Cloud Network Security

Using AWS

Day 1

Hello, I'm Franca

Platform Engineer @ SEEK

Currently responsible for supporting Seek's Shared Cloud Networking solutions!

Co-Organiser for DevOps Girls

'Fell' into Cloud Networking, but LOVE it!

Passionate about diversity, inclusion and non-traditional pathways to technology

Always learning

Code of Conduct

- Inclusive
- Judgement-free
- No feigning surprise
- No “well actuallys”
- No back-seat driving
- No subtle “isms”

Who are you?

Image sourced from: https://broadlygenderphotos.vice.com/

What we're NOT covering

- Application security – focus will be on the AWS networking resources only
- Hybrid
- Research methods – Blue team fun times only!
- Your snowflake networking problem

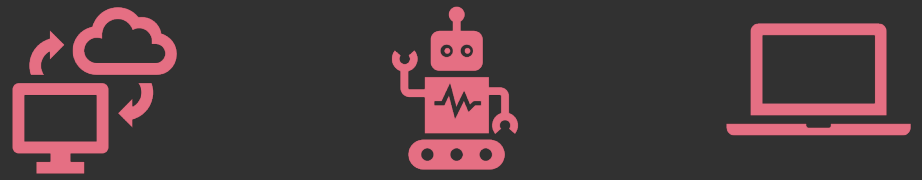
Two Modes of Learning

Theory

We'll introduce you to some concepts and answer questions

Hands On

We'll jump into the AWS console and start creating our cloud networks



Networking 101

Digital Copy:

Jvns.ca/networking-zine.pdf

Created by Julia Evans

@b0rk

The what and why of AWS

What is AWS?

- Over 200+ services to enable cloud based infrastructure that you can manage
- One of many providers of cloud infra such as MS Azure, Google, IBM, and more
- Data storage, compute power, networking, web hosting, etc

Why do we use AWS?

- Enables scalable infrastructure in a highly secure environment
- Reliable, flexible, and available
- Unparalleled service offerings (150+ more than Google)
- Best in class support, redundancy, and availability

History: What came before AWS?

Then:

- Long lived, dedicated servers
- Long lead times for new contracted infra
- Estimated infra, often over-provisioned
- Fixed hardware, low scalability

Now:

- Short lived, shared services
- Cost shared by consumers
- Infra on demand
- Virtual hardware, highly scalable

Shared Responsibility Model

Security OF the cloud

- Hardware
- Physical Access
- Software e.g. NGINX EC2 image

Security IN the cloud

- Application Security
- Configuration of AWS Resources e.g. s3
- IAM
- Cloud Network Security

Networking OSI Model (Open Systems Interconnection)

There is still a lot to configure securely

7 Application Layer

For human consumption – what we see eg. HTTP, SNMP, FTP

6 Presentation Layer

Processes data to be used by the app layer, including encryption/decryption, jpg, SSL, TLS

5 Session Layer

Creation/Tear down of network connections

4 Transportation Layer (TCP/UDP)

Responsible for transporting packets in a way that covers flow control and reliability

