

Topic

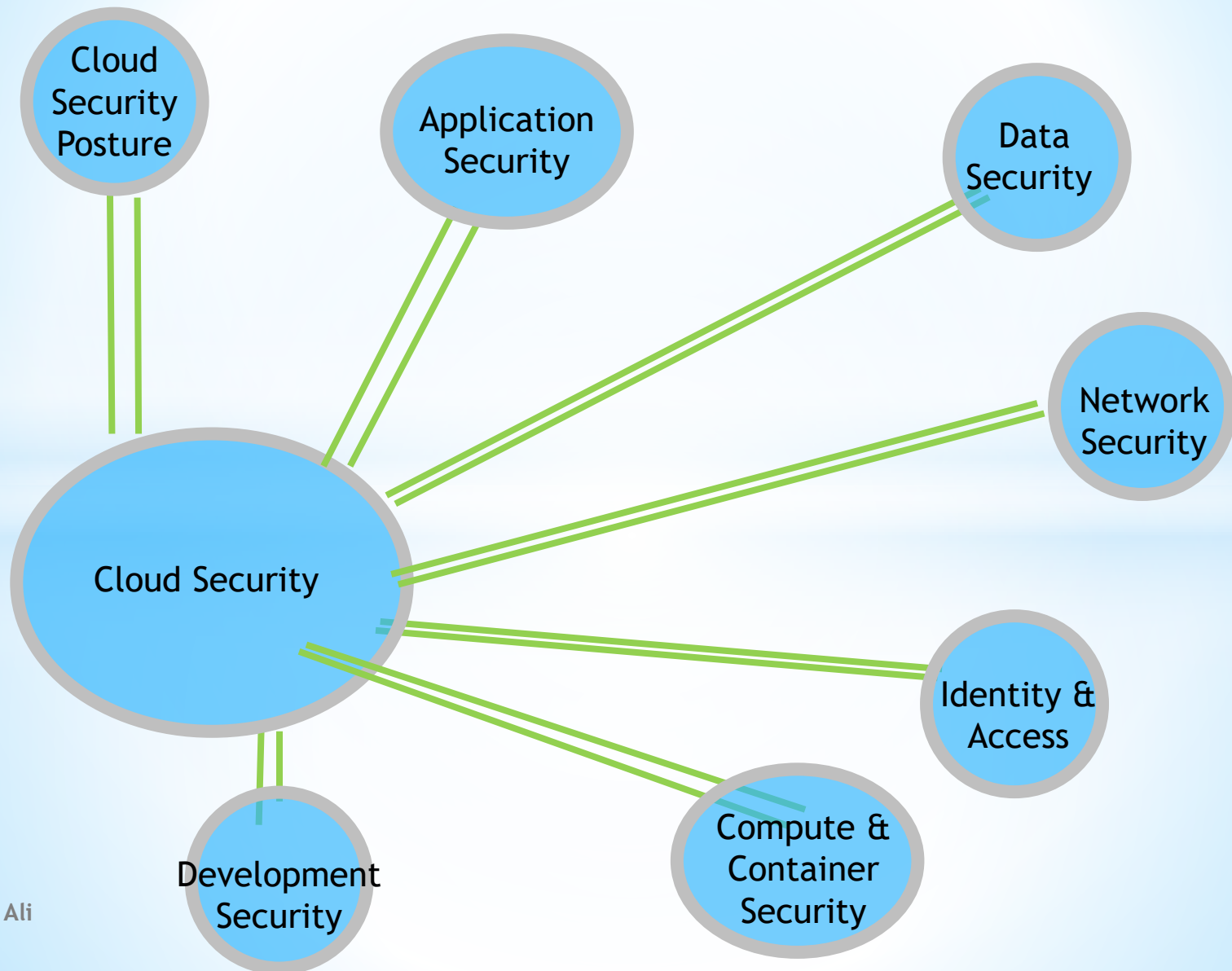
* Cloud Security

TOCI III Course

CS Department @ University of Karachi

Cloud Security Domains

Cloud Security Domains



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)

