

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various shades of blue and cyan, creating a sunburst effect that spreads across the right half of the image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Automating cloud networking with Cloud Network Controller and Terraform

A different approach

Marina Ferreira
Solutions Engineer, DC and Cloud

X @_marinalf
DEVNET-2280

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

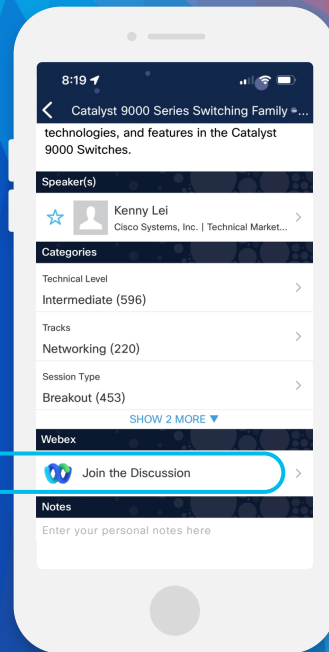
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



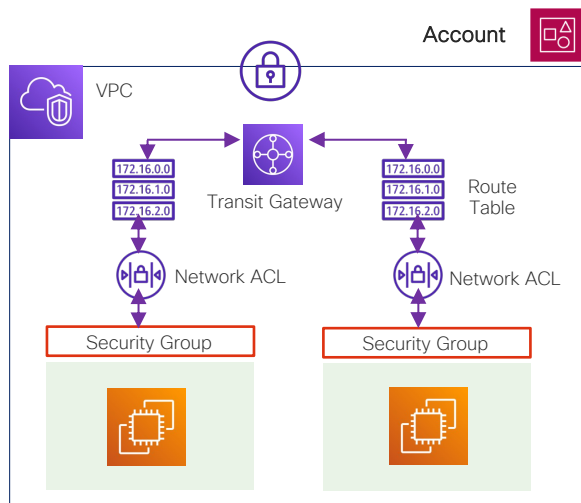
<https://ciscolive.ciscoevents.com/ciscolivebot/DEVNET-2280>

Agenda

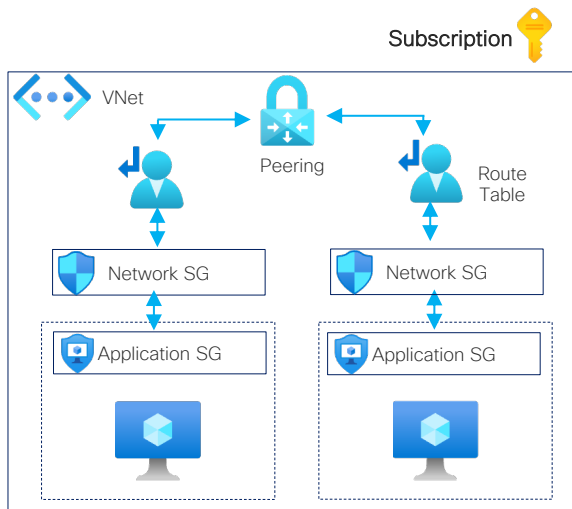
- Cloud Networking Constructs
- Cloud Network Controller (CNC) Overview
 - Policy Model
 - Programmability Options
- High-Level Architecture: Azure
- Demo Use Cases
- What's New: Terraform Resources

Cloud Networking Constructs

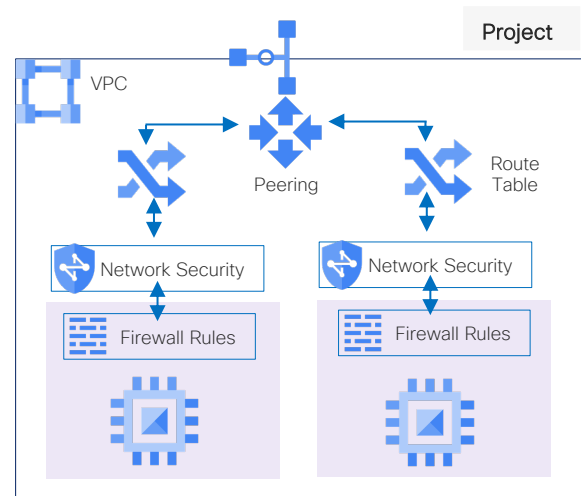
New Terminologies, Same Concepts



aws

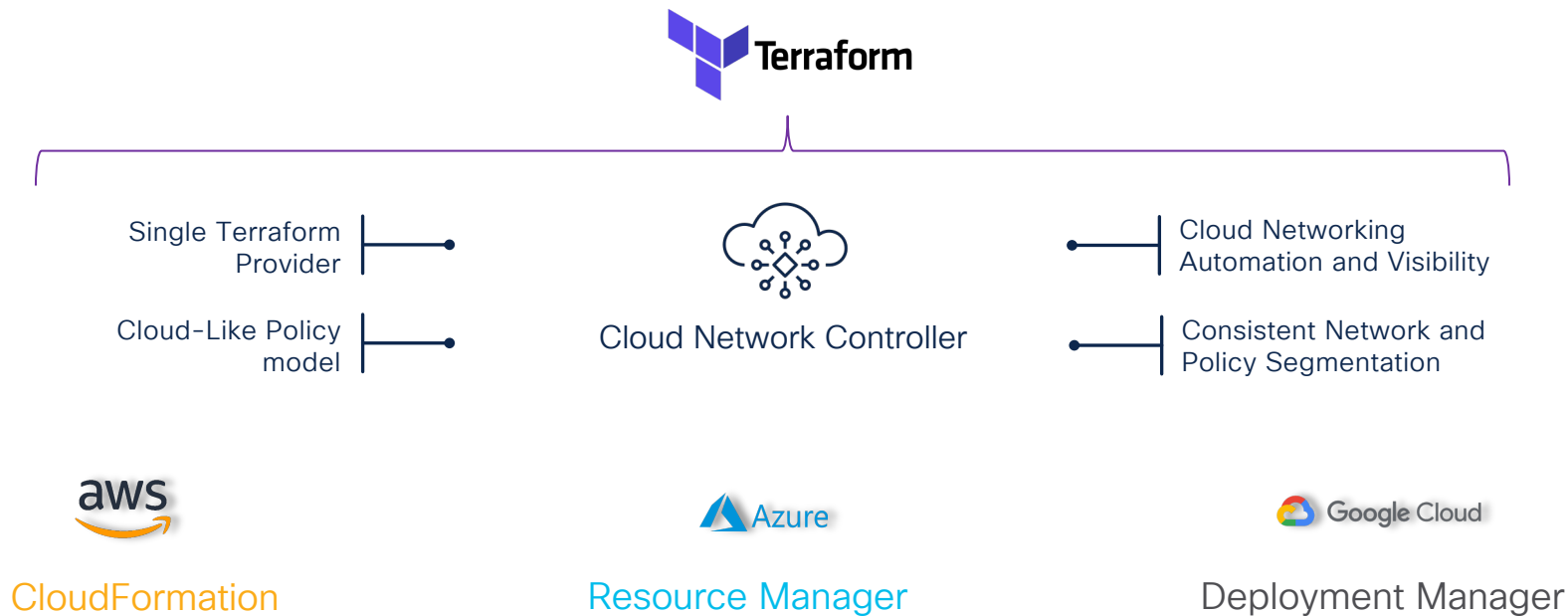


Azure

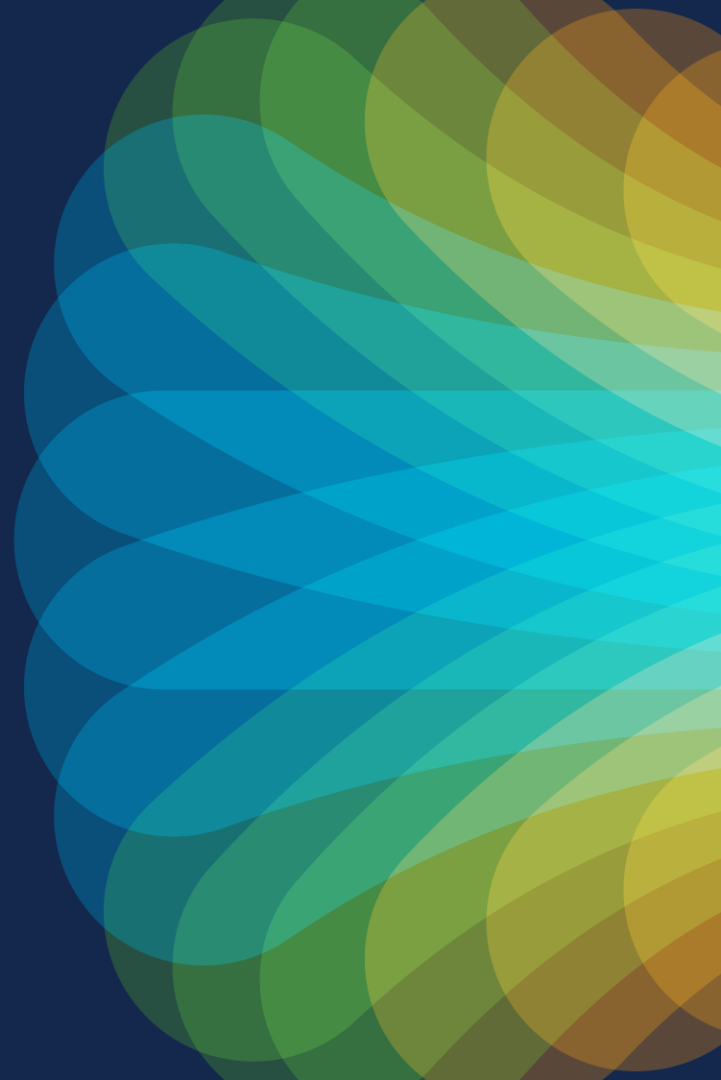


Google Cloud

Native Tools (Not Limited To)

