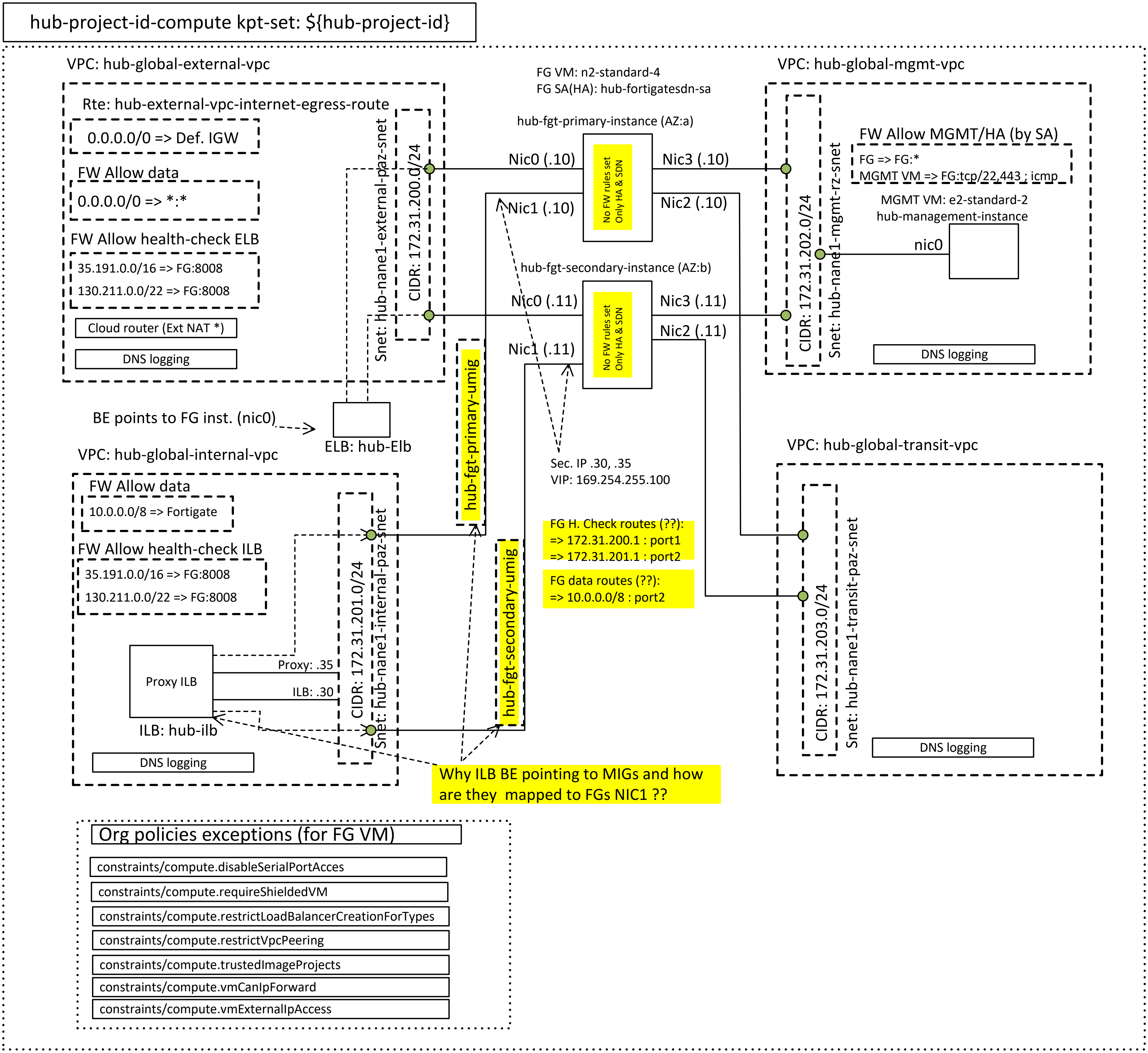
HUB-ENV (current)



hub-project-id-compute kpt-set: ${hub-project-id}

VPC: hub-global-external-vpc

Rte: hub-external-vpc-internet-egress-route

0.0.0.0/0 => Def. IGW

FW Allow data

0.0.0.0/0 => *:*

FW Allow health-check ELB

35.191.0.0/16 => FG:8008

130.211.0.0/22 => FG:8008

Cloud router (Ext NAT *)

DNS logging

Snet: hub-nane1-external-paz-snet

CIDR: 172.31.200.0/24

FG VM: n2-standard-4

FG SA(HA): hub-fortigatesdn-sa

hub-fgt-primary-instance (AZ:a)