3 Network Layer

Routing data from A to B going across boundaries – IP's, ICMP, IPsec, IGMP

AWS's Responsibility

2 Data Link Layer

How data is linked up from point A to B eg. ARP, MAC Address

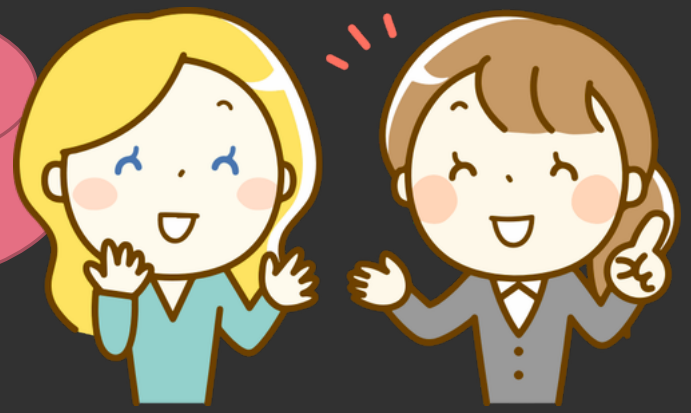
1 Physical Layer

Hardware responsible for data transmission – eg the physical cables, hubs

Cloud Networks - AWS

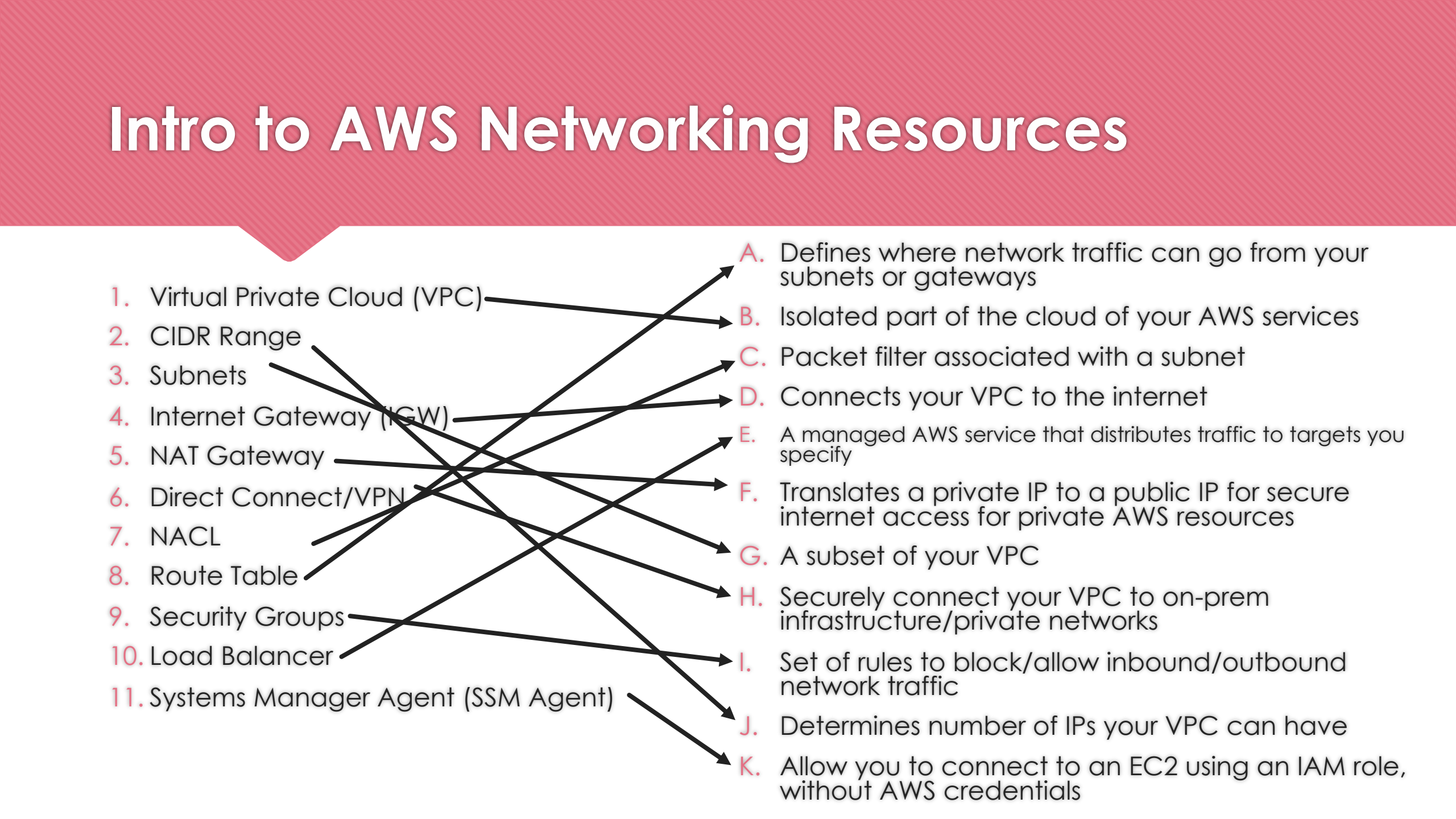
- 22 Regions - Australia's Region is **ap-southeast-2**
- 69 AZ's (availability zones) There are 3 in Sydney, Australia
- Every time you create a VPC, you're using part of this network

Group Activity Time!