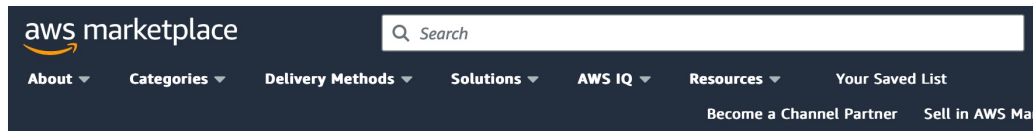
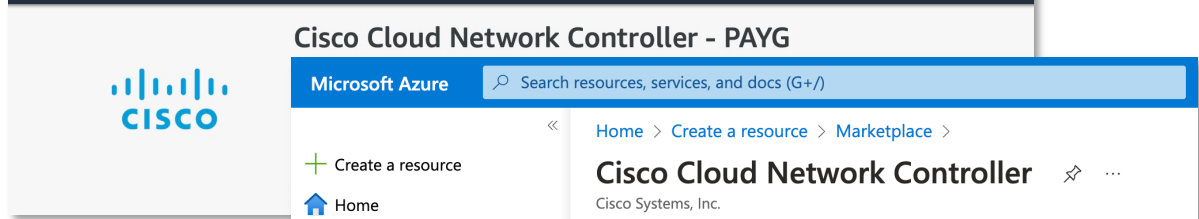
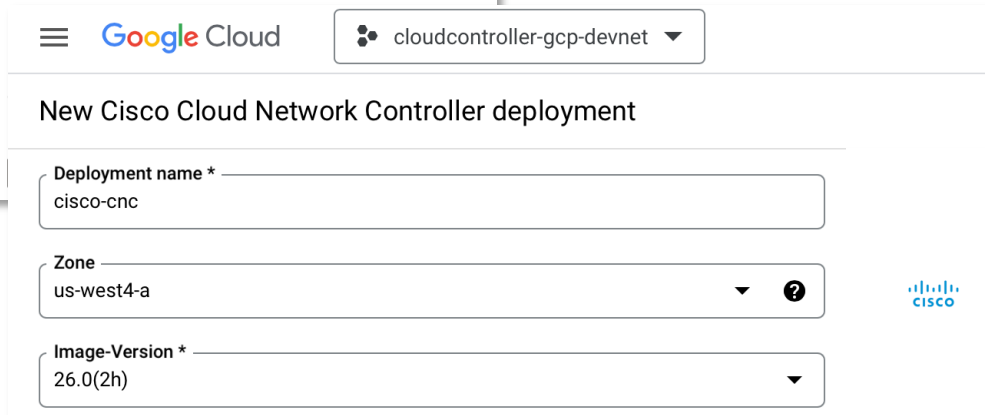


Cloud Network Controller Overview



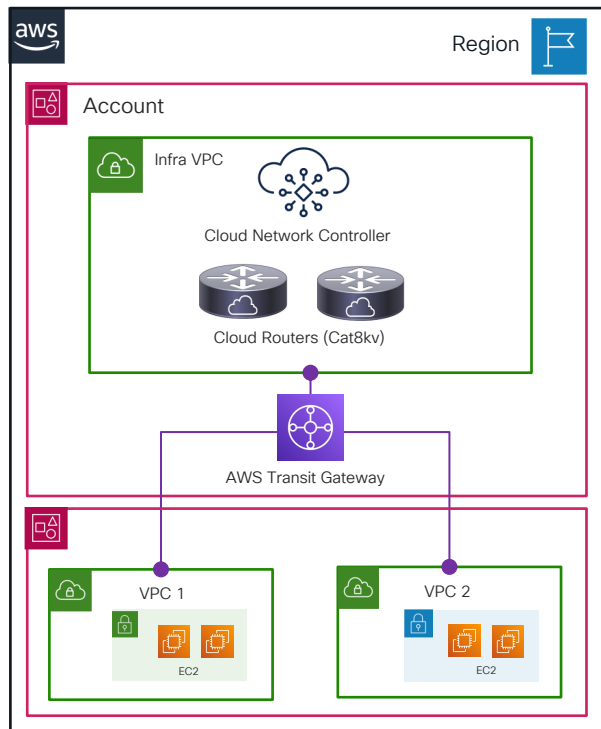
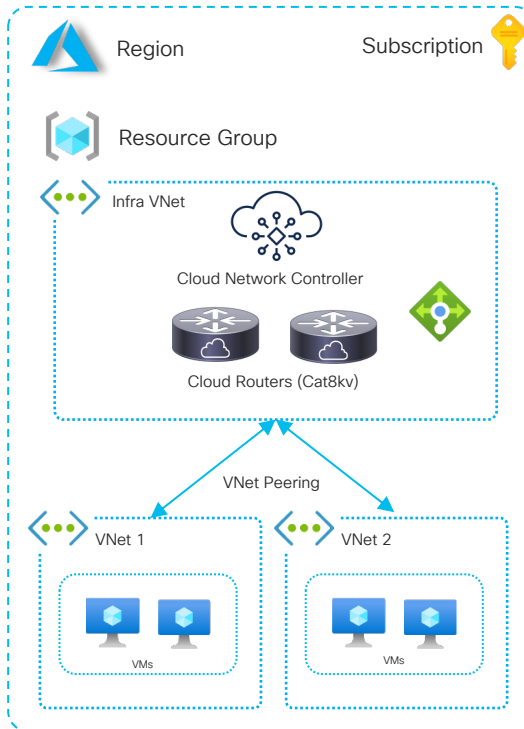
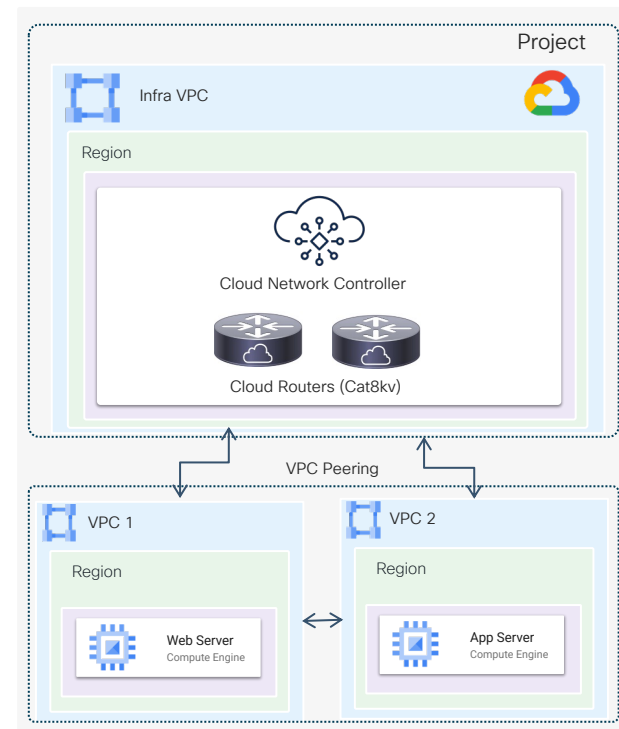
Cloud Network Controller

