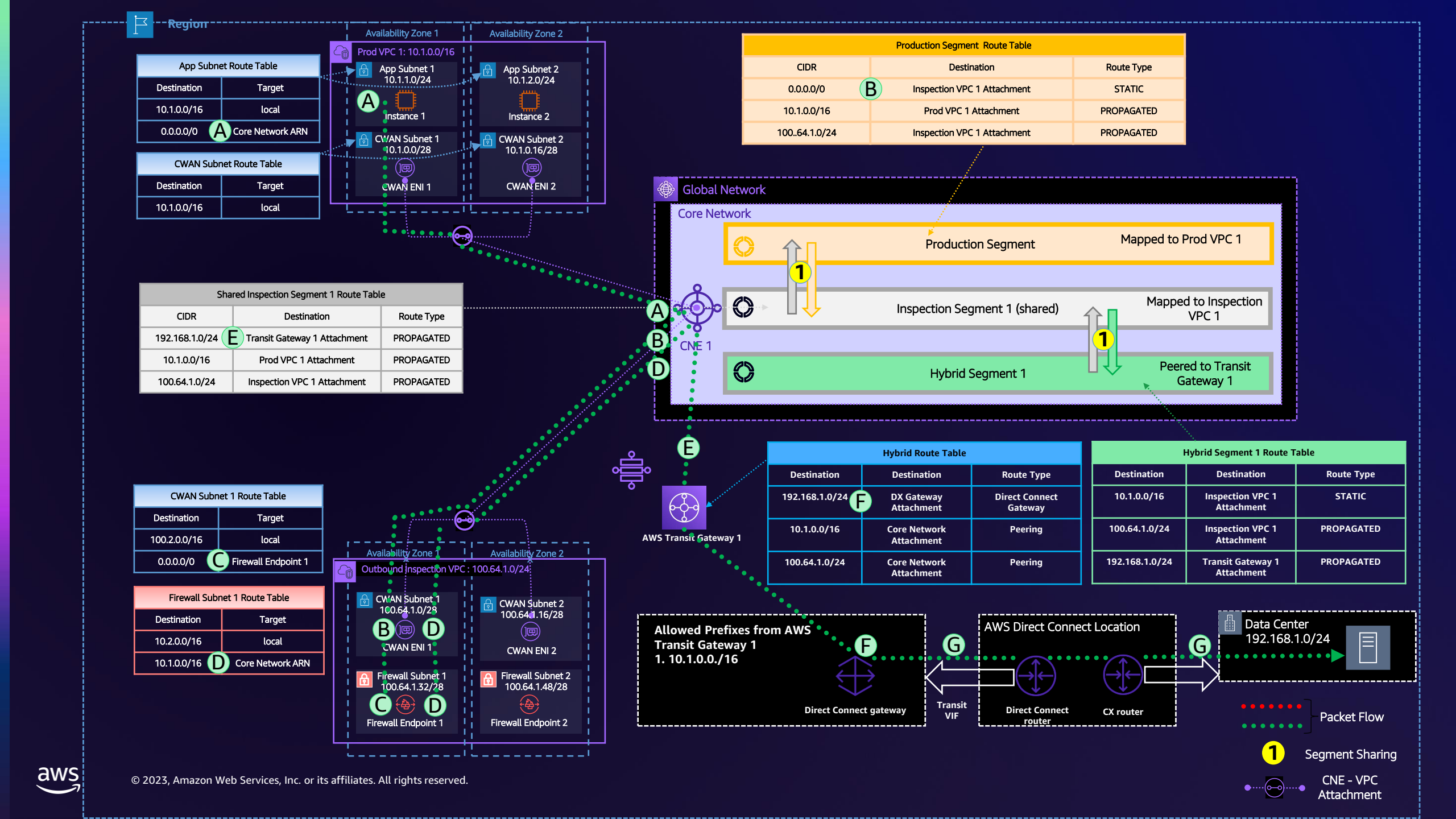
CWAN Subnet 2 Route Table

Destination	Target
100.64.2.0/24	local
0.0.0.0/0	Firewall Endpoint 2

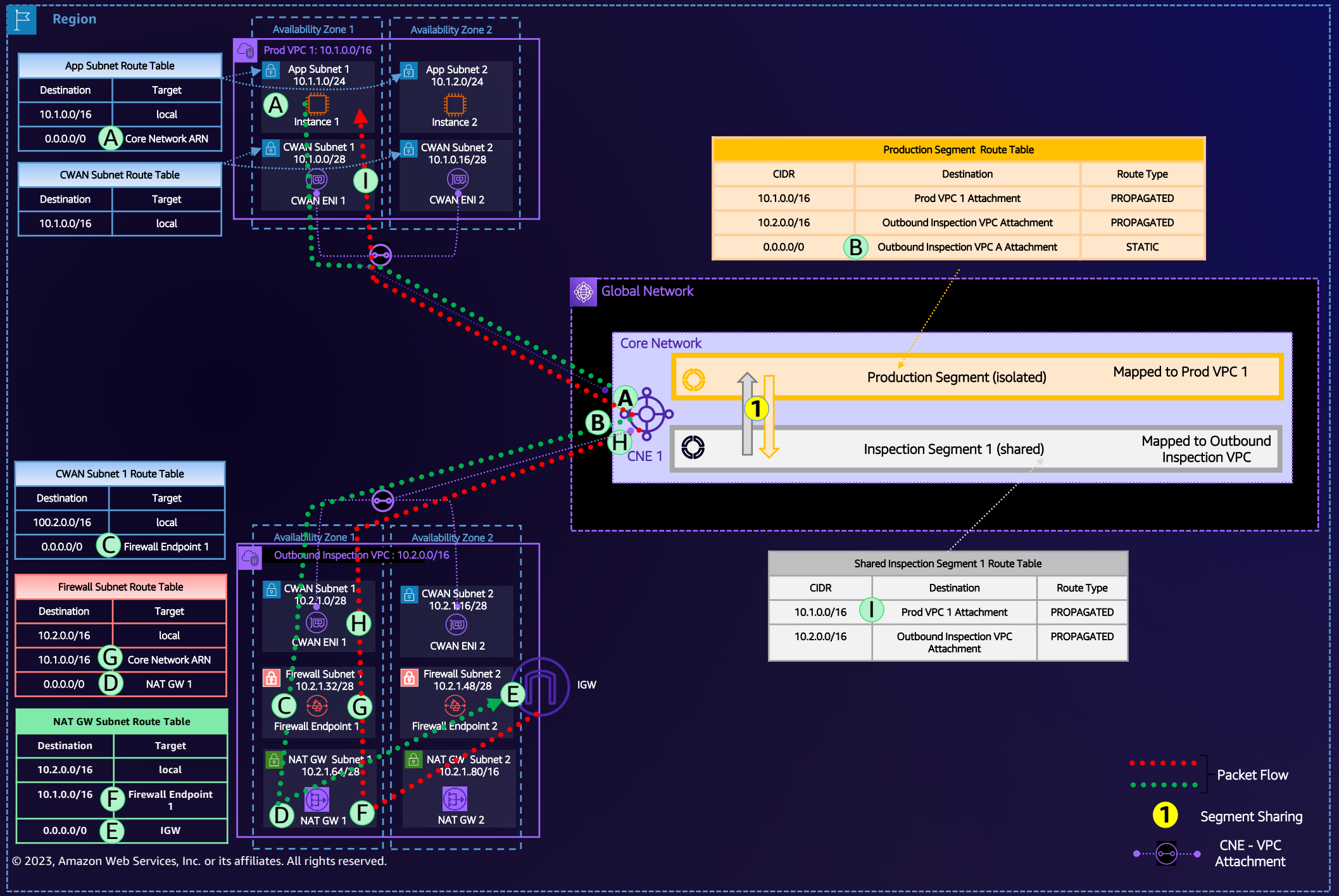
Firewall Subnet Route Table

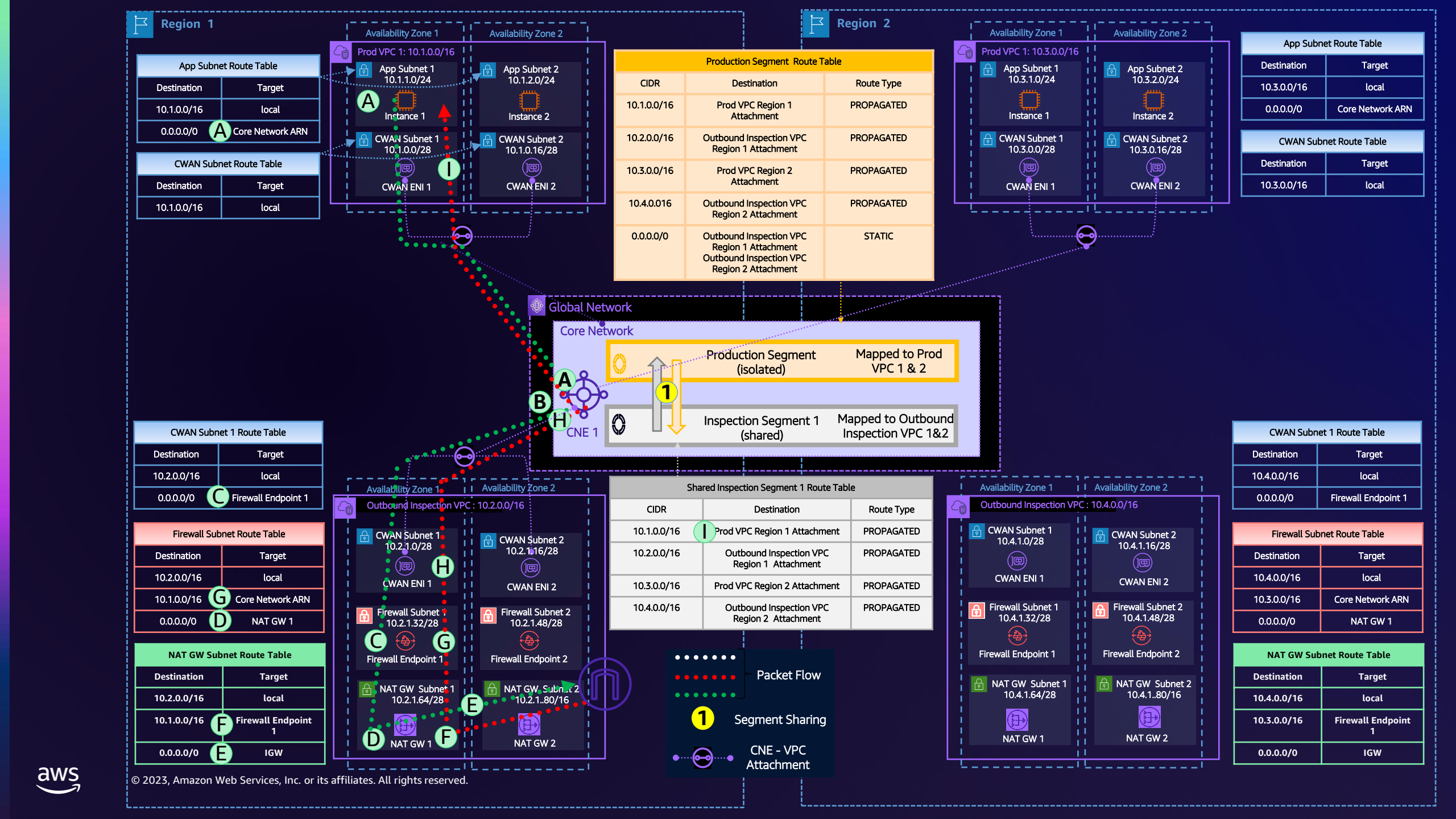
Destination	Target
100.64.2.0/24	local
0.0.0.0/0 G	Core Network ARN