Nic0 (.10)

Nic1 (.10)

Nic3 (.10)

Nic2 (.10)

No FW rules set
Only HA & SDN

hub-fgt-secondary-instance (AZ:b)

Nic0 (.11)

Nic1 (.11)

Nic3 (.11)

Nic2 (.11)

No FW rules set
Only HA & SDN

hub-fgt-primary-umig

hub-fgt-secondary-umig

VPC: hub-global-mgmt-vpc

FW Allow MGMT/HA (by SA)

FG => FG:*

MGMT VM => FG:tcp/22,443 ; icmp

MGMT VM: e2-standard-2

hub-management-instance

nic0

CIDR: 172.31.202.0/24

Snet: hub-nane1-mgmt-rz-snet

DNS logging

BE points to FG inst. (nic0)

ELB: hub-Elb

Sec. IP .30, .35

VIP: 169.254.255.100

VPC: hub-global-internal-vpc

FW Allow data

10.0.0.0/8 => Fortigate

FW Allow health-check ILB

35.191.0.0/16 => FG:8008

130.211.0.0/22 => FG:8008

Proxy ILB

Proxy: .35

ILB: .30

ILB: hub-ilb

DNS logging

CIDR: 172.31.201.0/24

Snet: hub-nane1-internal-paz-snet

FG H. Check routes (??):
=> 172.31.200.1 : port1
=> 172.31.201.1 : port2

FG data routes (??):
=> 10.0.0.0/8 : port2

VPC: hub-global-transit-vpc

CIDR: 172.31.203.0/24

Snet: hub-nane1-transit-paz-snet

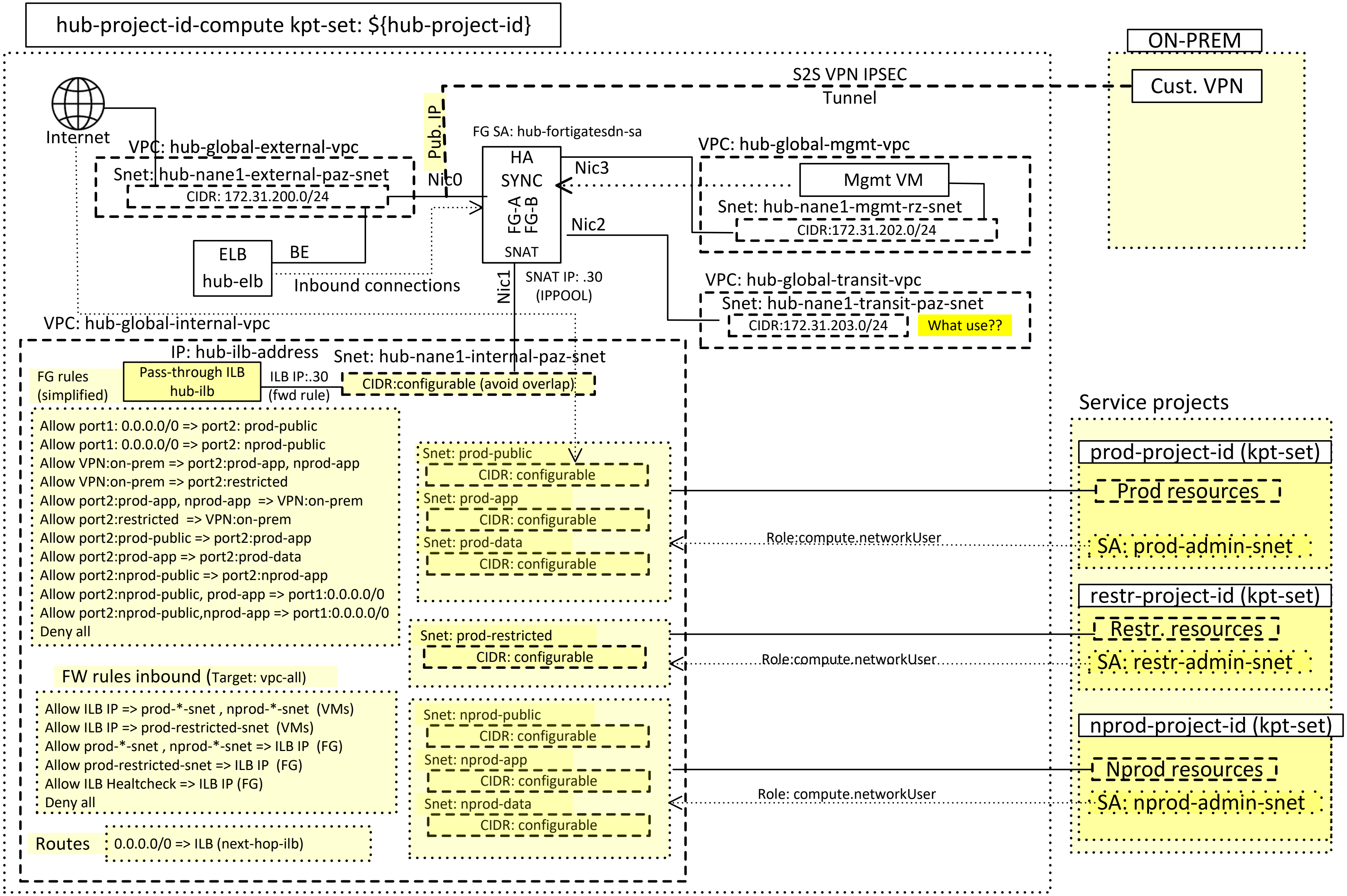
DNS logging

Why ILB BE pointing to MIGs and how are they mapped to FGs NIC1 ??

Org policies exceptions (for FG VM)

- constraints/compute.disableSerialPortAcces
- constraints/compute.requireShieldedVM
- constraints/compute.restrictLoadBalancerCreationForTypes
- constraints/compute.restrictVpcPeering
- constraints/compute.trustedImageProjects
- constraints/compute.vmCanIpForward
- constraints/compute.vmExternalIpAccess

Hub & Spoke « Light » (take 1, minimal) based on HUB-ENV (todo)



hub-project-id-compute kpt-set: ${hub-project-id}

ON-PREM

Cust. VPN

S2S VPN IPSEC
Tunnel

Internet

Pub. IP

FG SA: hub-fortigatesdn-sa

VPC: hub-global-external-vpc

Snet: hub-nane1-external-paz-snet

CIDR: 172.31.200.0/24

Nic0

HA
SYNC
FG-A
FG-B
SNAT

Nic3