Deploying from the Marketplace



Cloud Network Controller

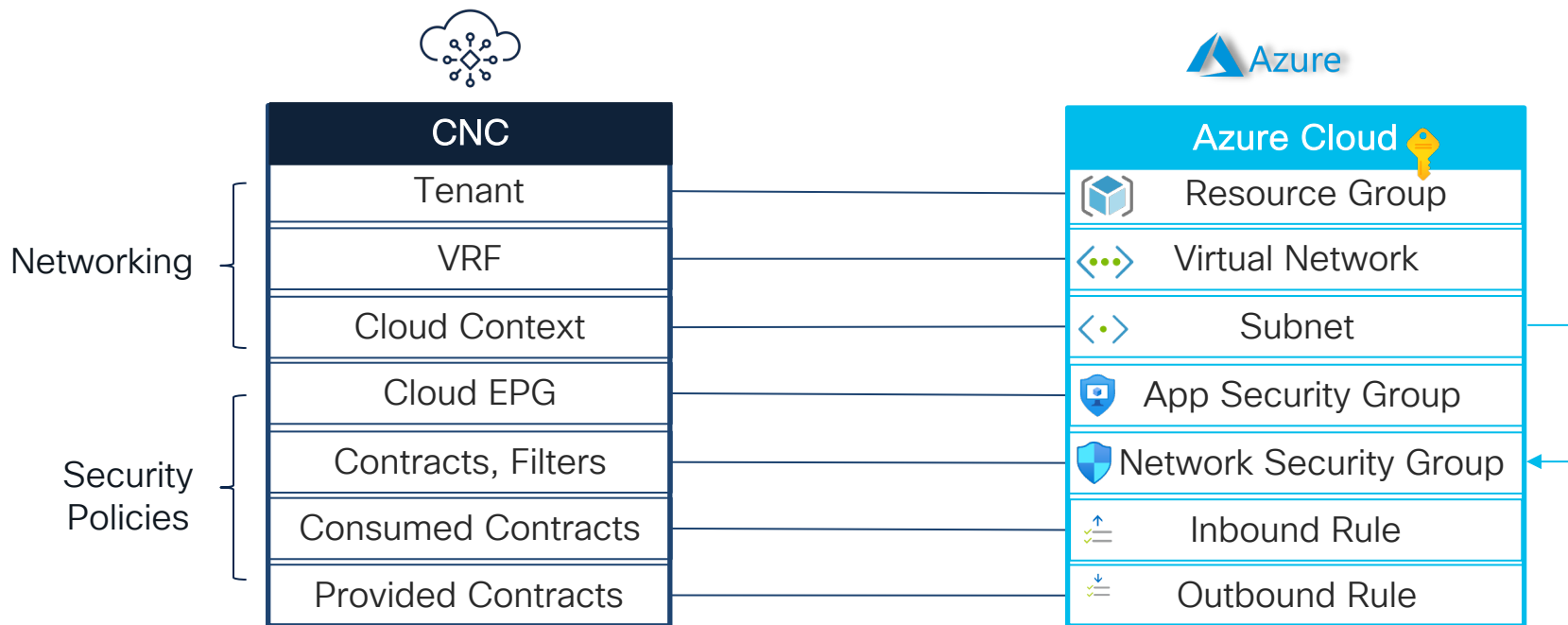
Solution Components



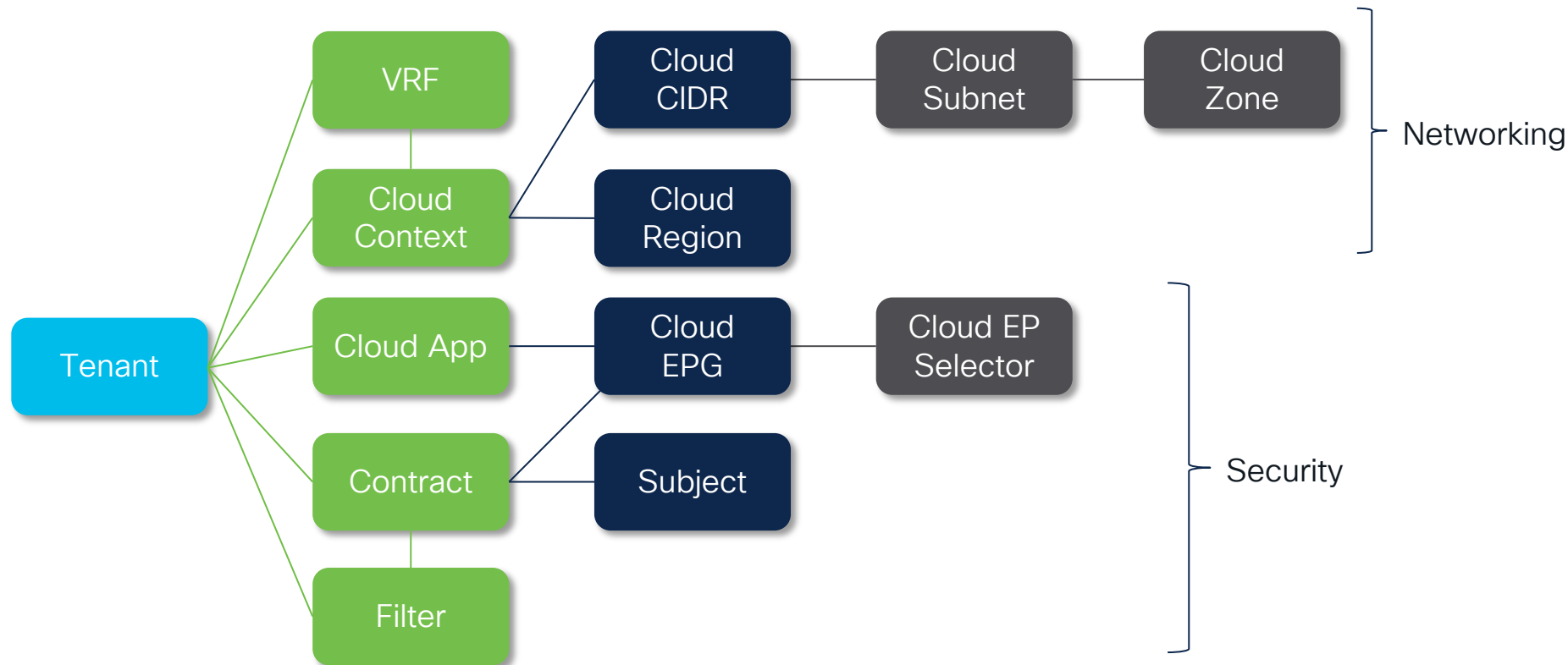
CNC Policy Model

Networking and Policy Translation

Cloud-like Policy Model



CNC Policy Model



Full Model: <https://developer.cisco.com/site/apic-mim-ref-api>

Programmability Options

CNC REST API

Interacting with the REST API

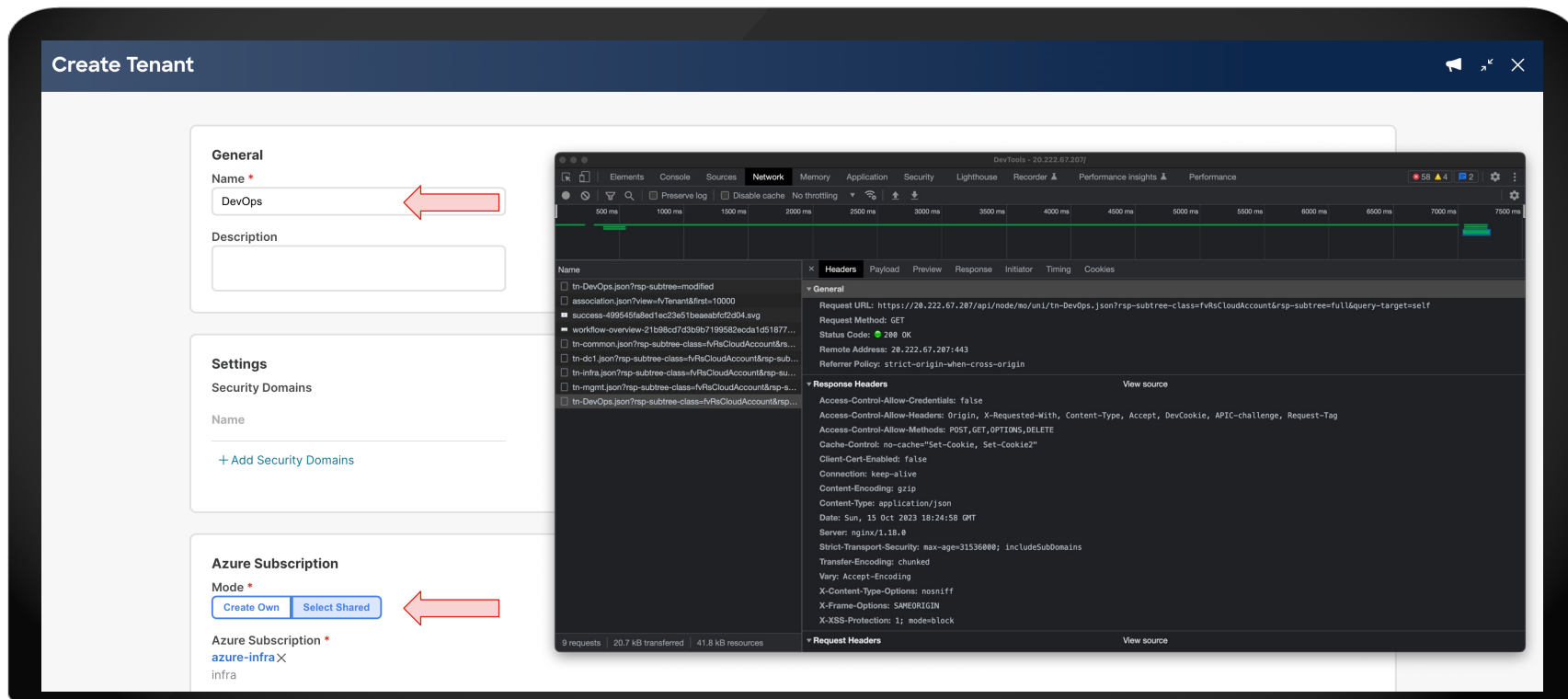
- There are several ways to interact with the CNC REST API
 - Graphical User Interface (GUI)
 - “Raw” API requests (e.g., via Postman)
 - Any programming language (JavaScript, Python, ...)
 - Ansible
 - Terraform



