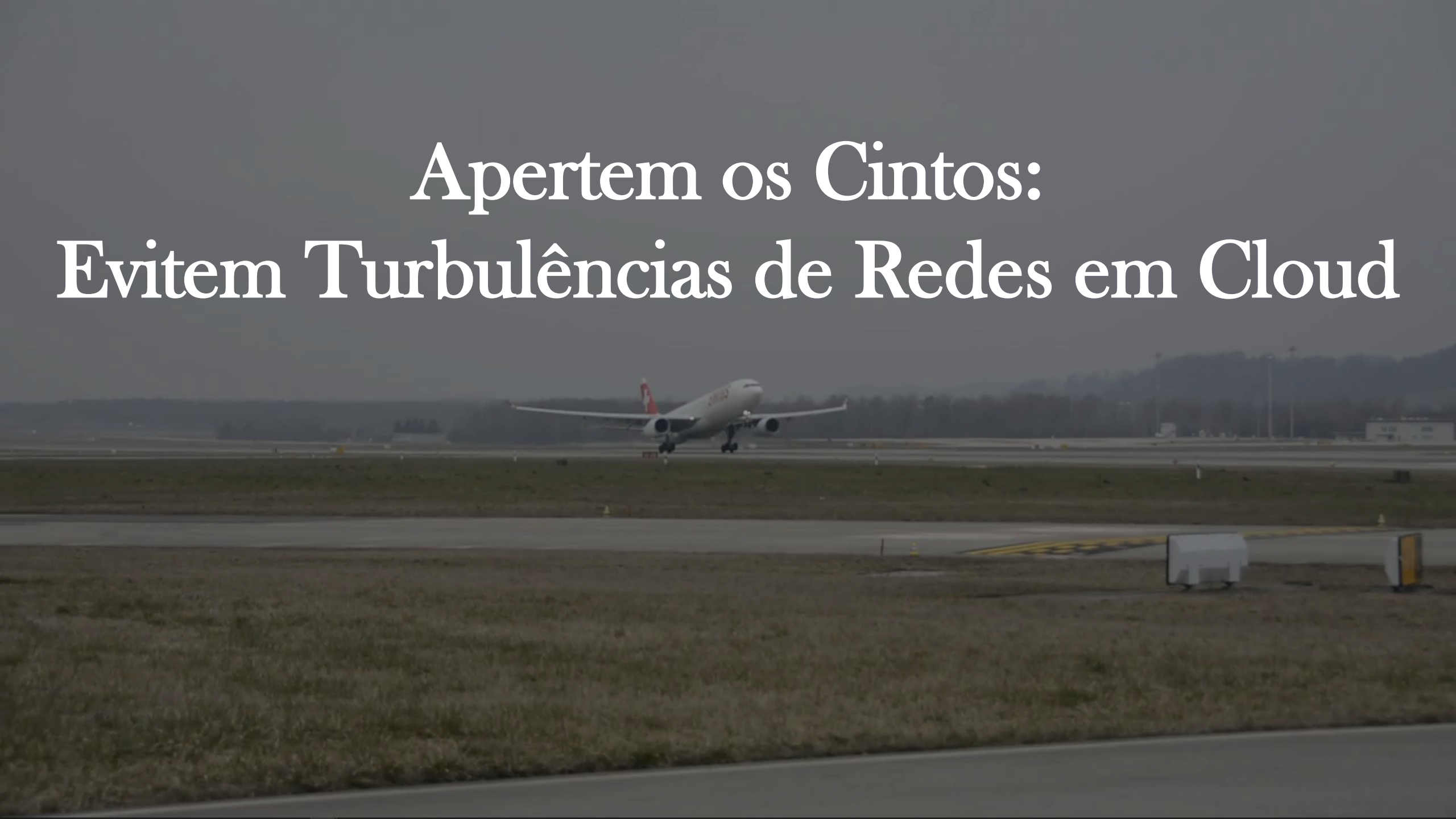

FORTINET
LINUXTIPS

Apertem os Cintos: Evitem Turbulências de Redes em Cloud




SWISS

LINUXTIPS

BONDE DA FORTINET®

SEGURANÇA EM CLOUD E CONTAINERS


Ataques
Proteções
Responsa-
bilidades


USA
Australia
Canada
China
France
Germany
India
Italy
Japan
Russia
Sweden

Jornada de Nuvem

Nuvem Pública?
Quando?
Quais serviços?
Quanto custa? $$


ARBEIT MACHT FREI

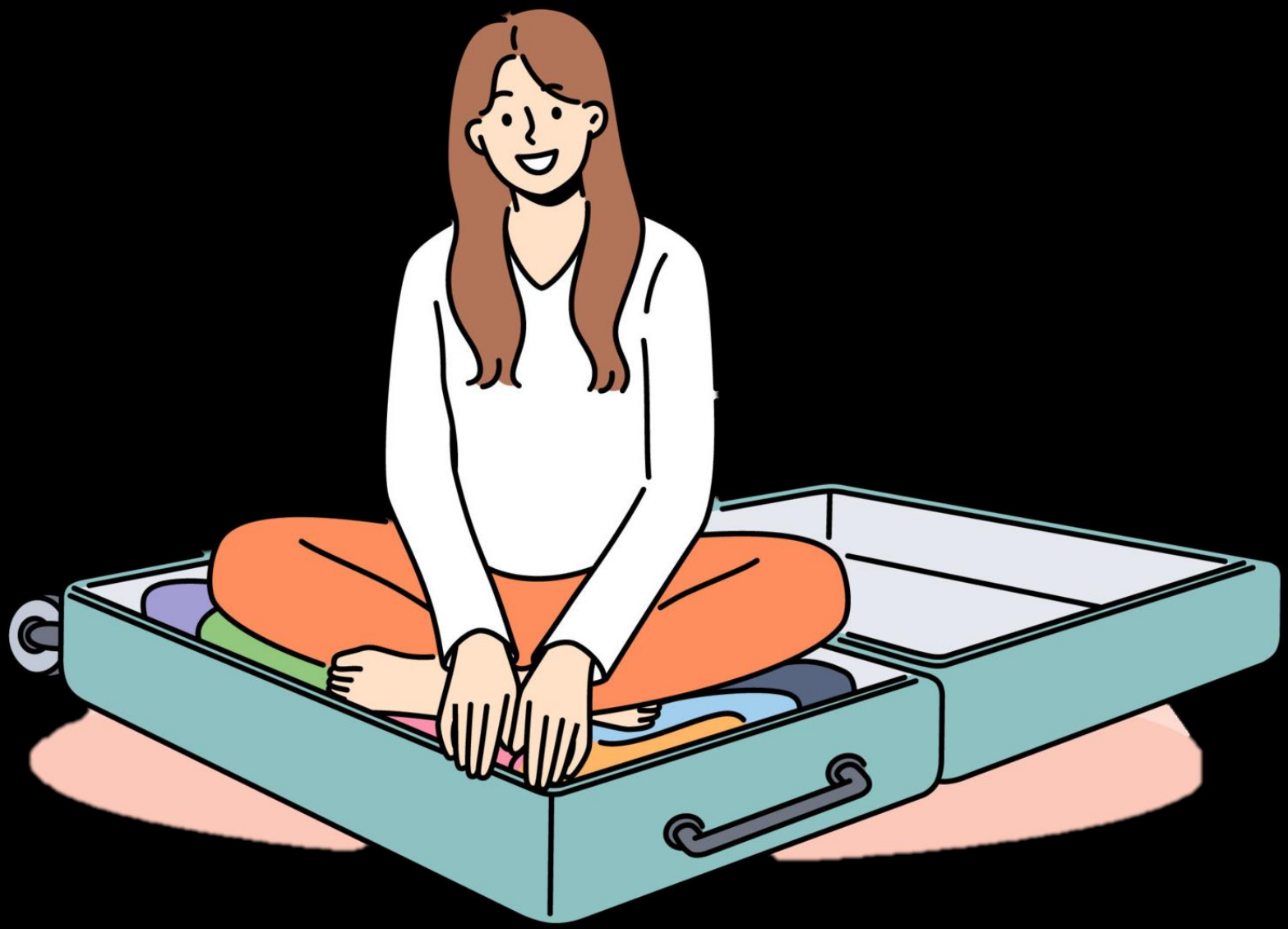




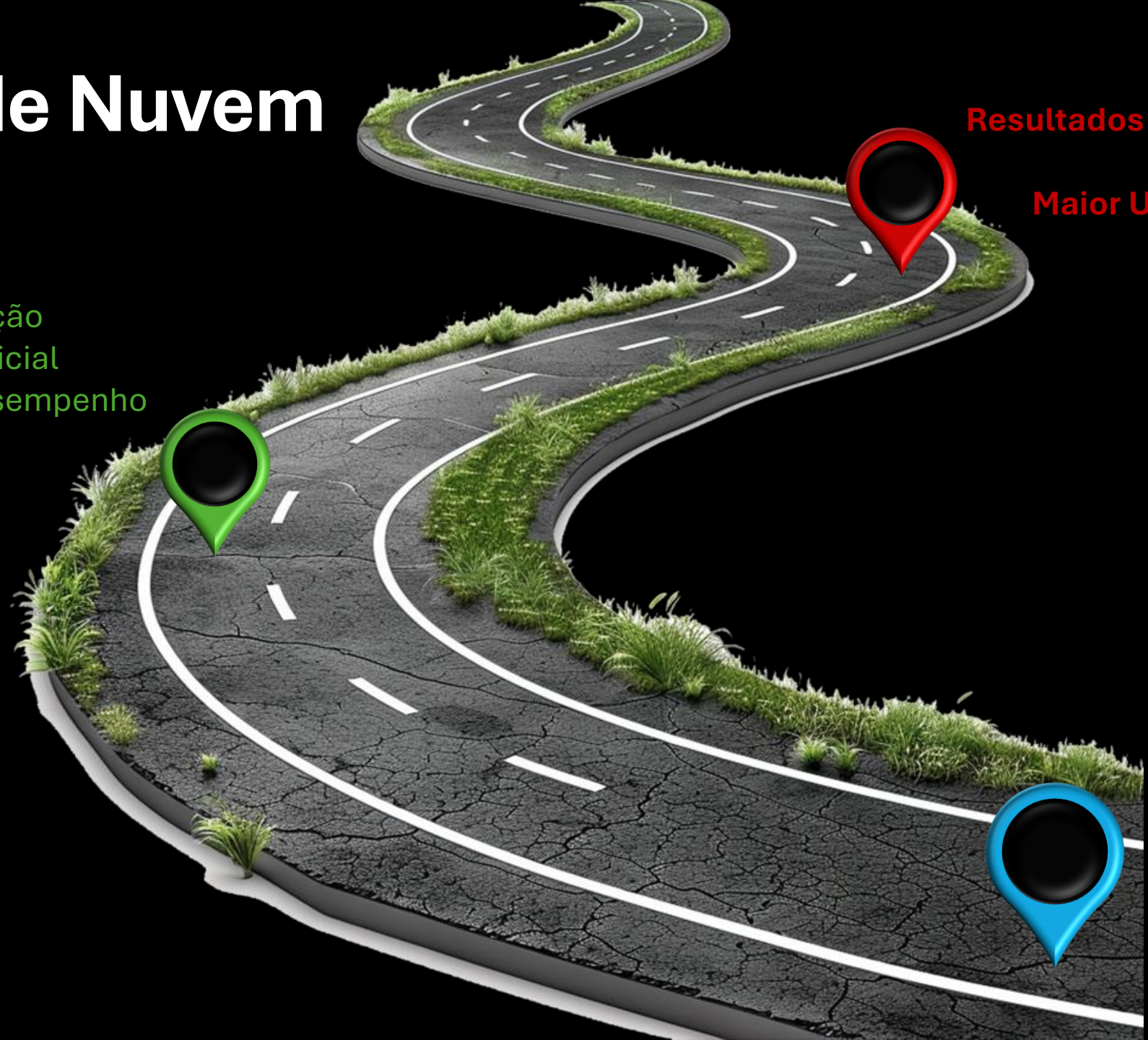

Jornada de Nuvem

Preparação
Deploy Inicial
Análises de Desempenho

Nuvem Pública?
Quando?
Quais serviços?
Quanto custa? $$



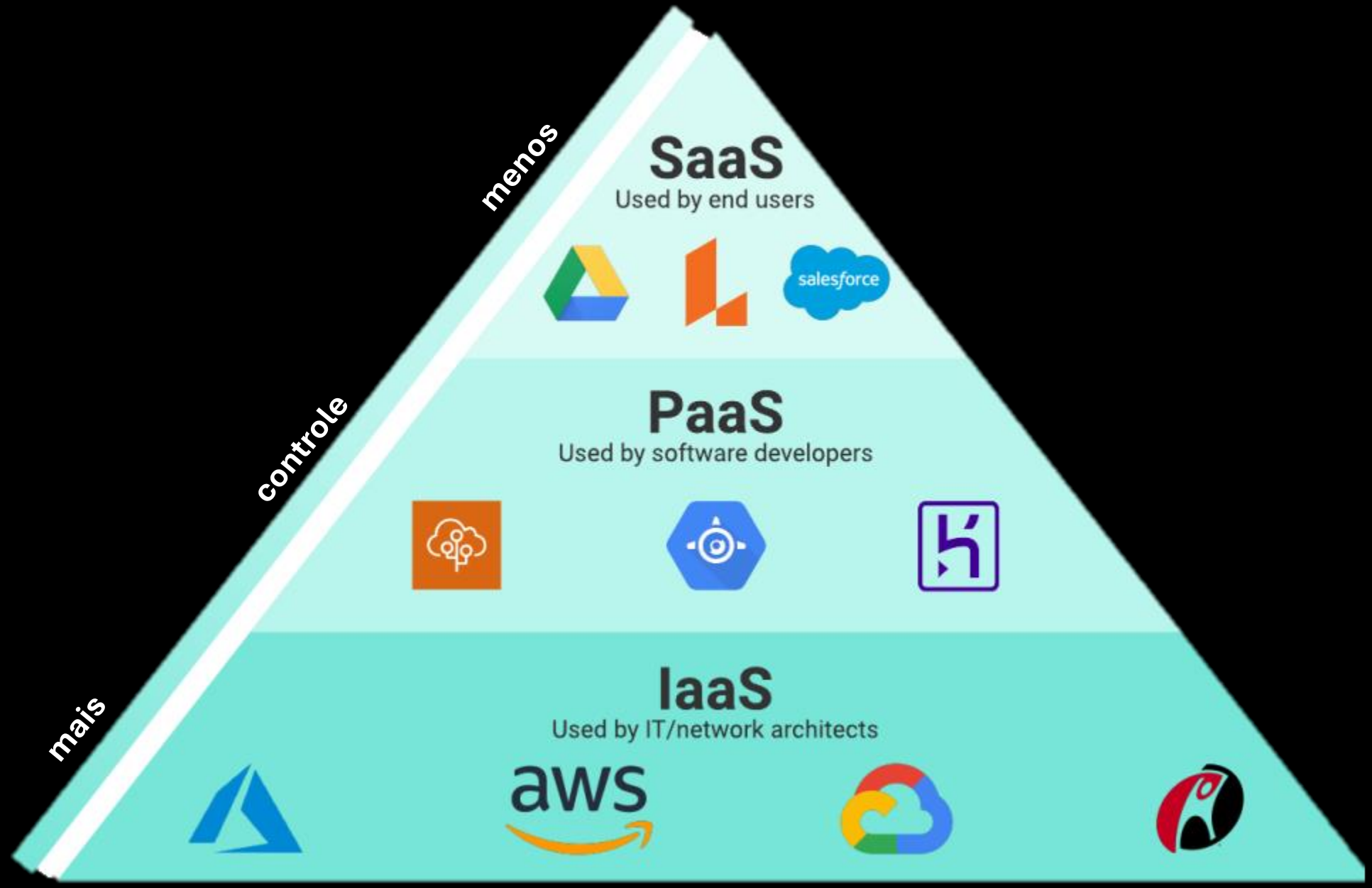
Jornada de Nuvem



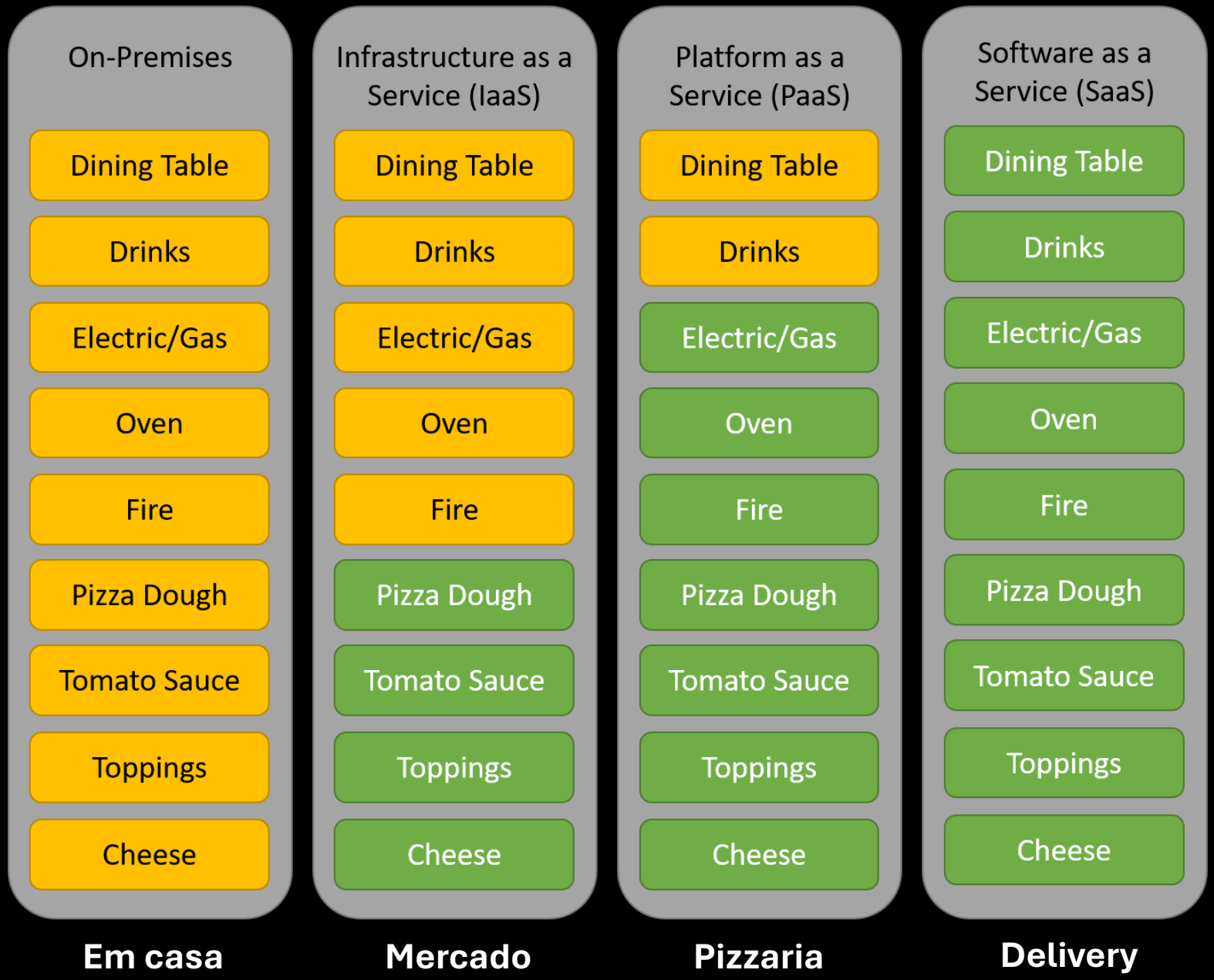
Preparação
Deploy Inicial
Análises de Desempenho

Resultados Satisfatórios
=
Maior Utilização

Nuvem Pública?
Quando?
Quais serviços?
Quanto custa? $$


menos
controle
mais
SaaS
Used by end users
salesforce
PaaS
Used by software developers
IaaS
Used by IT/network architects
aws

Pizza-as-a-Service



Responsabilidade Compartilhada

RESPONSABILIDADE CLIENTE

Segurança NA Nuvem

CLIENTE NA NUVEM

- DADOS
- IDENTIDADE E APLICAÇÕES
- REDE E PLATAFORMAS
- GESTÃO E OPERAÇÕES

Proteção
Controle de Acesso
Visibilidade
Conformidade
Rede

FORTINET

RESPONSABILIDADE PROVEDOR

Segurança DA Nuvem

PROVEDOR DE NUVEM

- CAMADA DE VIRTUALIZAÇÃO
- INFRAESTRUTURA FISICA
- ACESSO FÍSICO ÀS INSTALAÇÕES

aws
Google Cloud
Microsoft Azure
Alibaba Cloud
IBM Cloud
ORACLE Cloud

Segurança Inerente ao Processo

Validação de Identidade

Detector de Metais

Inspeção de Bagagem


#MANIFEST
NBC

Rust-Based
Payloads

Jun 27, 2024 Newsroo

The peer-to-peer malware
servers with ransomware

The development marks t
unclear motives to a finan

New APT Group "CloudSorcerer" Targets Russian Government Entities

Jul 08, 2024 Newsroom Cyber Espionage / Cloud Security

A previously undocumented advanced persistent threat (APT) group dubbed **CloudSorcerer** has been observed targeting Russian government entities by leveraging cloud services for command-and-control (C2) and data exfiltration.