Hybrid scenario



Egress scenario

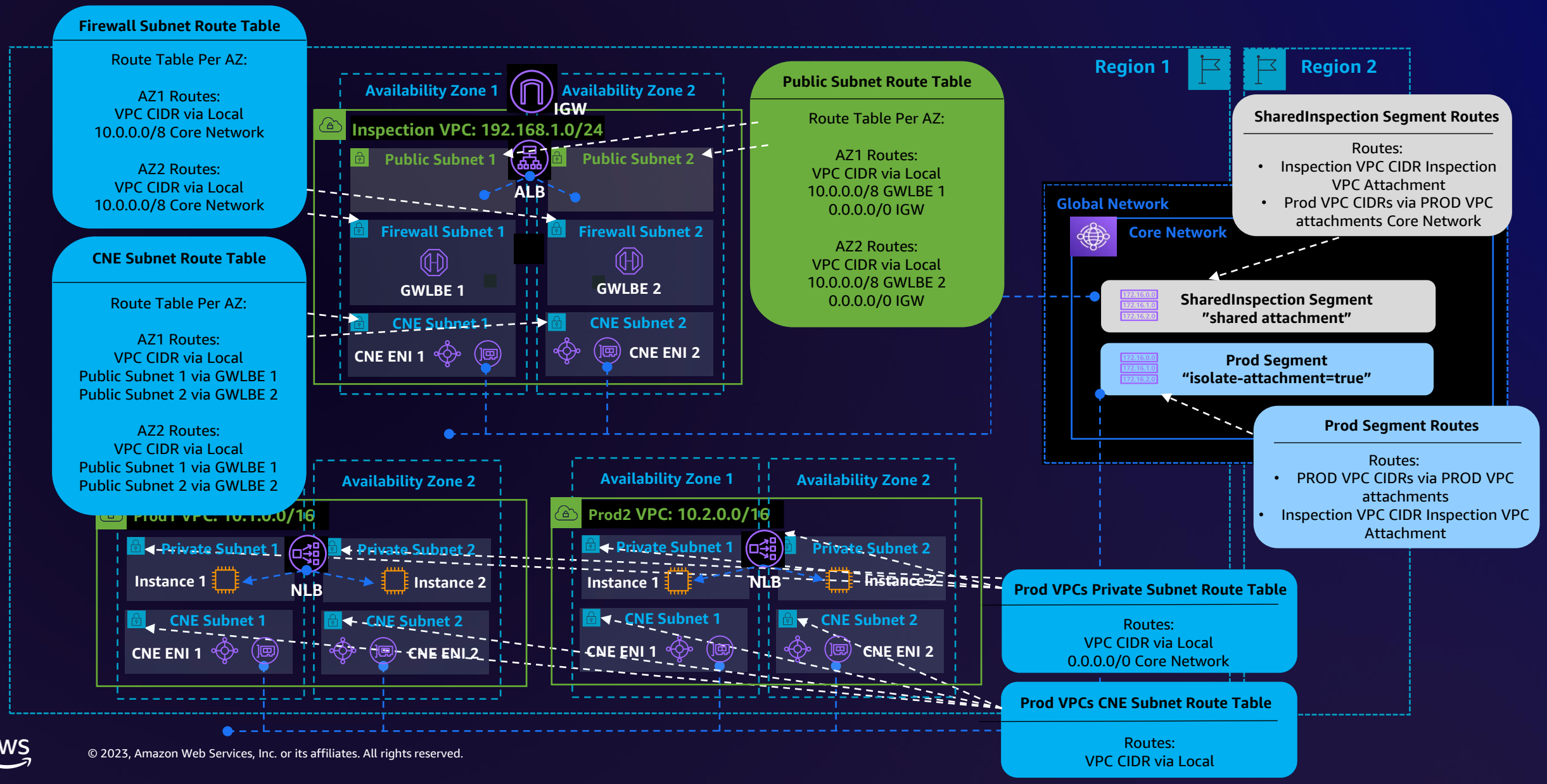




Ingress scenario

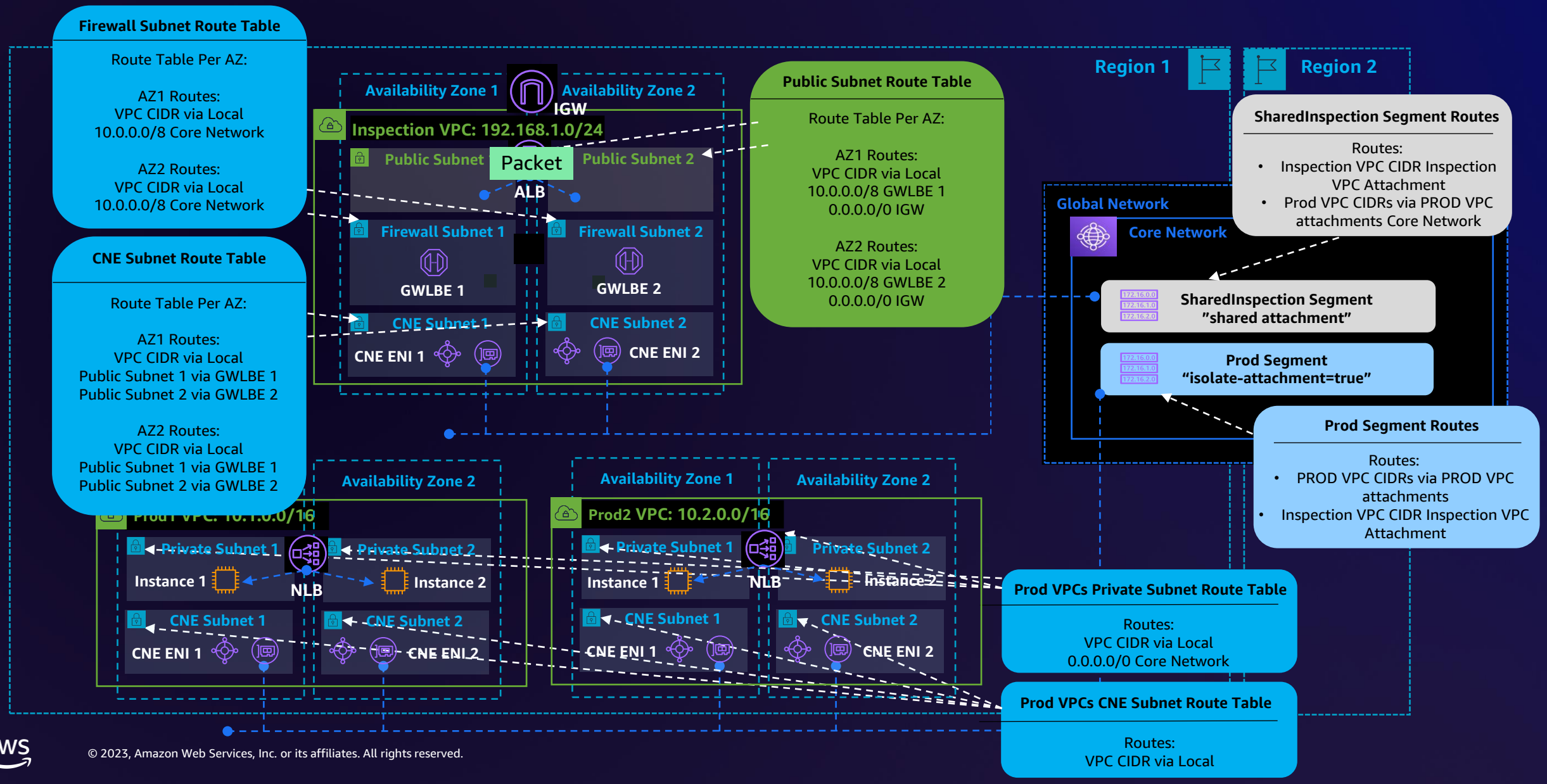
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



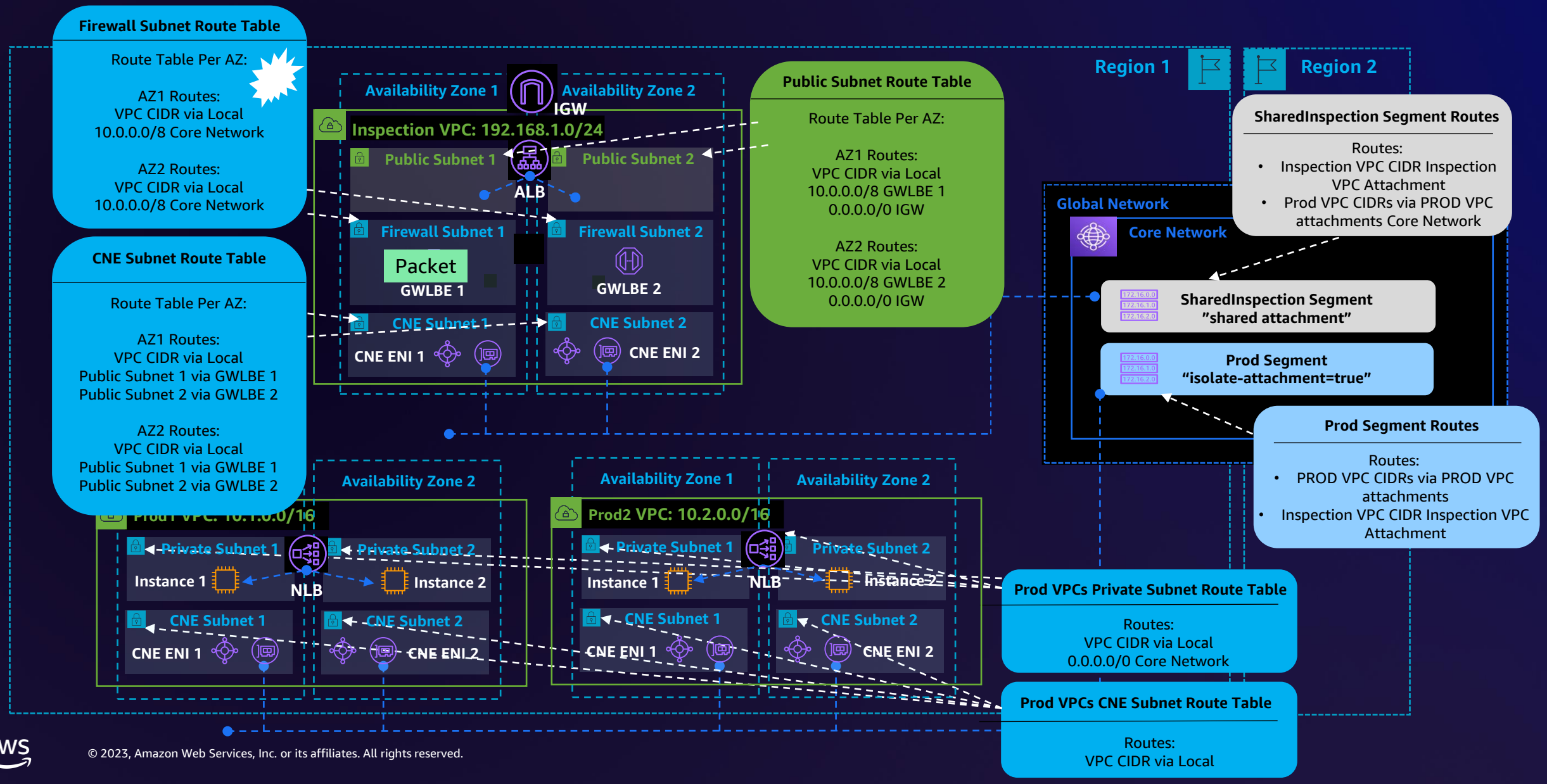
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



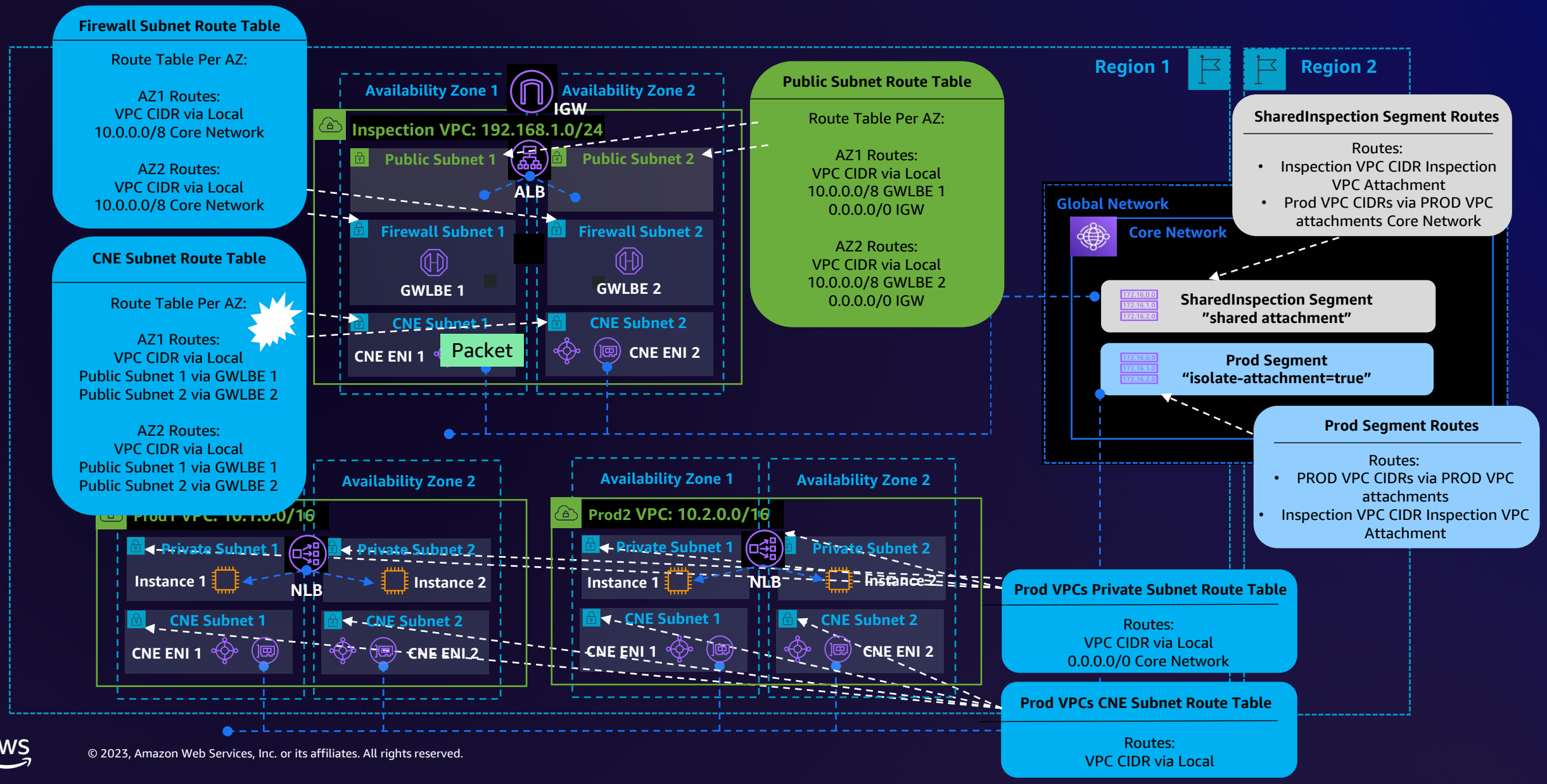
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



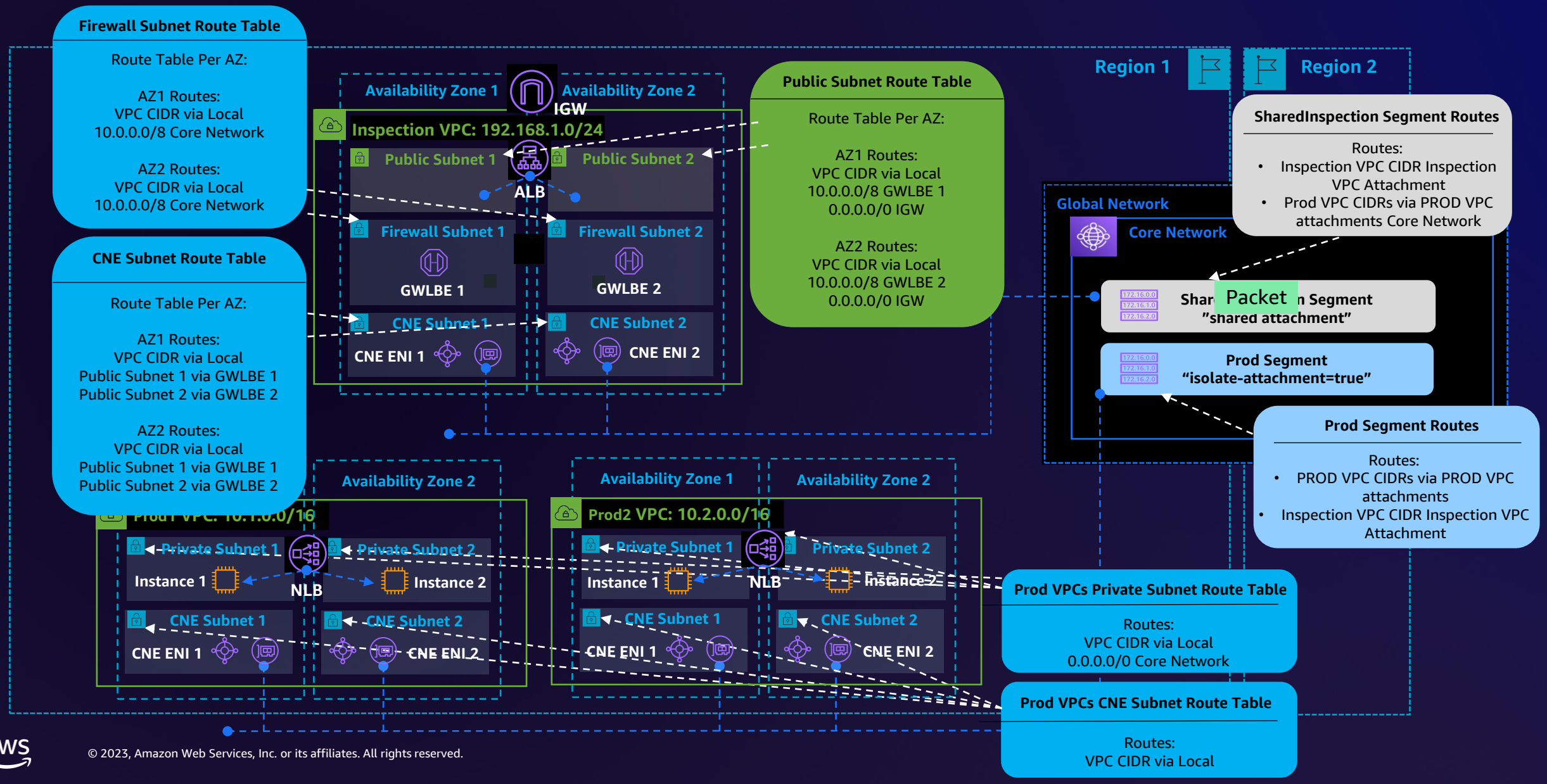
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