<https://{cnc-ip}/model-doc>

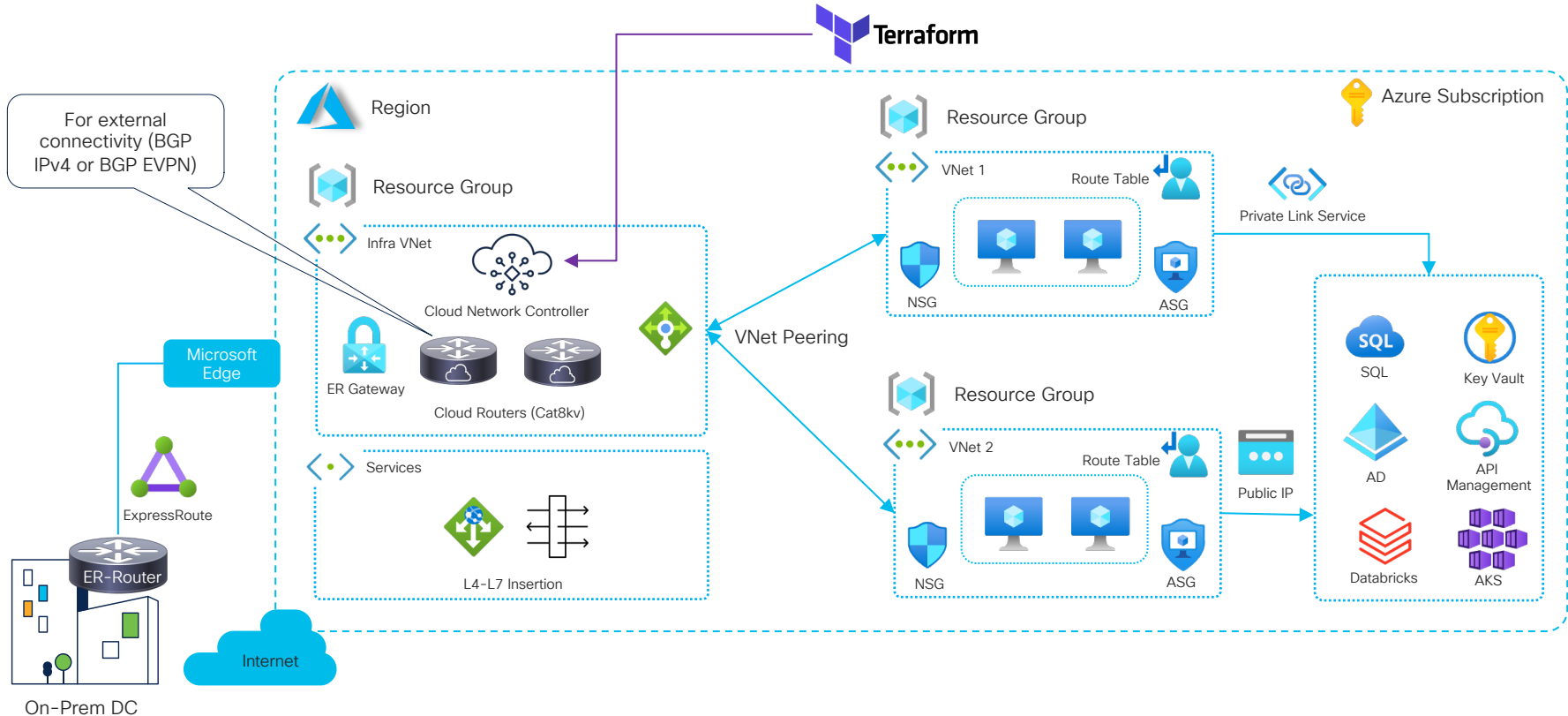
CNC REST API

API Inspector



High Level Architecture on Azure

High Level Architecture on Azure



Demo Use Cases



Git Repo

CNC & Terraform: Putting it Together

Building Blocks with Resources and Data Sources

provider.tf

```
terraform {
  required_providers {
    aci = {
      source = "cisco/devnet/aci"
      version = ">= 2.11.1"
    }
  }
  required_version = ">= 1.2"
}

provider "aci" {
  username = var.username
  password = var.password
  url      = var.url
  insecure = true
}
```

variables.tf

```
variable "tenant_name" {
  default = "devnet"
}

variable "cloud_vendor" {
  default = "azure"
}

variable "vnet1_name" {
  default = "vnet-1"
}

variable "vnet1_cidr" {
  default = "10.100.0.0/21"
}

variable "vnet1_region1" {
  default = "australiaeast"
}
```

main.tf

```
resource "aci_tenant" "tenant1" {
  name = var.tenant_name
}

resource "aci_tenant_to_cloud_account" "cloud_acct_ten1" {
  tenant_dn      = aci_tenant.tenant1.id
  cloud_account_dn = data.aci_cloud_account.aci_cloud_account_infra.id
}

resource "aci_vrf" "vnet1" {
  tenant_dn = aci_tenant.tenant1.id
  name      = var.vnet1_name
}

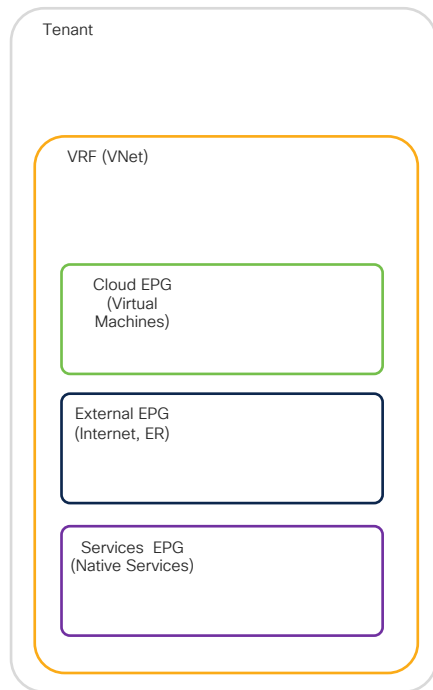
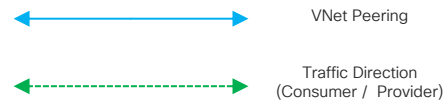
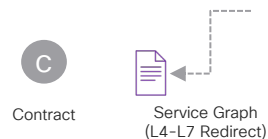
resource "aci_cloud_context_profile" "ctx_vnet1" {
  tenant_dn      = aci_tenant.tenant1.id
  name           = var.ctx_vnet1
  primary_cidr   = var.vnet1_cidr
  region         = var.vnet1_region1
  cloud_vendor   = var.cloud_vendor
  relation_cloud_rs_to_ctx = aci_vrf.vnet1.id
  hub_network    = "uni/tn-infra/gwrouterp-default" #Peering
}

resource "aci_cloud_subnet" "vnet1_subnets" {
  for_each      = var.vnet1_subnets
  cloud_cidr_pool_dn = data.aci_cloud_cidr_pool.vnet1_cidr.id
  name          = each.value.name
  ip            = each.value.ip
}
```

