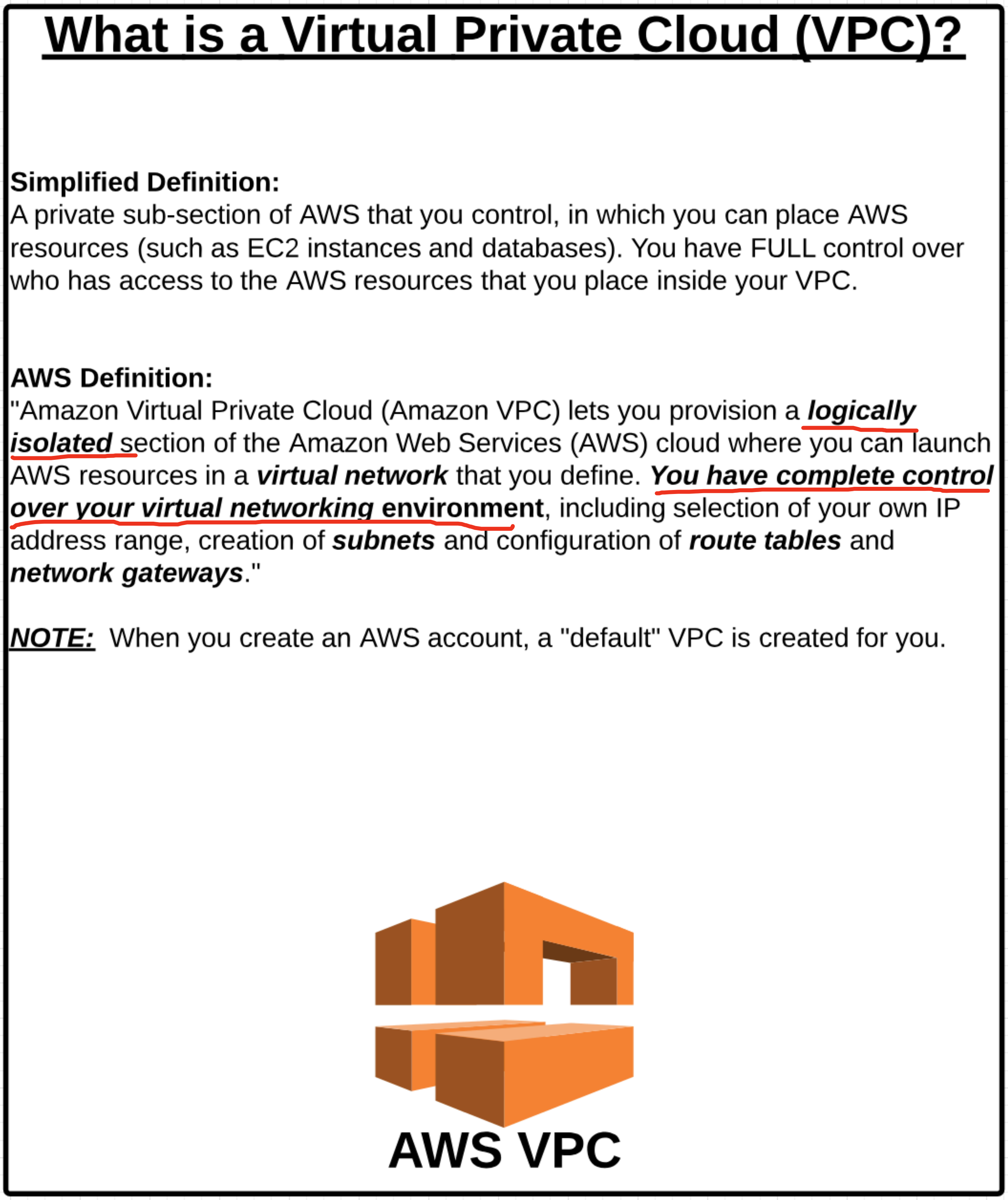
Networking Services

2019年2月10日 星期日 上午12:51



What is a Virtual Private Cloud (VPC)?