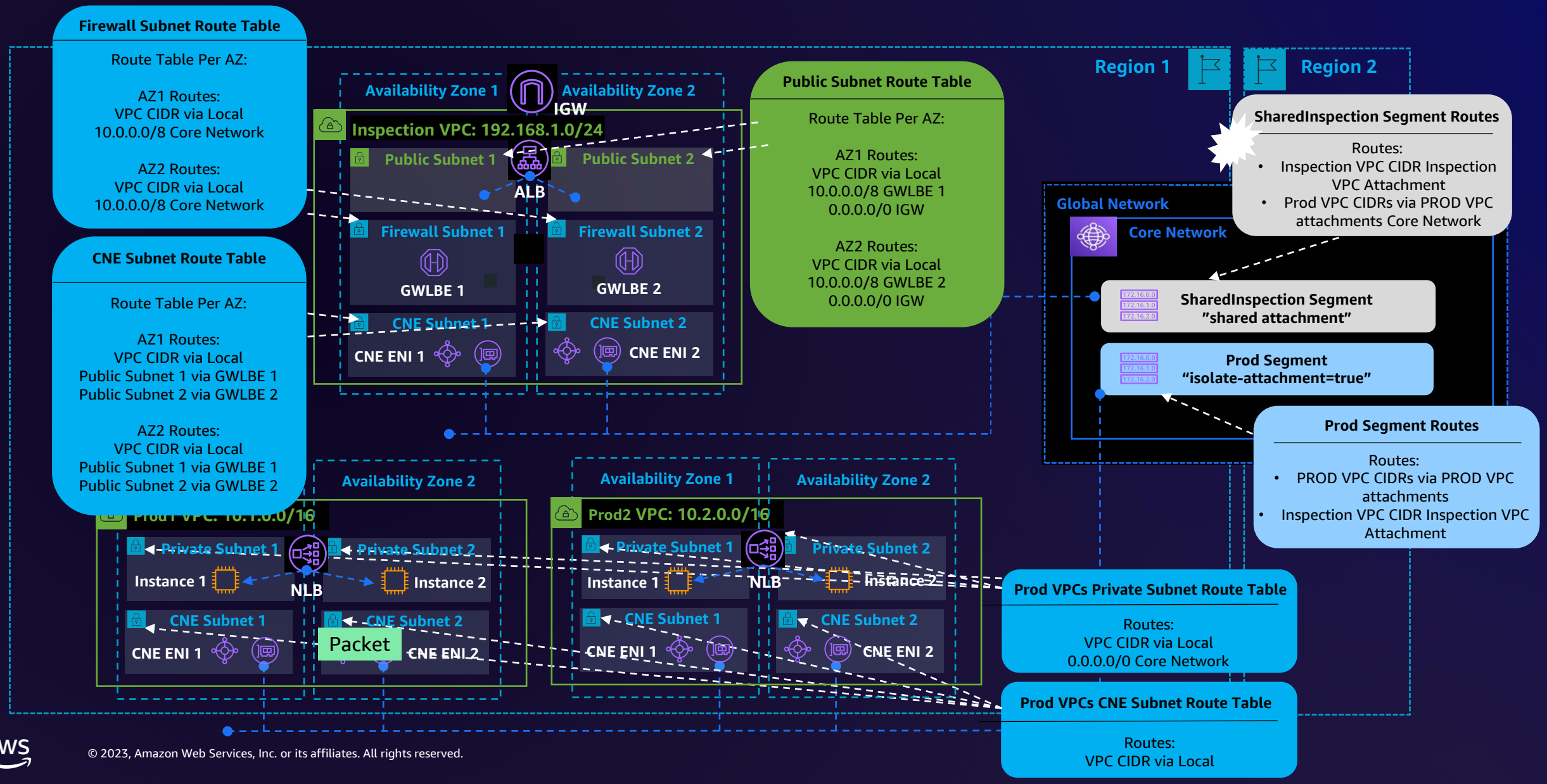
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



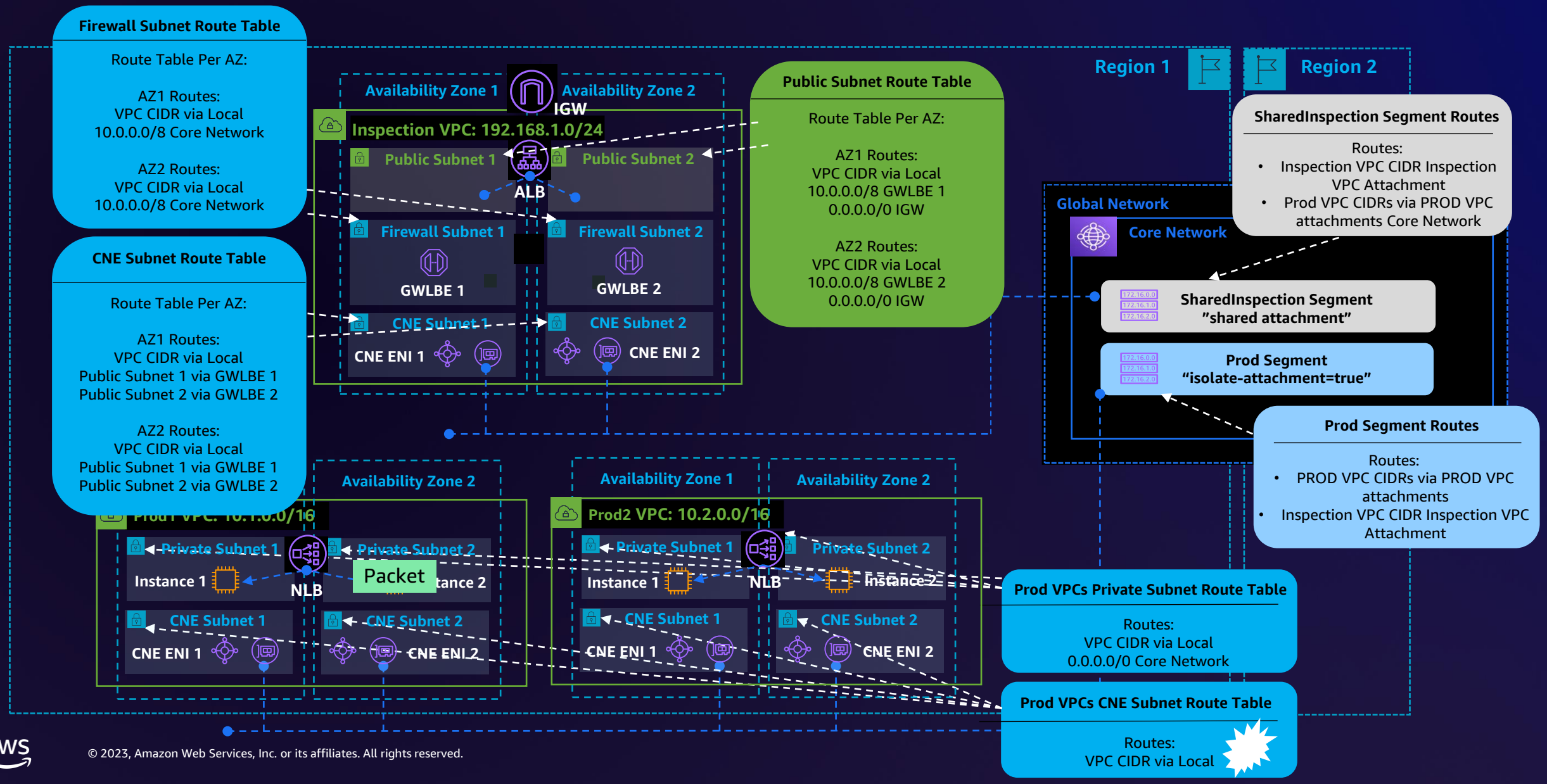
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



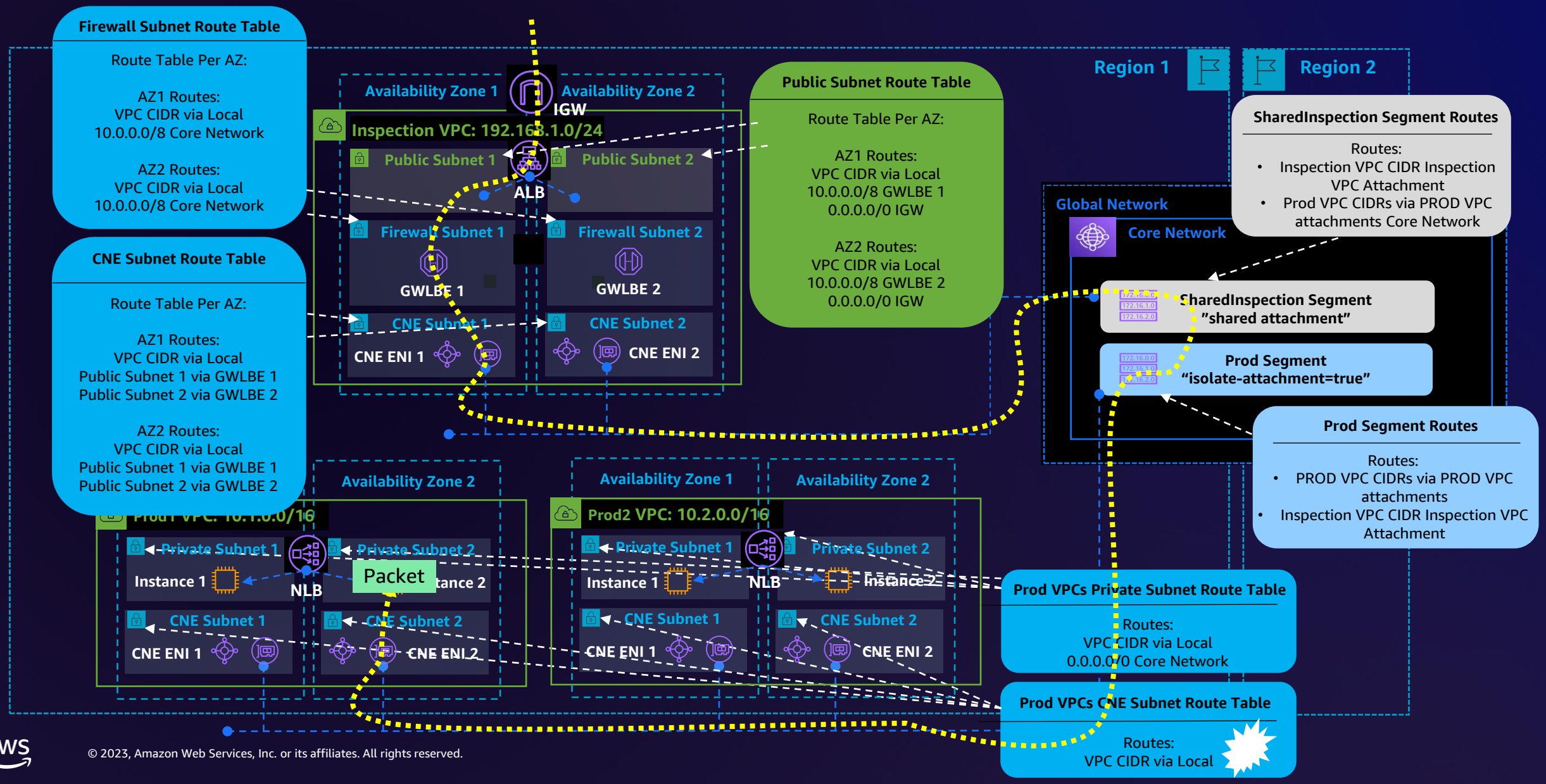
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



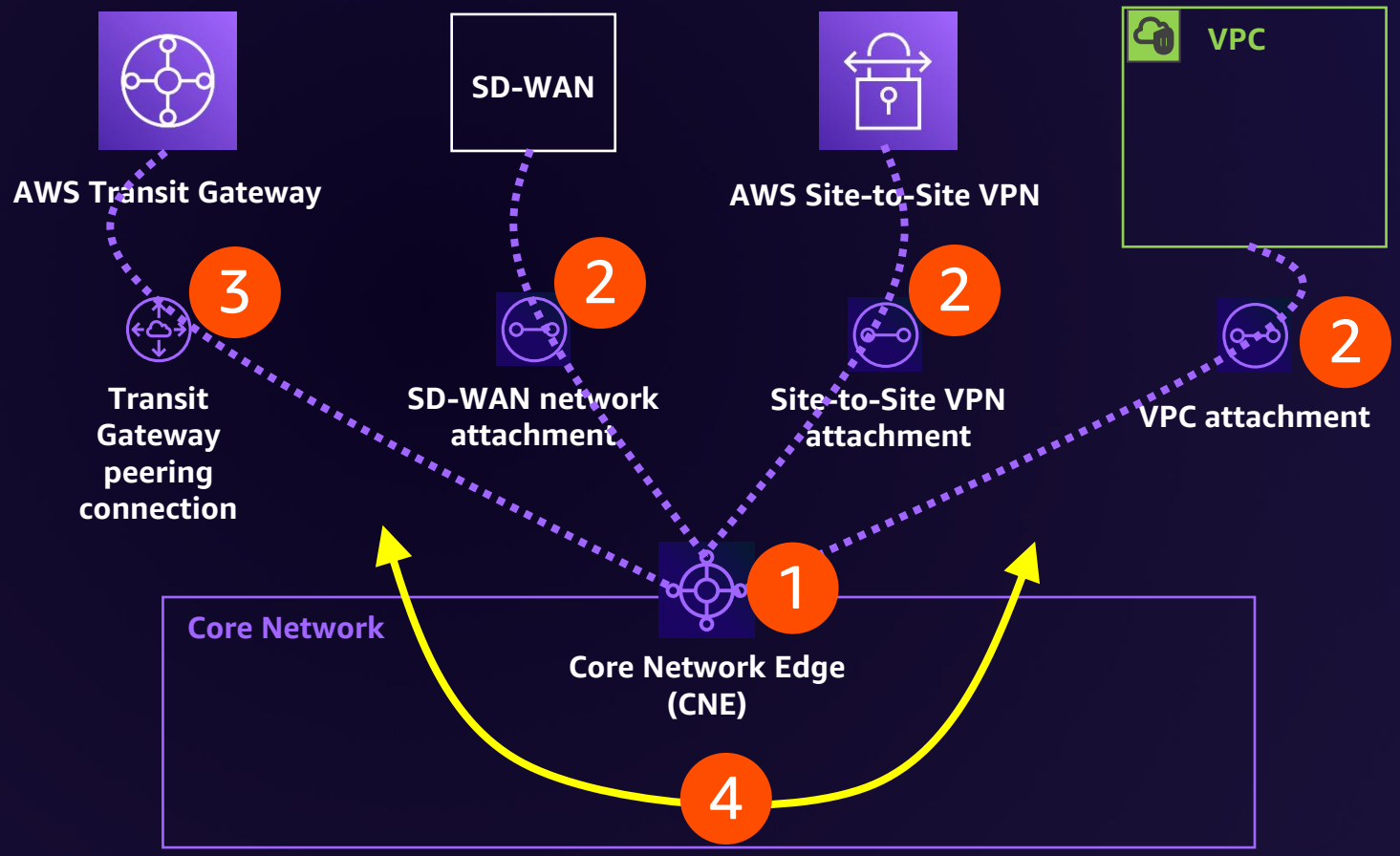
Centralized

MULTIPLE CLOUD WAN SEGMENTS WITH A SEPARATE SECURITY SEGMENT



AWS Cloud WAN detailed pricing

Pricing constructs

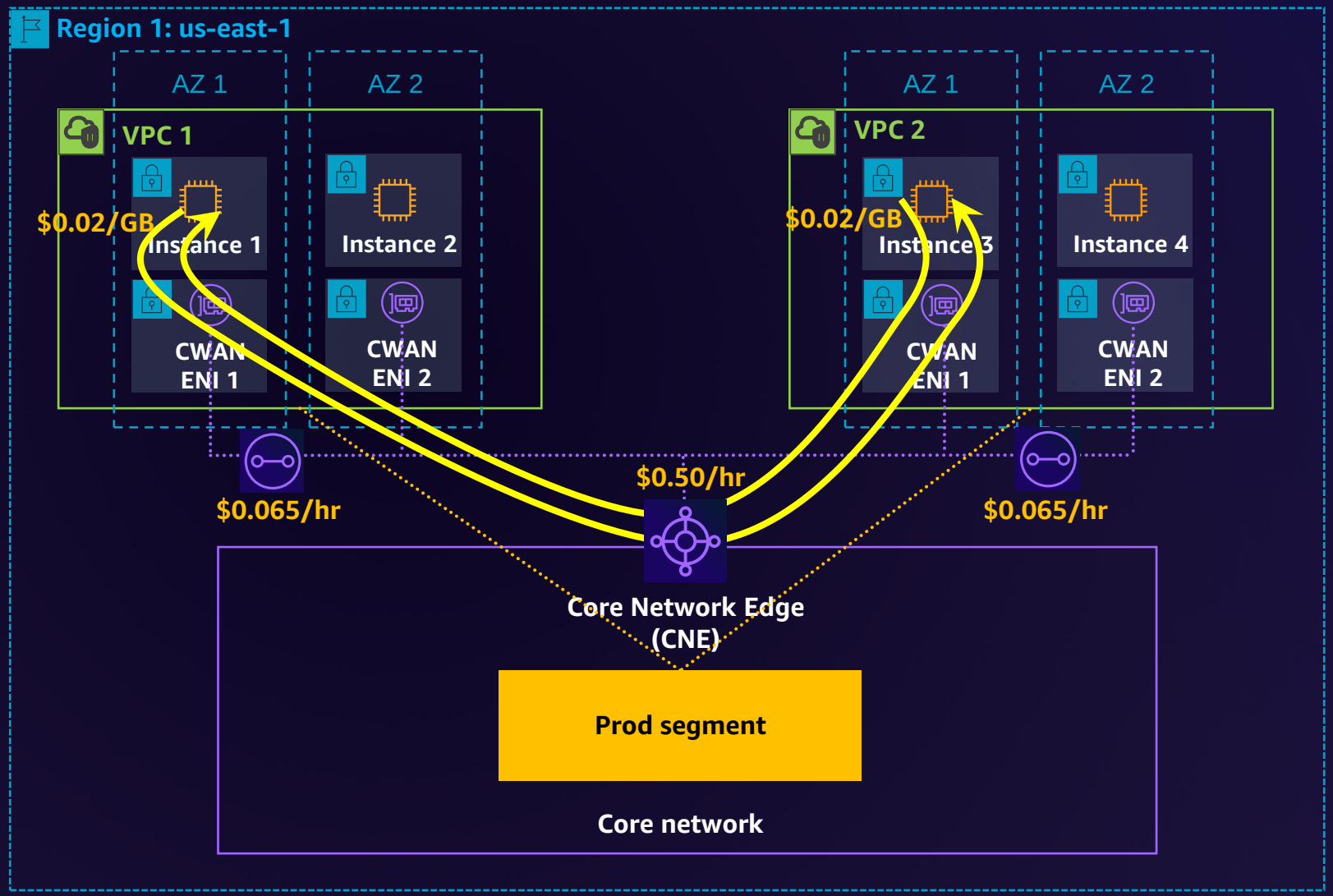


Four components

1. Core network edge, hourly charge
2. Core network attachments, hourly charge
3. Peering connection, hourly charge
4. Data processing, per-gigabyte charge