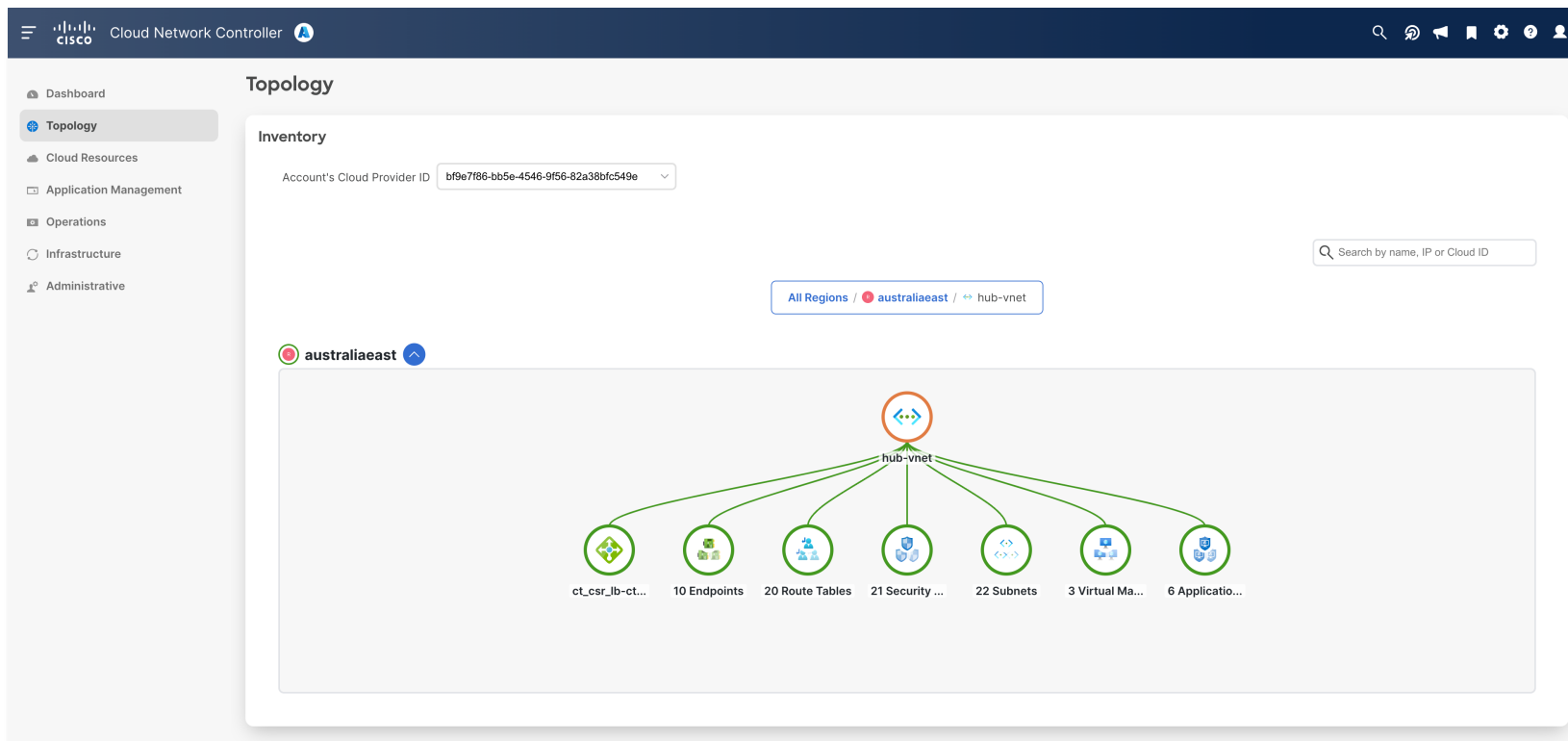
data_sources.tf

```
data "aci_cloud_account" "aci_cloud_account_infra" {
  tenant_dn = "uni/tn-infra"
  account_id = var.subscription_id
  vendor     = "azure"
}
```