Simplified Definition:
A private sub-section of AWS that you control, in which you can place AWS resources (such as EC2 instances and databases). You have FULL control over who has access to the AWS resources that you place inside your VPC.

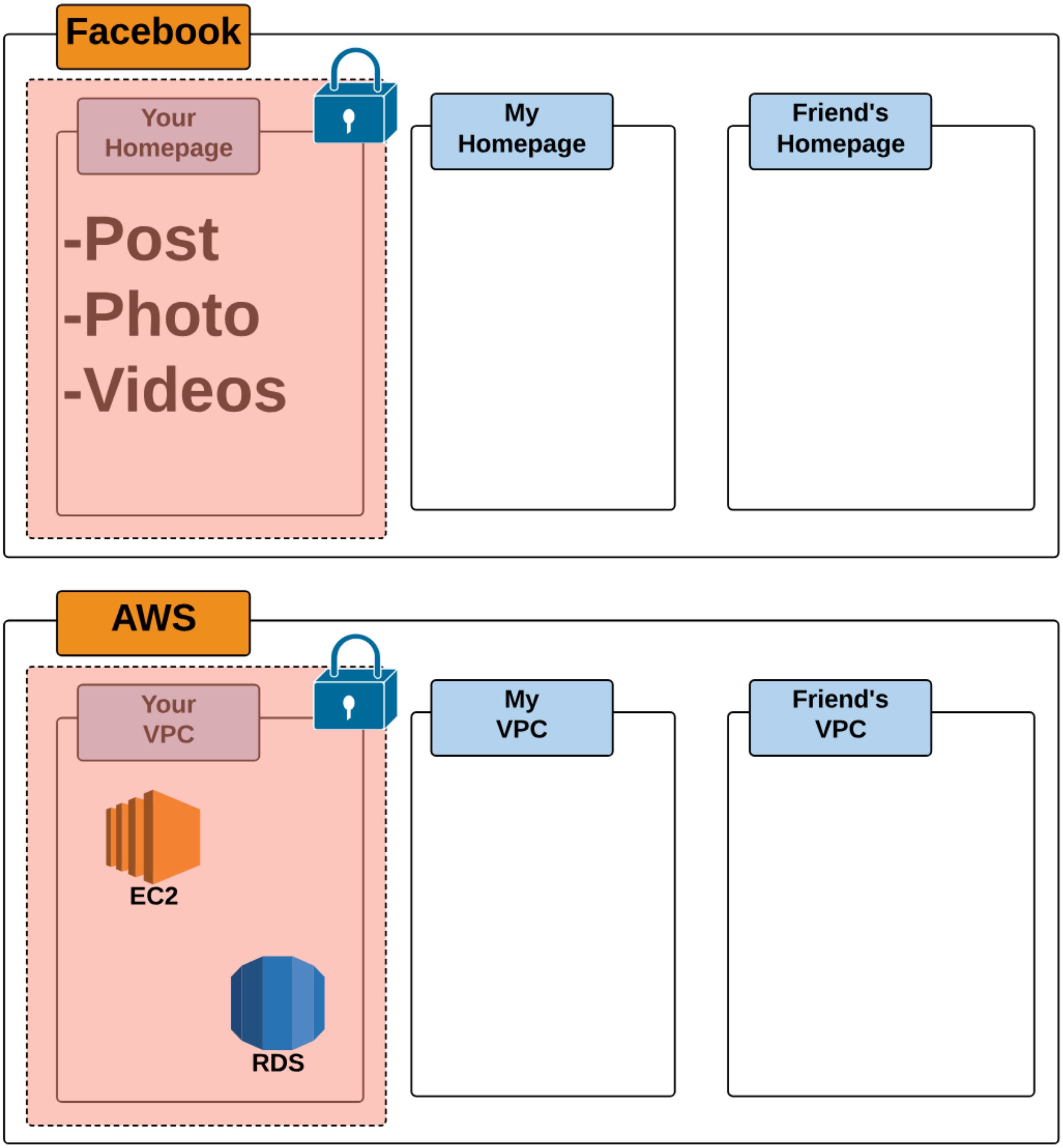
AWS Definition:
"Amazon Virtual Private Cloud (Amazon VPC) lets you provision a ***logically isolated*** section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a ***virtual network*** that you define. ***You have complete control over your virtual networking*** **environment**, including selection of your own IP address range, creation of ***subnets*** and configuration of ***route tables*** and ***network gateways***."

