* Cloud Security

TOCI III Course

CS Department @ University of Karachi

Cloud Security

- Internet is Cloud underlying connectivity bring security concerns
- Internet security is fundamental for Cloud Security
- Cloud should be as secure as traditional Datacenters
- Computer is not only the asset to be secured
- Public IP must be whitelisted to access Cloud jump / bastion host
- Data and application are more crucial to be protected
- Security in cloud doesn’t come free
- Cloud customer is ultimately accountable for its Security
- Customer should own key management
- Encryption or crypto shredding is the method for data deletion in Cloud

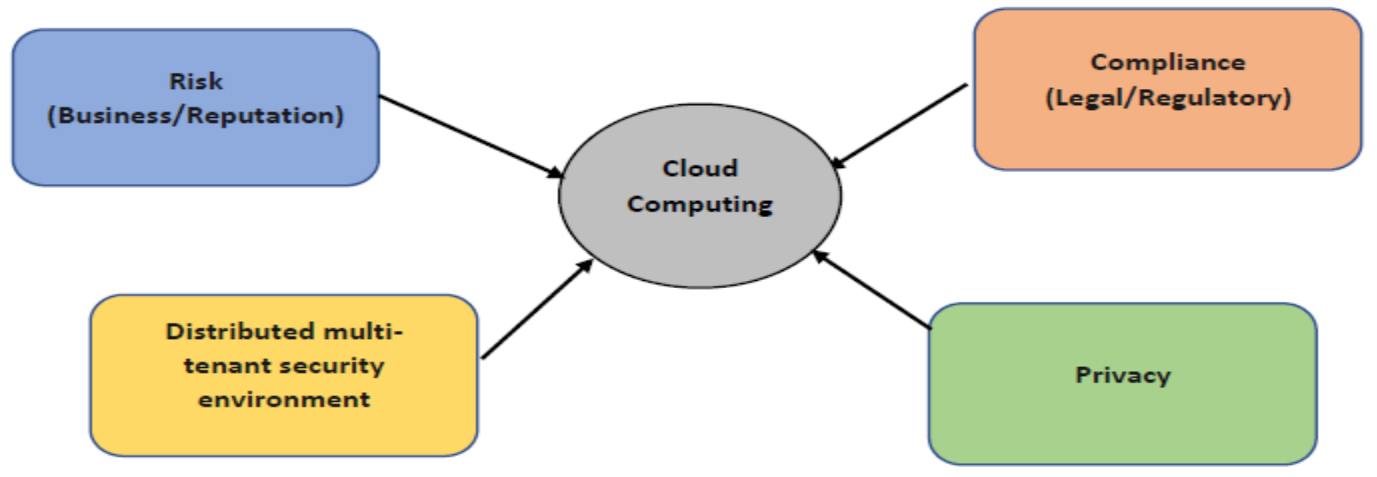
Cloud Security Controls

- **A security control** is a safeguard or countermeasure to protect information systems, networks, data, and physical assets from threats, risks, and vulnerabilities.

- **Security controls** are parameters implemented to protect various forms of data and infrastructure important to an organization.

