

Организация сети в Cloud Provider



Денис
Альмухаметов



Денис Альмухаметов

System Architect

Netcracker



[Денис Альмухаметов](#)

План занятия

1. [Cloud Providers](#)
2. [Virtual Private Cloud](#)
3. [Subnets](#)
4. [Routing Tables](#)
5. [Security Groups](#)
6. [Network ACL](#)
7. [Production ready VPC](#)
8. [Домашнее задание](#)

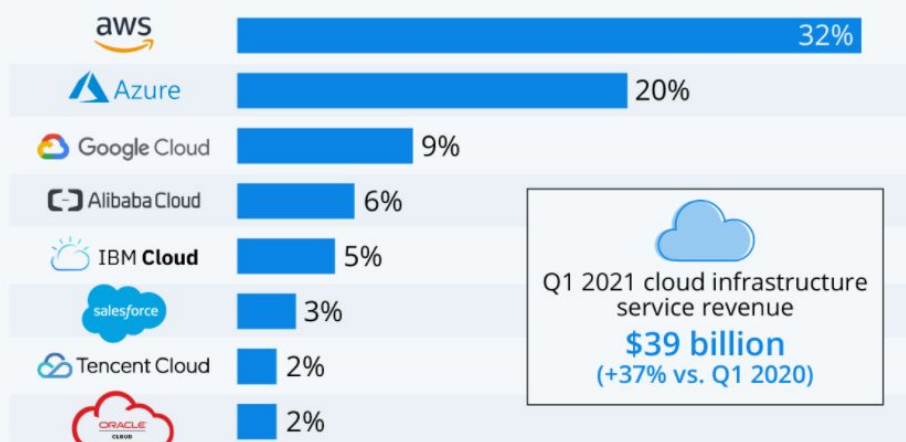


Cloud Providers

Global Cloud Market

Amazon Leads \$150-Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q1 2021*



* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group



statista



Virtual Private Cloud

[What is Amazon VPC? - Amazon Virtual Private Cloud](#)

[Как начать работать с VPC в Яндекс Облако](#)

VPC (Virtual Private Cloud)

VPC – это логически изолированный раздел облака, в котором можно запускать ресурсы в самостоятельно заданной виртуальной сети.

Таким образом можно полностью контролировать среду виртуальной сети, в том числе:

- выбирать собственный диапазон IP-адресов,
- создавать подсети,
- настраивать таблицы маршрутизации и сетевые шлюзы.

Регионы и зоны доступности AWS

AWS охватывает 77 зон доступности в 24 географических регионах по всему миру.



Регионы и зоны доступности ЯО

Платформа Yandex.Cloud на первом этапе размещается в трех дата-центрах Яндекса, расположенных во Владимирской, Рязанской и Московской областях.

- ru-central1-a;
- ru-central1-b;
- ru-central1-c.

VPC и зоны

VPC работает в рамках региона и объединяет в себе все зоны.

Для каждой AZ заводится своя подсеть (**subnet**).





Subnets

[VPCs and subnets - Amazon Virtual Private Cloud](#)

[Как начать работать с VPC в Яндекс Облако](#)

Subnets

Subnet – подсеть в VPC:

- привязана к зоне;
- в одной зоне может быть много подсетей;
- не могут пересекаться в рамках одного VPC;
- можно использовать одни и те же адреса в разных VPC.

