@awsgeek | AWS 2017 RE:INVENT | ANOTHER DAY, ANOTHER BILLION FLOWS | NET405 | jerry.hargrove

VPC101

WHAT'S A VPC?

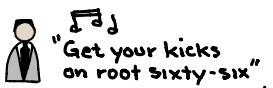
A SOFTWARE DEFINED NETWORK RUNNING ON PHYSICAL INFRASTRUCTURE

WHAT CAN YOU DO WITH YOUR VPC?

1. YOU CAN LAUNCH THINGS IN A VPC
2. YOU DEFINE THE RANGE OF YOUR VPC
3. THINGS IN YOUR VPC CAN TALK TO ONE ANOTHER
4. YOUR VPC FEELS LIKE A PHYSICAL NETWORK
5. YOU CAN CONNECT YOUR VPC TO OTHERS (DX, VPN, ETC)
6. YOU CAN DEFINE ROUTES BETWEEN NETWORKS
7. YOU USE GATEWAYS TO EXIT YOUR VPC

WHAT CAN YOUR VPC DO FOR YOU?

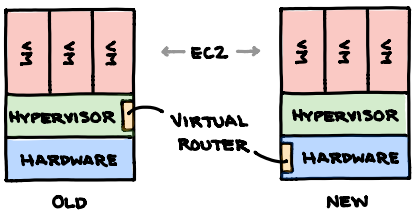
- APIs, AUDITING, FLOW LOGS
- DHCP & DNS
- FIREWALL (SGs & NACLs)
- X-REGION PEERING
- JUMBO PACKETS - 9001 BYTE MTU
- NO EXTRA COST

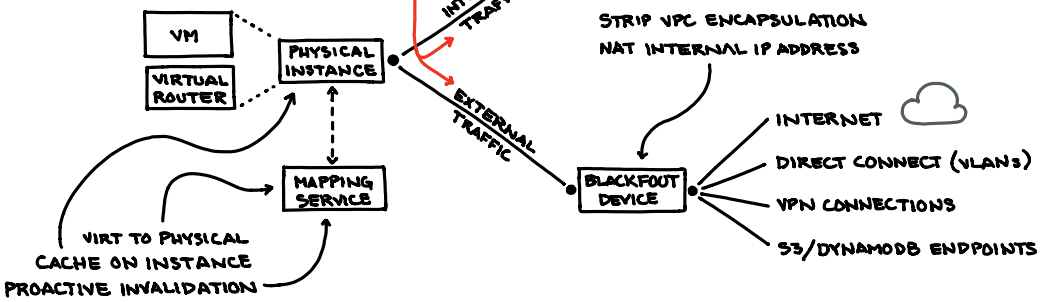


UNDER THE HOOD

YOUR IP PACKET
VPC ENCAPSULATION (VPC ID, ENI, etc)
IP ON PHYSICAL NETWORK

EVERY PHYSICAL INSTANCE HAS A VIRTUAL ROUTER





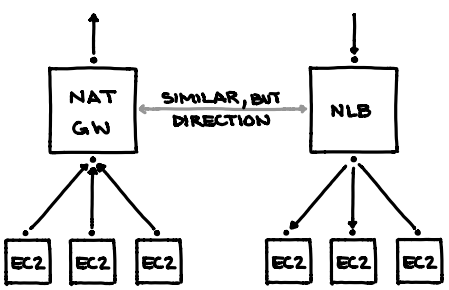
Q. WHAT IS A FLOW? FLOWS ARE A 5-TUPLE: PROTOCOL, SRC IP & PORT, DST IP & PORT
FLOWS ARE USED FOR STATEFUL CONNECTION TRACKING
FLOWS ARE USED BY FLOW LOGS, SECURITY GROUPS, NAT GATEWAYS, AND NLBs

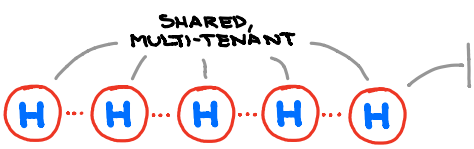
- TCP FLOWS ALSO INCLUDE SEQ & ACK FOR ADDITIONAL RELIABILITY & SECURITY
  - TCP PACKET #1 ALLOWED BY SECURITY GROUP
  - TCP PACKET #2 ALSO CHECK SEQ & ACK FOR VALIDITY
- UDP FLOWS INCLUDE DATAGRAM ID
- ICMP FLOWS ARE ... COMPLICATED

EFS — NAT GW — NLB — PRIVATELINK

HYPERPLANE NODES

- BASED ON S3 LOAD BALANCER ARCHITECTURE
- HYPERPLANE NODES ARE REALLY EC2 INSTANCES
- USED BY AWS TO MANAGE STATE & ROUTE PACKETS





DEFAULT 5GB/s CAPACITY
SCALABLE TO TB/s IN 5GB/s INCR

REAL TIME, DISTRIBUTED CONCENSUS PROBLEM

NAT GW MUST ENSURE ALL CONNECTIONS TO DEST IP/PORT COME FROM UNIQUE SOURCE PORT

NLBs MUST SELECT & ROUTE CONNECTIONS TO SAME TARGET

DEALING WITH NOISY NEIGHBORS? SHUFFLE SHARDING

- GIVE EACH CUSTOMER N RANDOM NODES AMONG MANY
- ONLY A SMALL PERCENTAGE WILL OVERLAP
- ISOLATE REALLY NOISY NEIGHBORS