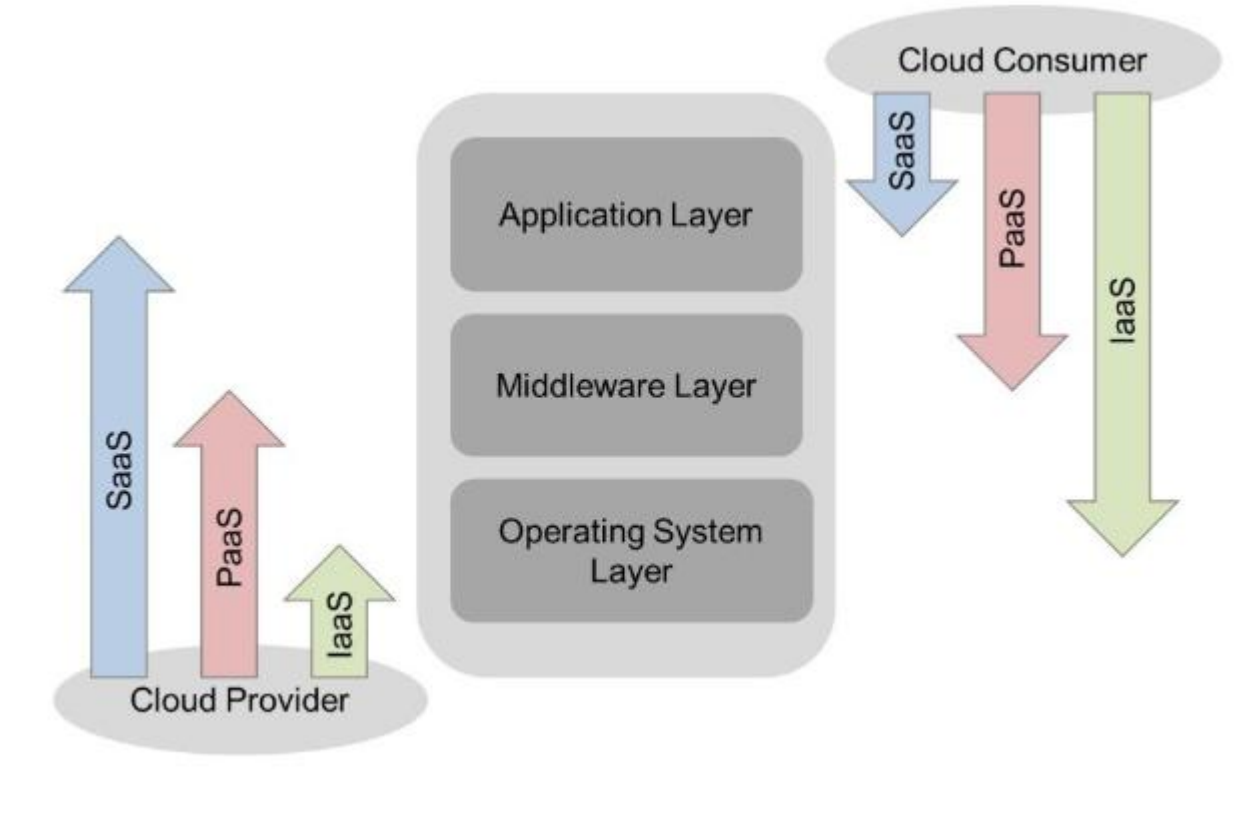
- These parametners and frameworks are, such as the Secure Controls Framework (SCF), NIST Cybersecurity Framework, or ISO 27001.