Cybersecurity firm Kaspersky, which discovered the activity in May 2024, said the tradecraft adopted by the threat actor bears similarities with that of CloudWizard, but pointed out the differences in the malware source code. The attacks wield an innovative data-gathering program and a slew of evasion

Cloud-Native Application Security Top 10

CNAS-1
Insecure cloud, container or orchestration configuration

CNAS-2
Injection flaws (app layer, cloud events, cloud services)

CNAS-3
Improper authentication & authorization

CNAS-4
CI/CD pipeline & software supply chain flaws

CNAS-5
Insecure secrets storage

CNAS-6
Over-permissive or insecure network policies

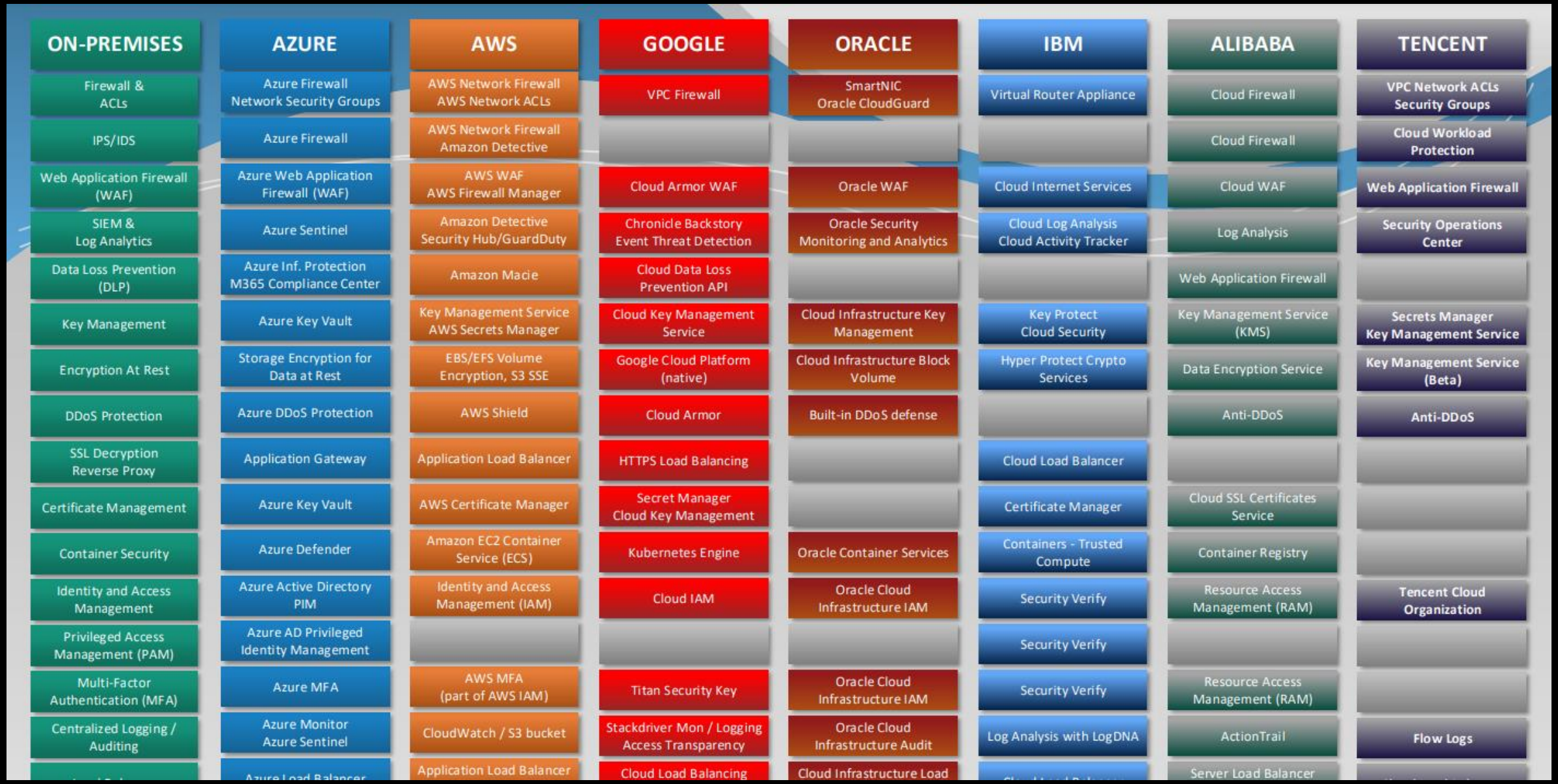
CNAS-7
Using components with known vulnerabilities

CNAS-8
Improper assets management

CNAS-9
Inadequate 'compute' resource quota limits

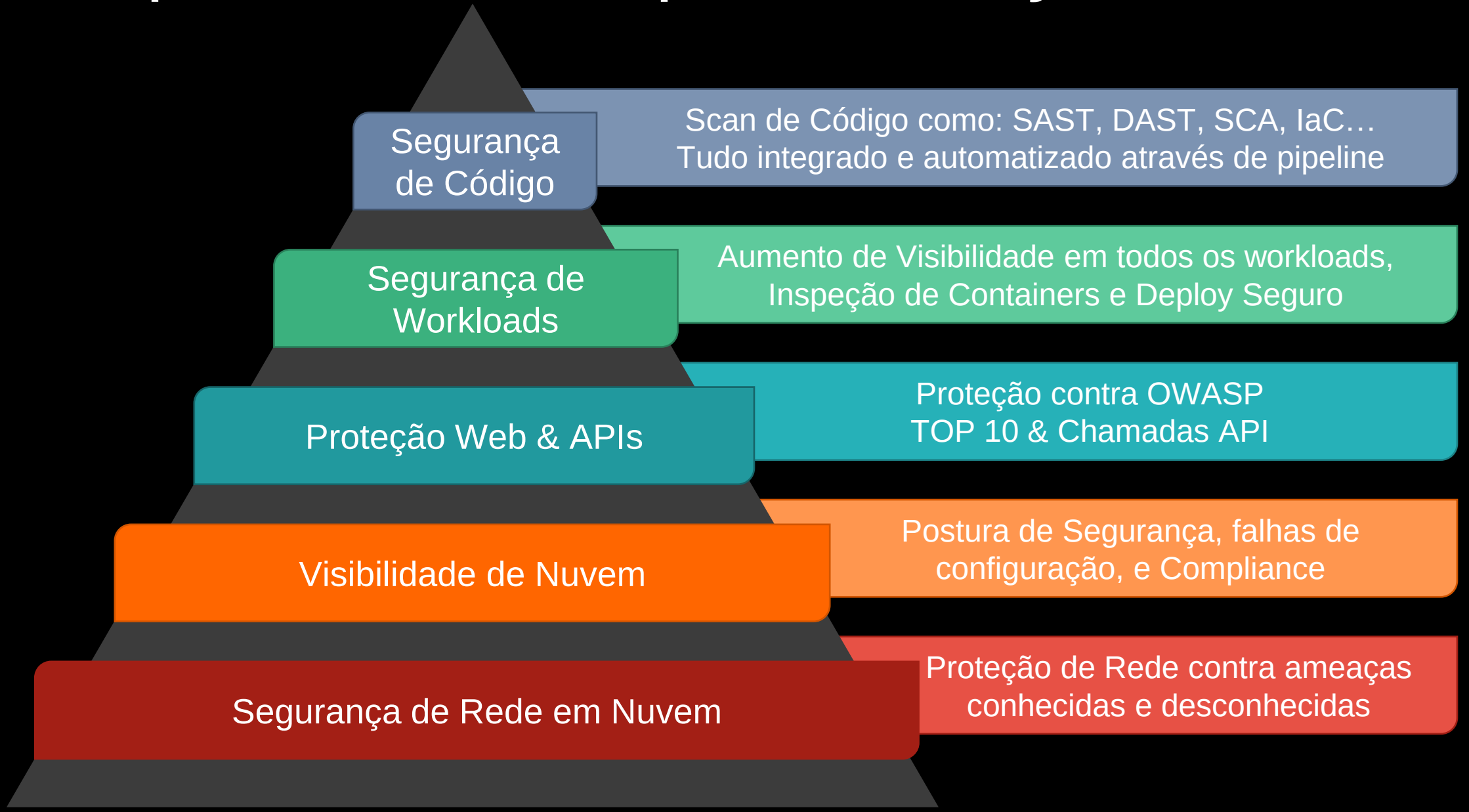
CNAS-10
Ineffective logging & monitoring (e.g. runtime activity)

Camadas de Segurança “Cloud-Native”



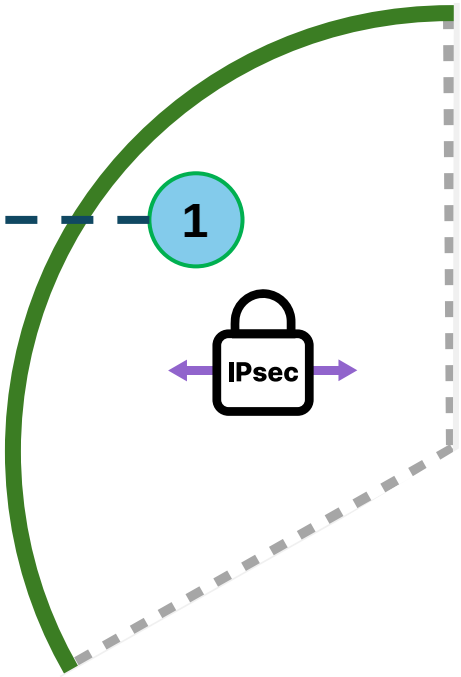
ON-PREMISES	AZURE	AWS	GOOGLE	ORACLE	IBM	ALIBABA	TENCENT
Firewall & ACLs	Azure Firewall Network Security Groups	AWS Network Firewall AWS Network ACLs	VPC Firewall	SmartNIC Oracle CloudGuard	Virtual Router Appliance	Cloud Firewall	VPC Network ACLs Security Groups
IPS/IDS	Azure Firewall	AWS Network Firewall Amazon Detective				Cloud Firewall	Cloud Workload Protection
Web Application Firewall (WAF)	Azure Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Cloud Armor WAF	Oracle WAF	Cloud Internet Services	Cloud WAF	Web Application Firewall
SIEM & Log Analytics	Azure Sentinel	Amazon Detective Security Hub/GuardDuty	Chronicle Backstory Event Threat Detection	Oracle Security Monitoring and Analytics	Cloud Log Analysis Cloud Activity Tracker	Log Analysis	Security Operations Center
Data Loss Prevention (DLP)	Azure Inf. Protection M365 Compliance Center	Amazon Macie	Cloud Data Loss Prevention API			Web Application Firewall	
Key Management	Azure Key Vault	Key Management Service AWS Secrets Manager	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service (KMS)	Secrets Manager Key Management Service
Encryption At Rest	Storage Encryption for Data at Rest	EBS/EFS Volume Encryption, S3 SSE	Google Cloud Platform (native)	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Data Encryption Service	Key Management Service (Beta)
DDoS Protection	Azure DDoS Protection	AWS Shield	Cloud Armor	Built-in DDoS defense		Anti-DDoS	Anti-DDoS
SSL Decryption Reverse Proxy	Application Gateway	Application Load Balancer	HTTPS Load Balancing		Cloud Load Balancer		
Certificate Management	Azure Key Vault	AWS Certificate Manager	Secret Manager Cloud Key Management		Certificate Manager	Cloud SSL Certificates Service	
Container Security	Azure Defender	Amazon EC2 Container Service (ECS)	Kubernetes Engine	Oracle Container Services	Containers - Trusted Compute	Container Registry	
Identity and Access Management	Azure Active Directory PIM	Identity and Access Management (IAM)	Cloud IAM	Oracle Cloud Infrastructure IAM	Security Verify	Resource Access Management (RAM)	Tencent Cloud Organization
Privileged Access Management (PAM)	Azure AD Privileged Identity Management				Security Verify		
Multi-Factor Authentication (MFA)	Azure MFA	AWS MFA (part of AWS IAM)	Titan Security Key	Oracle Cloud Infrastructure IAM	Security Verify	Resource Access Management (RAM)	
Centralized Logging / Auditing	Azure Monitor Azure Sentinel	CloudWatch / S3 bucket	Stackdriver Mon / Logging Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA	ActionTrail	Flow Logs
		Application Load Balancer	Cloud Load Balancing	Cloud Infrastructure Load		Server Load Balancer	

5 Principais Domínios para Proteção de Nuvem

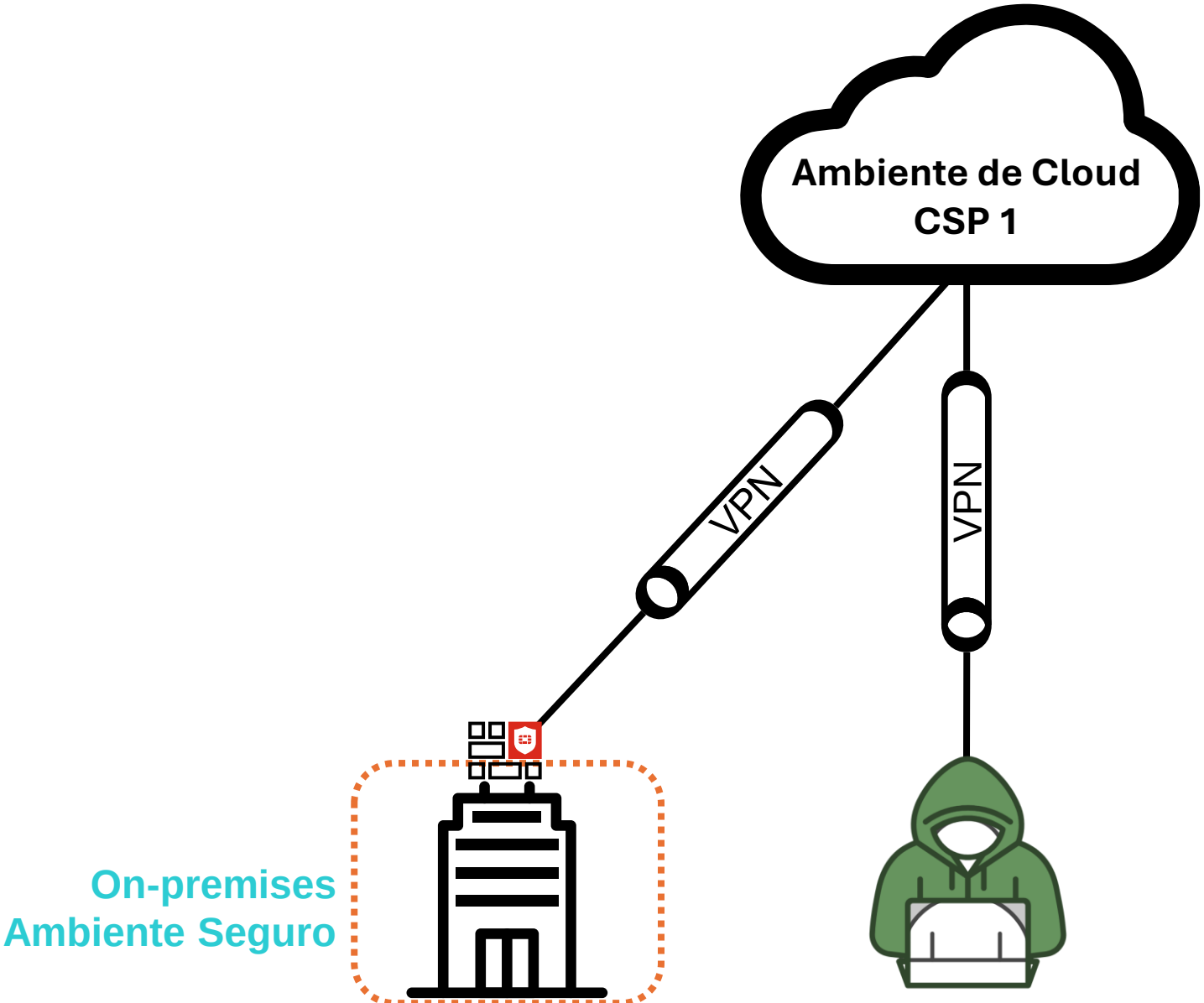


Principais Desafios de Rede em Nuvem

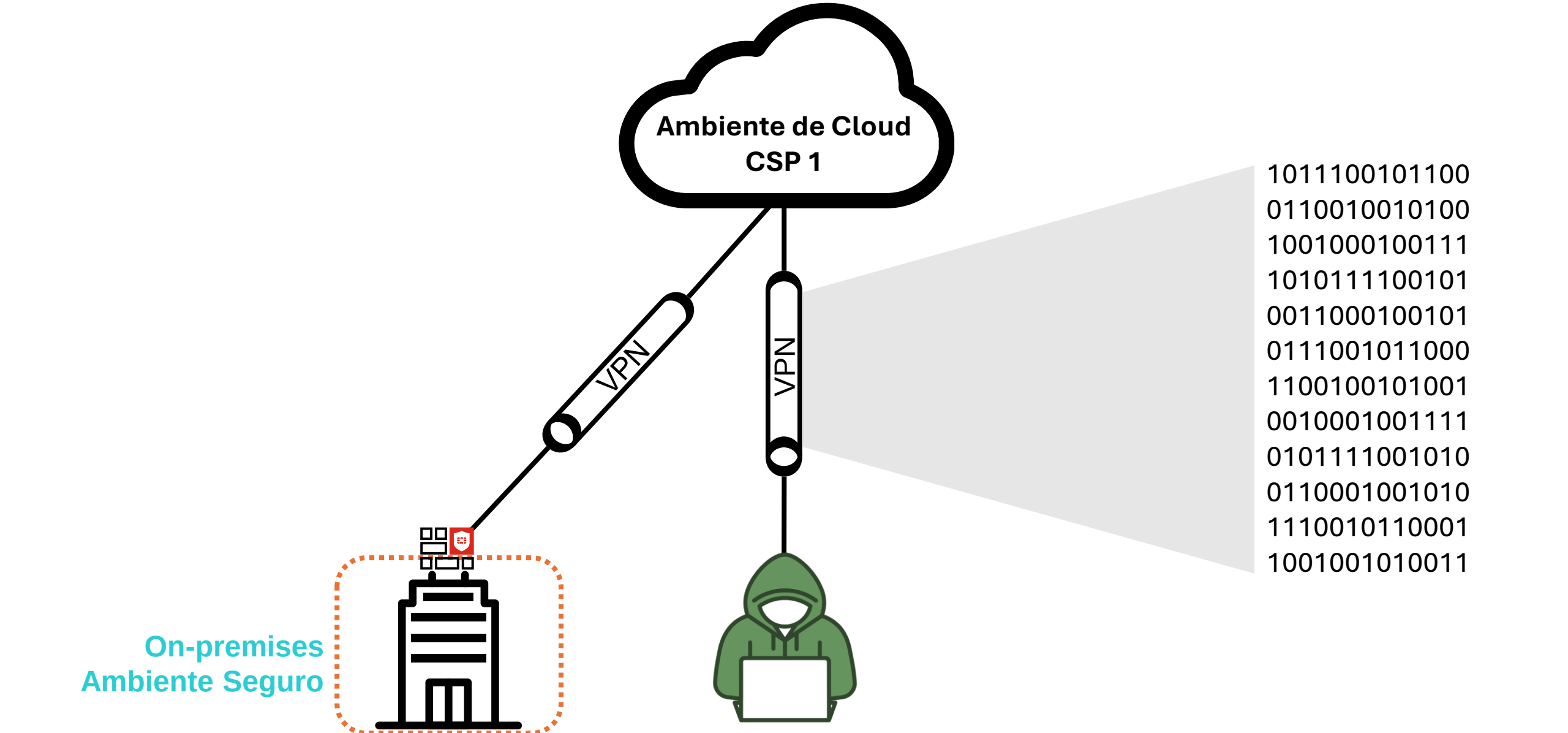
1. Conectividade Segura aos Recursos em Nuvem