Nic2

Nic1

SNAT IP: .30
(IPPOOL)

ELB
hub-elb

BE

Inbound connections

VPC: hub-global-mgmt-vpc

Mgmt VM

Snet: hub-nane1-mgmt-rz-snet

CIDR:172.31.202.0/24

VPC: hub-global-transit-vpc

Snet: hub-nane1-transit-paz-snet

CIDR:172.31.203.0/24

What use??

VPC: hub-global-internal-vpc

IP: hub-ilb-address

Snet: hub-nane1-internal-paz-snet

Pass-through ILB
hub-ilb

ILB IP:.30
(fwd rule)

CIDR:configurable (avoid overlap)

FG rules
(simplified)

Allow port1: 0.0.0.0/0 => port2: prod-public
Allow port1: 0.0.0.0/0 => port2: nprod-public
Allow VPN:on-prem => port2:prod-app, nprod-app
Allow VPN:on-prem => port2:restricted
Allow port2:prod-app, nprod-app => VPN:on-prem
Allow port2:restricted => VPN:on-prem
Allow port2:prod-public => port2:prod-app
Allow port2:prod-app => port2:prod-data
Allow port2:nprod-public => port2:nprod-app
Allow port2:nprod-public, prod-app => port1:0.0.0.0/0
Allow port2:nprod-public,nprod-app => port1:0.0.0.0/0
Deny all

FW rules inbound (Target: vpc-all)

Allow ILB IP => prod-*-snet , nprod-*-snet (VMs)
Allow ILB IP => prod-restricted-snet (VMs)
Allow prod-*-snet , nprod-*-snet => ILB IP (FG)
Allow prod-restricted-snet => ILB IP (FG)
Allow ILB Healtcheck => ILB IP (FG)
Deny all

Routes

0.0.0.0/0 => ILB (next-hop-ilb)

Snet: prod-public
CIDR: configurable
Snet: prod-app
CIDR: configurable
Snet: prod-data
CIDR: configurable

Snet: prod-restricted
CIDR: configurable

Snet: nprod-public
CIDR: configurable
Snet: nprod-app
CIDR: configurable
Snet: nprod-data
CIDR: configurable

Role:compute.networkUser

Role:compute.networkUser

Role: compute.networkUser

Service projects

prod-project-id (kpt-set)

Prod resources

SA: prod-admin-snet

restr-project-id (kpt-set)

Restr. resources

SA: restr-admin-snet

nprod-project-id (kpt-set)

Nprod resources

SA: nprod-admin-snet