Cloud Security Controls



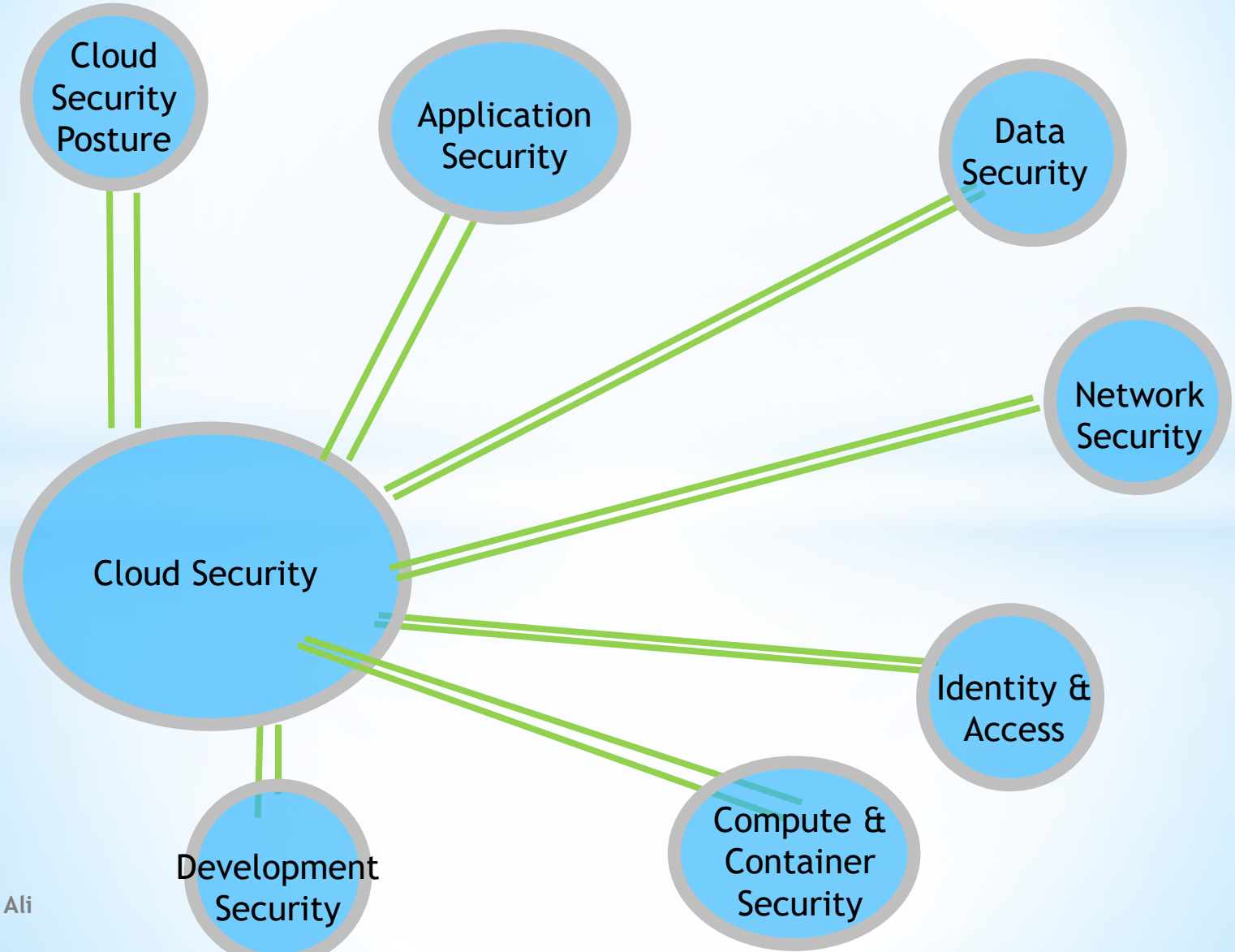
Cloud Security Controls

Control between consumer and provider

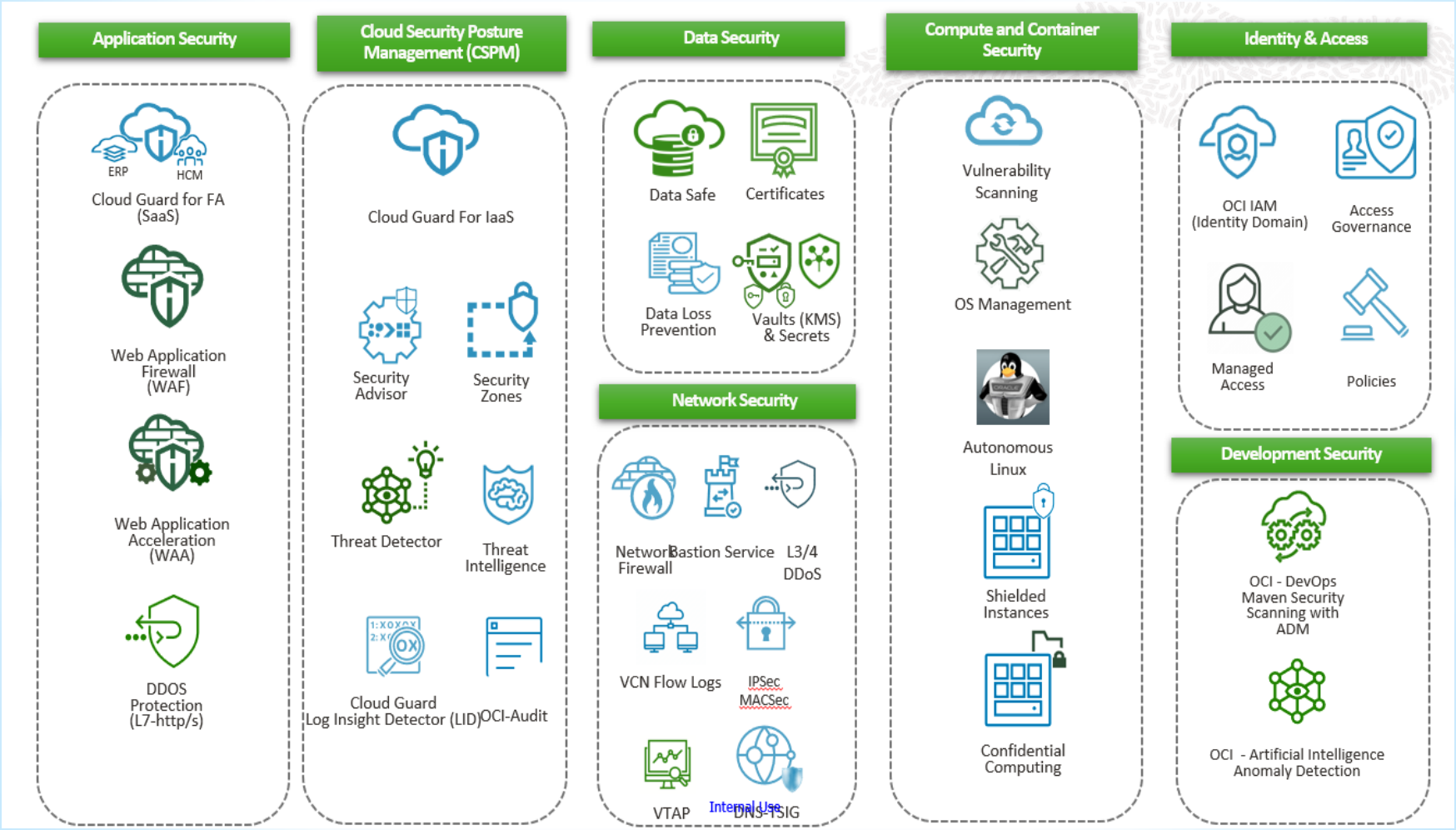


Cloud Security Domains

Cloud Security Domains



Cloud Security Domains



Cloud Security Domains