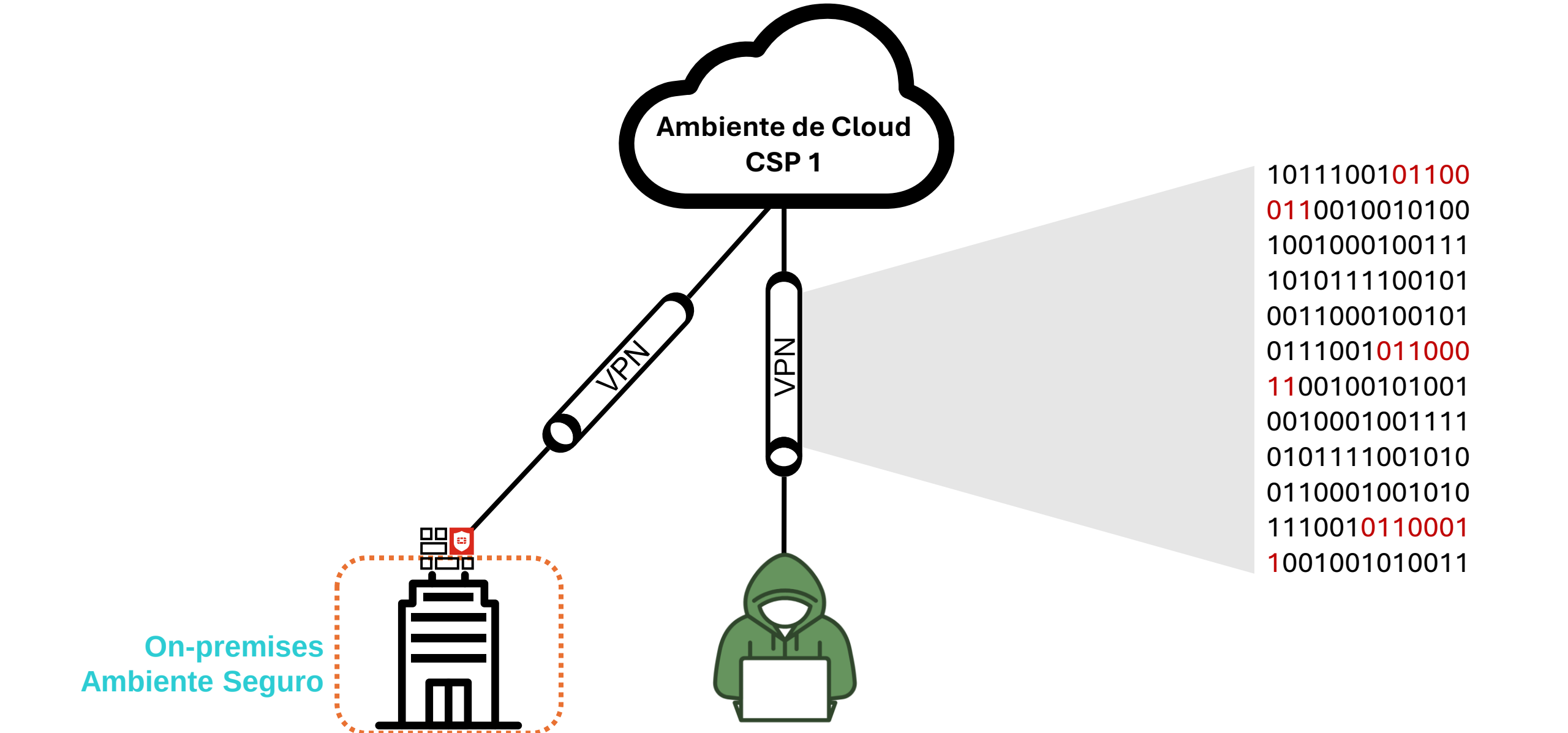
Conectividade Segura é Muito Mais que “Simples” VPN



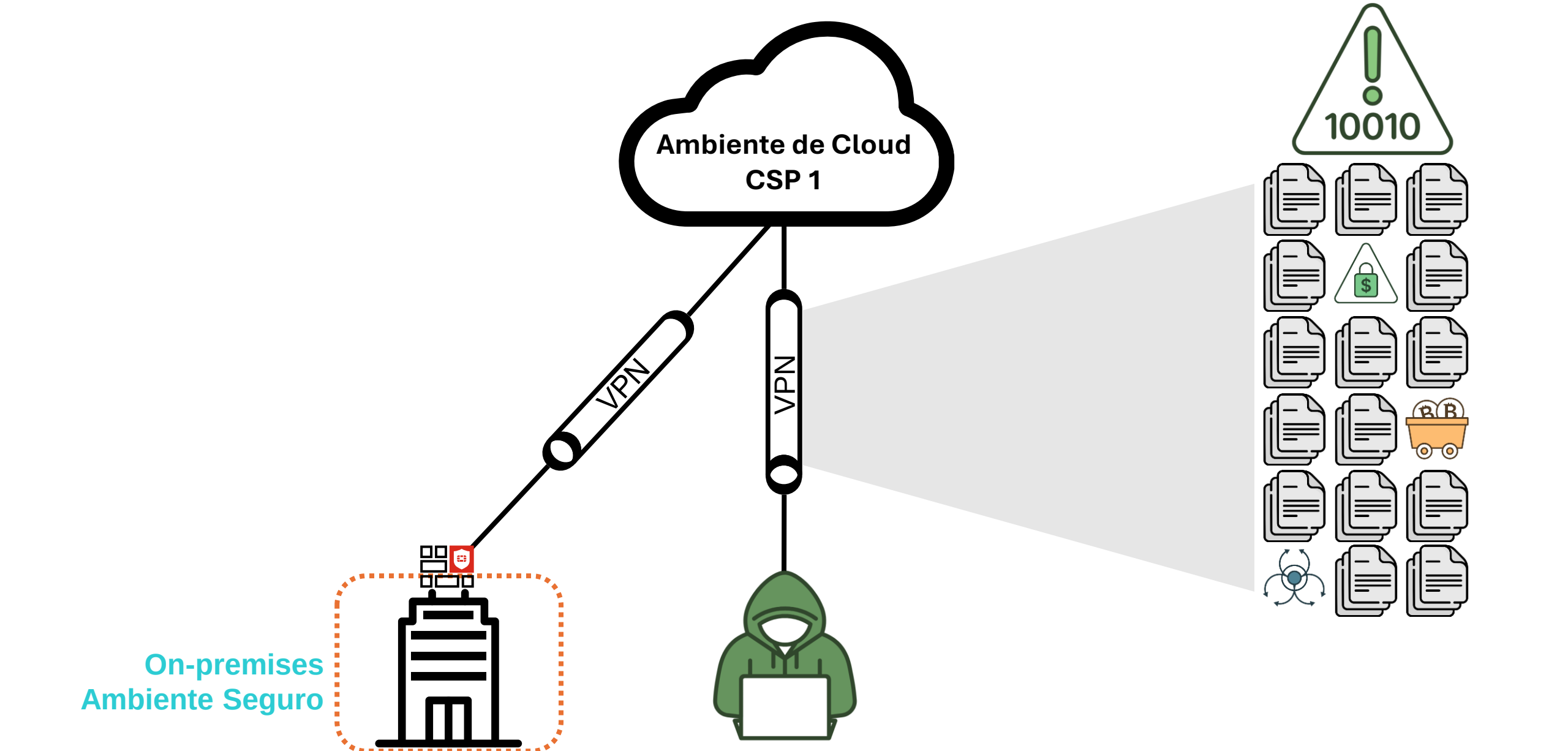
Conectividade Segura é Muito Mais que “Simples” VPN



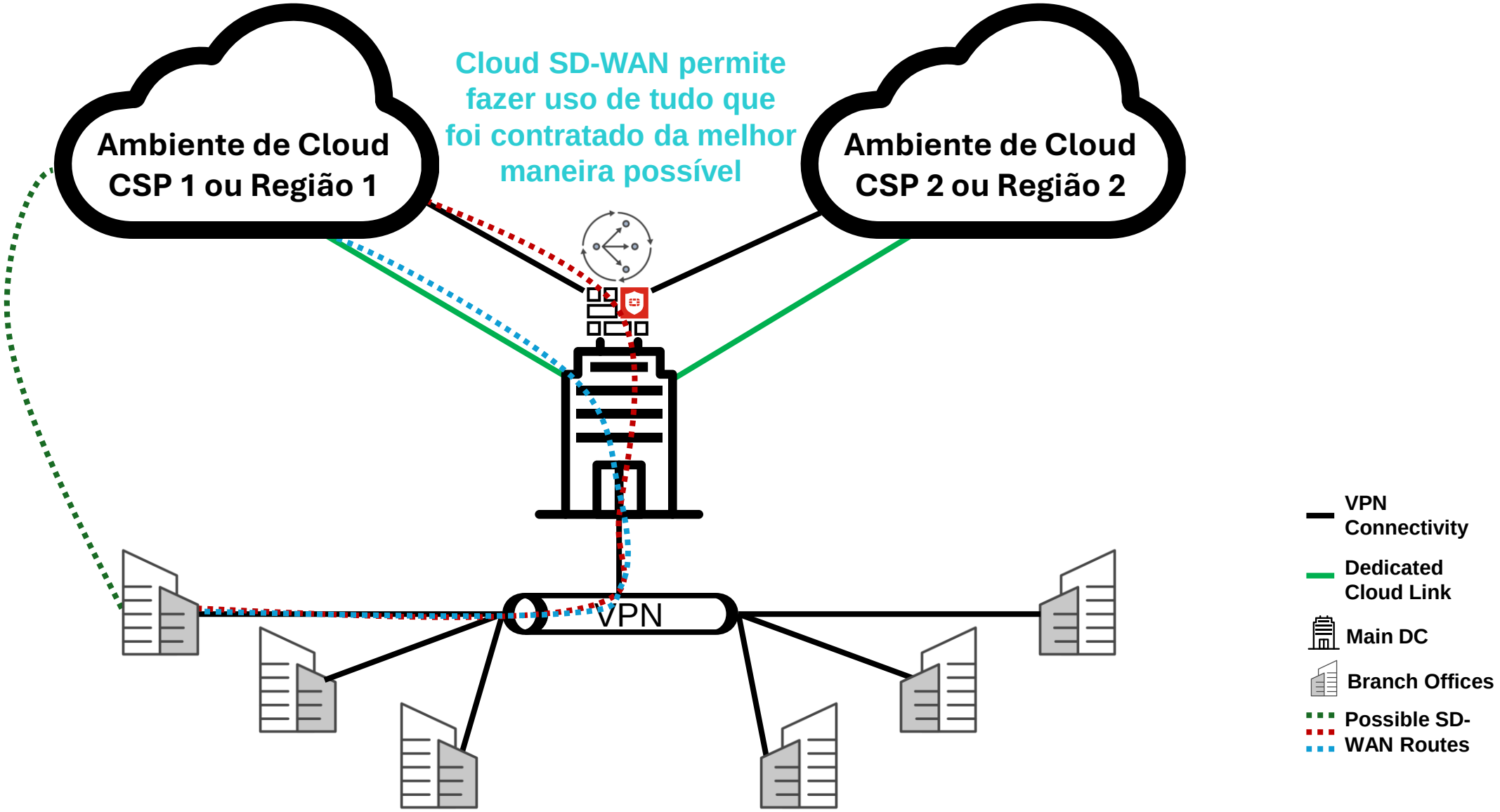
Conectividade Segura é Muito Mais que “Simples” VPN



Conectividade Segura é Muito Mais que “Simples” VPN



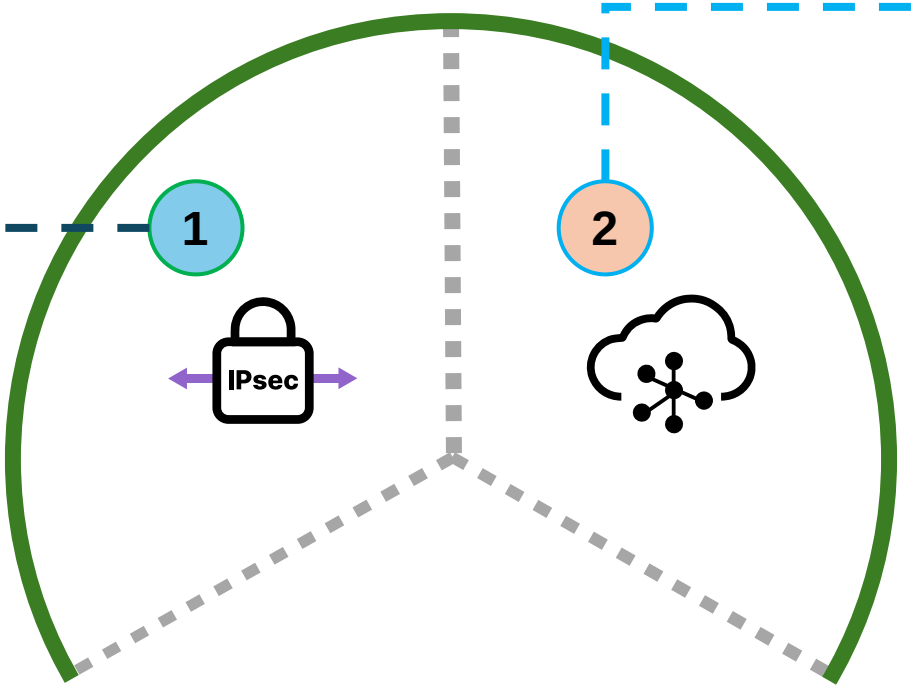
Conectividade Segura é Muito Mais que “Simples” VPN



Principais Desafios de Rede em Nuvem

1. Conectividade Segura aos Recursos em Nuvem

2. Segmentação & Microssegmentação de Tráfego



Propagação Lateral de Malware em Nuvem

October 3, 2023

Cloud security

Identity and access management

Microsoft Defender for Cloud

more

Microsoft security researchers recen
attempted to move laterally to a clo
instance. This attack technique dem
cloud services such as VMs and Kub
attackers initially exploited a SQL inj
the target's environment. This allow
permissions on a Microsoft SQL Ser
Machine (VM). The attackers then us

Kinsing crypto mining campaign targets 75 cloud-native applications

News Analysis

May 08, 2024 • 6 mins

Application Security | Cryptocurrency | Malware

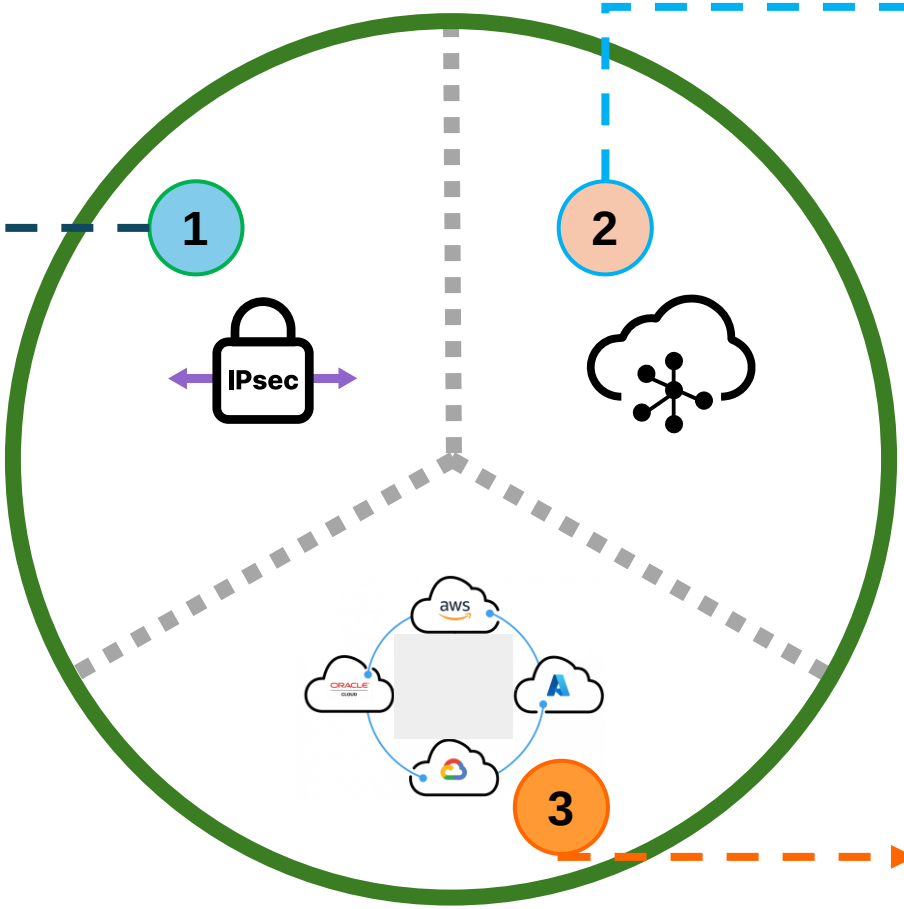
Five years after being discovered, the Kinsing cryptojacking operation remains very active against organizations, employing daily probes for vulnerable applications using an ever-growing list of exploits.

Credit: Shutterstock

Principais Desafios de Rede em Nuvem

1. Conectividade Segura aos Recursos em Nuvem

2. Segmentação & Microssegmentação de Tráfego



3. Gerenciamento Multi-Cloud, com foco em Conectividade & Automação

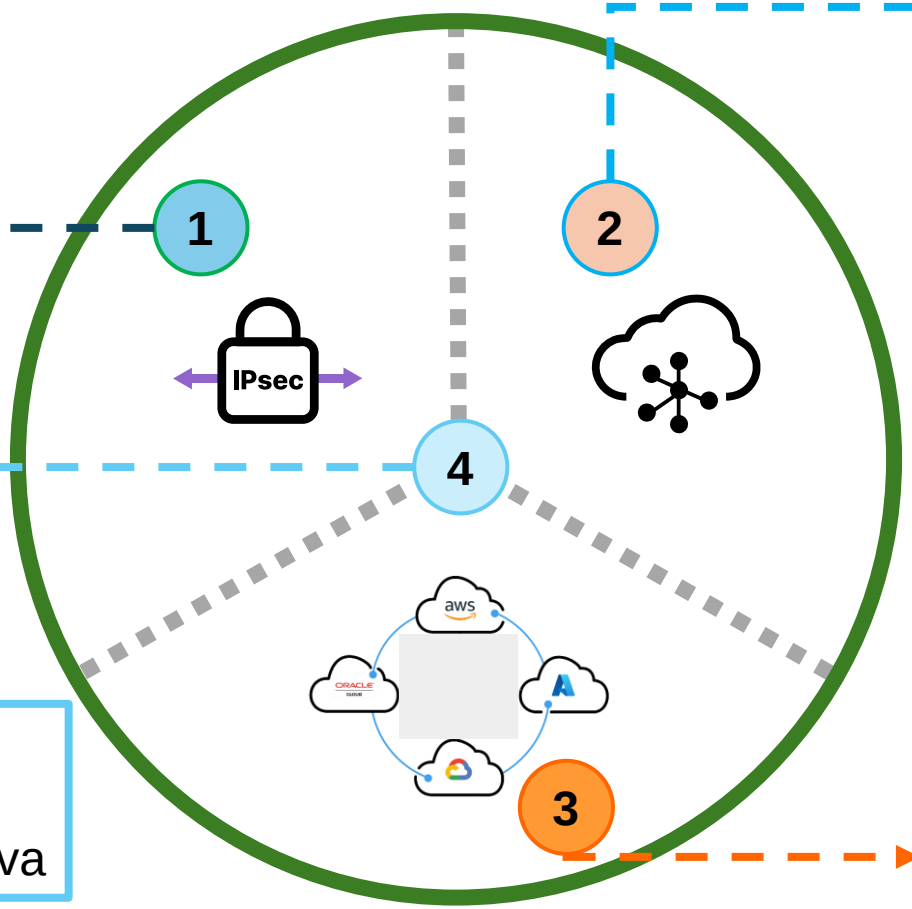
Multi-Tasking Nem Sempre é Algo Bom...