https://aws.amazon.com/cloud-wan/pricing/

AWS Cloud WAN – Data transfer same Region

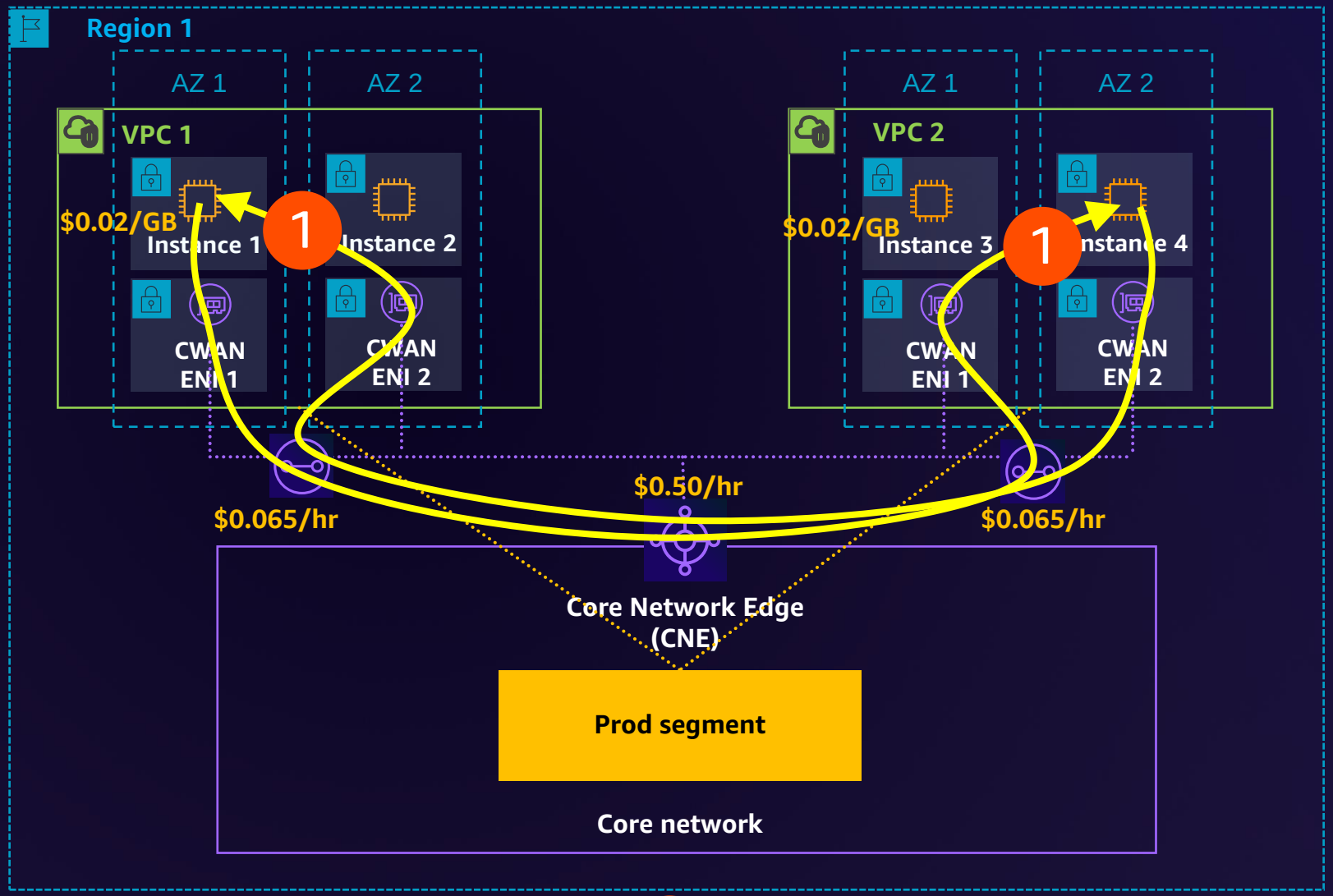


Instance 1 sending 1 gigabyte of data to Instance 3 and Instance 3 responding back with 1 gigabyte

Data processing: $0.04
- VPC 1 owner charged $0.02/GB
- VPC 2 owner charged $0.02/GB

Hourly charges: $.63/hr
- VPC 1 owner charged $0.065/hr
- VPC 2 owner charged $0.065/hr
- AWS Cloud WAN owner charged $0.50/hr

AWS Cloud WAN – Data transfer same Region cross AZ



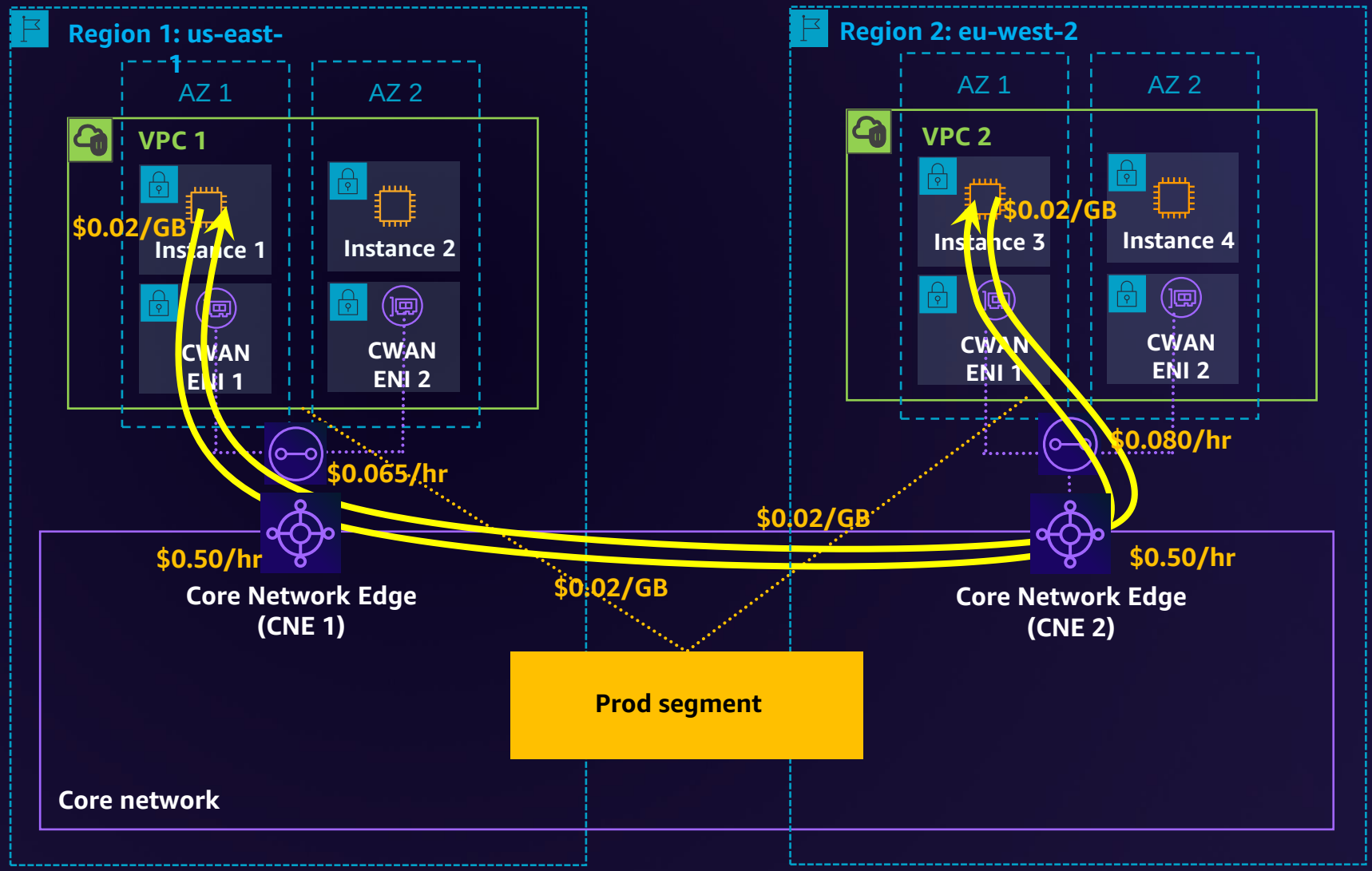
Instance 1 sending 1 gigabyte of data to Instance 3 and Instance 3 responding back with 1 gigabyte

Data processing: $0.04
- VPC 1 owner charged $0.02/GB
- VPC 2 owner charged $0.02/GB

Hourly charges: $.63/hr
- VPC 1 owner charged $0.065/hr
- VPC 2 owner charged $0.065/hr
- AWS Cloud WAN owner charged $0.50/hr

1 No inter-AZ data transfer charges

AWS Cloud WAN – Data transfer cross-Region



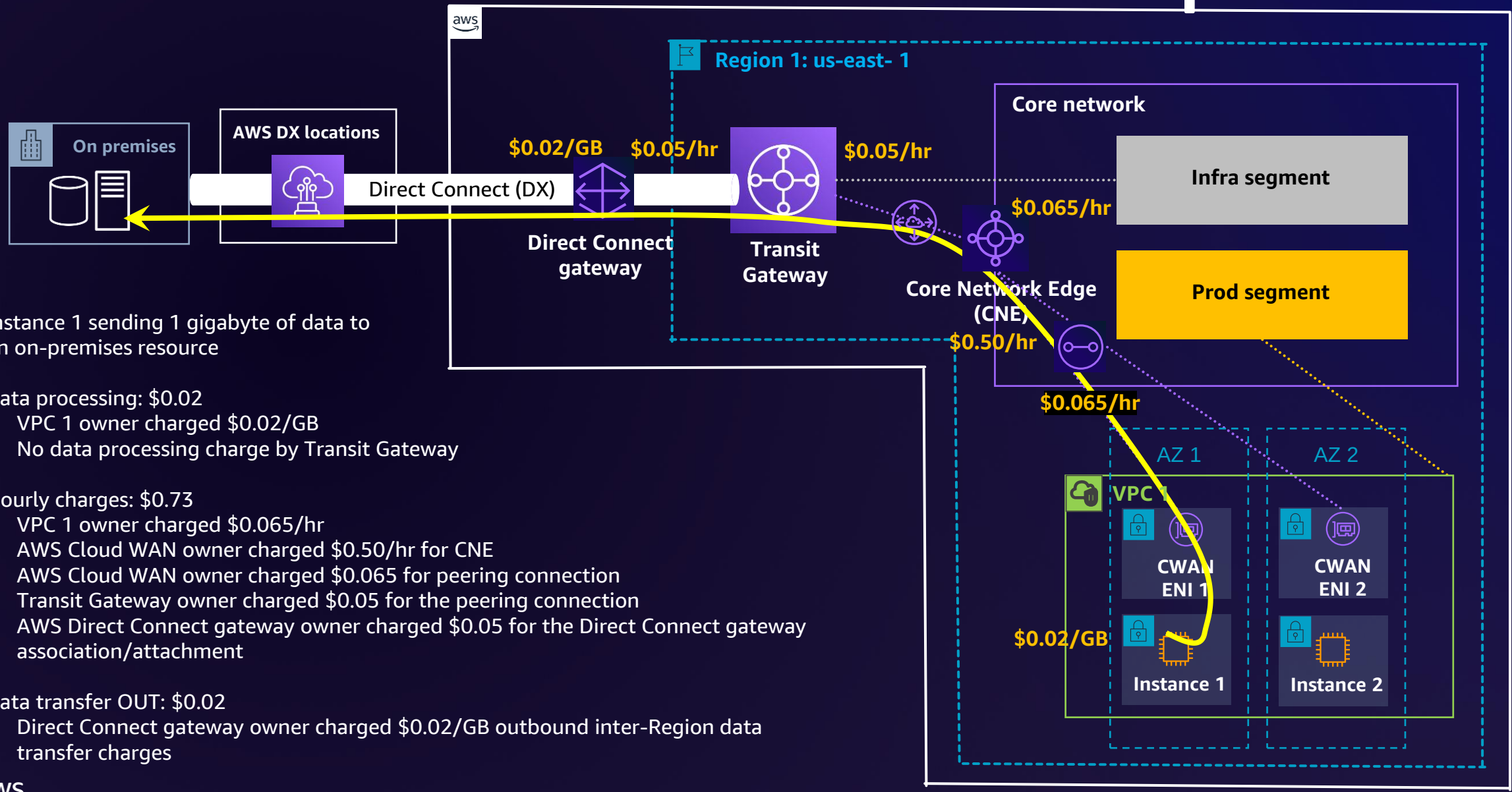
Instance 1 sending 1 gigabyte of data to Instance 3 and Instance 3 responding back with 1 gigabyte

Data processing: $0.04
- VPC 1 owner charged $0.02/GB
- VPC 2 owner charged $0.02/GB
- No data processing charge by CNE 2

Hourly charges: $1.145
- VPC 1 owner charged $0.065/hr
- VPC 2 owner charged $0.080/hr
- AWS Cloud WAN owner charged $0.50/hr or each CNE (CNE 1 and CNE 2)

Cross-Region data transfer: $0.04
- VPC 1: $0.02/GB outbound inter-Region data transfer charges
- VPC 2: $0.02/GB outbound inter-Region data transfer charges