Identity and Access

- OCI IAM
- Access Governace (why and who)
- Managed Access (how grant access)
- Policies

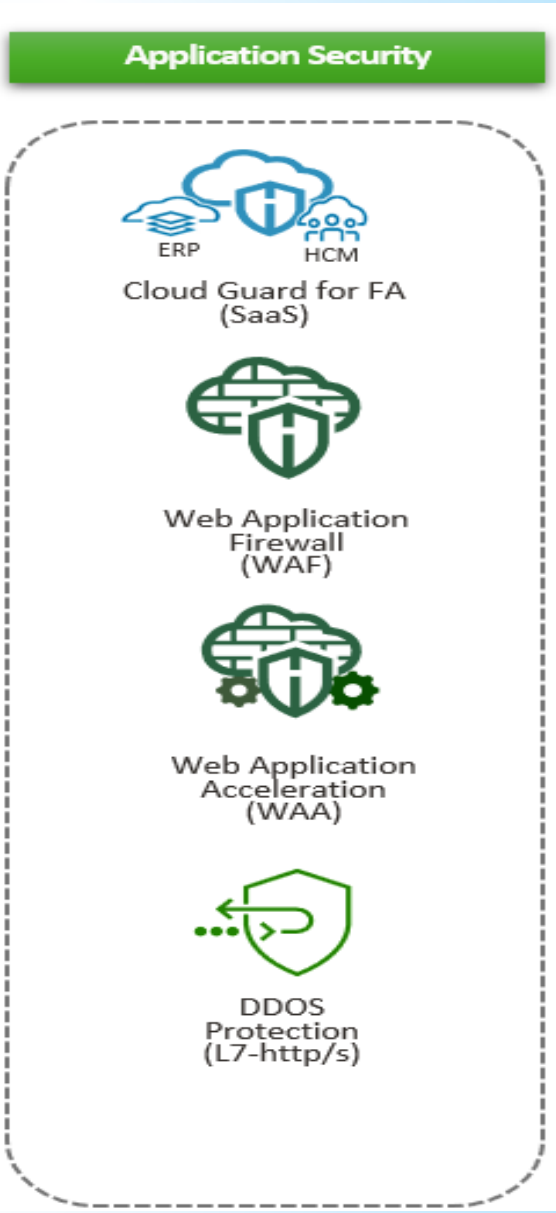
Development Security

- OCI – DevOps Maven Security scanning with ADM
- OCI – Artificial Intelligence Anomaly Detection