CNC and Azure Icons

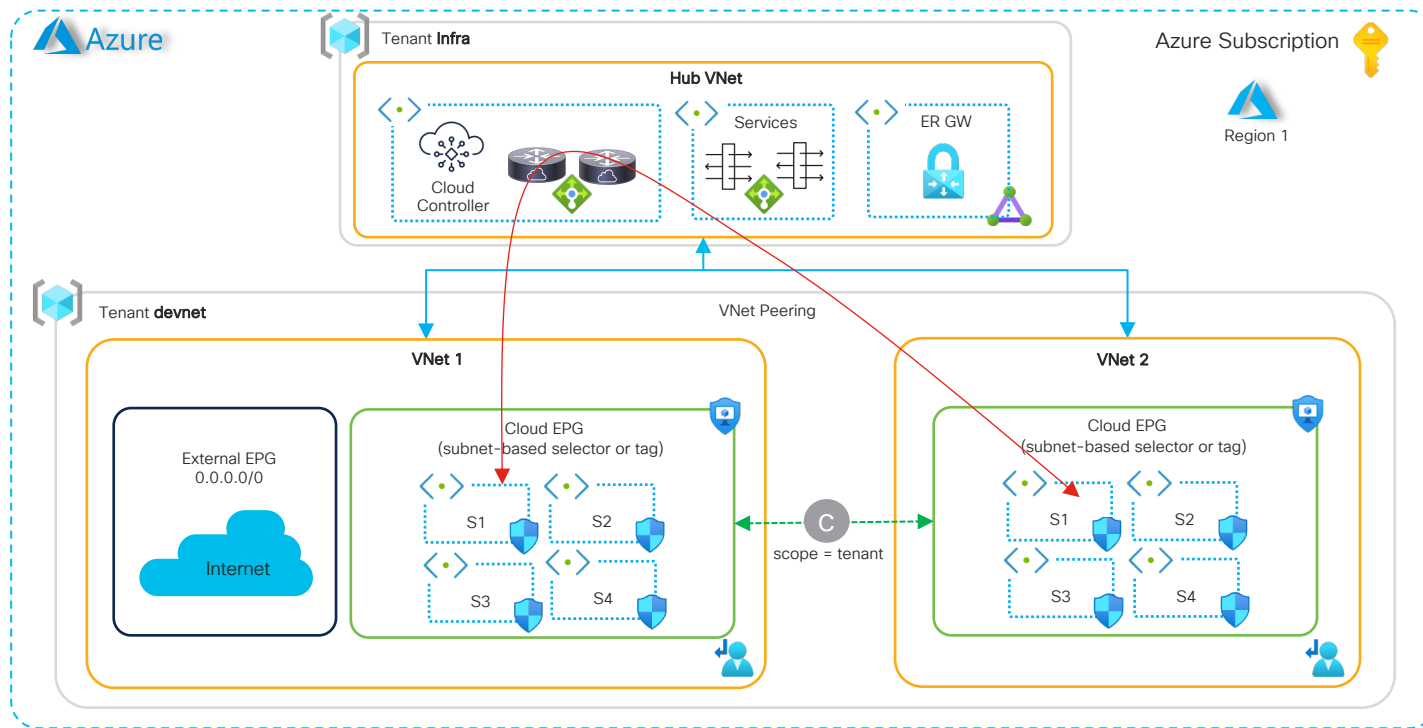


Topology View



Use Case 1: Inter-VNet Same Region

Spoke to Spoke Traffic

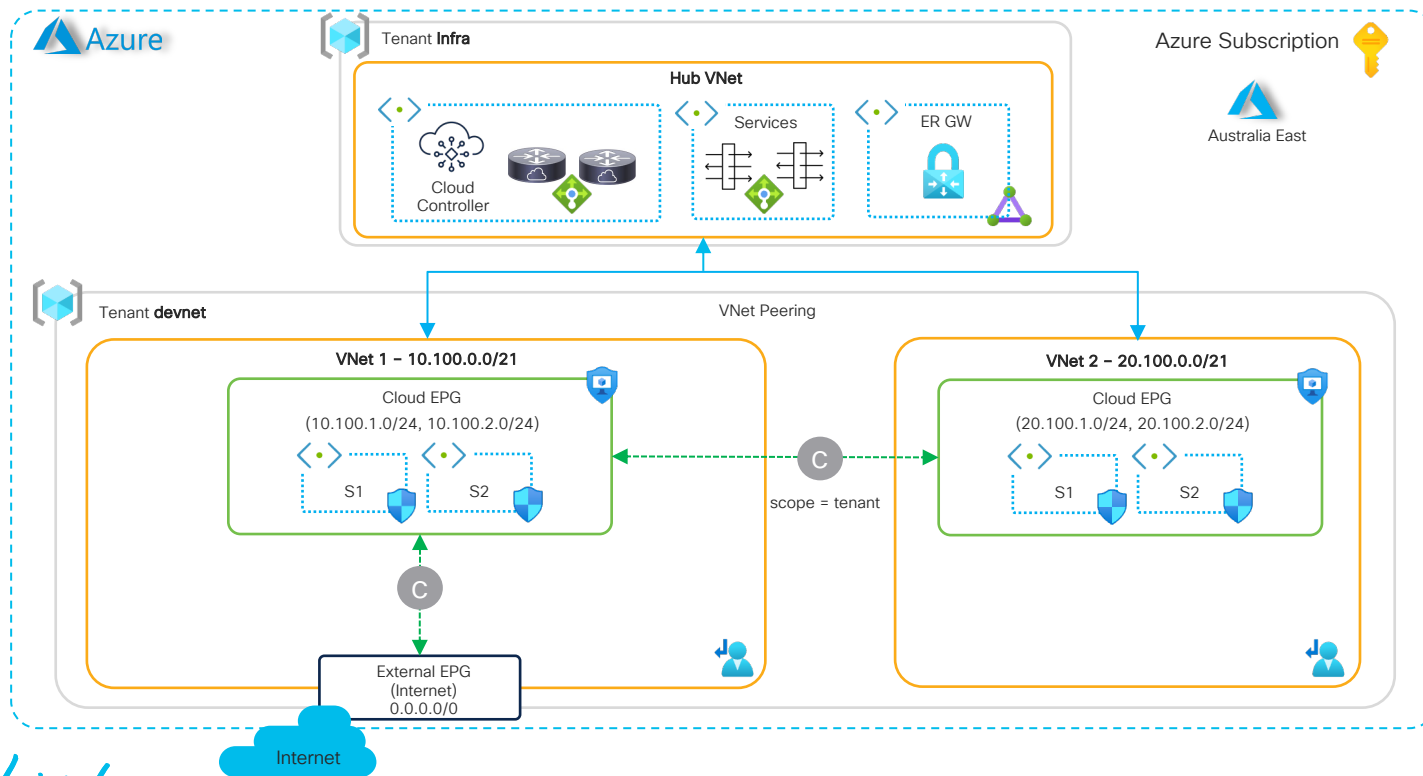




Git Repo

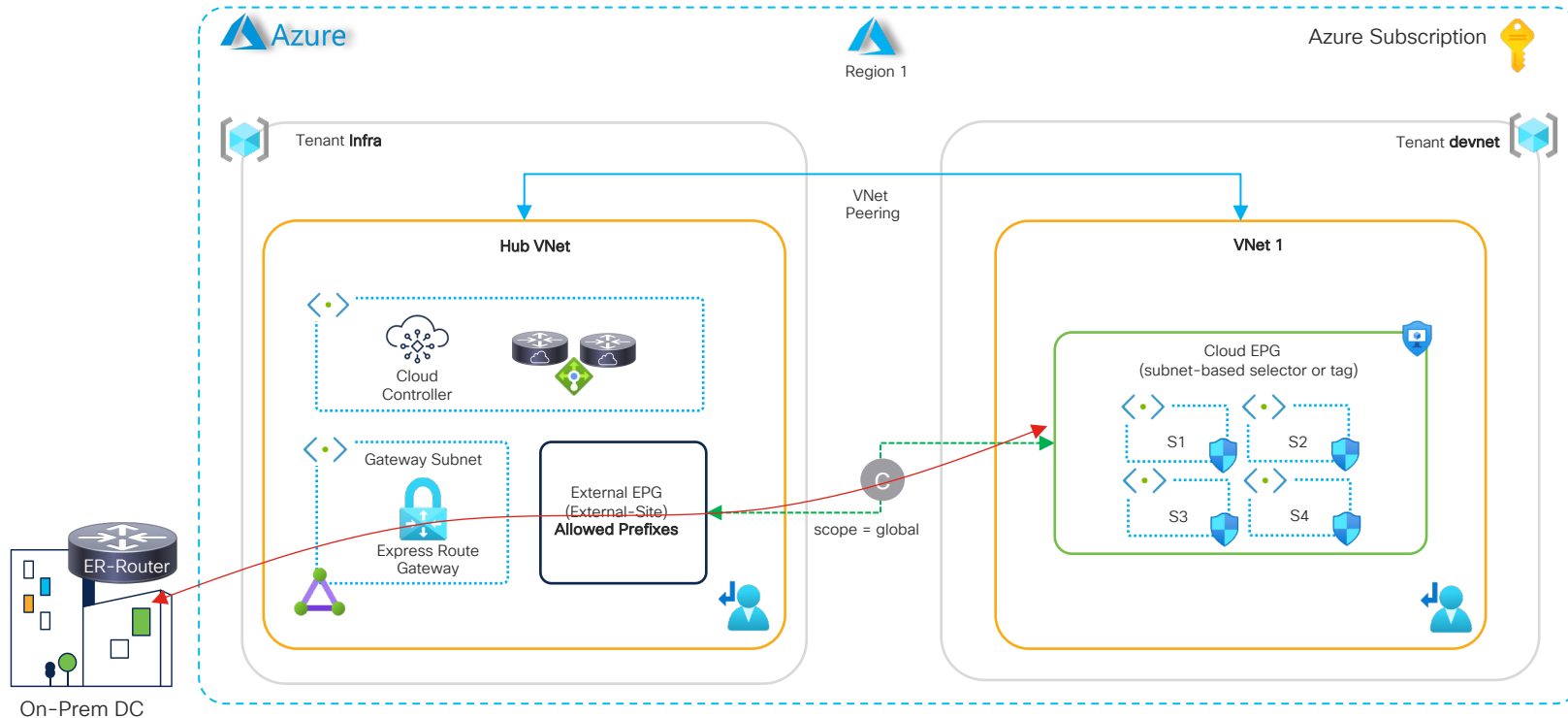
Demo 1: Inter-VNet Same Region

Spoke to Spoke Traffic



Use Case 2: Hub VNet with ER Gateway

To/From On-prem Traffic

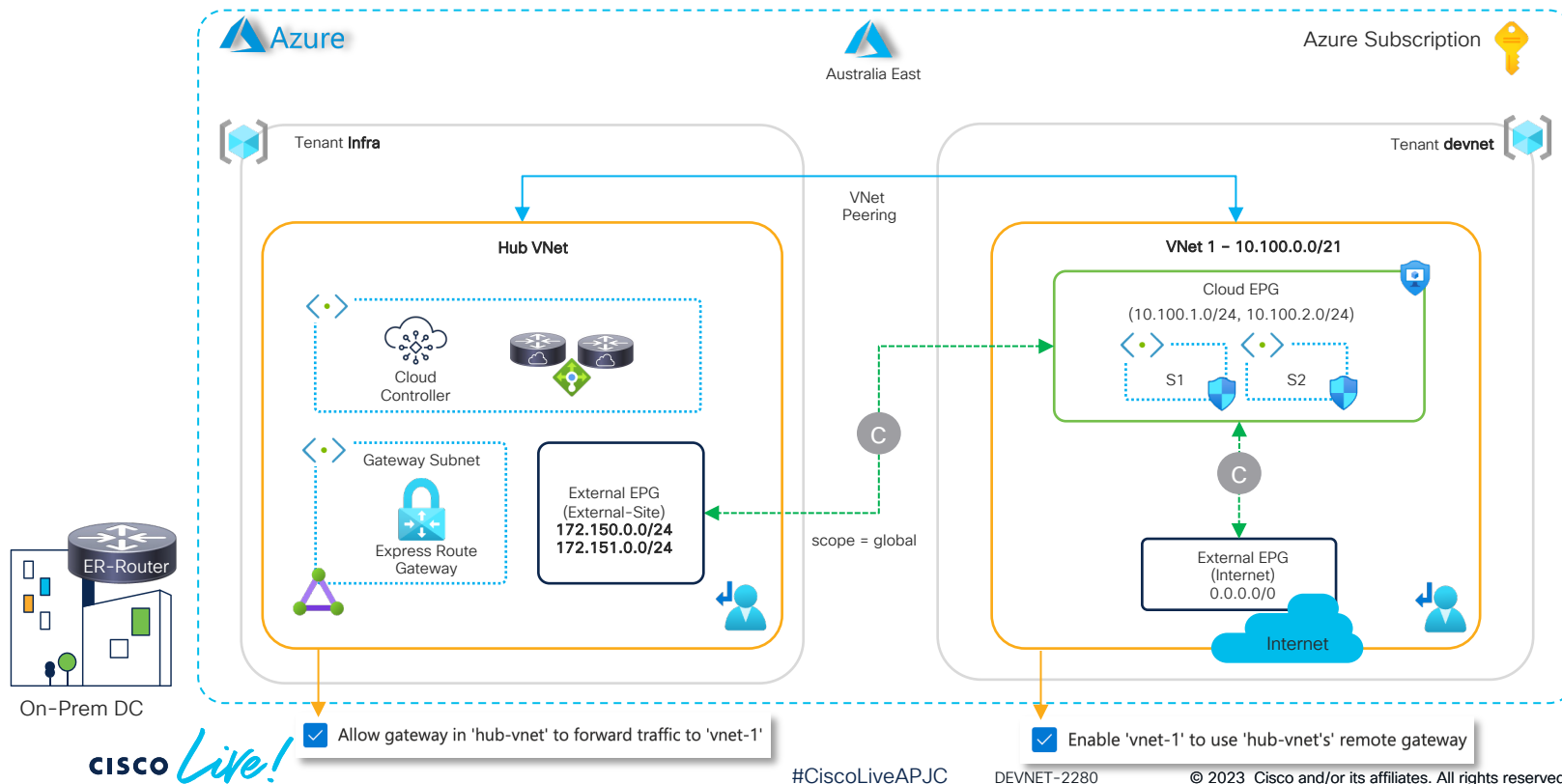




Git Repo

Demo 2: Hub VNet with ER Gateway

To/From On-prem Traffic



CISCO *Live!*

#CiscoLiveAPJC

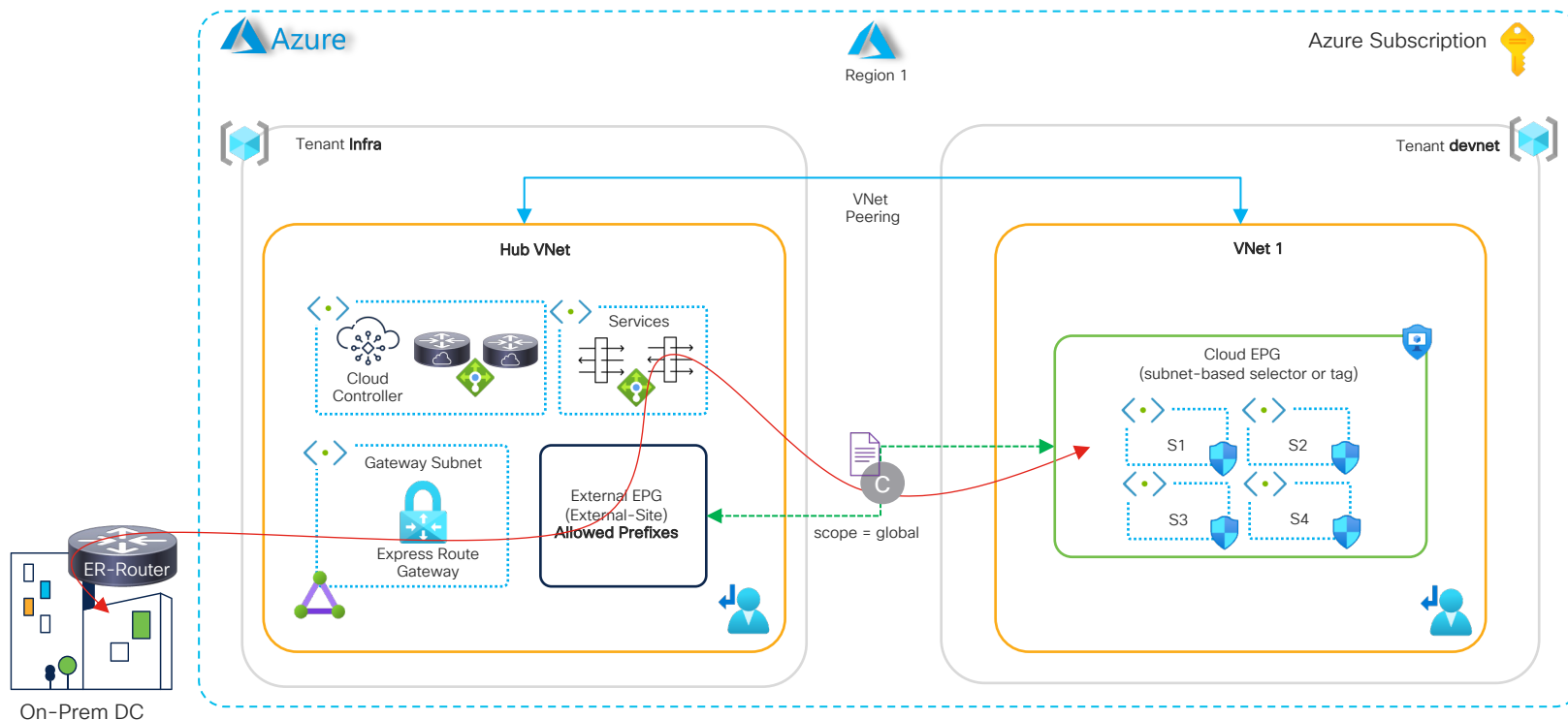
DEVNET-2280

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

27

Use Case 3: Hub VNet with ER GW + Redirect

To/From On-prem Traffic

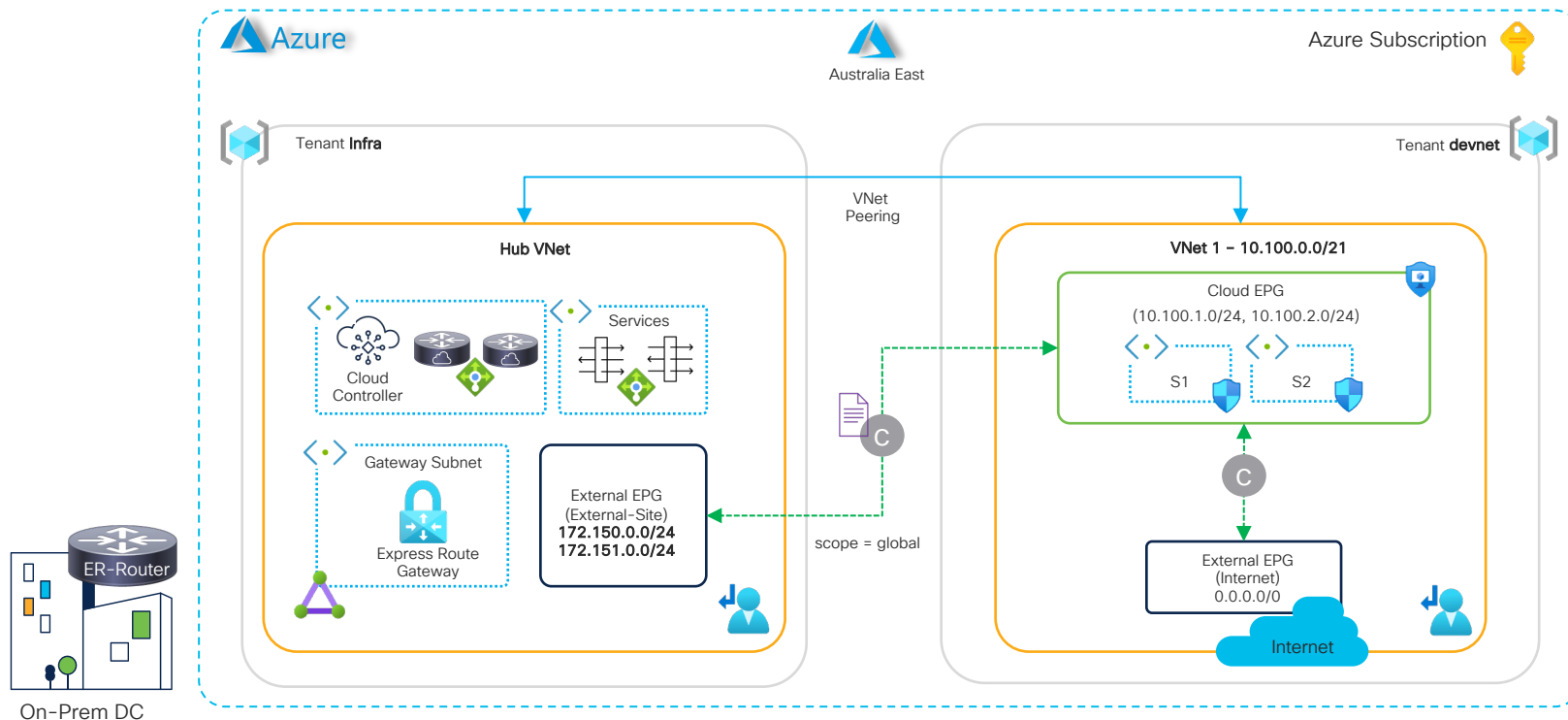




Git Repo

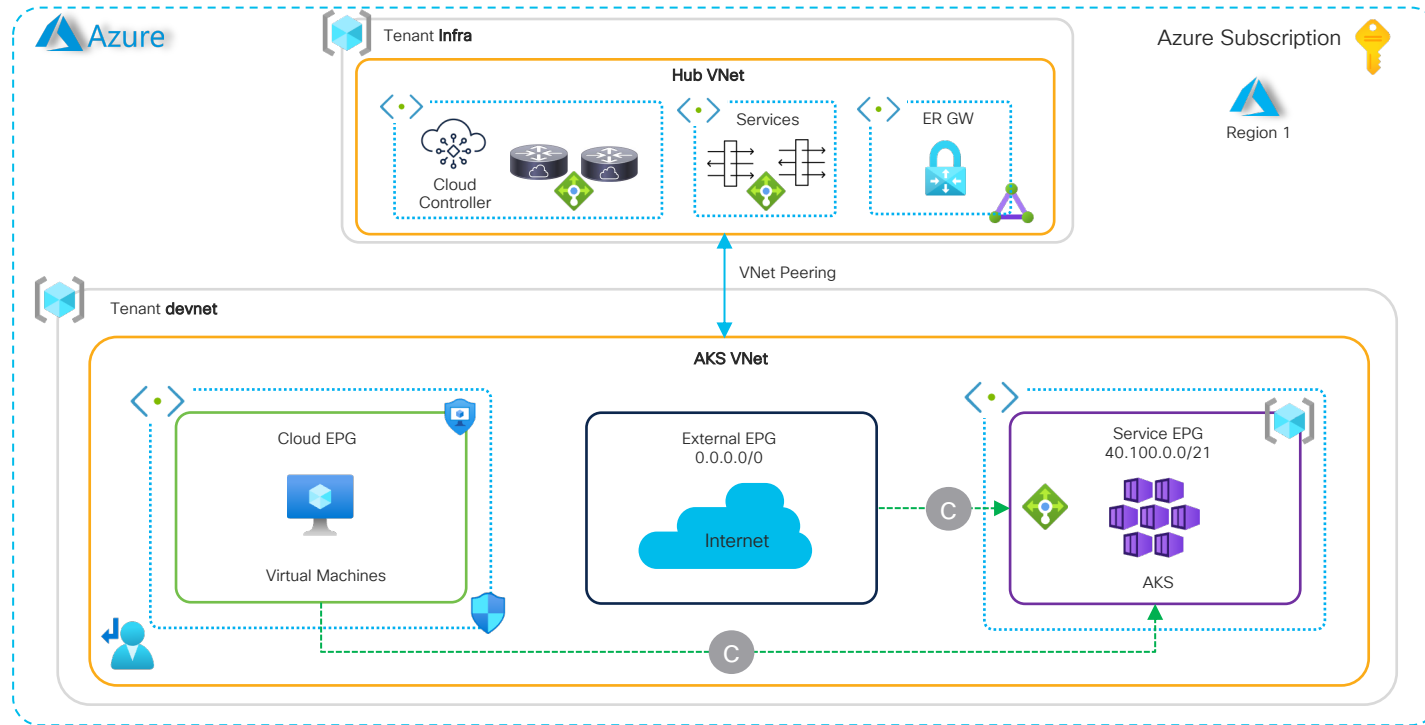
Demo 3: Hub VNet with ER GW + Redirect

To/From On-prem Traffic



Use Case 4: Cloud Native Managed Connectivity

Azure Kubernetes Services with Services EPG

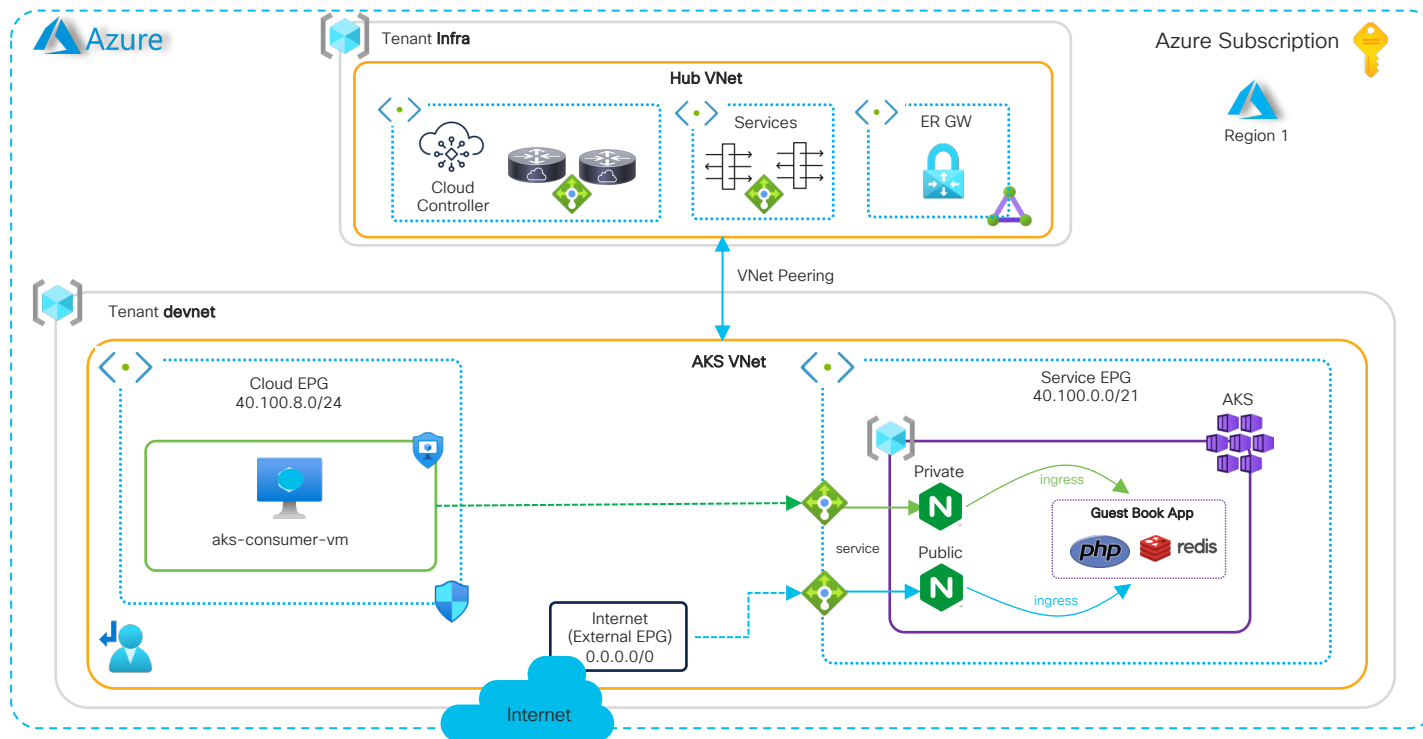


Demo 4: Cloud Native Managed Connectivity

Azure Kubernetes Services with Services EPG



Git Repo



What's New: Terraform Resources

What's New: CNC Terraform Resources

<https://registry.terraform.io/providers/CiscoDevNet/aci/latest>

The screenshot displays the Terraform Registry interface for the CiscoDevNet/aci provider. The top navigation bar includes the Terraform logo, a search bar, and links for Browse, Publish, and a user profile. The breadcrumb trail shows the path: Providers > CiscoDevNet > aci > Version 2.11.1 > Latest Version. The main content area is titled 'aci' and includes tabs