Multi-Tasking Nem Sempre é Algo Bom...

Principais Desafios de Rede em Nuvem

1. Conectividade Segura aos Recursos em Nuvem

2. Segmentação & Microssegmentação de Tráfego

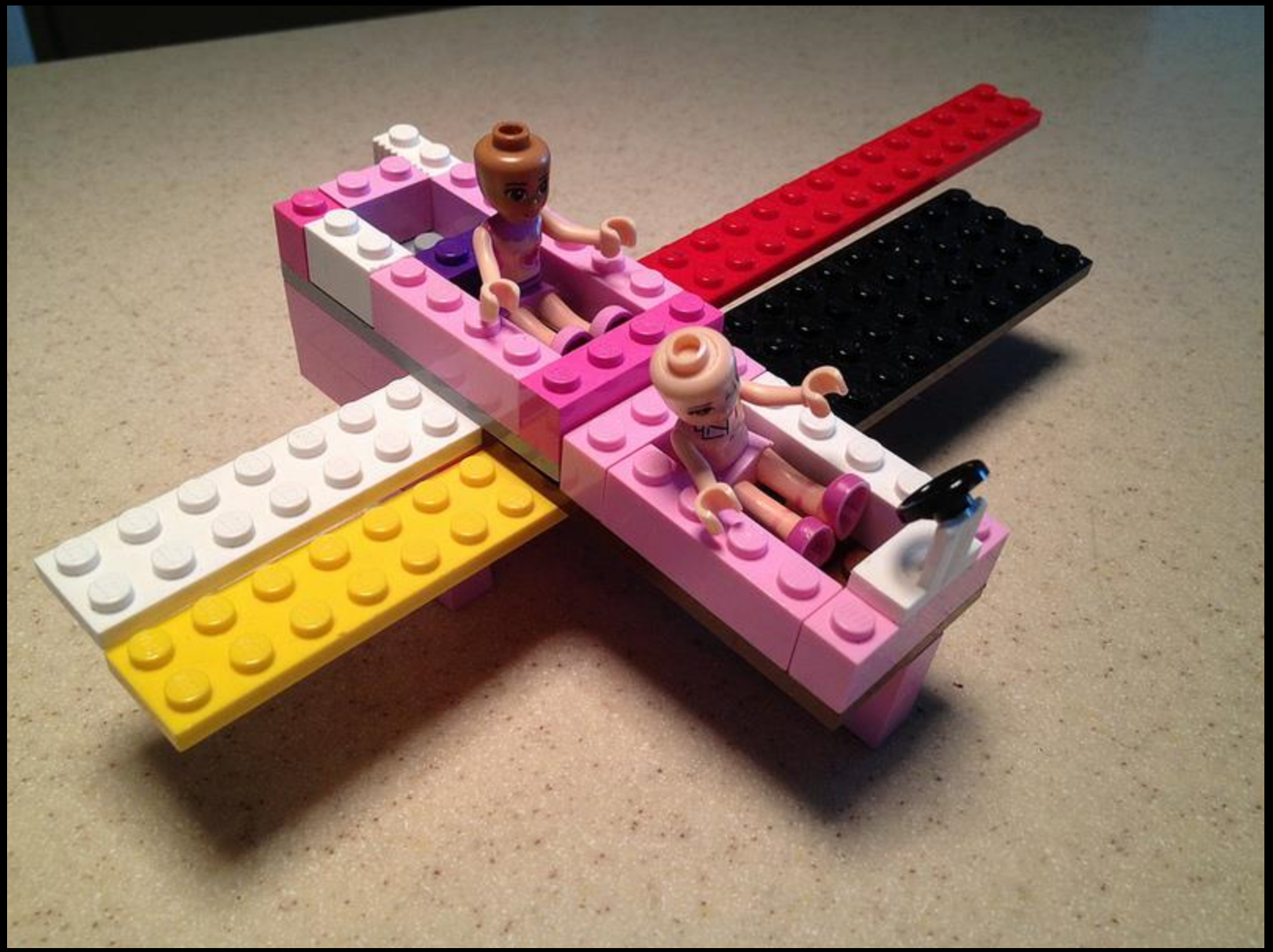


4. Deep Inspection, Visibilidade de Aplicações, Operação de Segurança Efetiva

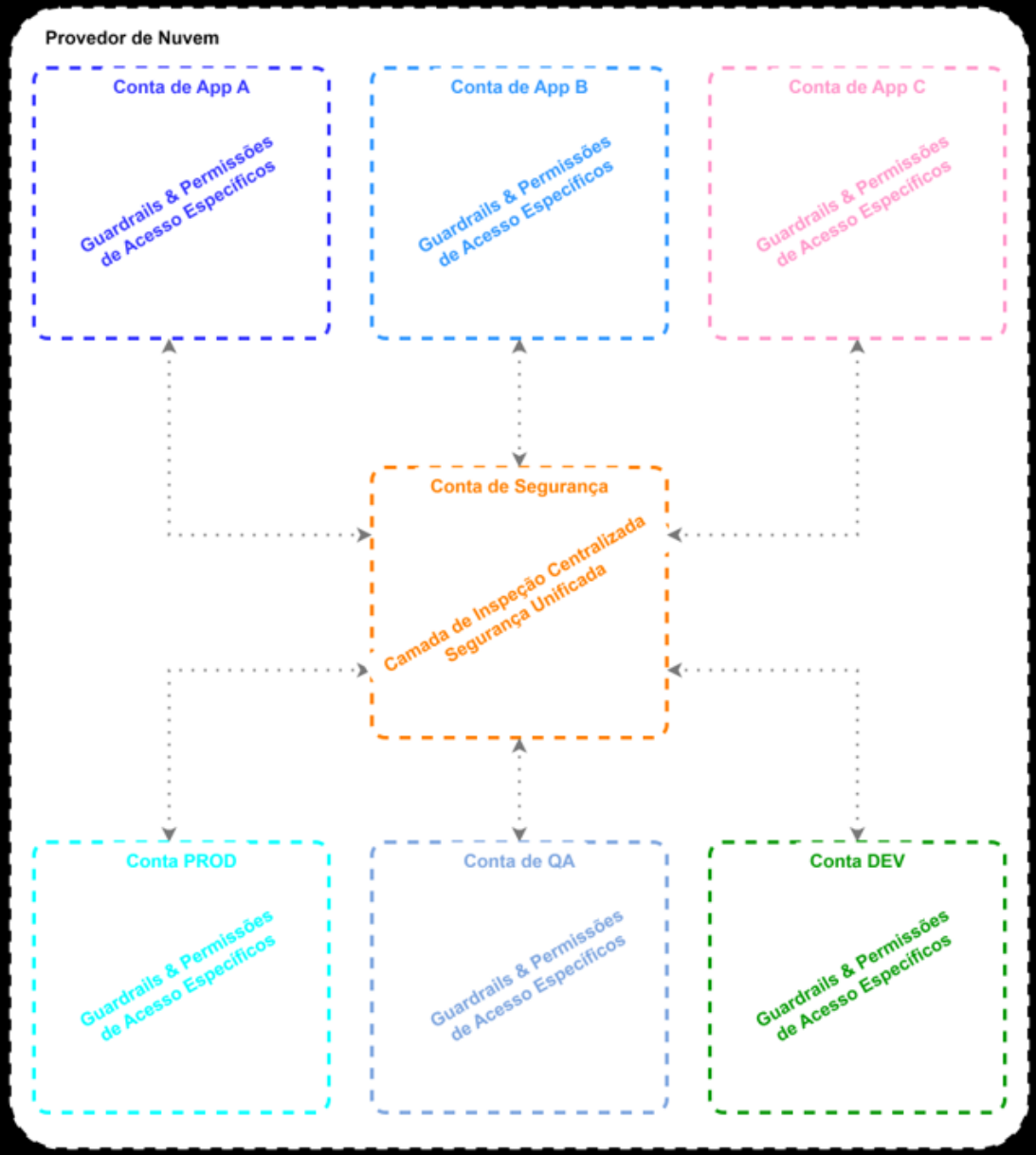
3. Gerenciamento Multi-Cloud, com foco em Conectividade & Automação

Segurança não é “apenas” uma ferramenta...

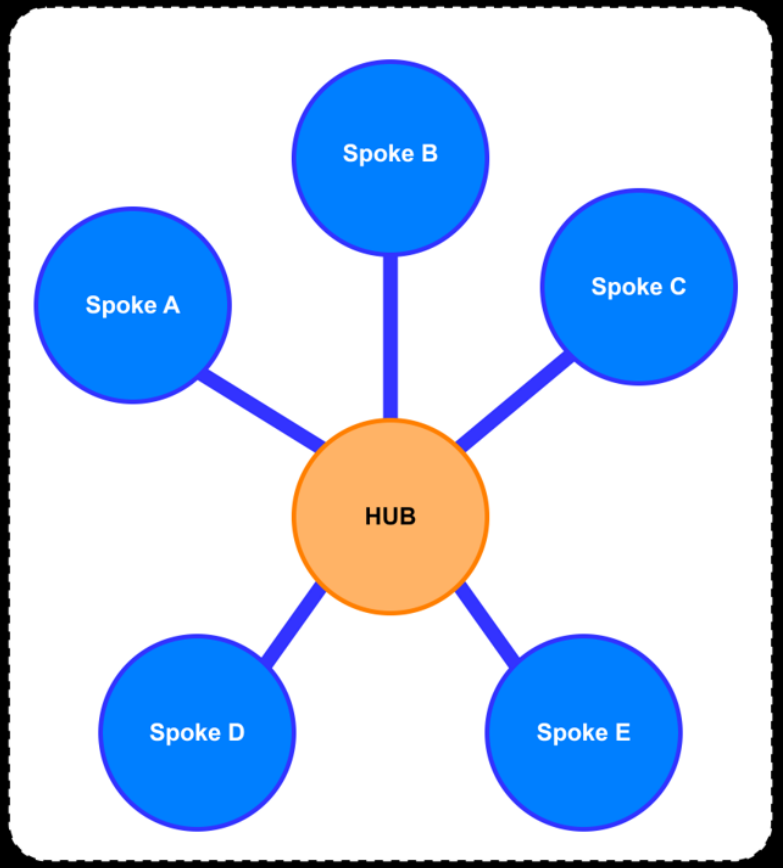
Mas então...
Por onde começar?