Cloud Security Domains

Application Security

- Cloud Access Security Broker (App)
- Web Application Firewall
- DDoS Protection L7-https
- Web Application Acceleration



Cloud Security Domains

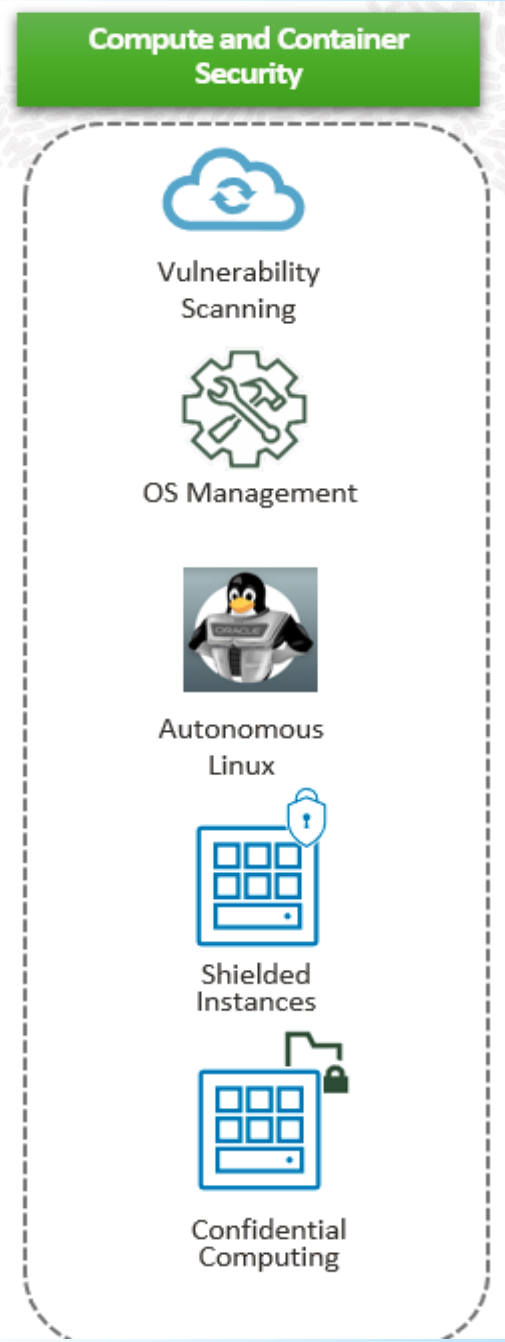
Cloud Security Posture Management

- CSPM for IaaS (Infra.)
- Security Advisor
- Security Zones
- Threat Detector
- Threat Intelligence

Cloud Security Domains

Compute and Container Security

- Vulnerability Scanning
- OS Management
- Autonomous Linux (self patching)
- Shielded Instances (for boot / kernel)
- Confidential Computing (encryption for as well memory and CPU)