for Overview, Documentation, and a 'USE PROVIDER' button. The left sidebar, labeled 'ACI DOCUMENTATION', contains a search bar and a tree view of the provider's resources. The 'Cloud' category is expanded, and the 'aci_cloud_account' resource is selected. The main content area displays the resource name 'aci_cloud_account' and a description: 'Manages Cloud Network Controller Cloud Account Note: This resource is supported in Cloud Network Controller only.' Below this, a list of related resources is shown: aci_cloud_vrf_leak_routes, aci_cloud_private_link_label, aci_cloud_service_endpoint_selector, aci_cloud_service_epg, aci_cloud_l4_l7_native_load_balancer, and aci_cloud_l4_l7_third_party_device. The right sidebar, titled 'ON THIS PAGE', lists links for API Information, GUI Information, Example Usage, Argument Reference, Importing, and a 'Report an issue' link.

aci  Overview Documentation [USE PROVIDER](#)

ACI DOCUMENTATION

Filter

- aci provider
 - > AAA
 - > Access Policies
 - > Application Management
 - ▼ Cloud
 - ▼ Resources
 - [aci_cloud_account](#)
 - aci_cloud_ad

aci_cloud_account

Manages Cloud Network Controller Cloud Account Note: This resource is supported in Cloud Network Controller only.

```
aci_cloud_vrf_leak_routes
aci_cloud_private_link_label
aci_cloud_service_endpoint_selector
aci_cloud_service_epg
aci_cloud_l4_l7_native_load_balancer
aci_cloud_l4_l7_third_party_device
```

ON THIS PAGE

- API Information
- GUI Information
- Example Usage
- Argument Reference
- Importing

[Report an issue](#)

Cisco Developer Portal



CNC



APIC



Orchestrator