Intro to AWS Networking Resources

1. Virtual Private Cloud (VPC)
2. CIDR Range
3. Subnets
4. Internet Gateway (IGW)
5. NAT Gateway
6. Direct Connect/VPN
7. NACL
8. Route Table
9. Security Groups
10. Load Balancer
11. Systems Manager Agent (SSM Agent)



A. Defines where network traffic can go from your subnets or gateways

B. Isolated part of the cloud of your AWS services

C. Packet filter associated with a subnet

D. Connects your VPC to the internet

E. A managed AWS service that distributes traffic to targets you specify

F. Translates a private IP to a public IP for secure internet access for private AWS resources

G. A subset of your VPC

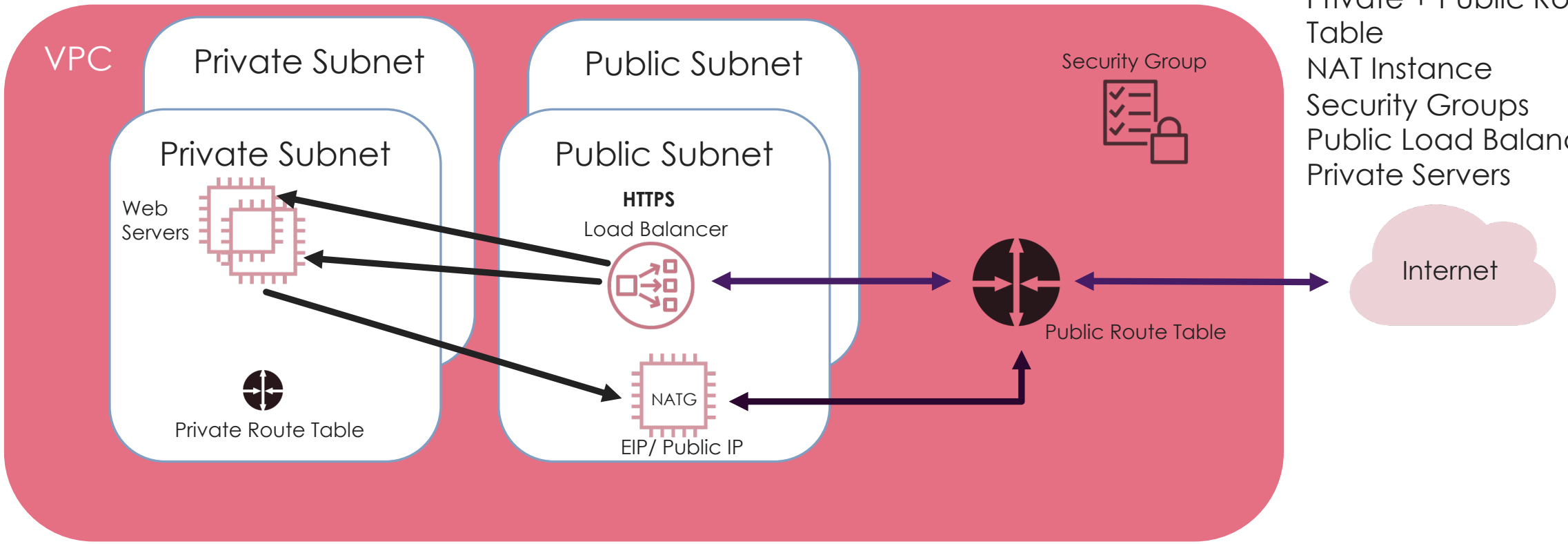
H. Securely connect your VPC to on-prem infrastructure/private networks

I. Set of rules to block/allow inbound/outbound network traffic

J. Determines number of IPs your VPC can have

K. Allow you to connect to an EC2 using an IAM role, without AWS credentials

What does this look like as infra?



VPC + Subnets
Internet Gateway
Private + Public Route Table
NAT Instance
Security Groups
Public Load Balancer
Private Servers

This white area is the rest of the internet/cloud!

IPs and CIDR Ranges

IPs

It's an identifying address for a routable resource.