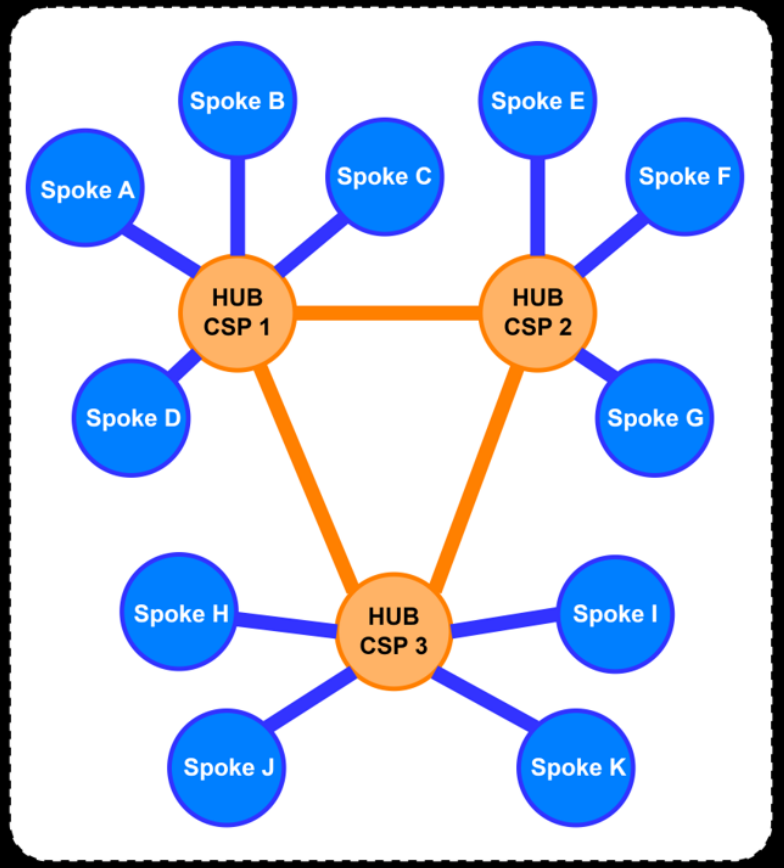
Cloud Landing Zones



Arquitetura Hub & Spoke



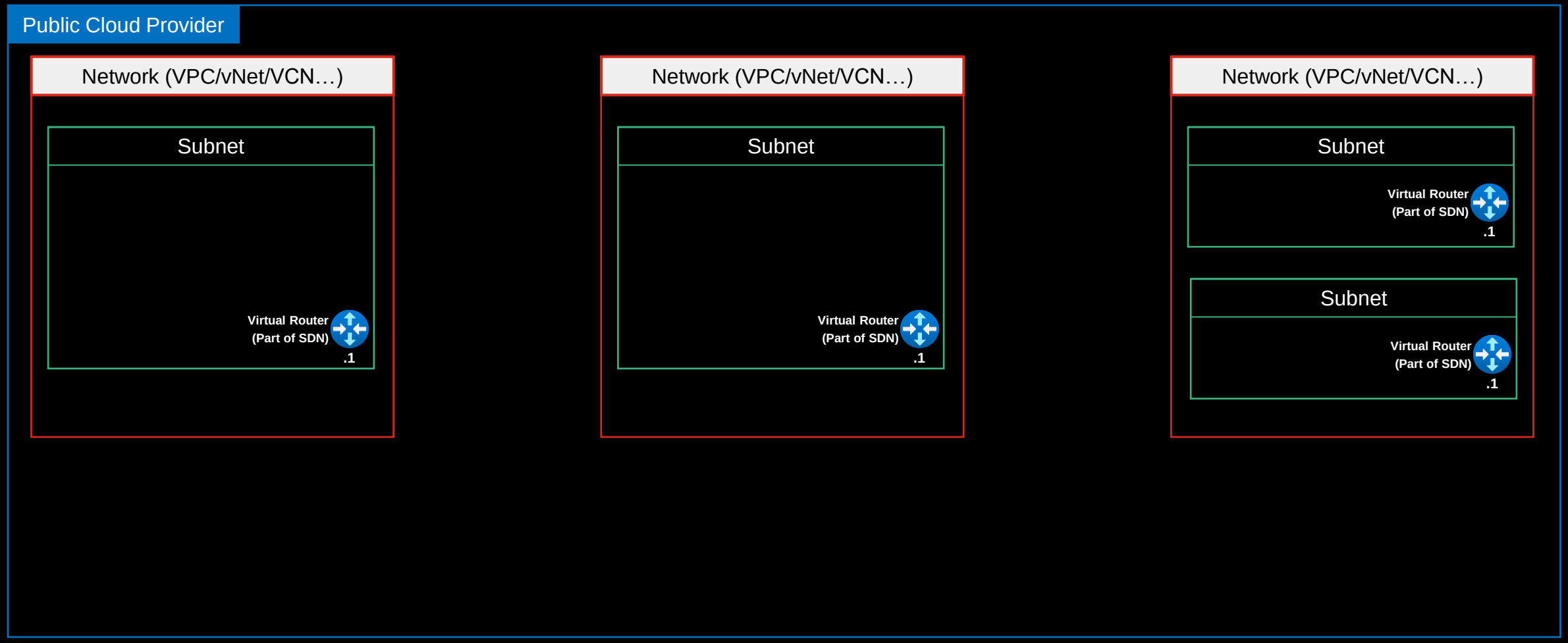
Hub & Spoke Única Nuvem



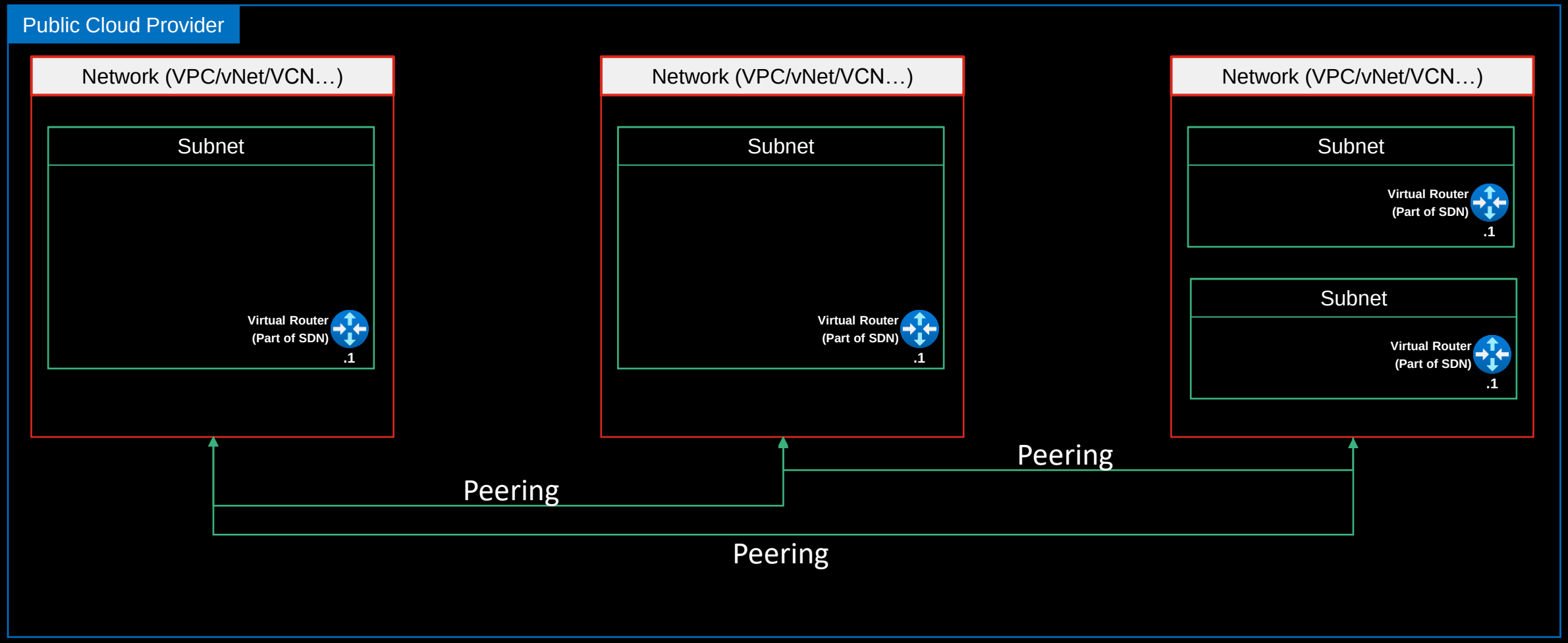
Hub & Spoke Multi-Cloud

Arquitetura de Rede em Nuvem

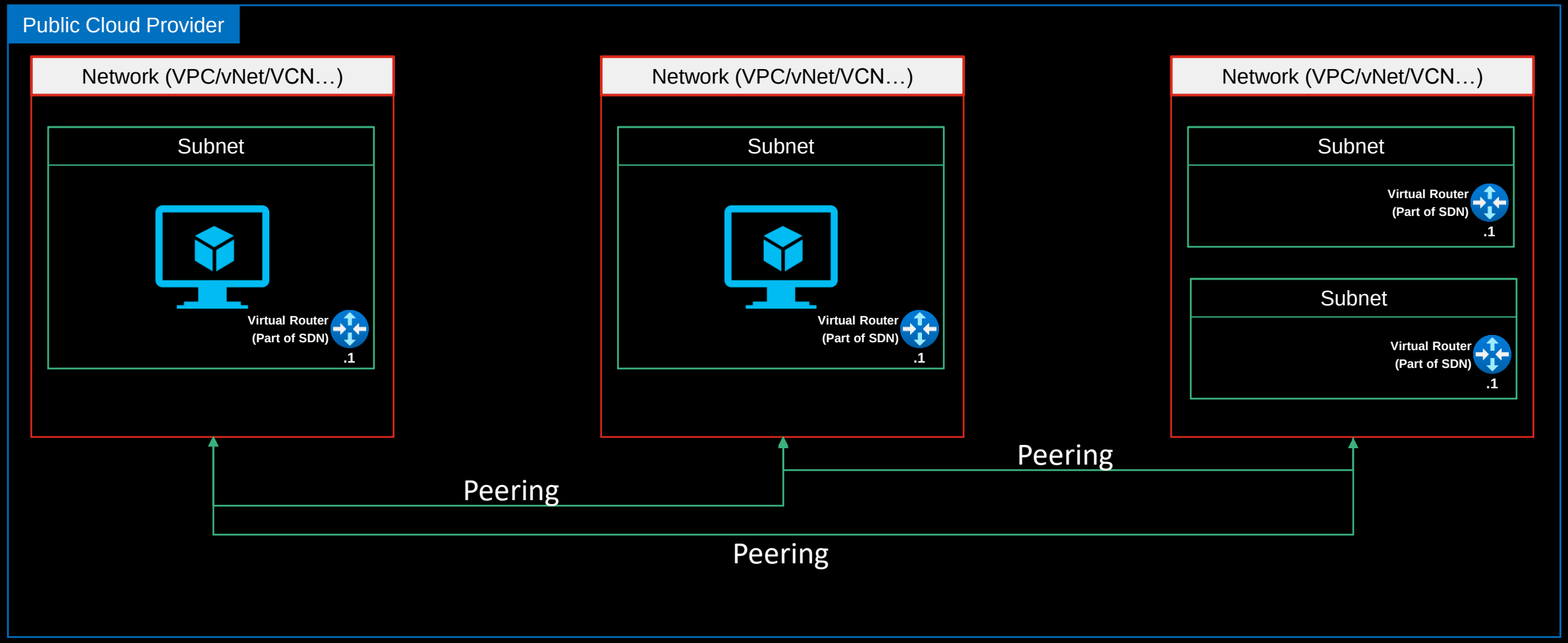
Arquitetura de Rede em Nuvem



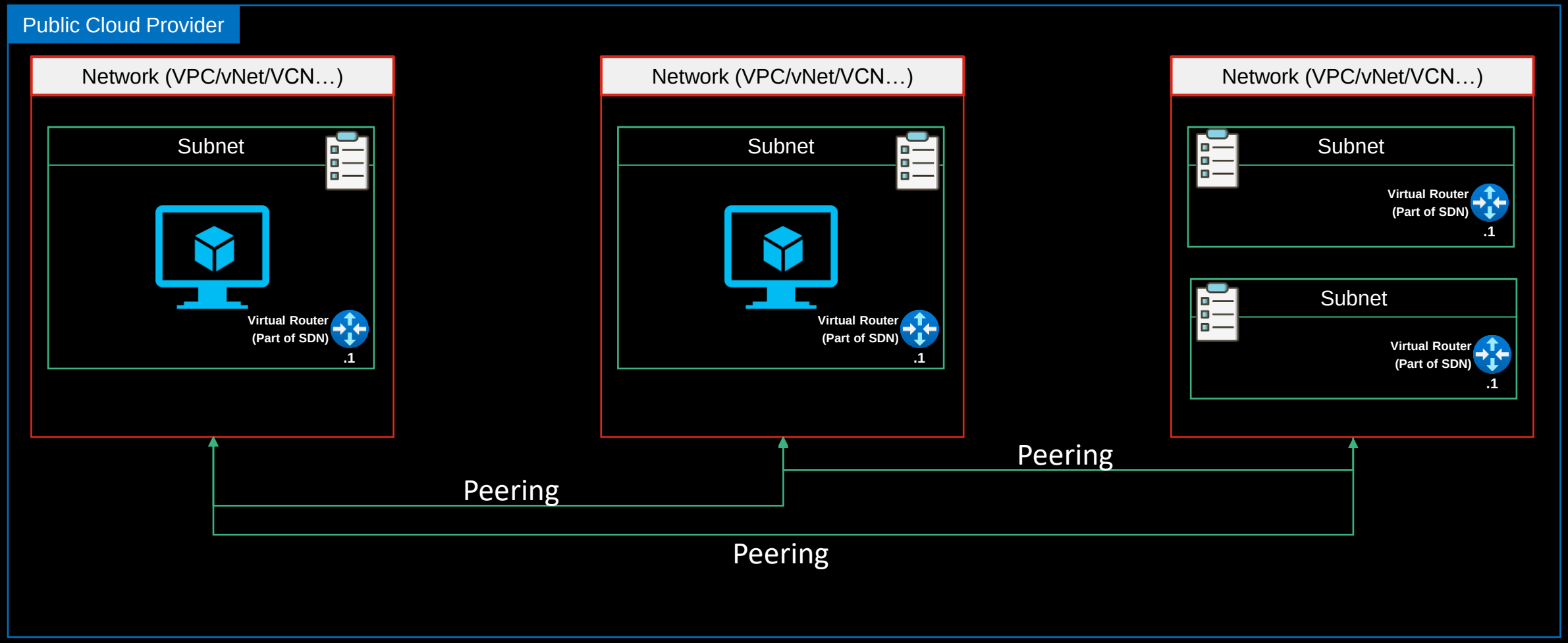
Arquitetura de Rede em Nuvem



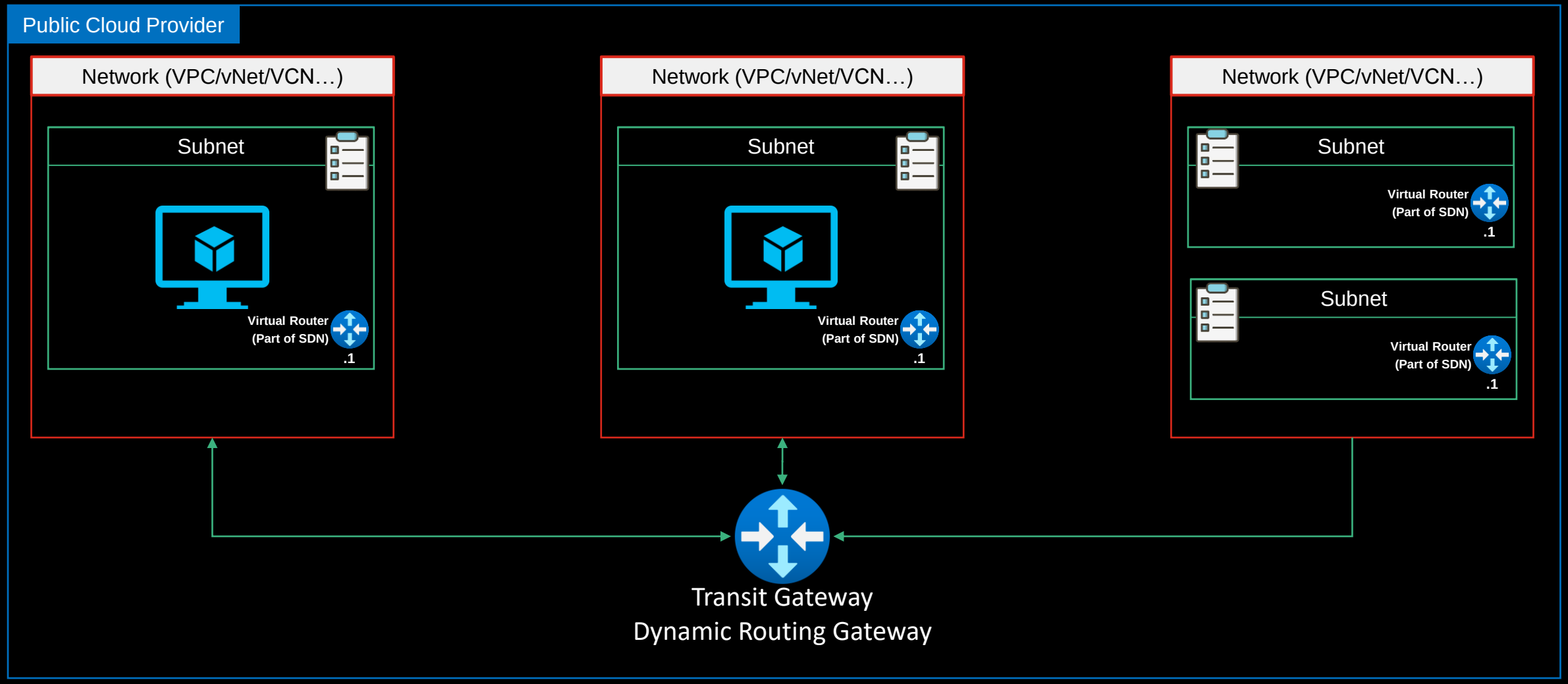
Arquitetura de Rede em Nuvem



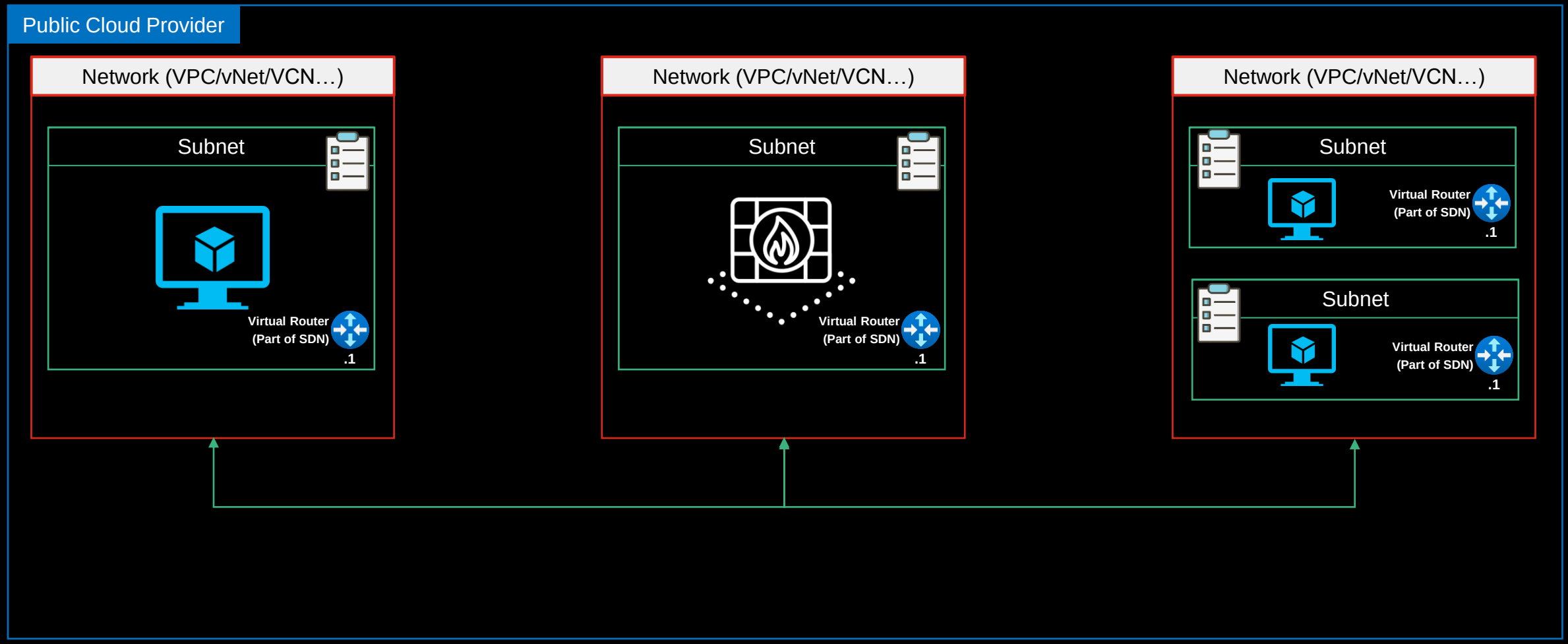
Arquitetura de Rede em Nuvem



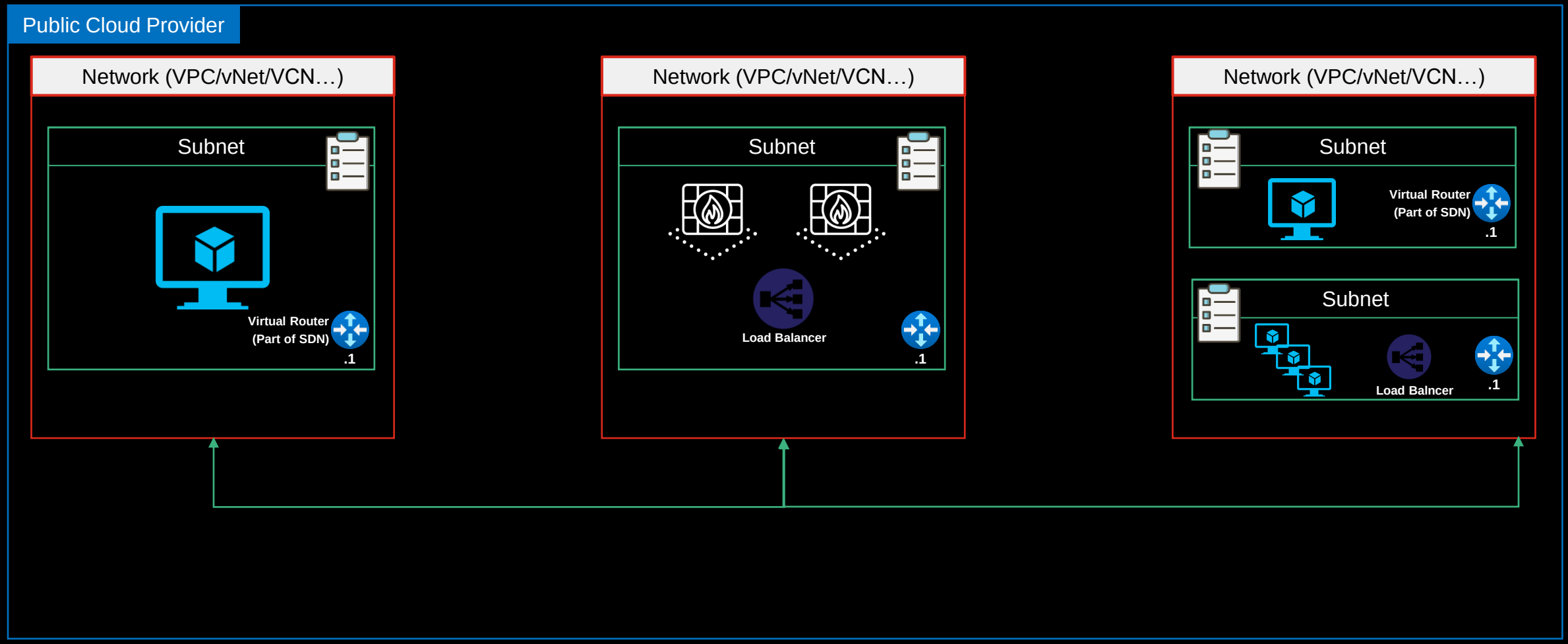
Arquitetura de Rede em Nuvem



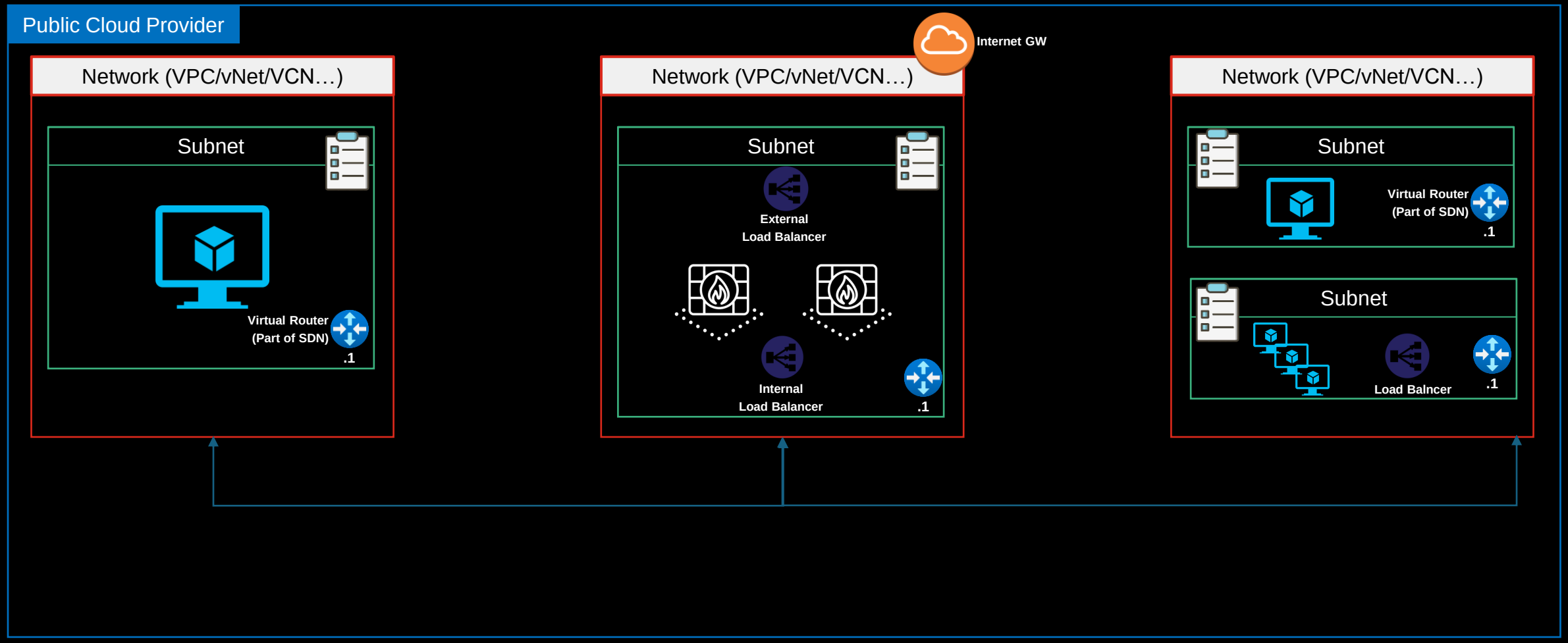
Arquitetura de Rede em Nuvem



Arquitetura de Rede em Nuvem



Arquitetura de Rede em Nuvem

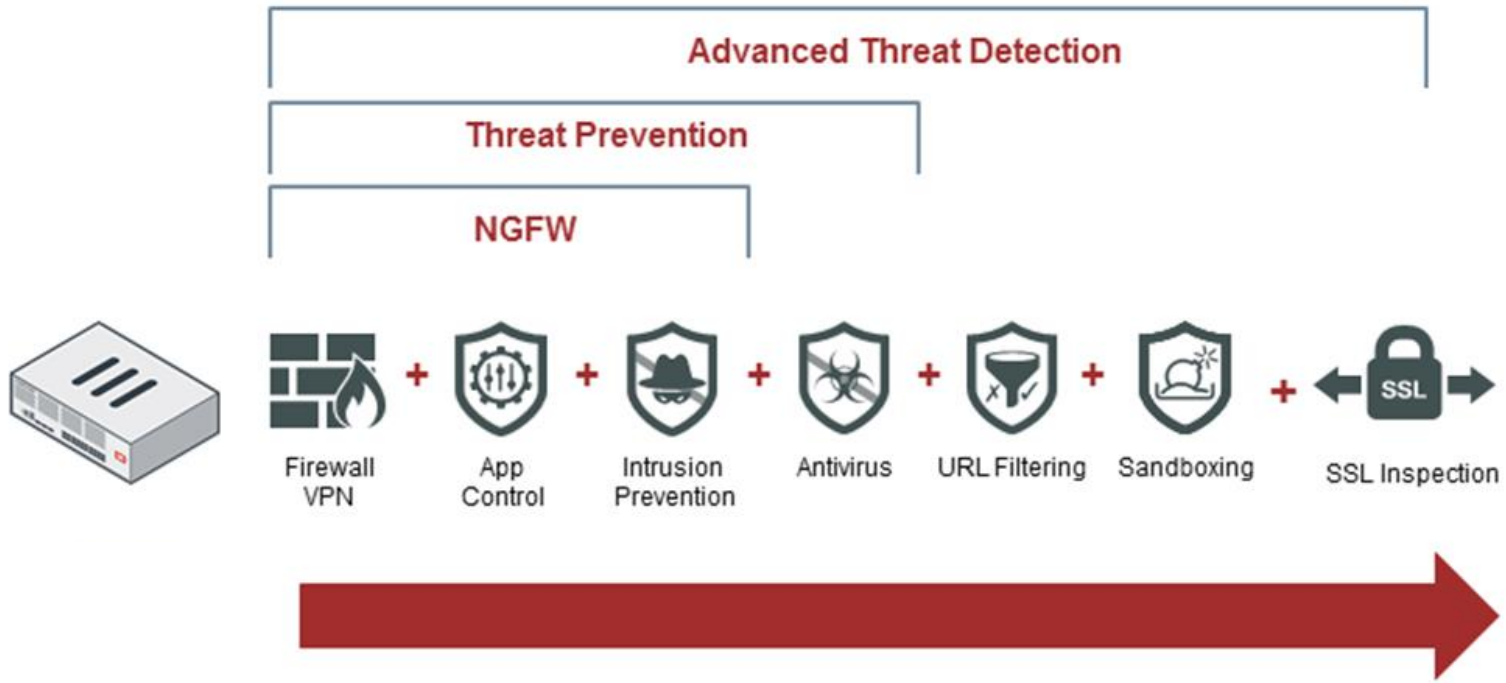


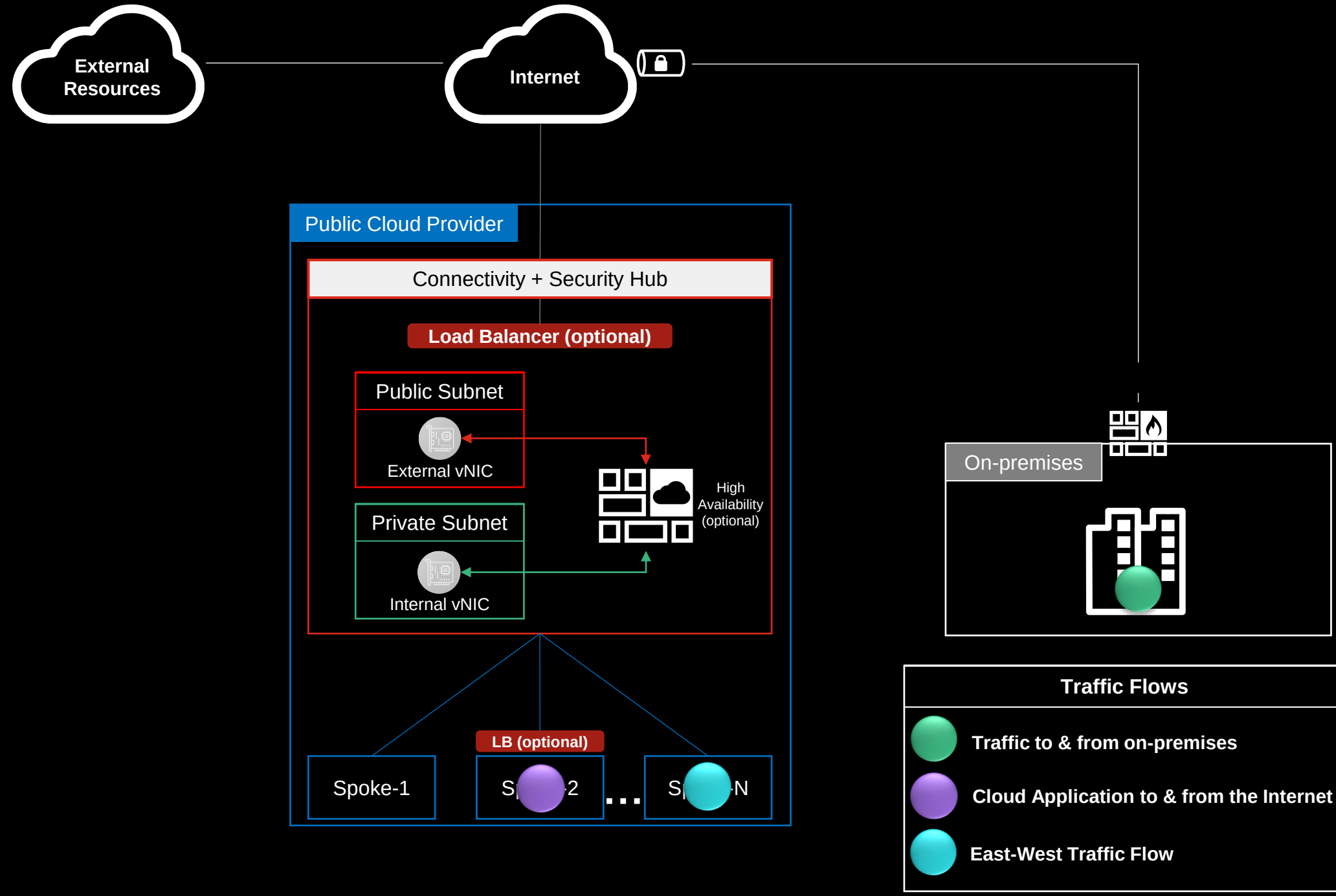
Next Generation Firewall

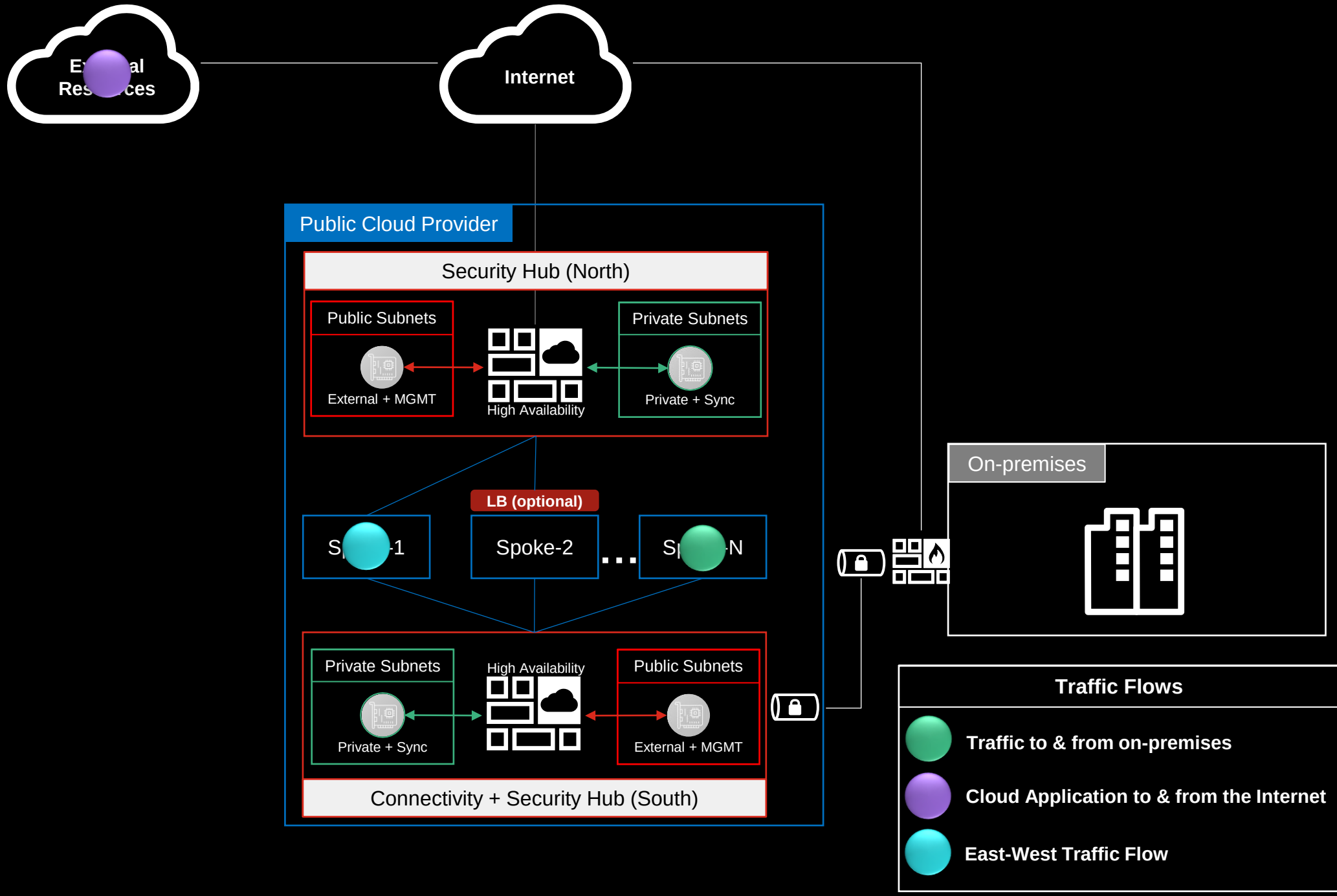
Standalone

- Firewall/VPN
- Intrusion Prevention