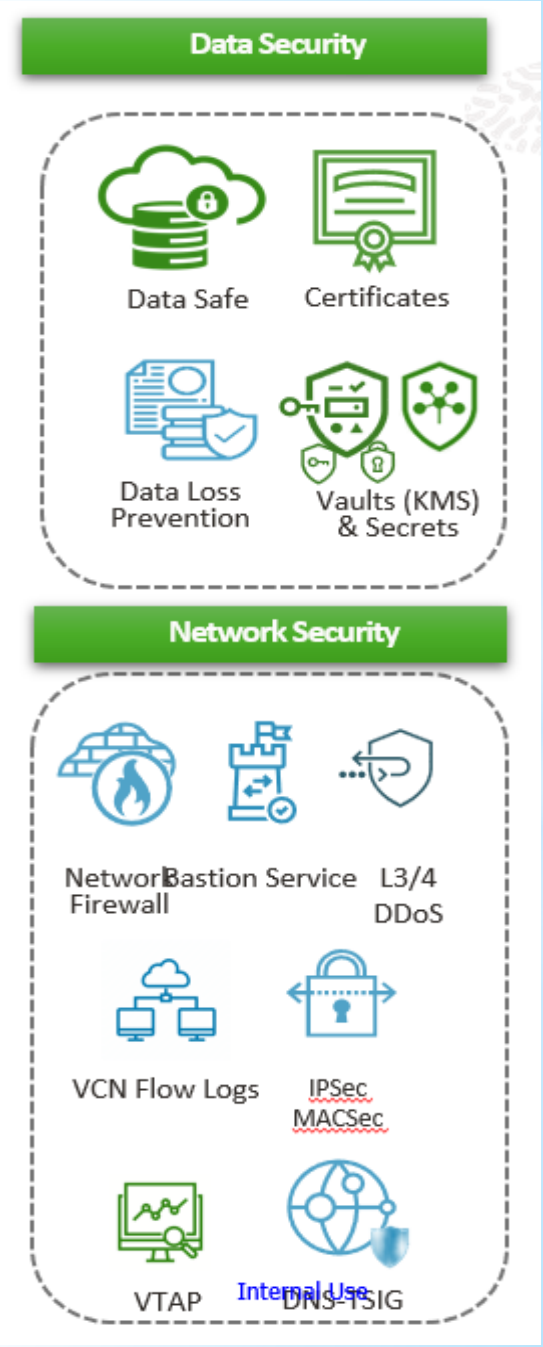
Cloud Security Domains

Data Security

- Data Safe
- Certificates
- Data Loss Prevention DLP
- Vaults & Secrets (KMS)

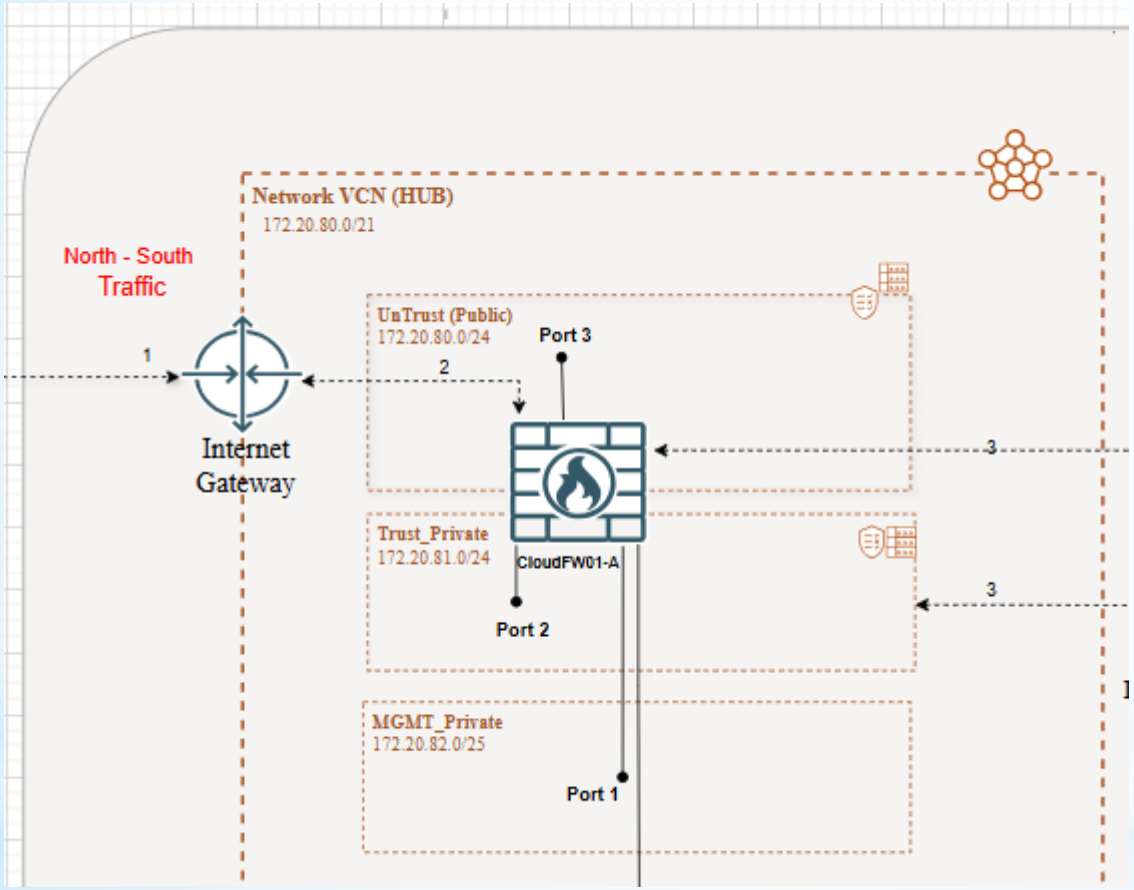
Network Security

- Network Firewall
- Bastion Service
- L3/4 DDoS
- IPSec, MACSec
- DNS TSIG (Shared secrets)