AWS Cloud WAN – Data transfer to on premises



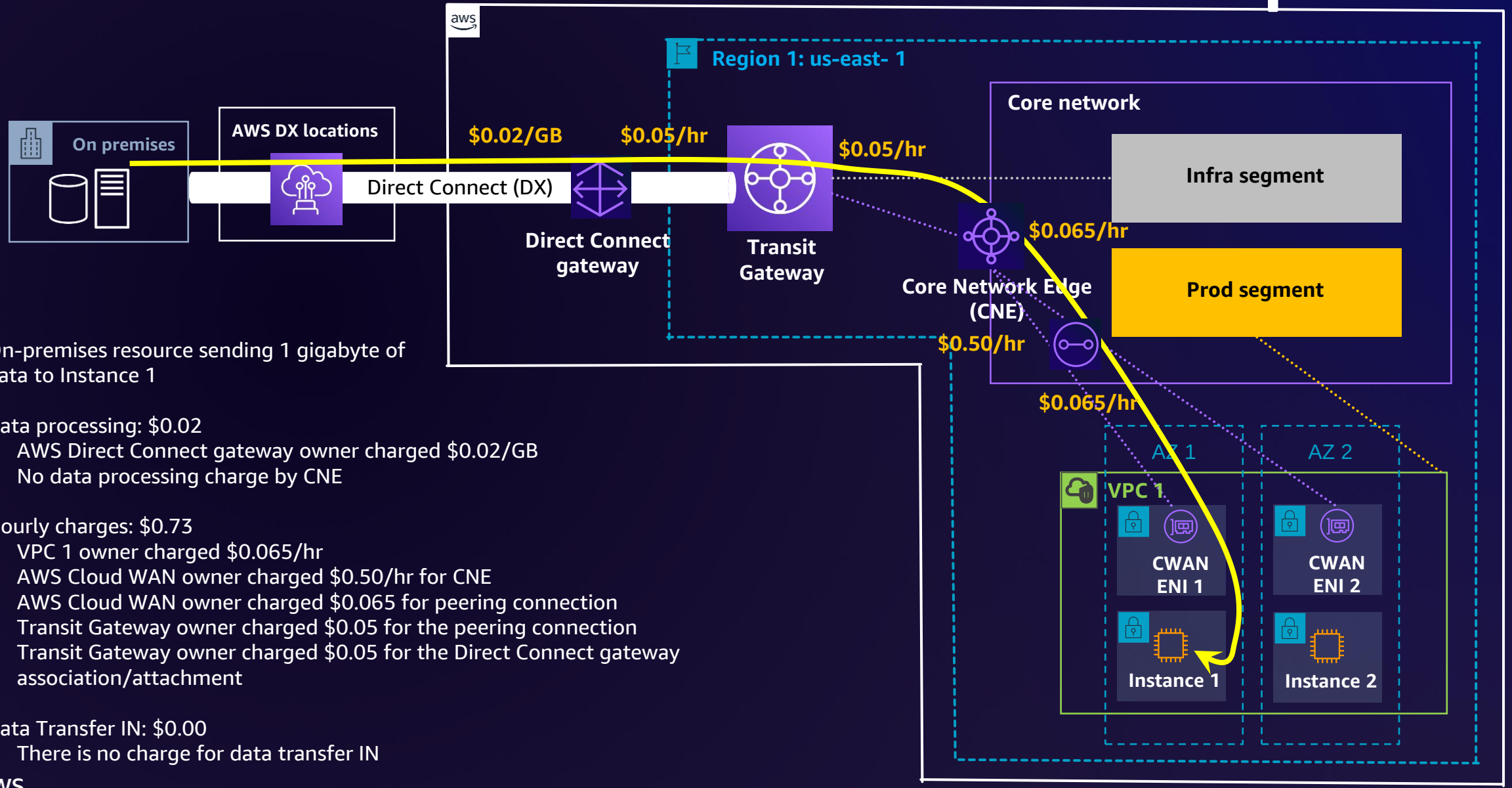
Instance 1 sending 1 gigabyte of data to an on-premises resource

Data processing: $0.02
- VPC 1 owner charged $0.02/GB
- No data processing charge by Transit Gateway

Hourly charges: $0.73
- VPC 1 owner charged $0.065/hr
- AWS Cloud WAN owner charged $0.50/hr for CNE
- AWS Cloud WAN owner charged $0.065 for peering connection
- Transit Gateway owner charged $0.05 for the peering connection
- AWS Direct Connect gateway owner charged $0.05 for the Direct Connect gateway association/attachment

Data transfer OUT: $0.02
- Direct Connect gateway owner charged $0.02/GB outbound inter-Region data transfer charges

AWS Cloud WAN – Data transfer from on premises



On-premises resource sending 1 gigabyte of data to Instance 1

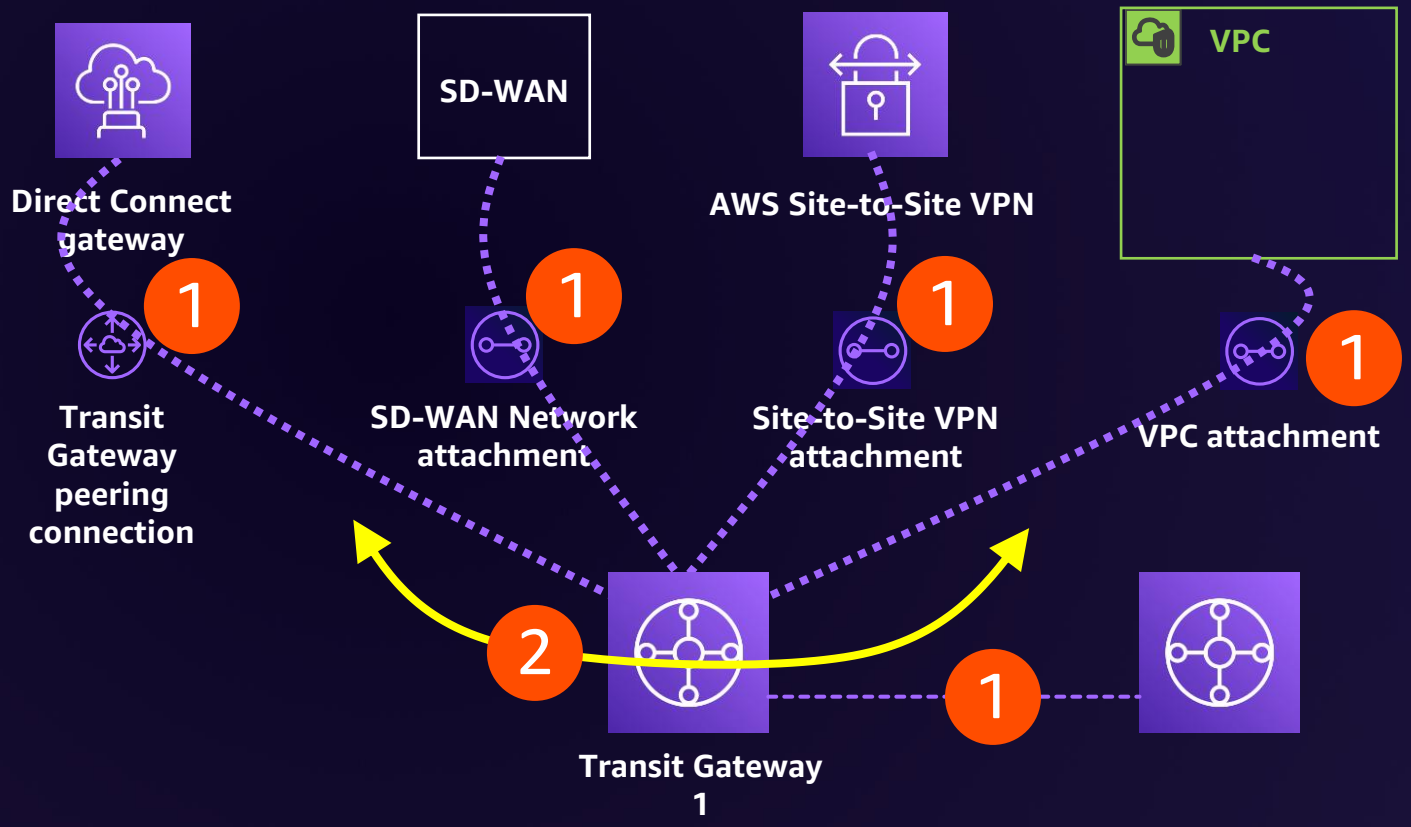
Data processing: $0.02
- AWS Direct Connect gateway owner charged $0.02/GB
- No data processing charge by CNE

Hourly charges: $0.73
- VPC 1 owner charged $0.065/hr
- AWS Cloud WAN owner charged $0.50/hr for CNE
- AWS Cloud WAN owner charged $0.065 for peering connection
- Transit Gateway owner charged $0.05 for the peering connection
- Transit Gateway owner charged $0.05 for the Direct Connect gateway association/attachment

Data Transfer IN: $0.00
- There is no charge for data transfer IN

AWS Transit Gateway pricing

Transit Gateway pricing constructs

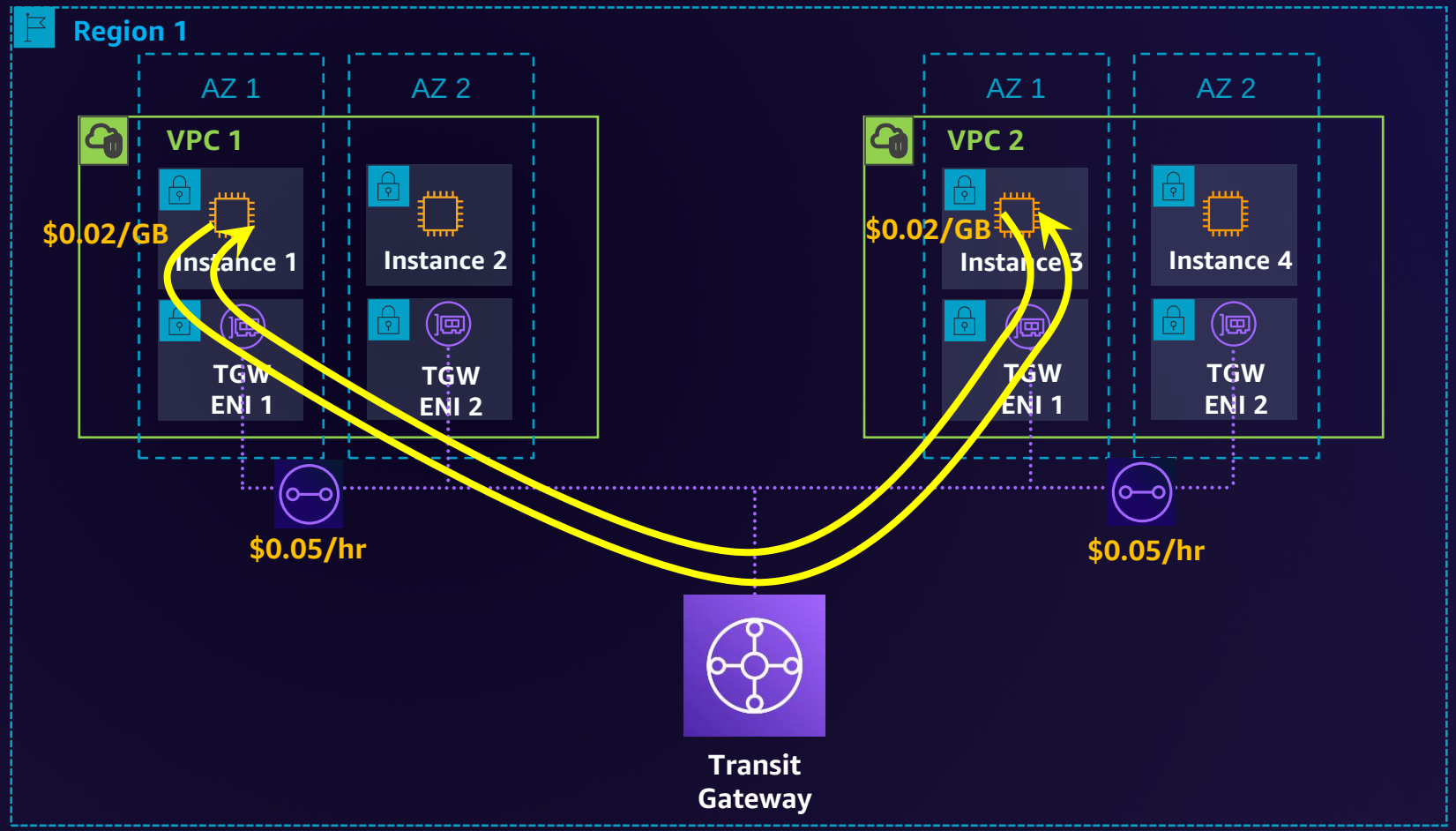


Two components

1. Transit Gateway, attachment hourly charge
2. Data processing, per-gigabyte charge

https://aws.amazon.com/transit-gateway/pricing/

Transit Gateway data transfer same Region

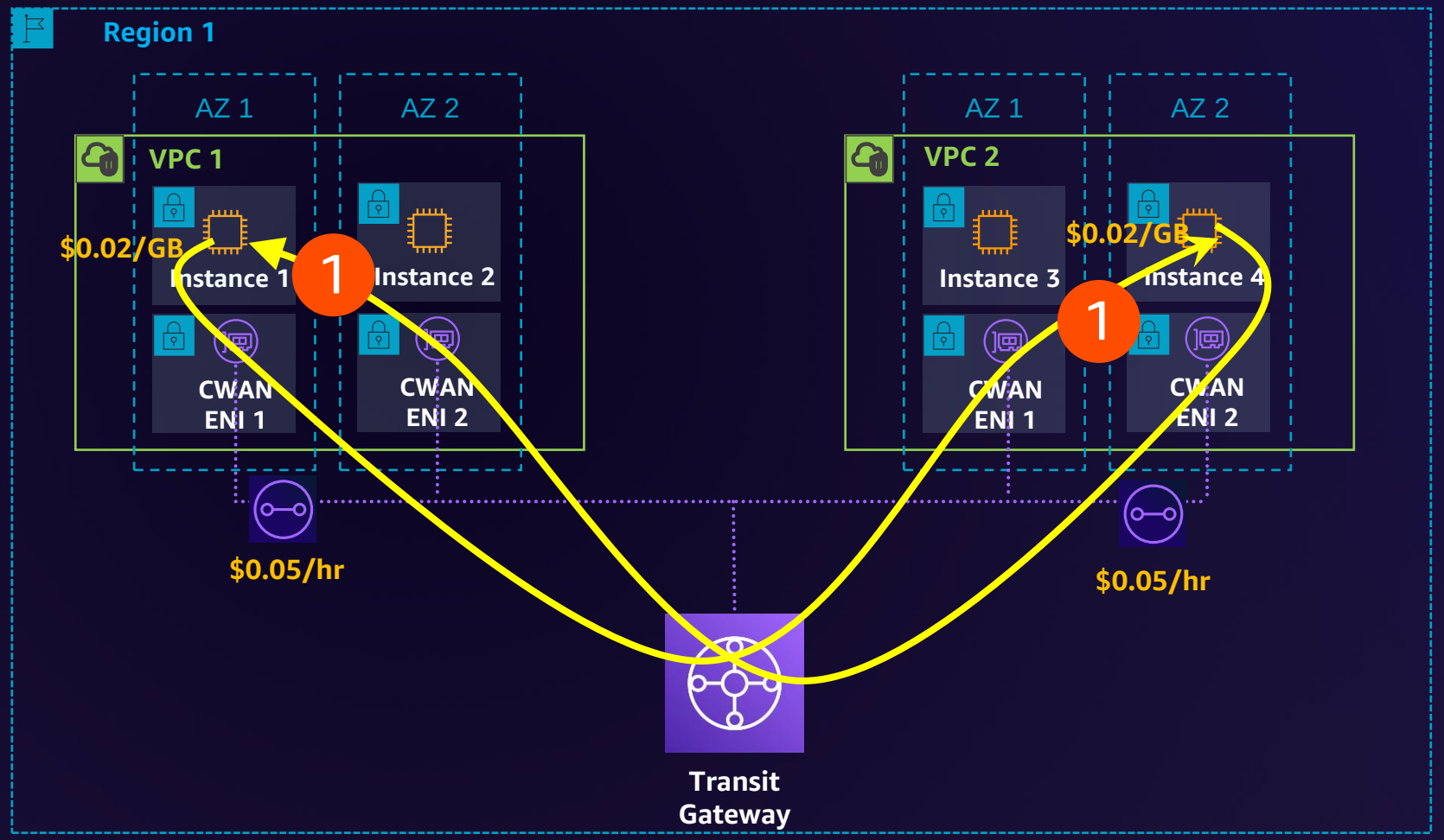


Instance 1 sending 1 gigabyte of data to Instance 3 and Instance 3 responding back with 1 gigabyte

Data processing: $0.04
- VPC 1 owner charged $0.02/GB
- VPC 2 owner charged $0.02/GB

Hourly charges: $.10/hr
- VPC 1 owner charged $0.05/hr
- VPC 2 owner charged $0.05/hr

Transit Gateway – Data transfer same Region cross-AZ



Instance 1 sending 1 gigabyte of data to Instance 3 and Instance 3 responding back with 1 gigabyte