- Web Proxy
- Antivirus
- Web-Filter
- Sand-box
- SSL Inspection

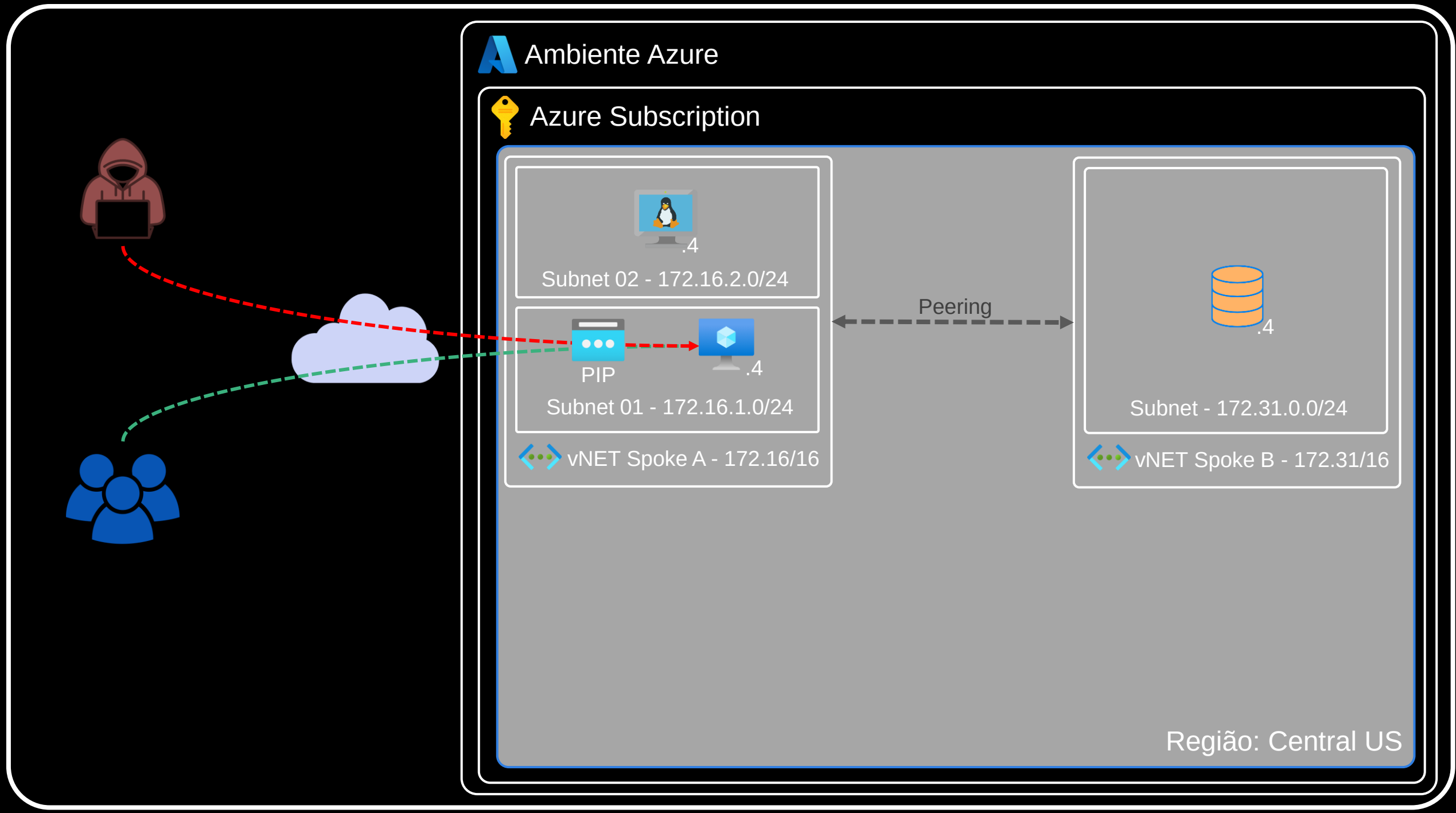
FortiGate Next Generation Firewalls

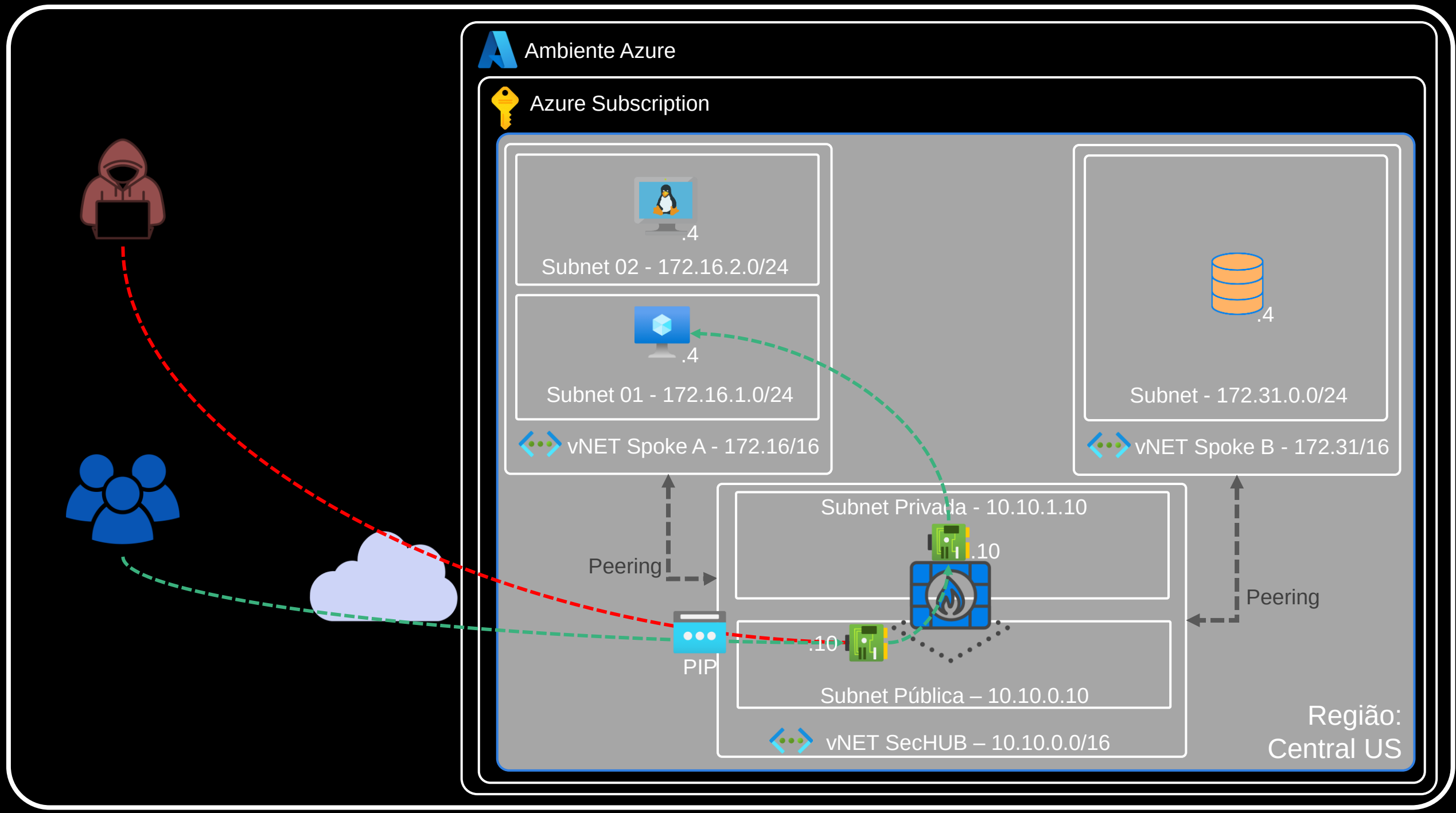



External Resources
Internet
Public Cloud Provider
Connectivity + Security Hub
Load Balancer (optional)
Public Subnet
External vNIC
Private Subnet
Internal vNIC
High Availability (optional)
LB (optional)
Spoke-1
On-premises
Traffic Flows
Traffic to & from on-premises
Cloud Application to & from the Internet
East-West Traffic Flow

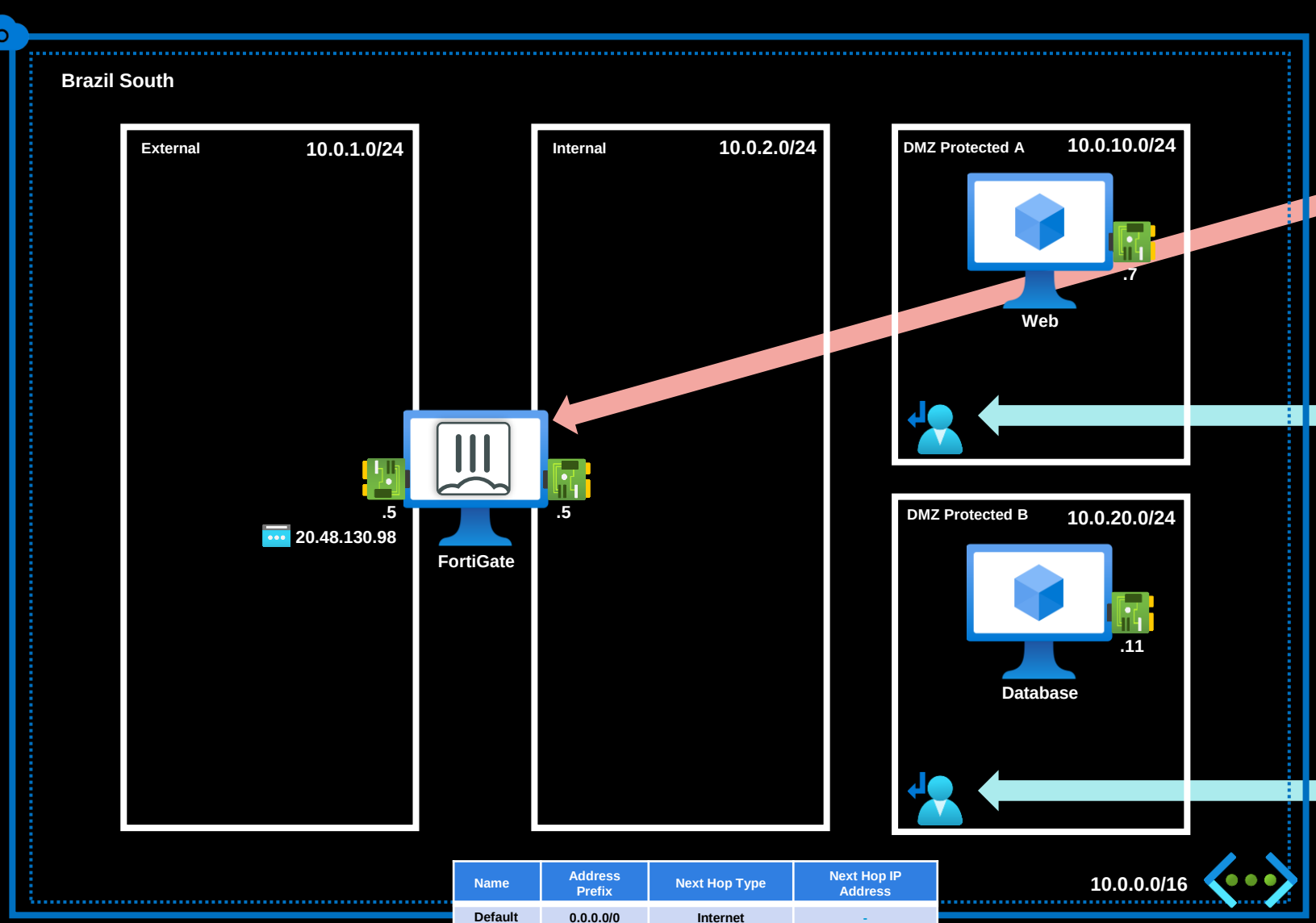

Internet
Public Cloud Provider
Security Hub (North)
Public Subnets
External + MGMT
High Availability
Private Subnets
Private + Sync
LB (optional)
Spoke-2
Private Subnets
Private + Sync
High Availability
Public Subnets
External + MGMT
Connectivity + Security Hub (South)
On-premises
Traffic Flows
Traffic to & from on-premises
Cloud Application to & from the Internet
East-West Traffic Flow