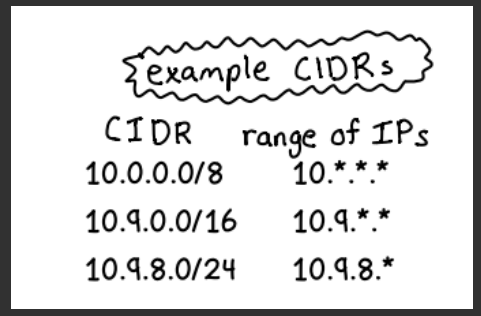
IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 and 255

CIDR (Classless Inter-Domain Routing)

A CIDR is a group of IP's allocated to a part of your network.

Taken from Julia Evan's zine.

As the netmask gets bigger, you get less IPs



Key Terms…

Netmask

/x tells you how many IP's are available in your CIDR – the smaller the number, the more IPs you have. E.g. /24 indicates there are 265 IP's available

Network ID

This is part of your IP that is shared for all resources within your network. E.g. 193.164.2.44 and 193.164.2.35 are part of the same network

Host ID

This is part of your IP that is unique to one resource. E.g. 193.164.2.44 and 193.164.2.35 are IP's for different resources

Subnetting

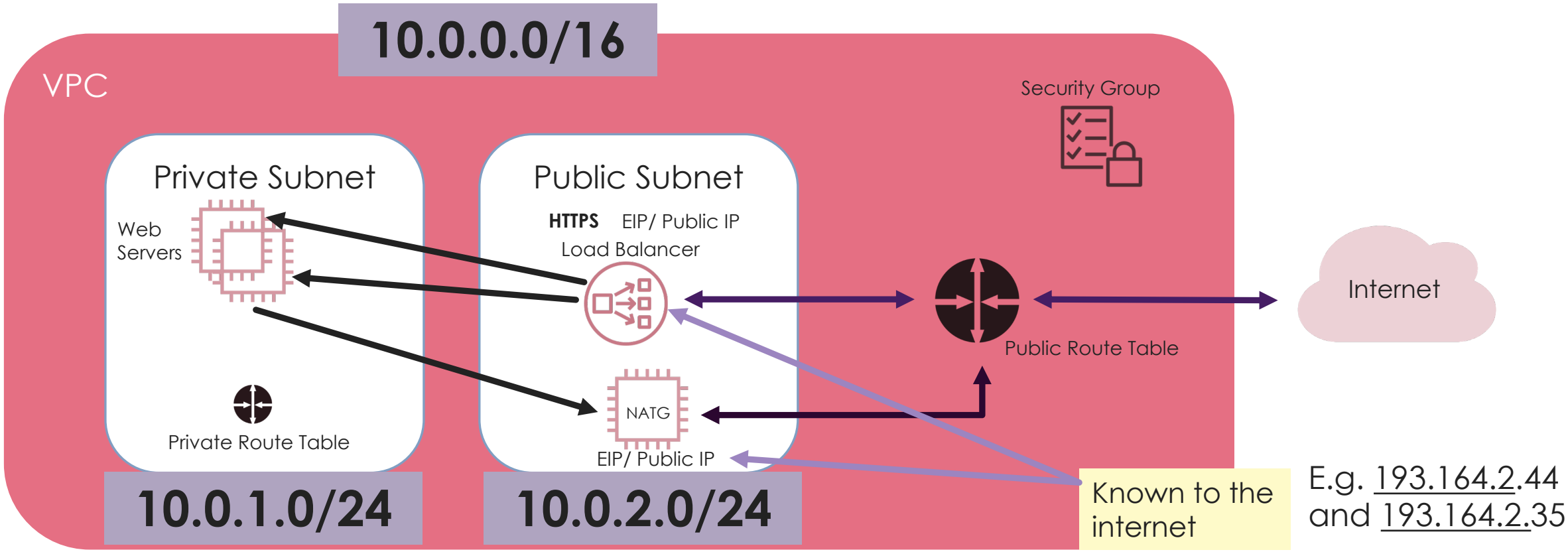
Once you know how many IP's are available in your network, you can split this into subnets.

We will not be covering subnetting today

Play around with subnetting though:

https://cidr.xyz

How does this apply to our network?



E.g. 193.164.2.44 and 193.164.2.35

Let's get into the console!

- We're going to use step-by-step guides in GitHub to build….
  - VPC
  - Public Subnet
  - Private Subnet