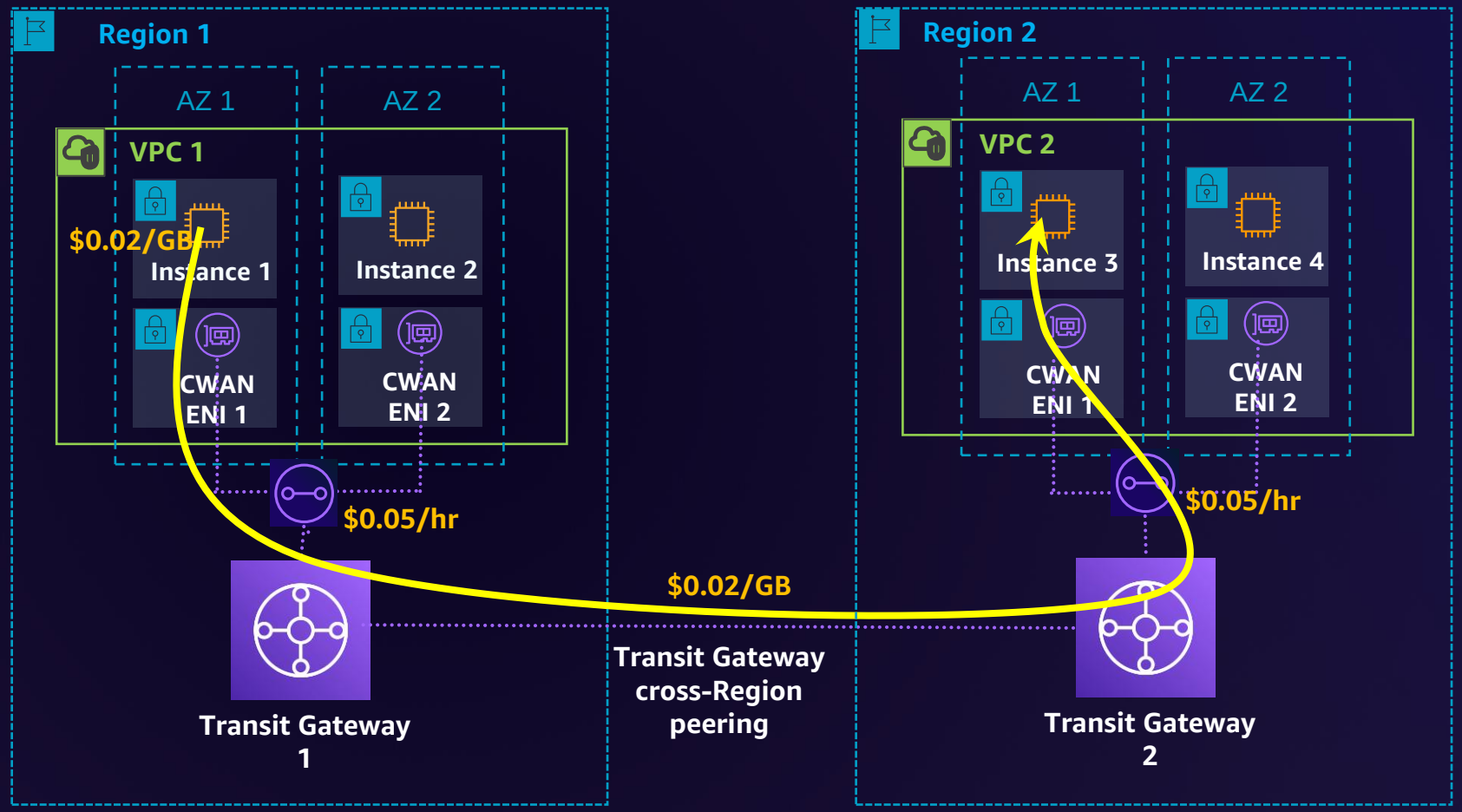
Data processing: $0.04

- VPC 1 owner charged $0.02/GB
- VPC 2 owner charged $0.02/GB

Hourly charges: $.10/hr

- VPC 1 owner charged $0.05/hr
- VPC 2 owner charged $0.05/hr

Transit Gateway – Data transfer cross-Region



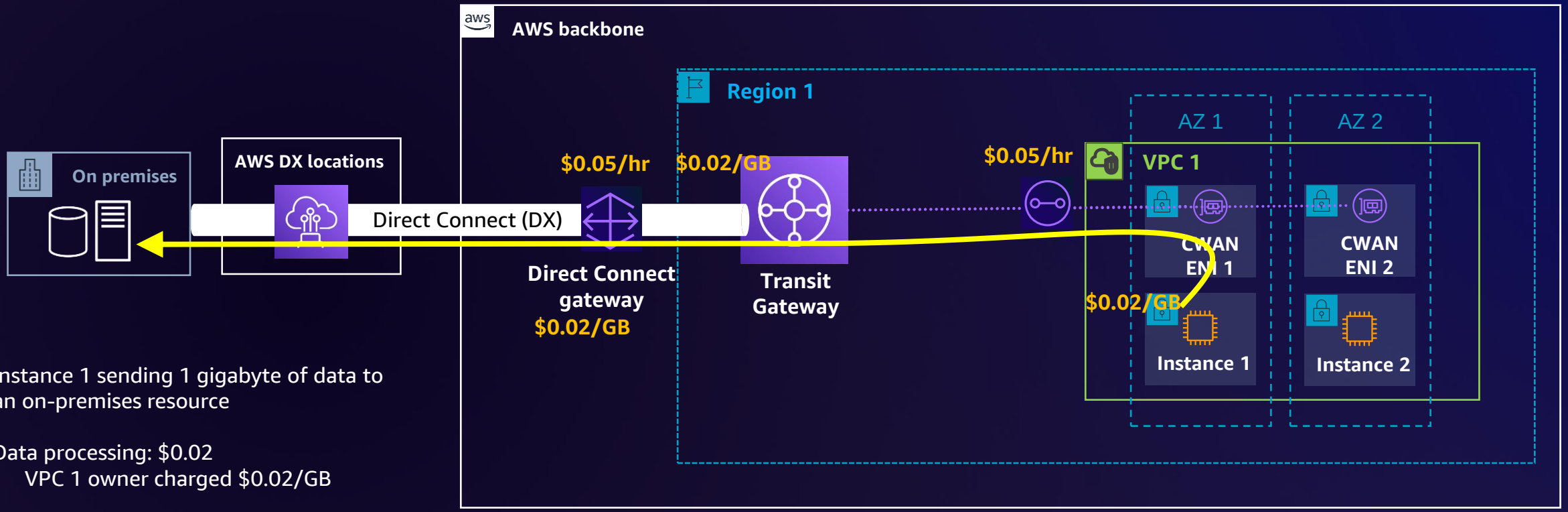
Instance 1 sending 1 gigabyte of data to Instance 3

Data processing
- VPC 1 owner charged $0.02/GB
- No data processing charge by Transit Gateway 2

Hourly charges
- VPC 1 owner charged $0.05/hr
- VPC 2 owner charged $0.05/hr

Cross-Region data transfer
- $0.02/GB outbound inter-Region data transfer charges

Transit Gateway – Data transfer to on premises



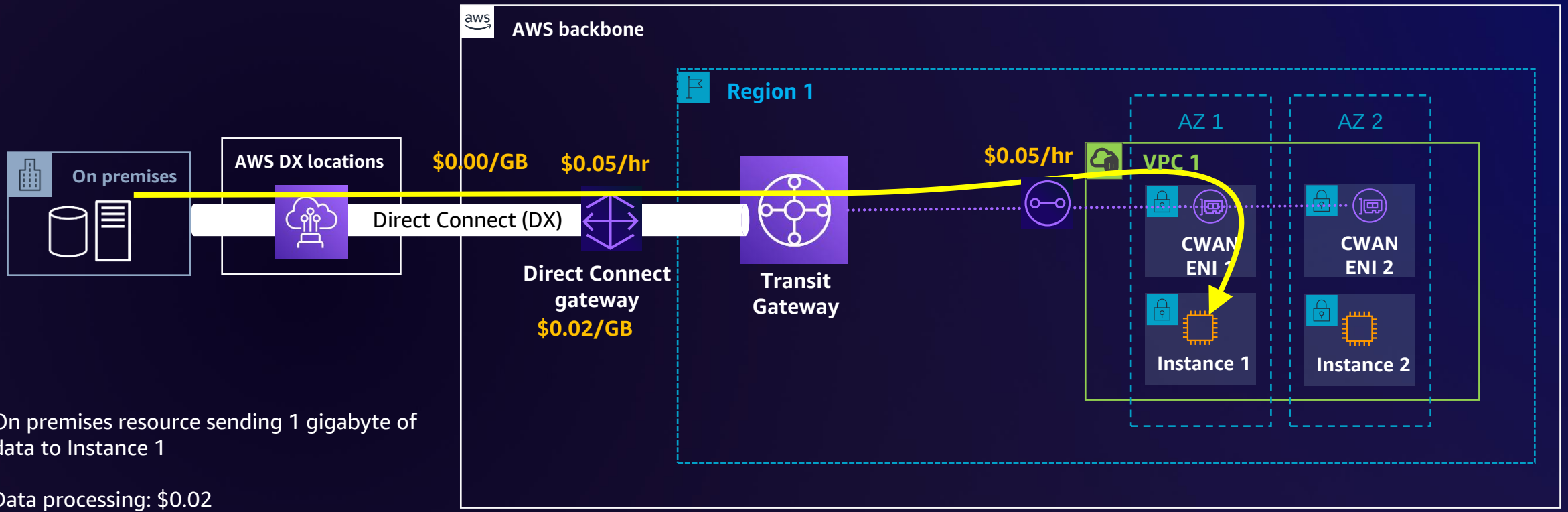
Instance 1 sending 1 gigabyte of data to an on-premises resource

Data processing: $0.02
- VPC 1 owner charged $0.02/GB

Hourly charges: $0.10
- VPC 1 owner charged $0.05/hr
- AWS Direct Connect gateway owner charged $0.05 for the Direct Connect gateway association/attachment

Data transfer OUT: $0.02
- AWS Direct Connect gateway owner charged $0.02/GB outbound inter-Region data transfer charges

Transit Gateway – Data transfer from on premises



On premises resource sending 1 gigabyte of data to Instance 1

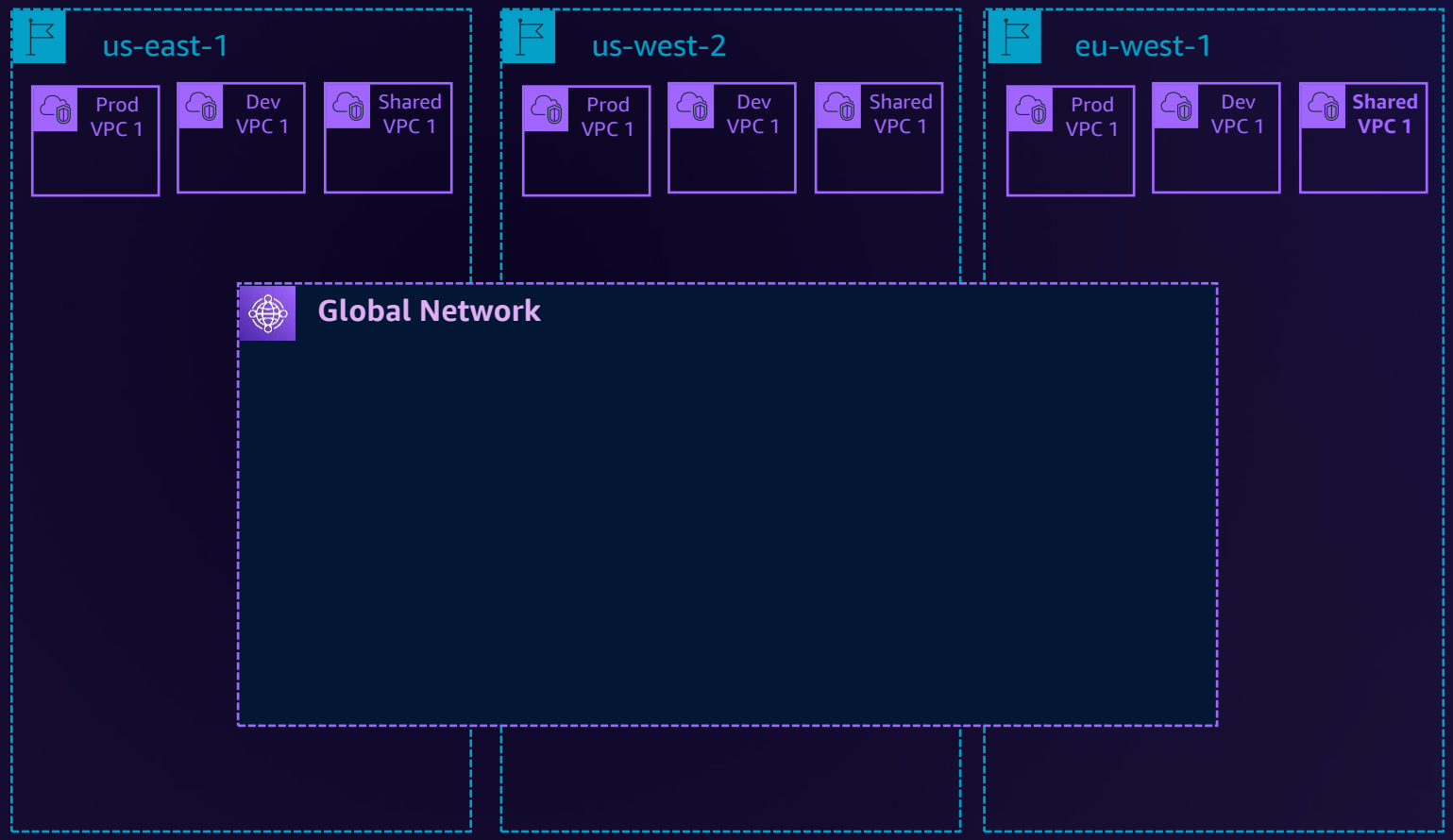
Data processing: $0.02
- AWS Direct Connect gateway owner charged $0.02/GB

Hourly charges: $0.10
- VPC 1 owner charged $0.05/hr
- AWS Direct Connect gateway owner charged $0.05 for the Direct Connect gateway association/attachment