CLASSIC
LEGO


Ambiente Azure
Azure Subscription
.4
Subnet 02 - 172.16.2.0/24
PIP
.4
Subnet 01 - 172.16.1.0/24
vNET Spoke A - 172.16/16
Peering
.4
Subnet - 172.31.0.0/24
vNET Spoke B - 172.31/16
Região: Central US


Ambiente Azure
Azure Subscription
.4
Subnet 02 - 172.16.2.0/24
.4
Subnet 01 - 172.16.1.0/24
vNET Spoke A - 172.16/16
.4
Subnet - 172.31.0.0/24
vNET Spoke B - 172.31/16
Peering
Subnet Privada - 10.10.1.10
.10
Peering
PIP
.10
Subnet Pública – 10.10.0.10
vNET SecHUB – 10.10.0.0/16
Região:
Central US

FortiGate-VM Tabelas de Roteamento



Destination	Gateway Address	Interface
0.0.0.0/0	10.0.1.1	Port1
10.0.10.0/24	10.0.2.1	Port2
10.0.20.0/24	10.0.2.1	Port2

FortiGate Static Routes

Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.5
User	10.0.20.0/24	Virtual appliance	10.0.2.5

DMZ Protected A Route Table

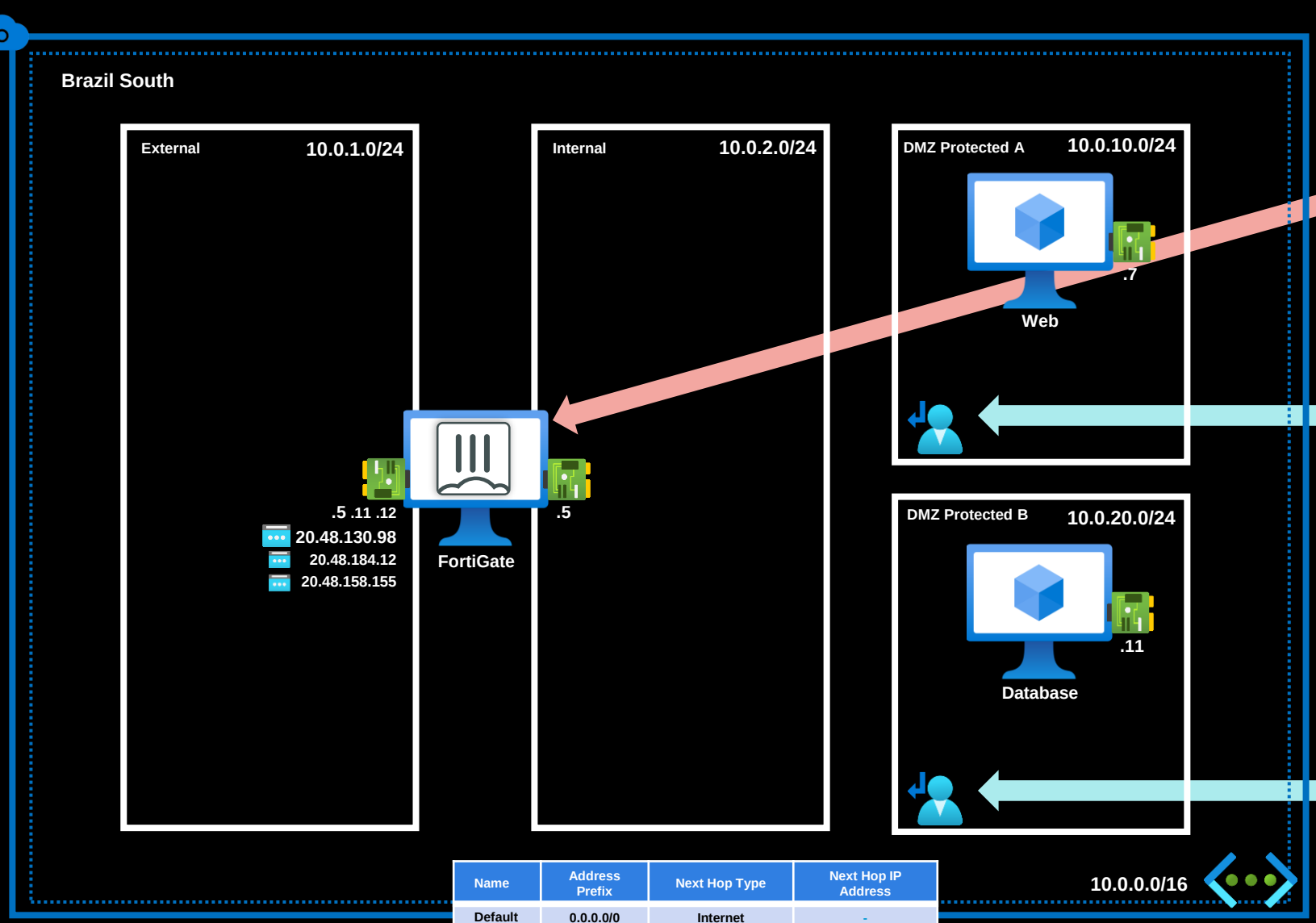
Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.5
User	10.0.10.0/24	Virtual appliance	10.0.2.5

DMZ Protected B Route Table

Name	Address Prefix	Next Hop Type	Next Hop IP Address
Default	0.0.0.0/0	Internet	-
Default	10.0.0.0/16	Virtual network	-

VNET Default Routing

Múltiplos IPs Públicos



Destination	Gateway Address	Interface
0.0.0.0/0	10.0.1.1	Port1
10.0.10.0/24	10.0.2.1	Port2
10.0.20.0/24	10.0.2.1	Port2

FortiGate Static Routes

Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.5
User	10.0.20.0/24	Virtual appliance	10.0.2.5

DMZ Protected A Route Table

Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.5
User	10.0.10.0/24	Virtual appliance	10.0.2.5

DMZ Protected B Route Table

Name	Address Prefix	Next Hop Type	Next Hop IP Address
Default	0.0.0.0/0	Internet	-
Default	10.0.0.0/16	Virtual network	-

VNET Default Routing

Arquiteturas FortiGate-VM

Single Gateway

- Apenas 1x VM
- Mínimo 2x vNICs
- Sem Alta-Disponibilidade

aws Azure Google Cloud ORACLE

Ativo-Passivo (Fabric)

- 2x VMs formando HA
- Necessário 4x vNICs
- Load Balancers NÃO necessários
- Failover = API call

aws Azure Google Cloud ORACLE

Ativo-Passivo (Sanduiche)

- 2x VMs formando HA
- Necessário 4x vNICs
- Load Balancers SÃO necessários
- Failover via Cloud LB

aws Azure Google Cloud ORACLE

HA Ativo-Ativo

- 2x VMs formando HA
- Necessário 2x vNICs
- Load Balancers SÃO necessários
- Failover via Cloud LB

aws Azure Google Cloud ORACLE

Auto Scaling

- Múltiplas VMs (in & out)
- Escalabilidade baseado no tráfego de rede
- Modelo Ativo-Ativo

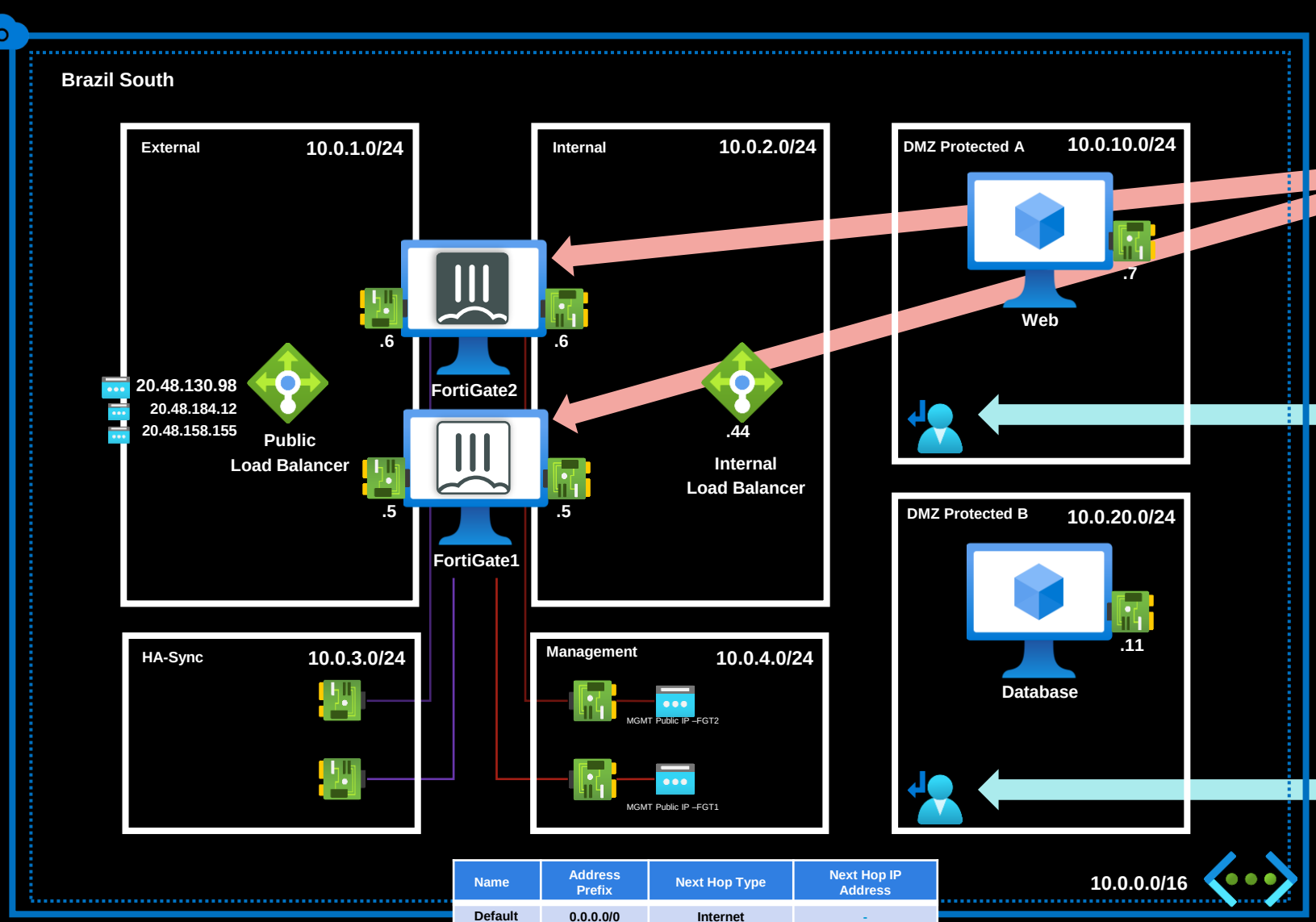
aws Azure Google Cloud

GWLB

- Integração com Serviço de GWLB dos CSPs
- Melhor para cenários para ambientes de nuvem já pré existentes

aws Azure

Ativo-Passivo com Load Balancer & Múltiplos IPs



Destination	Gateway Address	Interface
0.0.0.0/0	10.0.1.1	Port1
10.0.10.0/24	10.0.2.1	Port2
10.0.20.0/24	10.0.2.1	Port2

FortiGate Static Routes

Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.44
User	10.0.20.0/24	Virtual appliance	10.0.2.44

DMZ Protected A Route Table

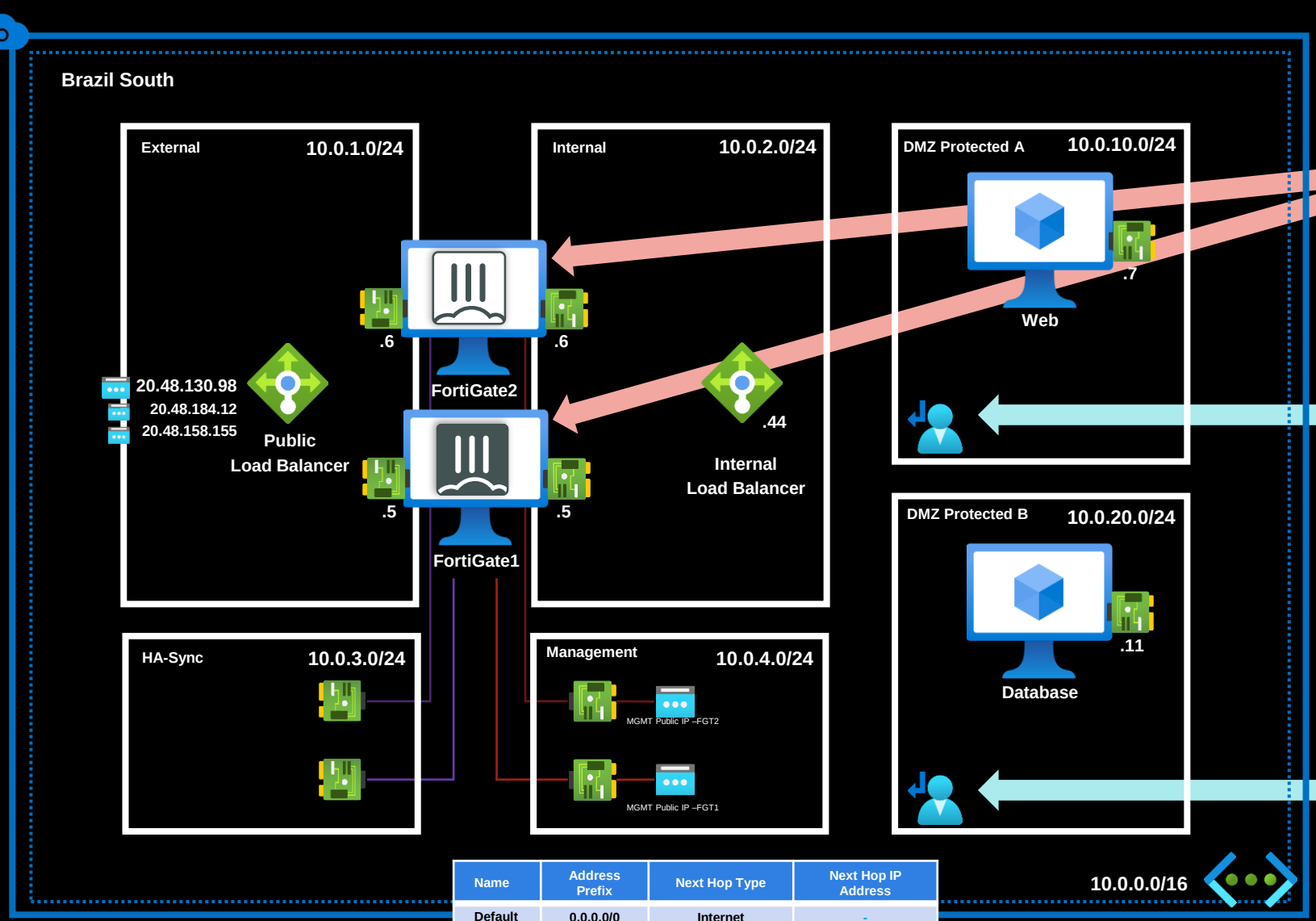
Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.44
User	10.0.10.0/24	Virtual appliance	10.0.2.44

DMZ Protected B Route Table

Name	Address Prefix	Next Hop Type	Next Hop IP Address
Default	0.0.0.0/0	Internet	-
Default	10.0.0.0/16	Virtual network	-

VNET Default Routing

Ativo-Passivo com Load Balancer & Múltiplos IPs



Destination	Gateway Address	Interface
0.0.0.0/0	10.0.1.1	Port1
10.0.10.0/24	10.0.2.1	Port2
10.0.20.0/24	10.0.2.1	Port2

FortiGate Static Routes

Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.44
User	10.0.20.0/24	Virtual appliance	10.0.2.44

DMZ Protected A Route Table

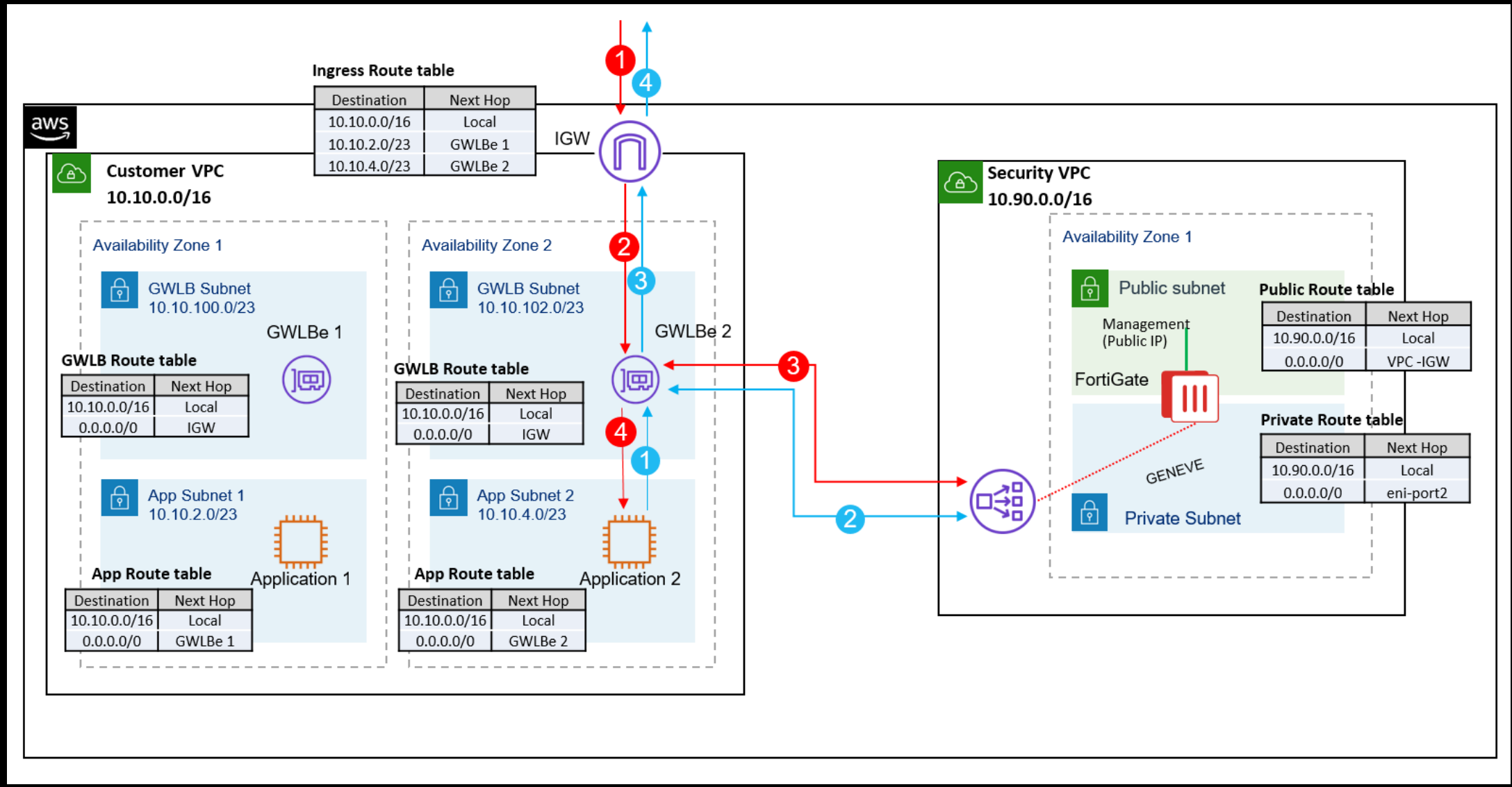
Name	Address Prefix	Next Hop Type	Next Hop IP Address
User	0.0.0.0/0	Virtual appliance	10.0.2.44
User	10.0.10.0/24	Virtual appliance	10.0.2.44