Data Security



Data Safe



Certificates



Data Loss
Prevention



Vaults (KMS)
& Secrets

Network Security



Network
Firewall



Bastion Service



L3/4
DDoS



VCN Flow Logs



IPSec
MACSec



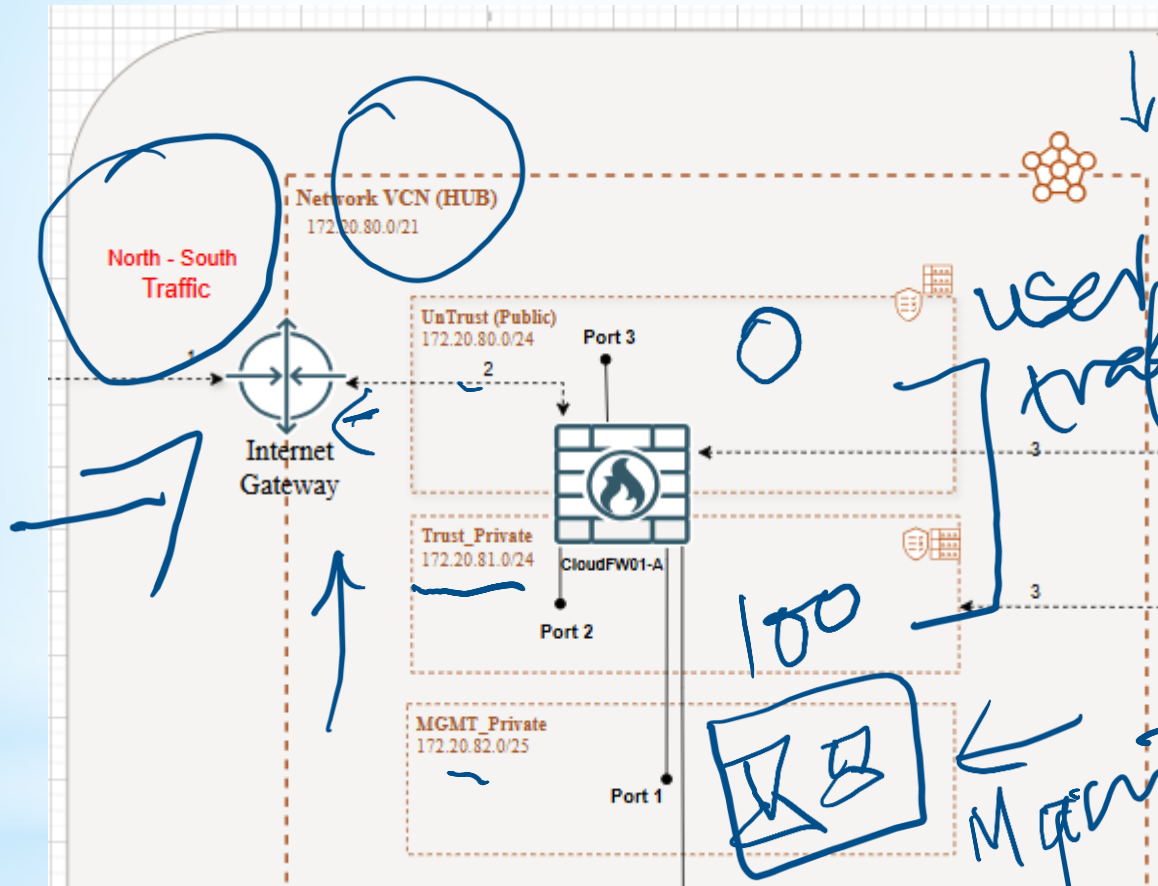