Data transfer IN: $0.00
- There is no charge for Data Transfer IN

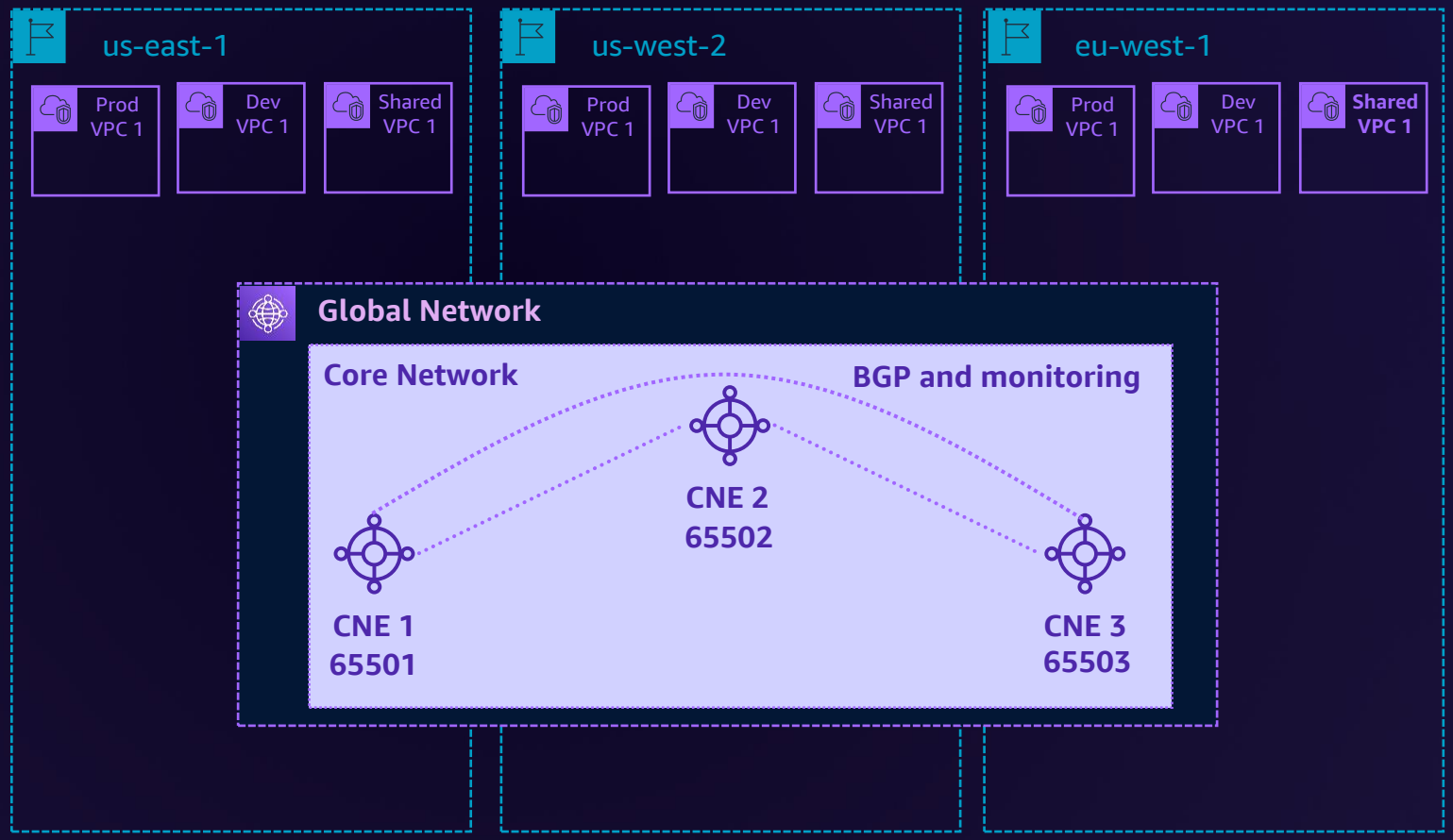
Network

Core network policy: Network configuration



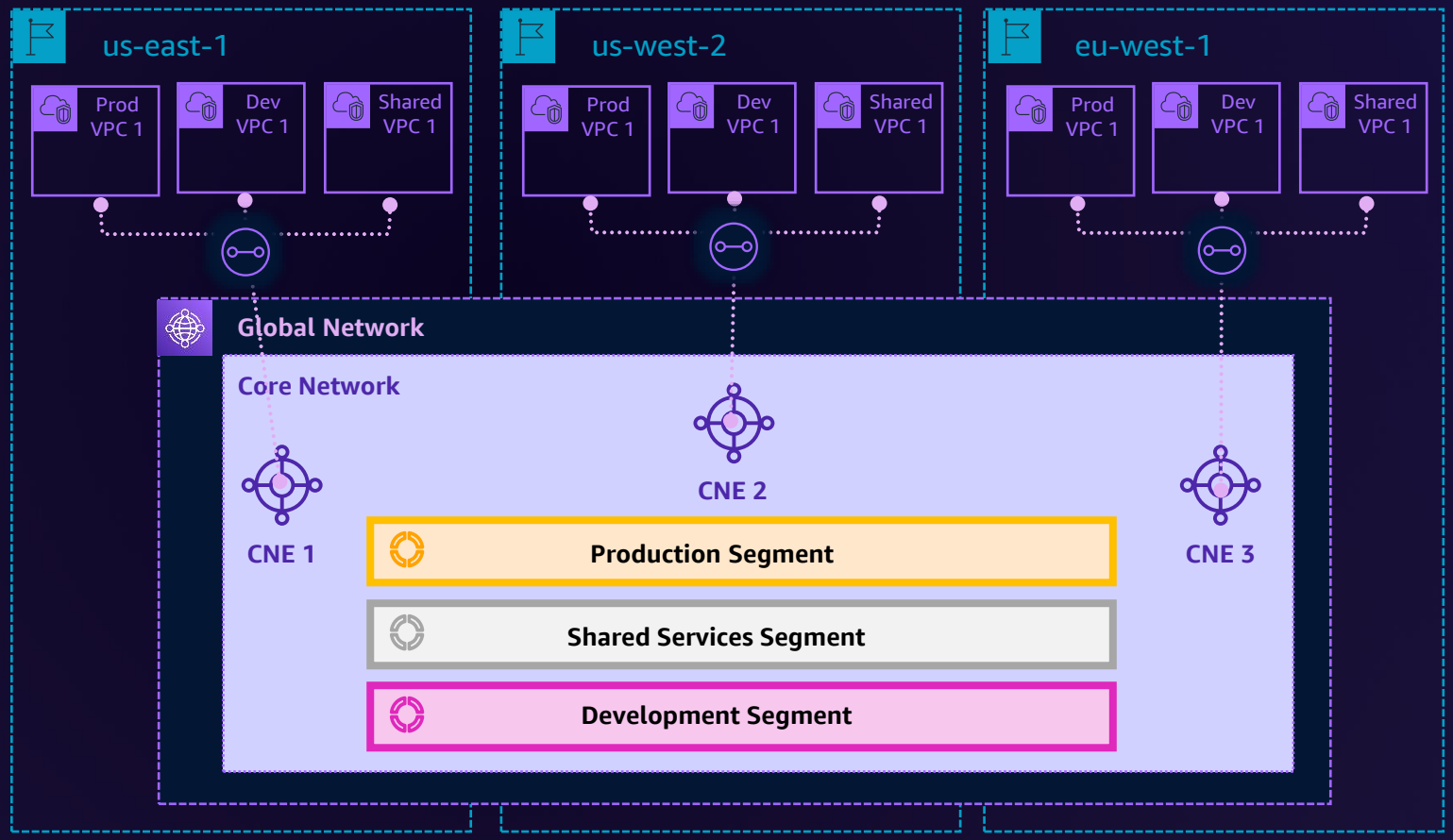

```
"core-network-configuration": {
    "vpn-ecmp-support": true,
    "asn-ranges": [
        "64512-65534"
    ],
    "edge-locations": [
        {
            "location": "us-east-1"
        },
        {
            "location": "us-west-2"
        },
        {
            "location": "eu-west-1"
        },
    ]
}
```

Core network policy: Network configuration



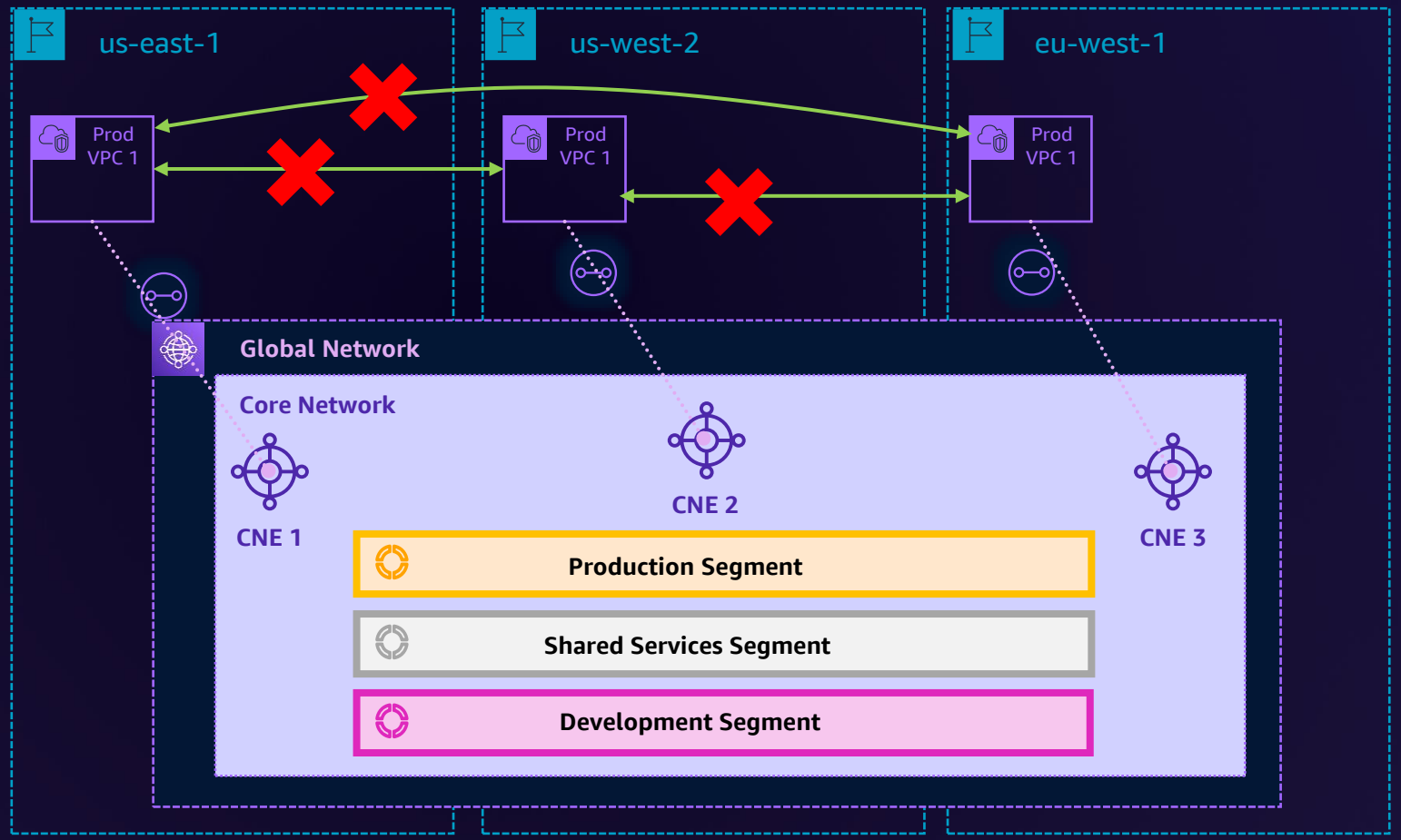

```
"core-network-configuration": {
    "vpn-ecmp-support": true,
    "asn-ranges": [
        "64512-65534"
    ],
    "edge-locations": [
        {
            "location": "us-east-1"
        },
        {
            "location": "us-west-2"
        },
        {
            "location": "eu-west-1"
        },
    ]
}
```

Core network policy: Segments



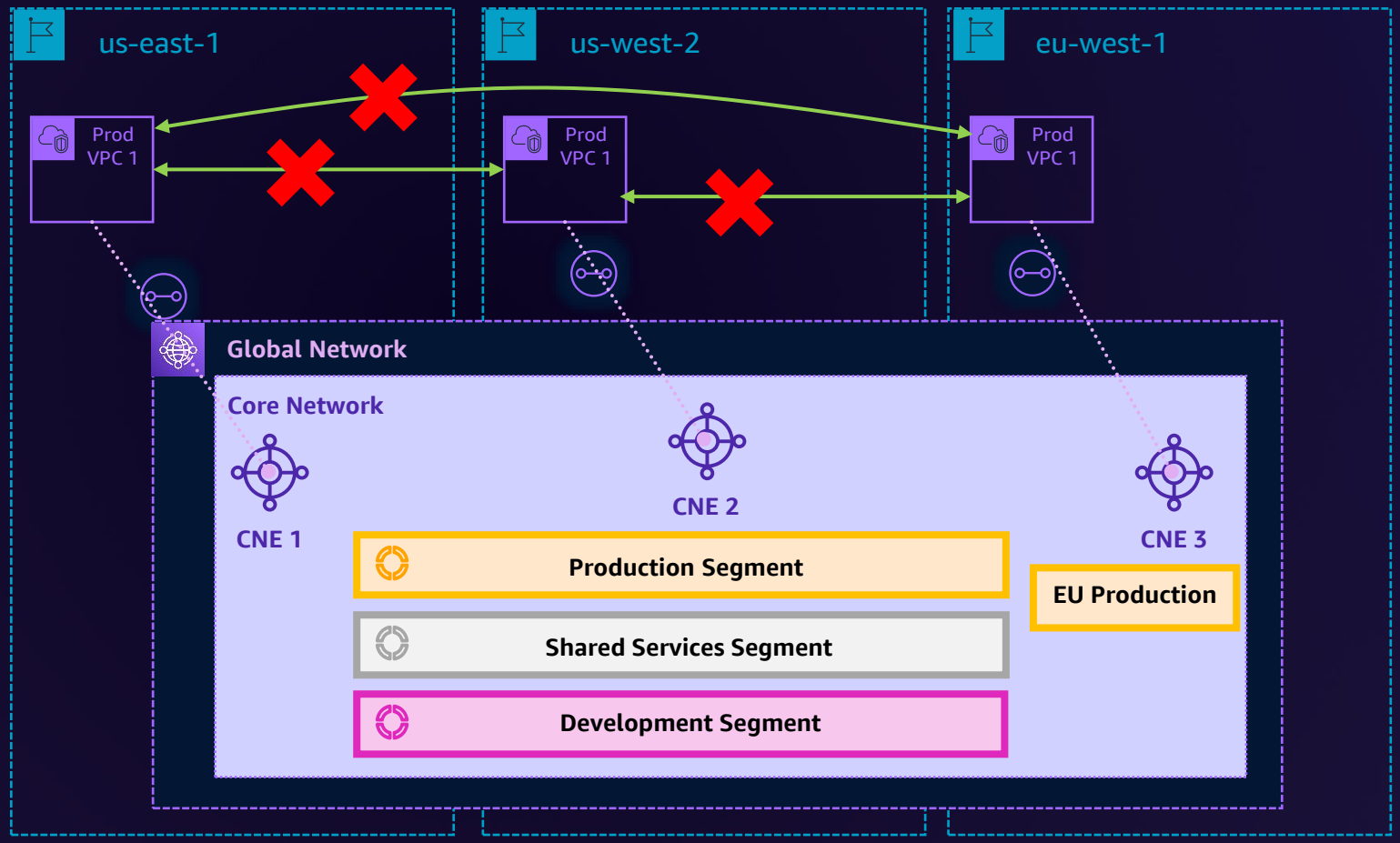

```
"segments": [
    {
        "name": "Production",
        "require-attachment-acceptance": false,
    },
    {
        "name": "Development",
        "require-attachment-acceptance": false
    },
    {
        "name": "Shared Service",
        "require-attachment-acceptance": false
    }
]
```

Core network policy: Segments




```
"segments": [
    {
        "name": "Production",
        "require-attachment-acceptance": false,
        "isolate-attachments": true
    },
    {
        "name": "Development",
        "require-attachment-acceptance": false
    },
    {
        "name": "Shared Service",
        "require-attachment-acceptance": false
    }
]
```

Core network policy: Segments

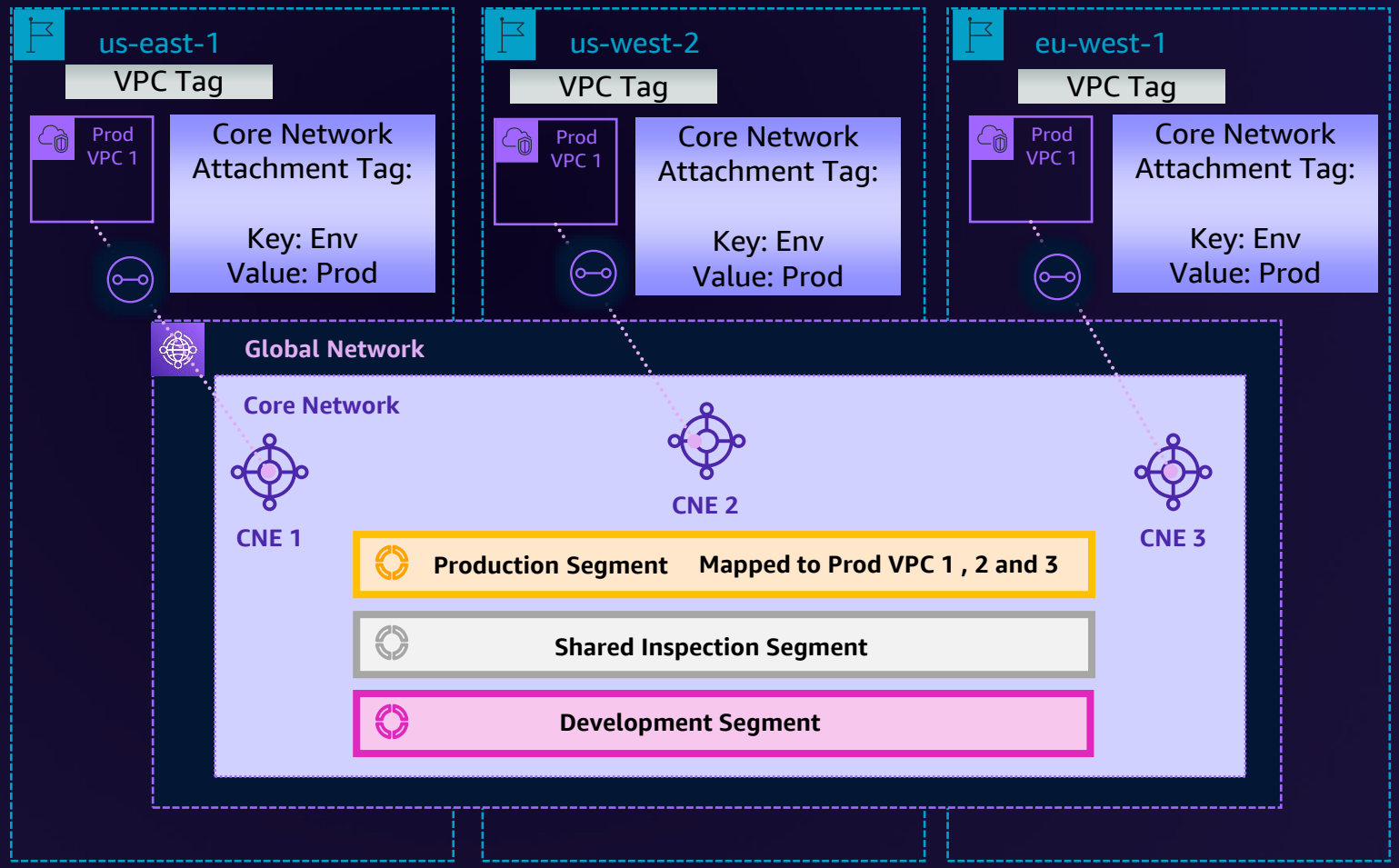



```
"segments": [
  {
    "name": "Production",
    "require-attachment-acceptance": false,
    "isolate-attachments": true
  },
  {
    "name": "Development",
    "require-attachment-acceptance": false
  },
  {
    "name": "Shared Service",
    "require-attachment-acceptance": false
  },
  {
    "name": "EU Production",
    "edge-locations": [
      "eu-west-1"
    ]
    "require-attachment-acceptance": false
  }
]
```

