3-networks-hub-and-spoke

3-networks-hub-and-spoke 1 — 1 **envs**

tfvars
common.auto
access_context.auto

Provided as.example.tfvars

tfvars
shared.auto

Provided as.example.tfvars

modules

development

non-production

production

hardcoding in locals
Inclusion .../../modules/base_env

shared 1

base-env 1 → base-shared-vpc 1

restricted-shared-vpc 1

dedicated-interconnect 1 → cloud-router / modules / interconnect-attachment (x 4)

hierarchical-firewall-policy 1 →
compute_org_security_policy
policy

compute_org_security_policy_rule
rule

partner-interconnect 1 →
compute_interconnect_attachment
interconnect_attachment1_region1
interconnect_attachment2_region1
interconnect_attachment1_region2
interconnect_attachment2_region2

transitivity 1   1

service_account

vm/instance-template

Legend

Resource	From terraform-google-modules	Hardcoded data
	From GoogleCloudPlatform	

Section 1

private-service-connect.tf —1— network / private-service-connect

dns.tf 1 ⤏ dns_policy **default_policy**

cloud-dns **peering_zone**

nat.tf ⤏ compute_router **nat_router_region1** **nat_router_region2**

firewall.tf 1 ⤏ compute_router_nat **egress_nat_1** **egress_nat_2**

network / modules / network-firewall-policy

compute_address **nat_external_addresses_region1** **nat_external_addresses_region2**

network / modules / network-peering

compute_global_address **private_service_access_address**

main.tf ⤏ service_networking_connection **private_vpc_connectiion**

cloud-router (x 4) — 1 — 1 — network

Section 2

private-service-connect.tf —1— network / private-service-connect

dns.tf 1 ⤏ dns_policy **default_policy**

cloud-dns **peering_zone**

nat.tf ⤏ compute_router **nat_router_region1** **nat_router_region2**

vm/mig

lb-internal

compute_route
routes

compute_network
firewall_policy_rule
allow_transitivity_ingress

compute_network
firewall_policy_rule
allow_transitivity_eggress

included in only
vpn.tf.example

vpn-ha 1 ◆→ vpn/vpn-ha
(x4)

cloud-dns
dns-forwarding-zone ← 1 dns-hub.tf

cloud-router (4x)
dns-hub-region[12]_router[12]

◆ hiearchical-
firewall.tf

interconnect.auto
.tfvars.example

◆ interconnect..tf
.example

◆ net-hubs.tf

◆ net-hubs-
transitivity.tf

partner-interconnect.auto
.tfvars.example

◆ interconnect..tf
partner-.example

1   1   1   1   1   1

firewall.tf
1

network / modules /
network-firewall-policy

network / modules /
network-peering

main.tf

1   1

cloud-router
(x 4)

network

compute_router_nat
egress_nat_1
egress_nat_2

compute_address
nat_external_addresses_region1
nat_external_addresses_region2

compute_global_address
private_service_access_address

service_networking_connection
private_vpc_connectiion

service_control.tf

1

1   1

vpc-service-controls /
access-level

vpc-service-controls /
regular_service_perimeter

sccess_context_manager
service_perimeter
bridge_to_network_hub_perim.