VTAP



DNS TSIG

Cloud Firewall

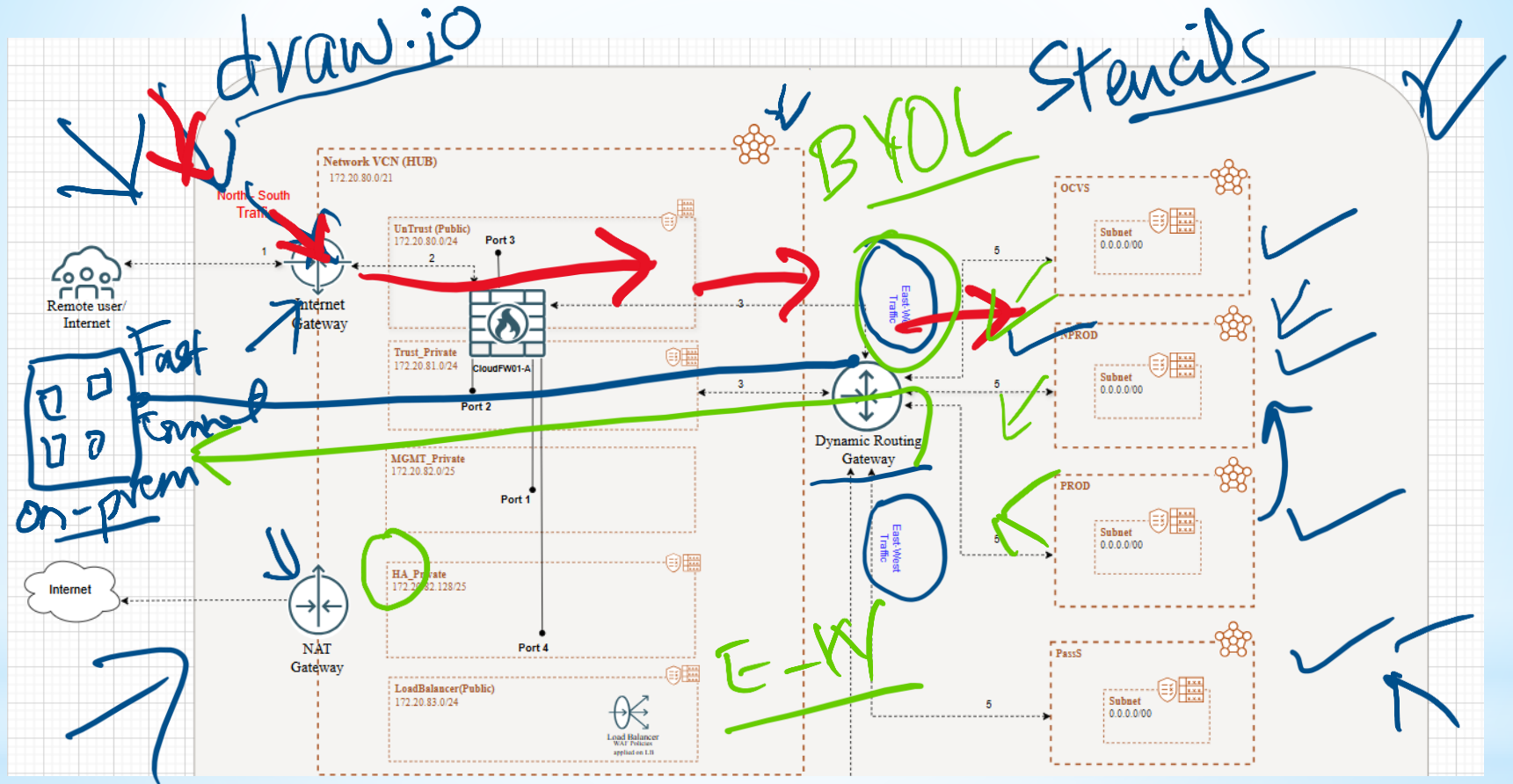
implicit deny