DMZ Protected B Route Table

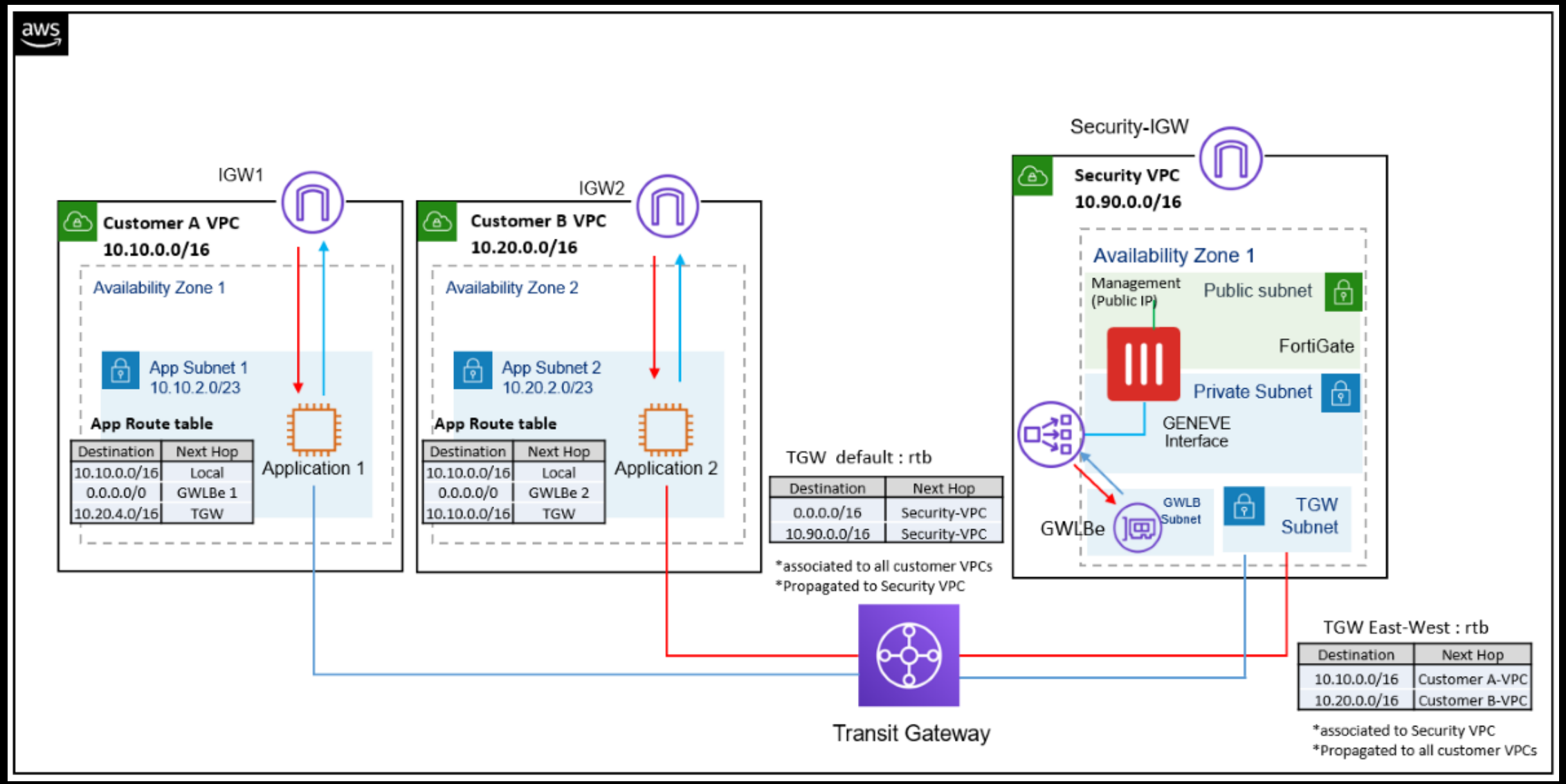
Name	Address Prefix	Next Hop Type	Next Hop IP Address
Default	0.0.0.0/0	Internet	-
Default	10.0.0.0/16	Virtual network	-

VNET Default Routing

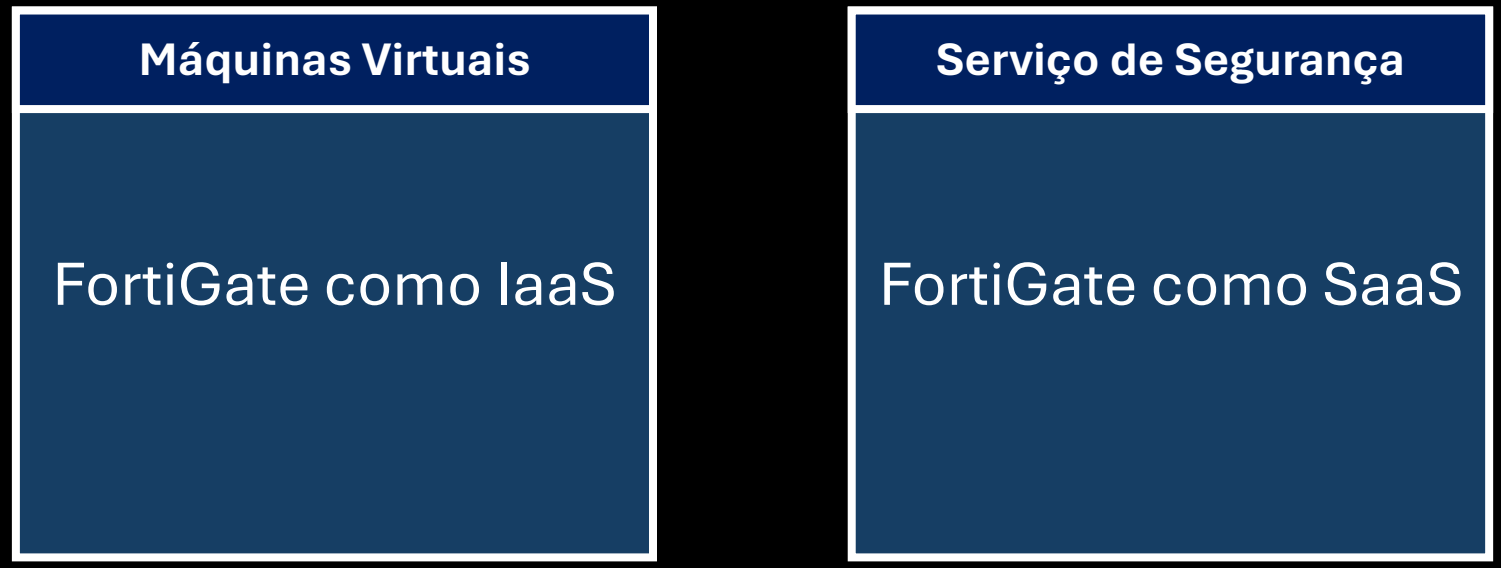
FortiGate-VM & Gateway Load Balancer



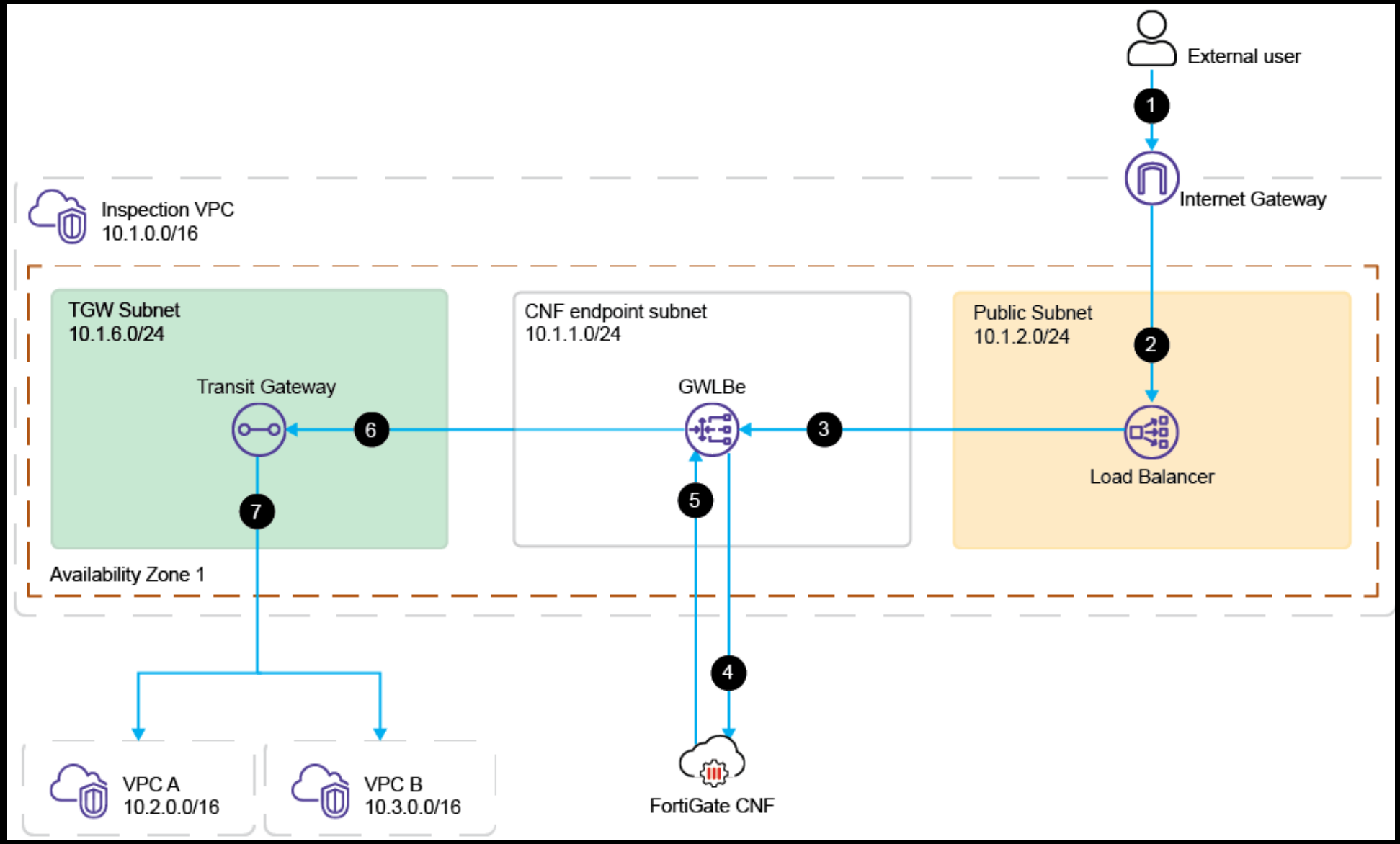
FortiGate-VM & Gateway Load Balancer



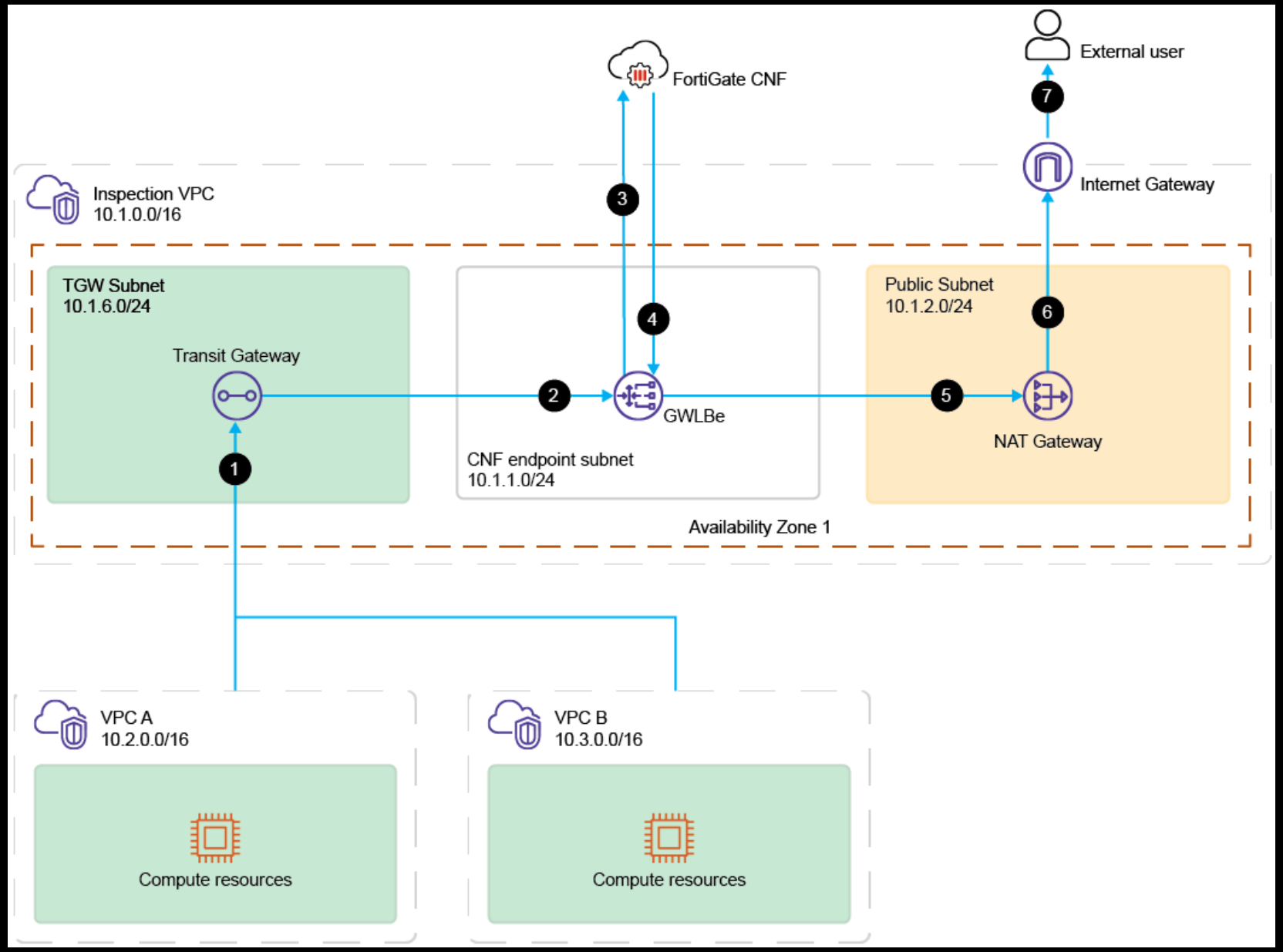
Diferentes Possibilidades



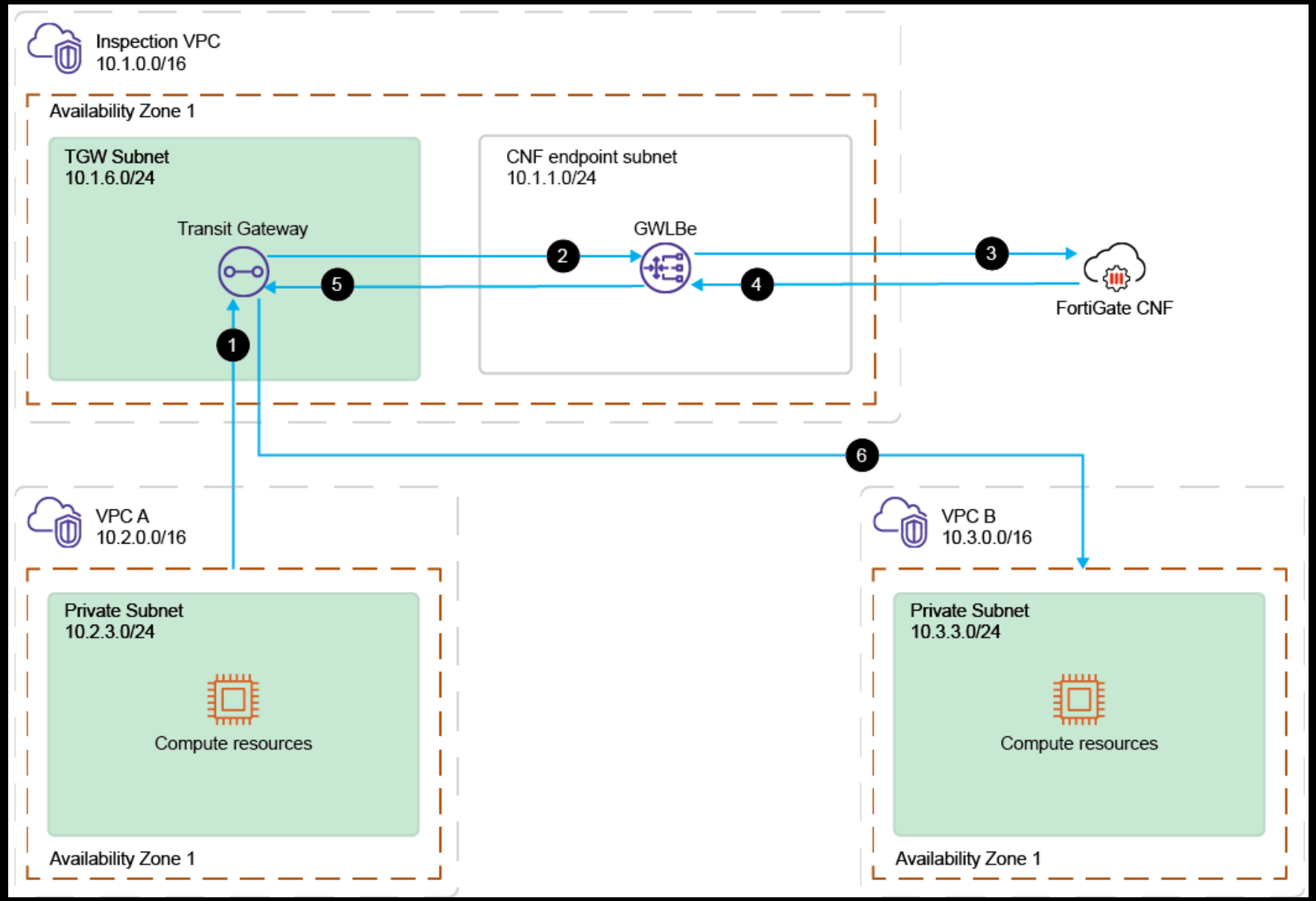
FortiGate as a Service - Ingress



FortiGate as a Service - Egress



FortiGate as a Service - Lateral



Segurança em Nuvem Consolidada