NOTE: When you create an AWS account, a "default" VPC is created for you.

AWS VPC

VPC Basics:

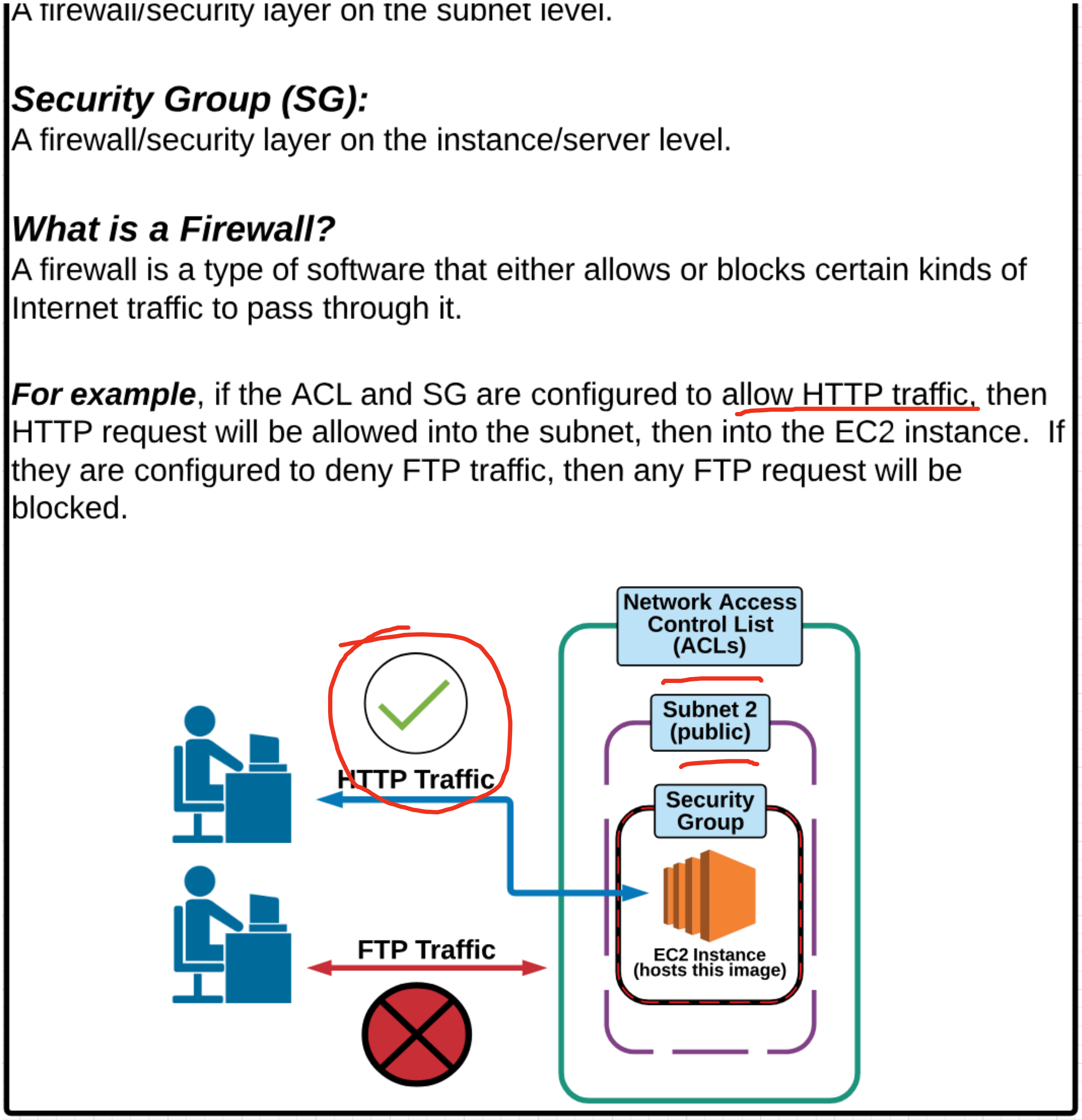
Facebook/VPC Analogy



Networking Security:

Network Access Control Lists (ACL):

A firewall/security layer on the subnet level



A firewall/security layer on the subnet level.

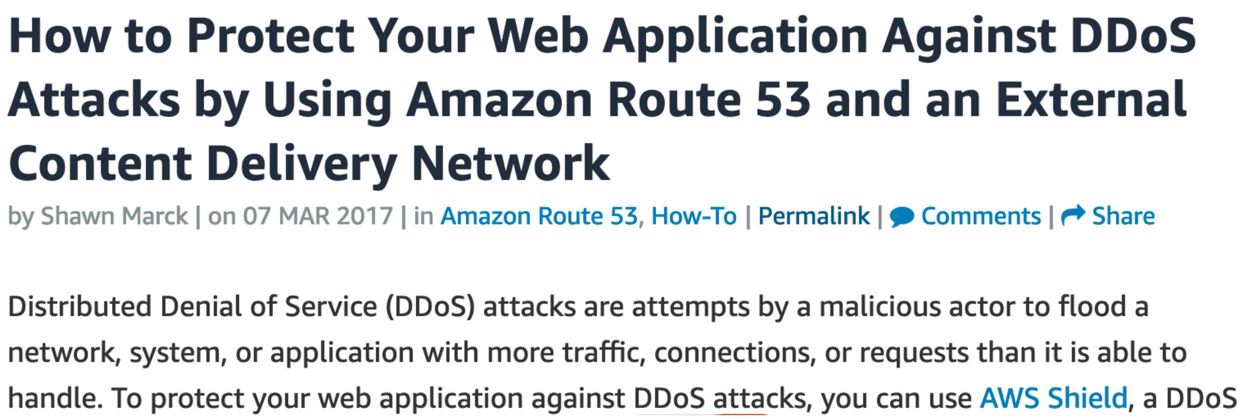
Security Group (SG):
A firewall/security layer on the instance/server level.

What is a Firewall?
A firewall is a type of software that either allows or blocks certain kinds of Internet traffic to pass through it.

For example, if the ACL and SG are configured to allow HTTP traffic, then HTTP request will be allowed into the subnet, then into the EC2 instance. If they are configured to deny FTP traffic, then any FTP request will be blocked.

Network Access Control List (ACLs)
Subnet 2 (public)
Security Group
EC2 Instance (hosts this image)
HTTP Traffic
FTP Traffic

Protection



How to Protect Your Web Application Against DDoS Attacks by Using Amazon Route 53 and an External Content Delivery Network

by Shawn Marck | on 07 MAR 2017 | in Amazon Route 53, How-To | Permalink | Comments | Share

Distributed Denial of Service (DDoS) attacks are attempts by a malicious actor to flood a network, system, or application with more traffic, connections, or requests than it is able to handle. To protect your web application against DDoS attacks, you can use AWS Shield, a DDoS protection service that AWS provides automatically to all AWS customers at no additional charge. You can use AWS Shield in conjunction with DDoS-resilient web services such as Amazon CloudFront and Amazon Route 53 to improve your ability to defend against DDoS attacks. Learn more about architecting for DDoS resiliency by reading the AWS Best Practices for DDoS Resiliency whitepaper.

You also have the option of using Route 53 with an externally hosted content delivery network (CDN). In this blog post, I show how you can help protect the zone apex (also known as the root domain) of your web application by using Route 53 to perform a secure redirect to prevent discovery of your application origin.