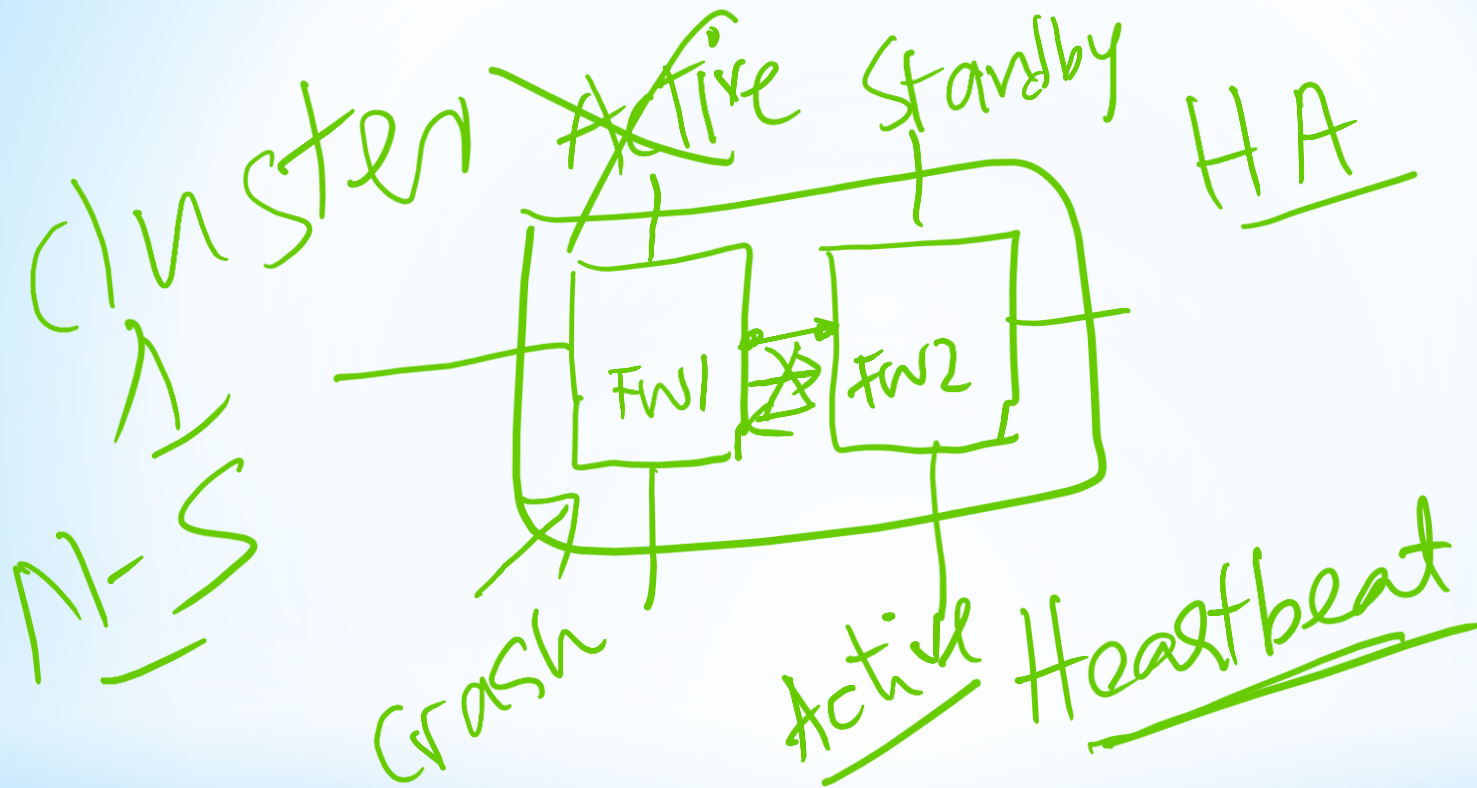


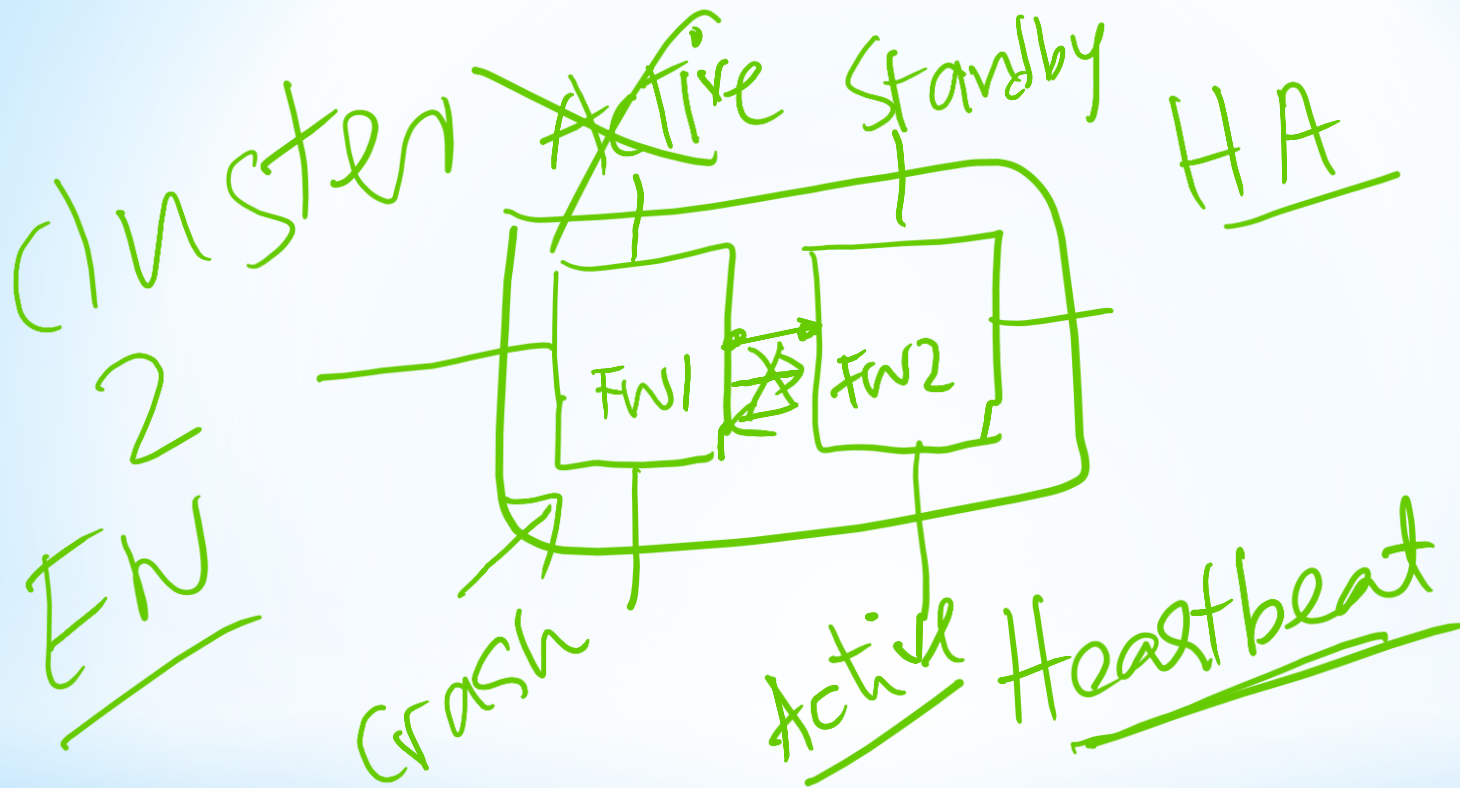
Handwritten notes and annotations:

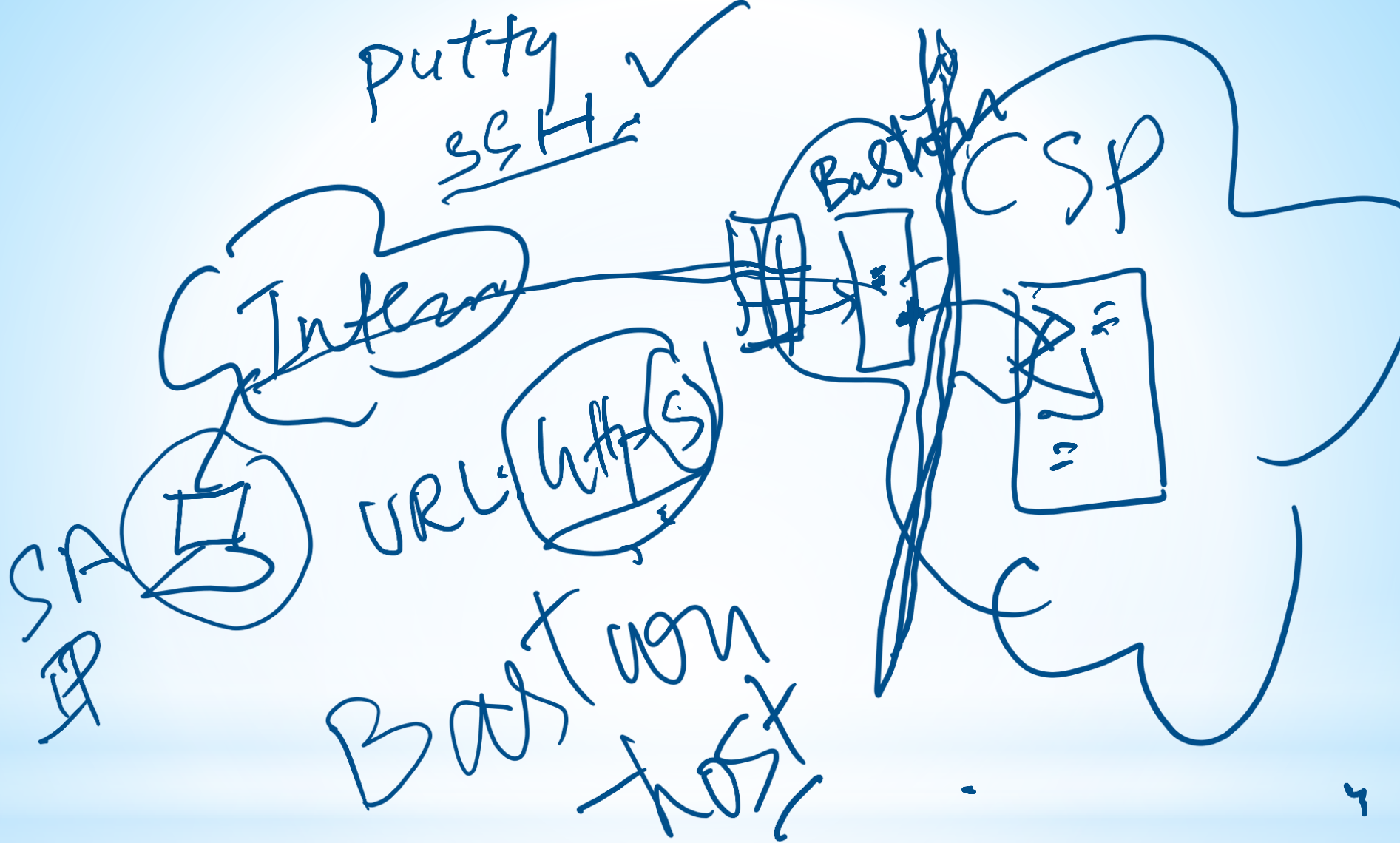
- Internet based traffic**: A bracket groups the UnTrust (Public) and Trust_Private subnets.
- 100**: A handwritten number next to the Trust_Private subnet.
- MGMT. Traffic**: A handwritten label with an arrow pointing to the MGMT_Private subnet.
- explicit permit**: A handwritten label in a box, with an arrow pointing to the MGMT_Private subnet.
- N/S Traffic**: A handwritten label with an arrow pointing to the Internet Gateway.
- user traffic**: A handwritten label with an arrow pointing to the UnTrust (Public) subnet.