Core network policy: Attachment policies

VPC owner
- Creates attachment request
- Tags the attachment request

VPC tags are not evaluated



AWS Cloud WAN owner
- Policy maps tags to segments
- Can also use metadata, e.g.: vpc-id

```
"attachment-policies": [
  {
    "rule-number": 100,
    "conditions": [
      {
        "type": "tag-value",
        "operator": "equals",
        "key": "Env",
        "value": "Prod"
      }
    ],
    "action": {
    "association-method": "constant",
    "segment": "Prod"
    }
  }
]
```

Making changes to AWS Cloud WAN

Making changes to AWS Cloud WAN

1. Generate a policy

Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy 

Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy 

2. Change set

Making changes to AWS Cloud WAN

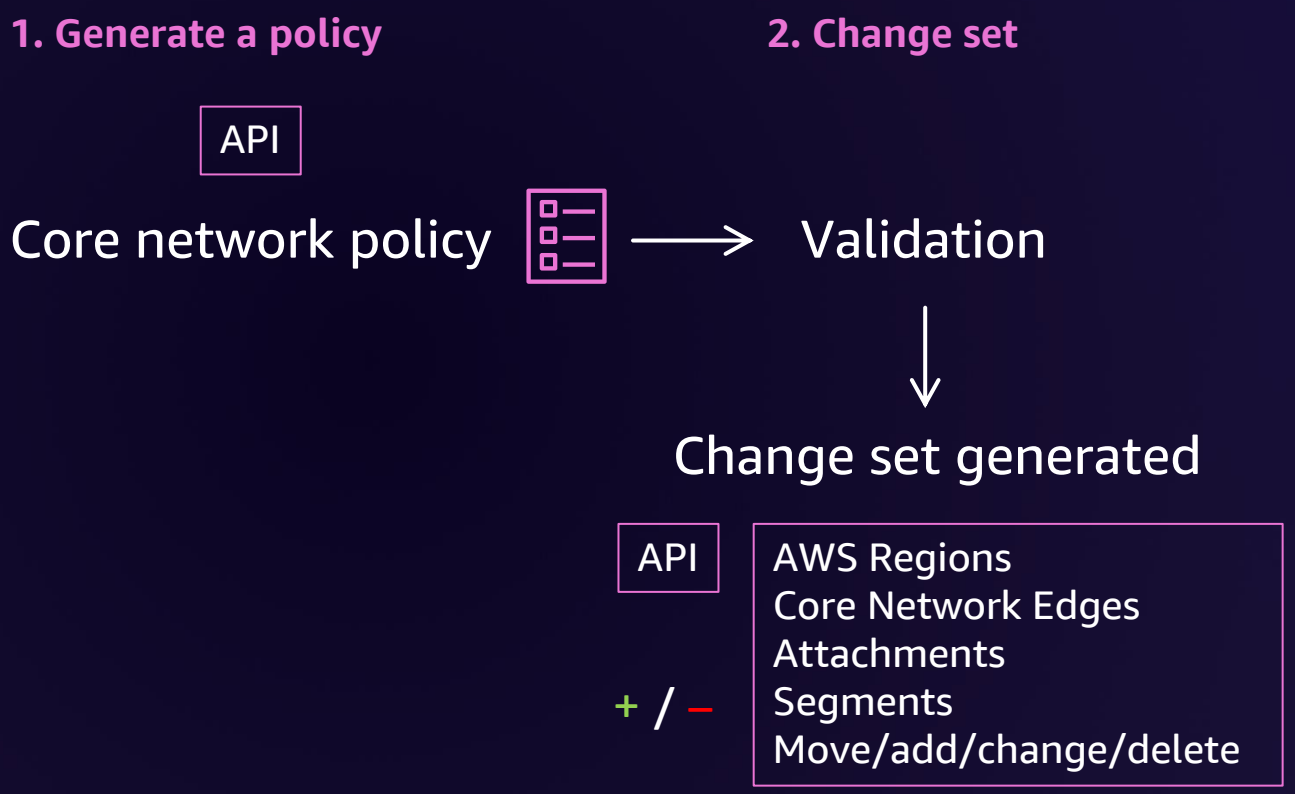
1. Generate a policy

API

Core network policy  Validation

2. Change set

Making changes to AWS Cloud WAN



Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

2. Change set

Validation

Change set generated

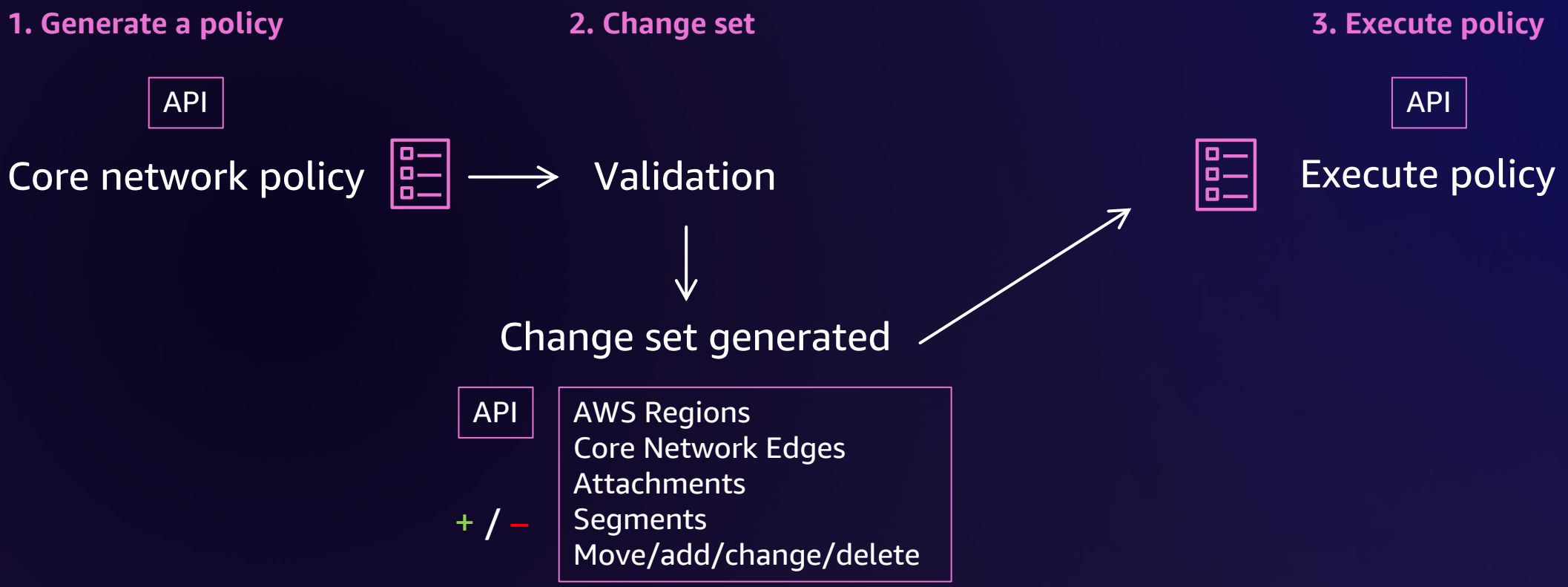
API

\+ / –

AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

3. Execute policy

Making changes to AWS Cloud WAN



Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

2. Change set

Validation

Change set generated

API

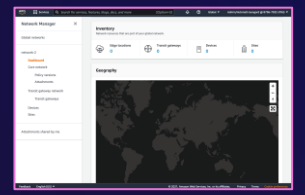
\+ / –

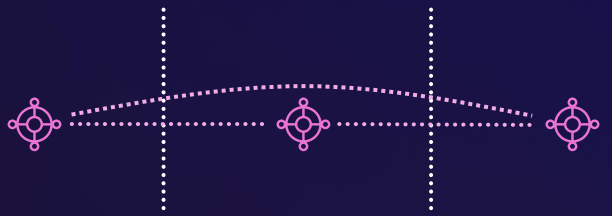
AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

3. Execute policy

API

Execute policy





Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

2. Change set

Validation

Change set generated

API

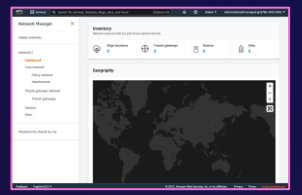
\+ / –

AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

3. Execute policy

API

Execute policy



Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

2. Change set

Validation

Change set generated

API

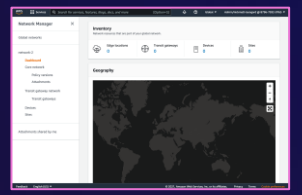
\+ / –

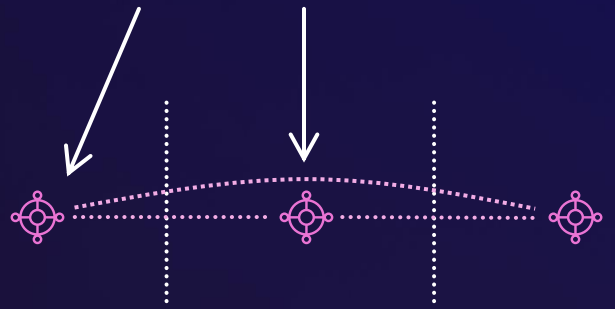
AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

3. Execute policy

API

Execute policy





Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

2. Change set

Validation

Change set generated

API

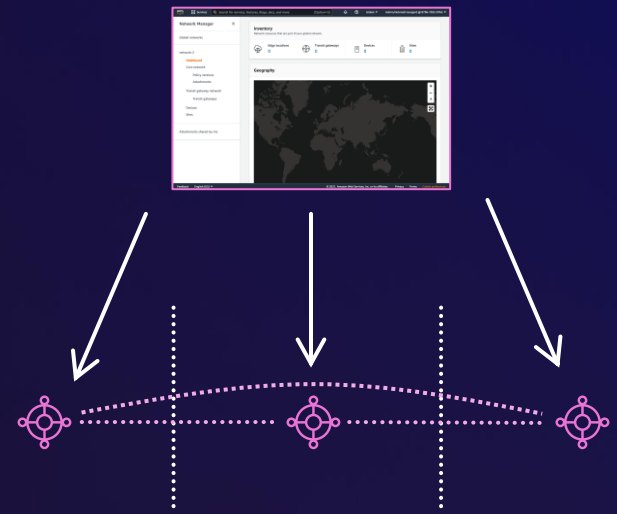
\+ / –

AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

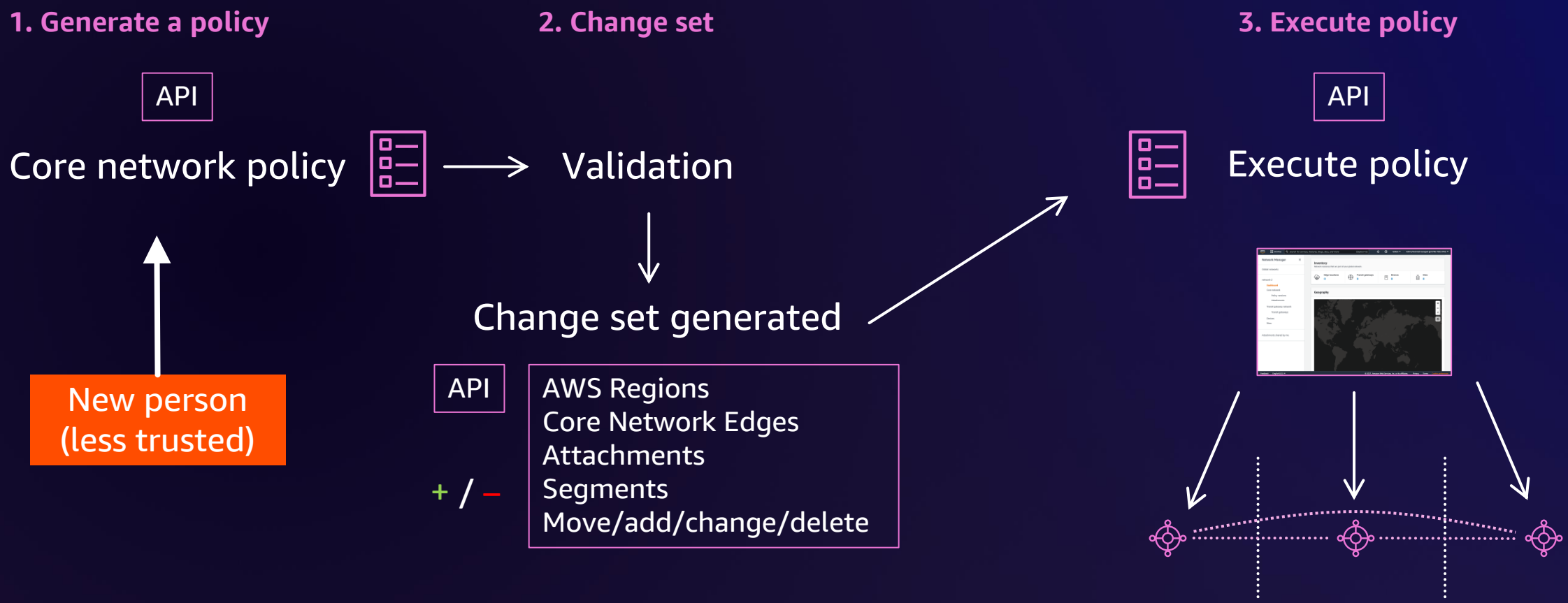
3. Execute policy

API

Execute policy



Making changes to AWS Cloud WAN



Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

New person
(less trusted)

2. Change set

Validation

Change set generated

API

AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

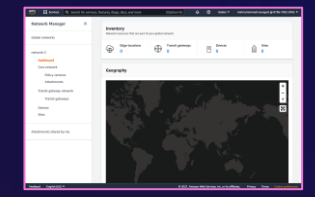
+ / –

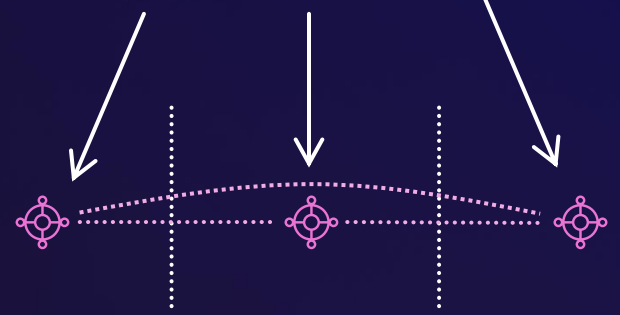
Change
advisory
board

3. Execute policy

API

Execute policy





Making changes to AWS Cloud WAN

1. Generate a policy

API

Core network policy

New person
(less trusted)

2. Change set

Validation

Change set generated

API

AWS Regions
Core Network Edges
Attachments
Segments
Move/add/change/delete

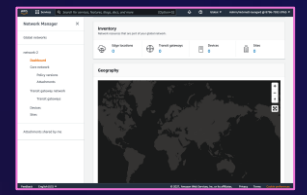
+ / –

Change
advisory
board

3. Execute policy

API

Execute policy



Admin
(trusted)