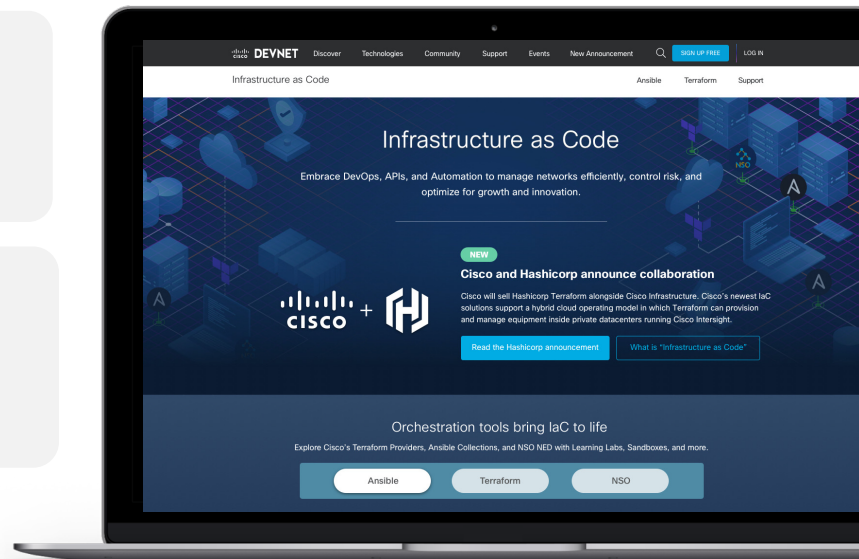


APIC & CNC resources/data sources available

<https://github.com/CiscoDevNet/terraform-provider-ac>

Orchestrator resources/data sources available

<https://github.com/CiscoDevNet/terraform-provider-mso>



<https://developer.cisco.com/iac>



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco
DevNet

WE
ARE
CISCO
DEVNET

Continue to Learn, Code, and Build with Cisco DevNet

Get access to exclusive resources including API documentation, Code Exchange, self-paced learning labs, sandboxes, community forums and events!

Scan QR Code to get started.





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC

Cloud EPG, Selectors, and Contracts



- 1) **Endpoint Groups (EPGs):** The cloud EPG is the most important object in the policy model. Cloud EPGs contain endpoints that have common policy requirements such as security or L4-L7 services. Rather than configure and manage endpoints individually, they are placed in a cloud EPG and are managed as a group. EPGs are created inside an application profile container.
- 2) **Selectors:** CNC uses endpoint selectors to assign endpoints to Cloud EPGs. The endpoint selector is essentially a set of rules that are run against the cloud instances that are assigned to the VNets managed by CNC. It can also be prefixes in the case of External EPGs and subnets in the case of Services EPGs for Native services.
- 3) **Contracts:** In addition to cloud EPGs, contracts are key objects in the policy model. Cloud EPGs can only communicate with other cloud EPGs according to contract rules.