Cloud Secure Landscape









Types of Firewall

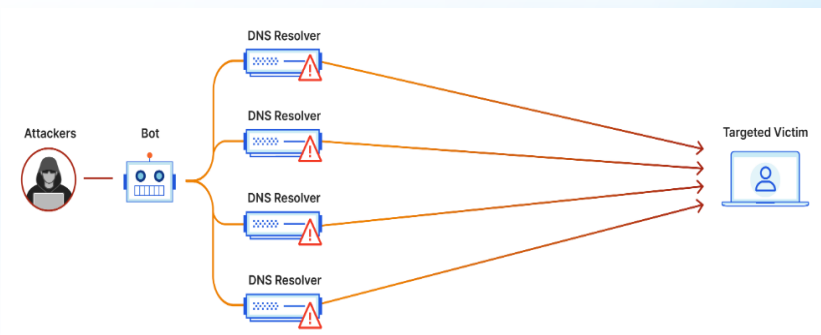
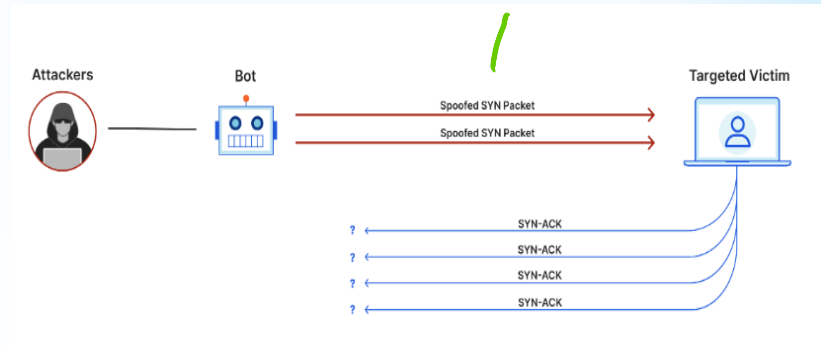
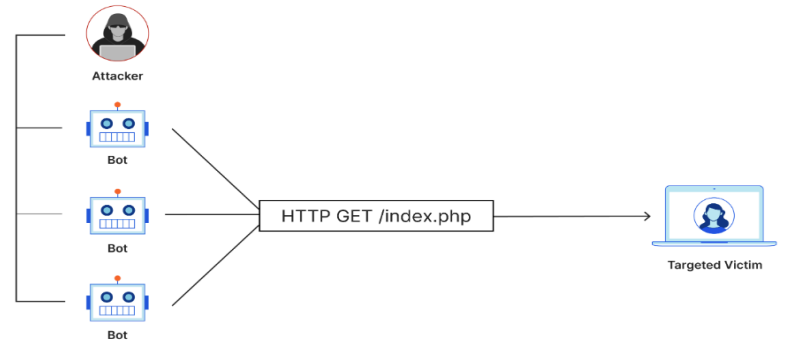
- What is Firewall
- Firewall Connectivity (East/West) (North/South)
- Firewall types
- NextGen Firewall
- Web Access Firewall
- Anti DDoS

Authentication & Authorization

- What is Authentication
- Multi-factor authentication
- Role Based Access
- Identity Access Management