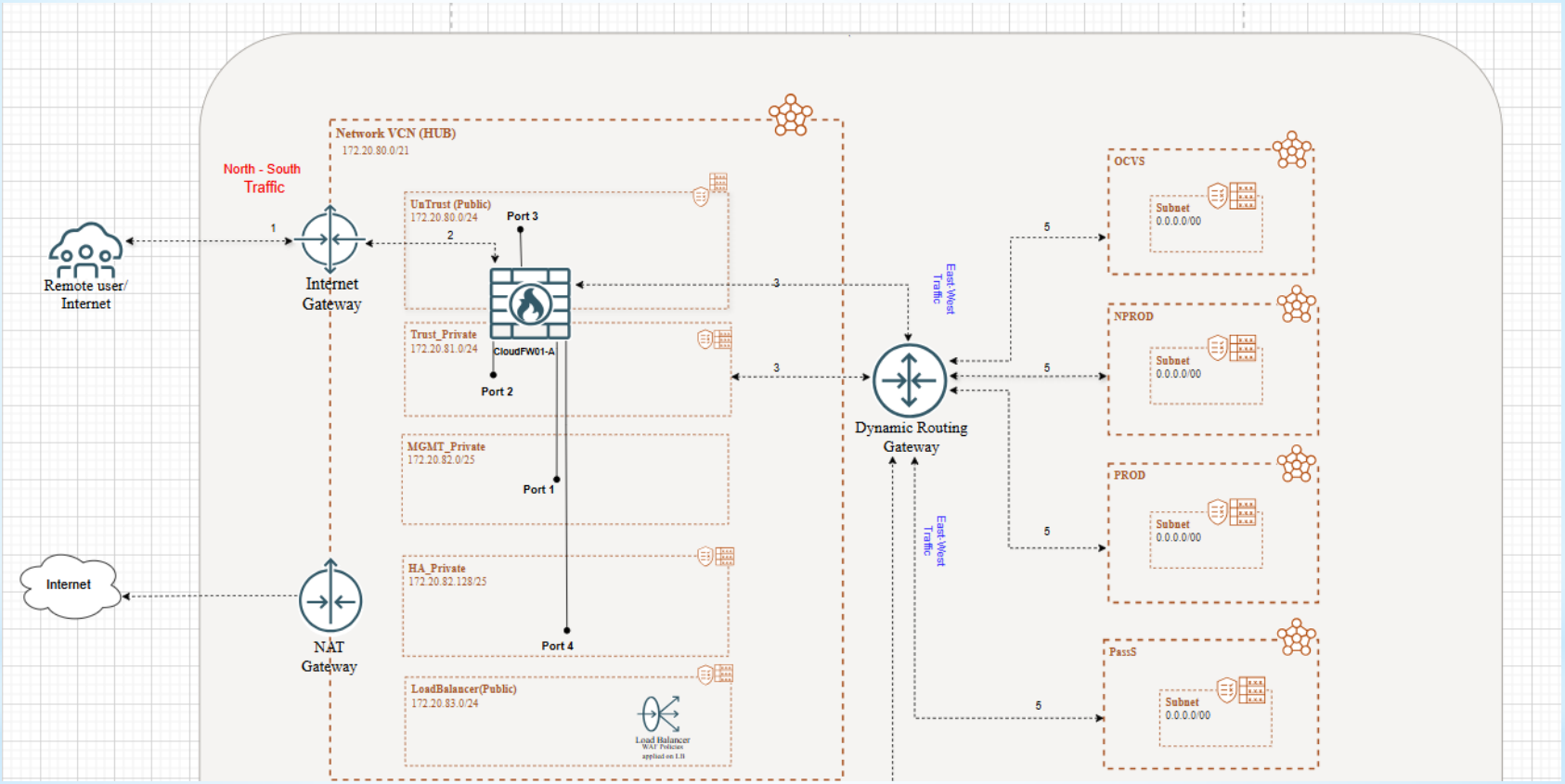


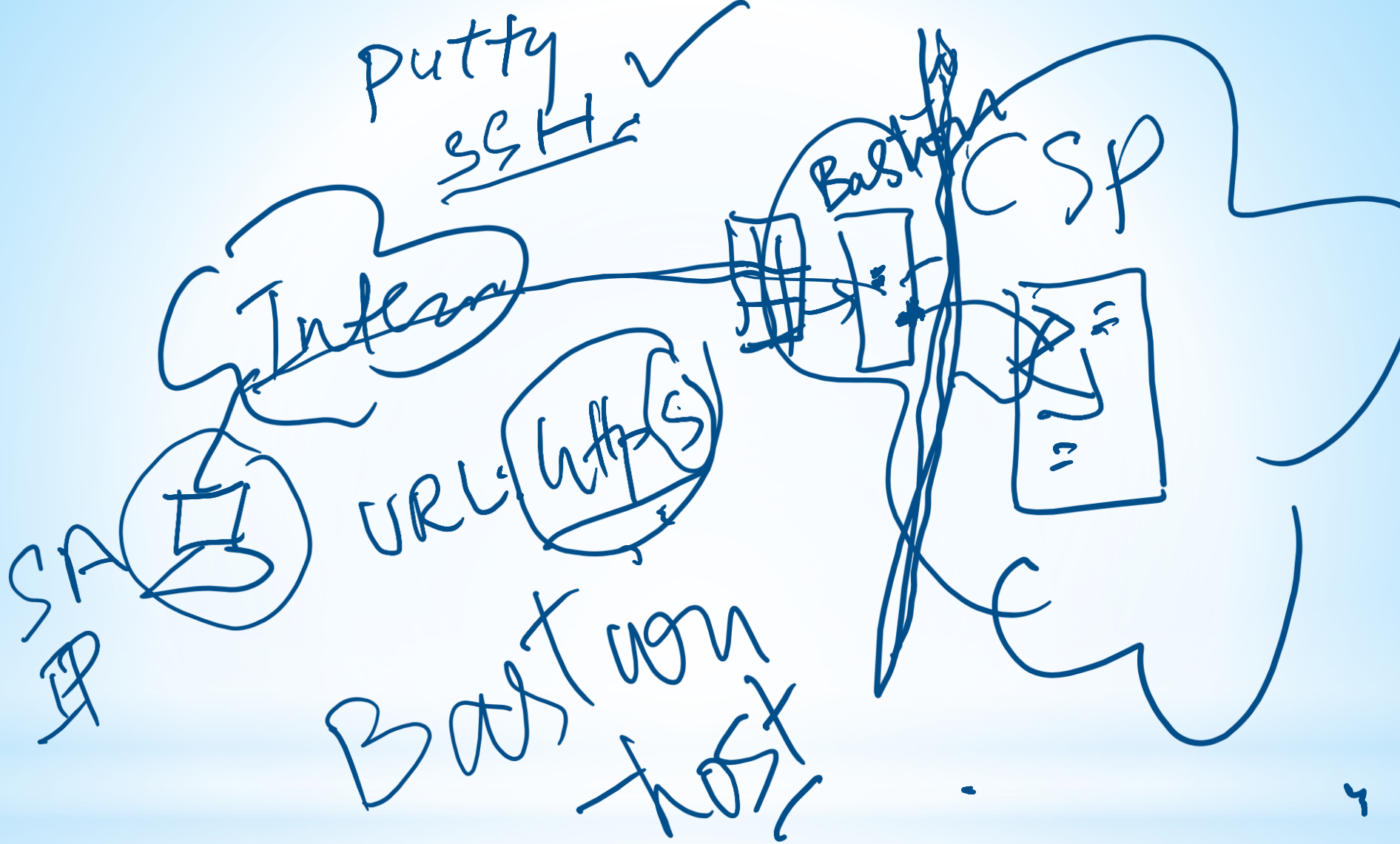
Internal Use

Cloud Security Domains



Cloud Security Domains




putty
SSH
Internet
Bastion
CSP
URL
https
SA
IP
Bastion host

Q & A