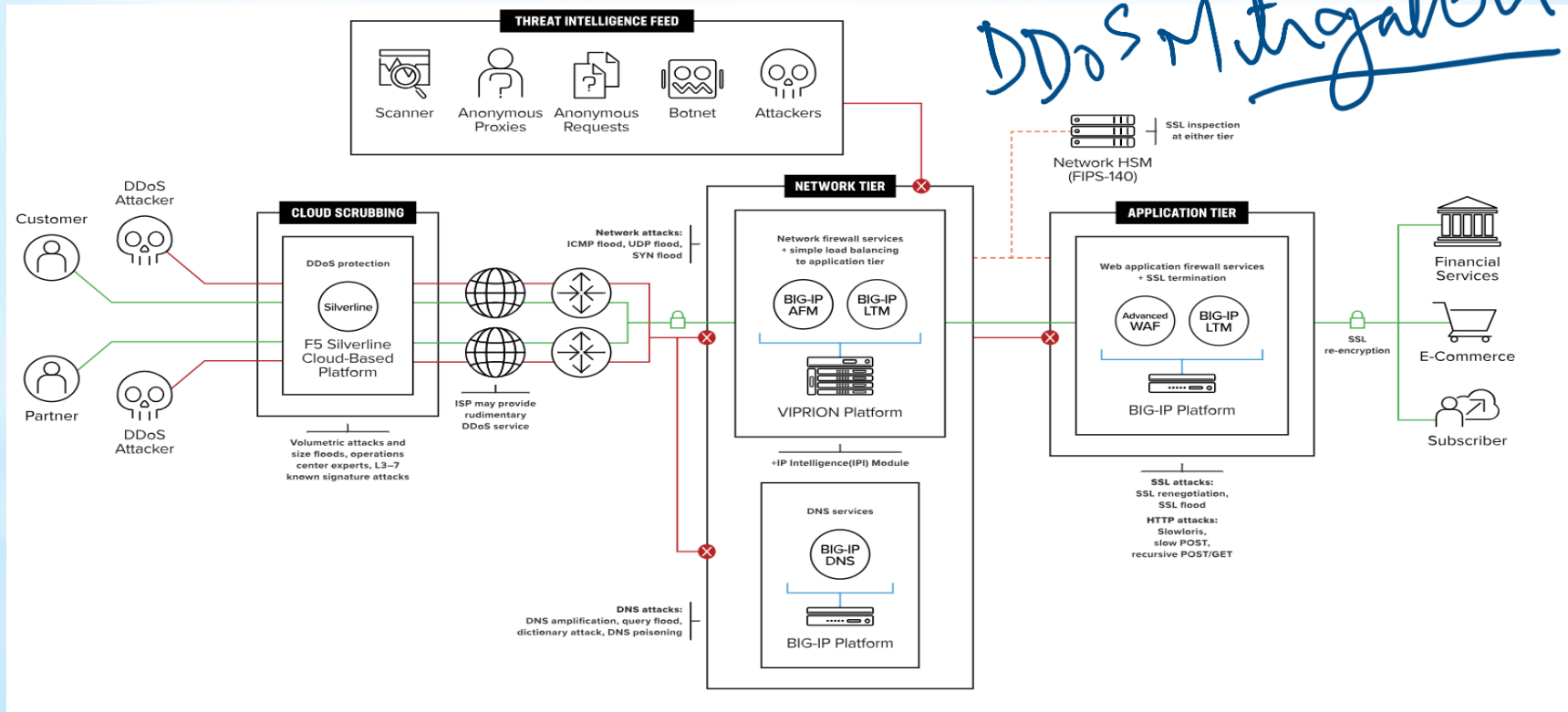
DDoS Types

- Application DDoS attacks
- Volumetric attacks
- DNS Amplification



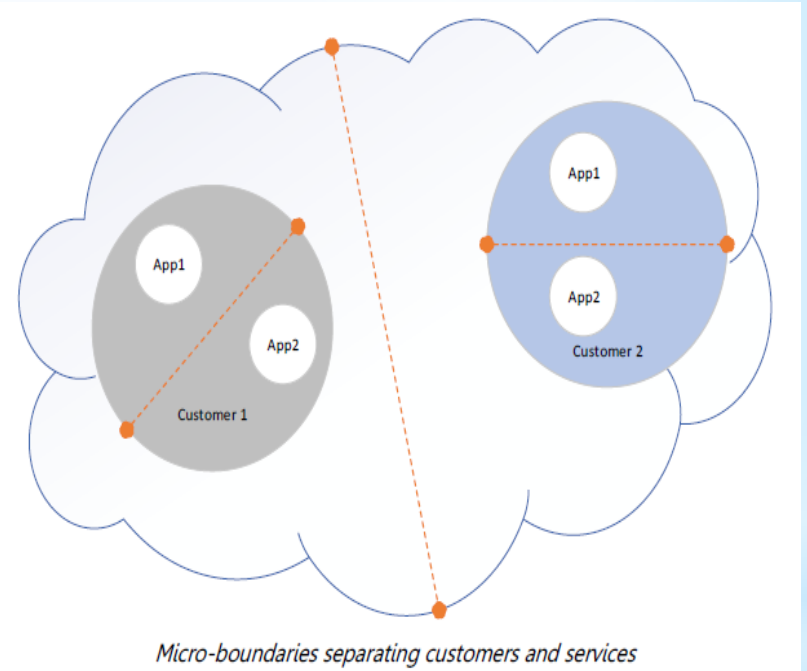
Anti DDoS

- What is Anti DDoS
- Why we need to protect from Anti DDoS
- Anti DDoS Connectivity



Network Security Perimeter

- Physical security ensures underlying physical resources protection
- Logical security consists link, protocol & application layer
- Perimeter is the demarcation point for some Cloud
- Other cloud network perimeter is dynamic micro-borders around individual customer solutions or services



Cloud Security Tools

S.No.	Suggested Solution	Domains to be covered
1	ManageEngine	Comprehensive Monitoring & Management for hosted VMs
2	ManageEngine Servicedesk plus	Helpdesk/Ticketing/Incident Management
3	Trend Micro Deep Security	Antivirus & Anti Malware
4	Patch Manager Plus	Patch Management Solution
5	Tenable	Vulnerability Assessment
6	ManageEngine Log360	SIEM
7	Symantec EndPoint & File Encription	Encryption Solution
9	Kasten	Backup Solution for Openshift
10	Veaam	Backup Solution for VM
11	Prisma Cloud	End Point Security
12	Fortigate	Firewall

Q & A