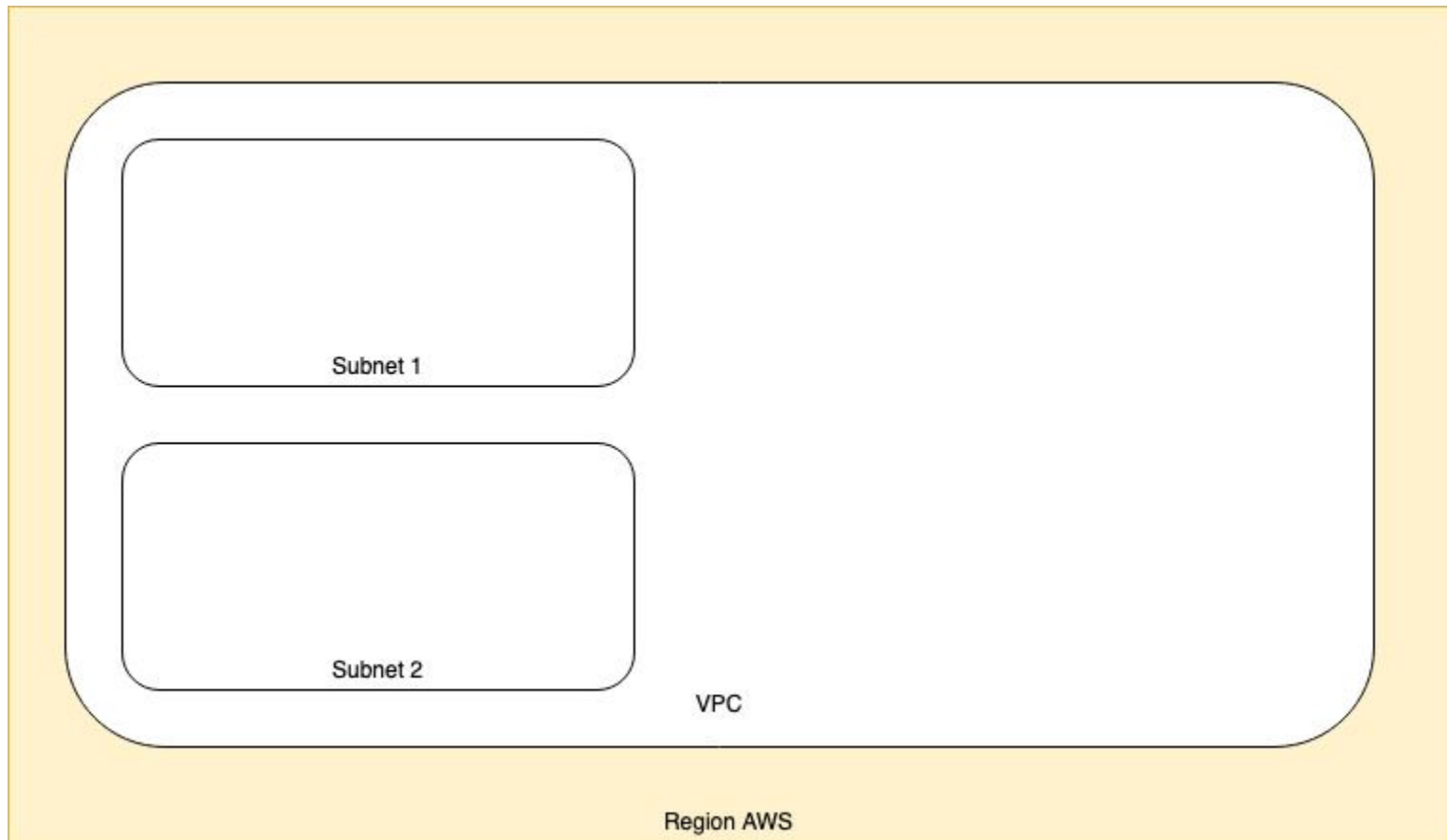
Что бывает в подсети?

- **Compute Cloud, EC2** – виртуалки;
- **DNS-серверы** для внутренних и внешних доменов;
- **Шлюз или Internet Gateway** отвечает за прием входящего и исходящего интернет трафика;
- **Egress Internet Gateway** – отвечает только за исходящий трафик в интернет;
- **NAT Gateway, NAT instance** – NAT в интернет с публичным IP;
- **VPN endpoints, VPN instance** – VPN как сервис, с доступом в подсеть.

Типы сетей

- **Public** – сеть с Internet Gateway, которая может принимать входящий трафик из интернета и выходить в интернет. В основном используется для приема входного трафика через балансировщики.
- **Private** – не может принимать входящий трафик напрямую, а в интернет выходит через NAT, запущенный в Public сети. В такой сети запускают основную часть инфраструктуры, запросы от пользователей попадают через балансировщик в Public сети.
- **Isolated** – не может принимать входящий интернет трафик или выходить в интернет.

Subnets





Routing Tables

[Route tables for your VPC - Amazon Virtual Private Cloud](#)

[Статическая маршрутизация | Yandex.Cloud - Документация](#)

Routing Tables

- Описывает, откуда куда трафик должен ходить;
- На вход принимает destination подсеть и target. В качестве target можно указывать сеть или объект облака (ip-адрес в случае YC)

Edit routes

Destination	Target
172.31.0.0/16	local
<input type="text"/>	<input type="text"/>

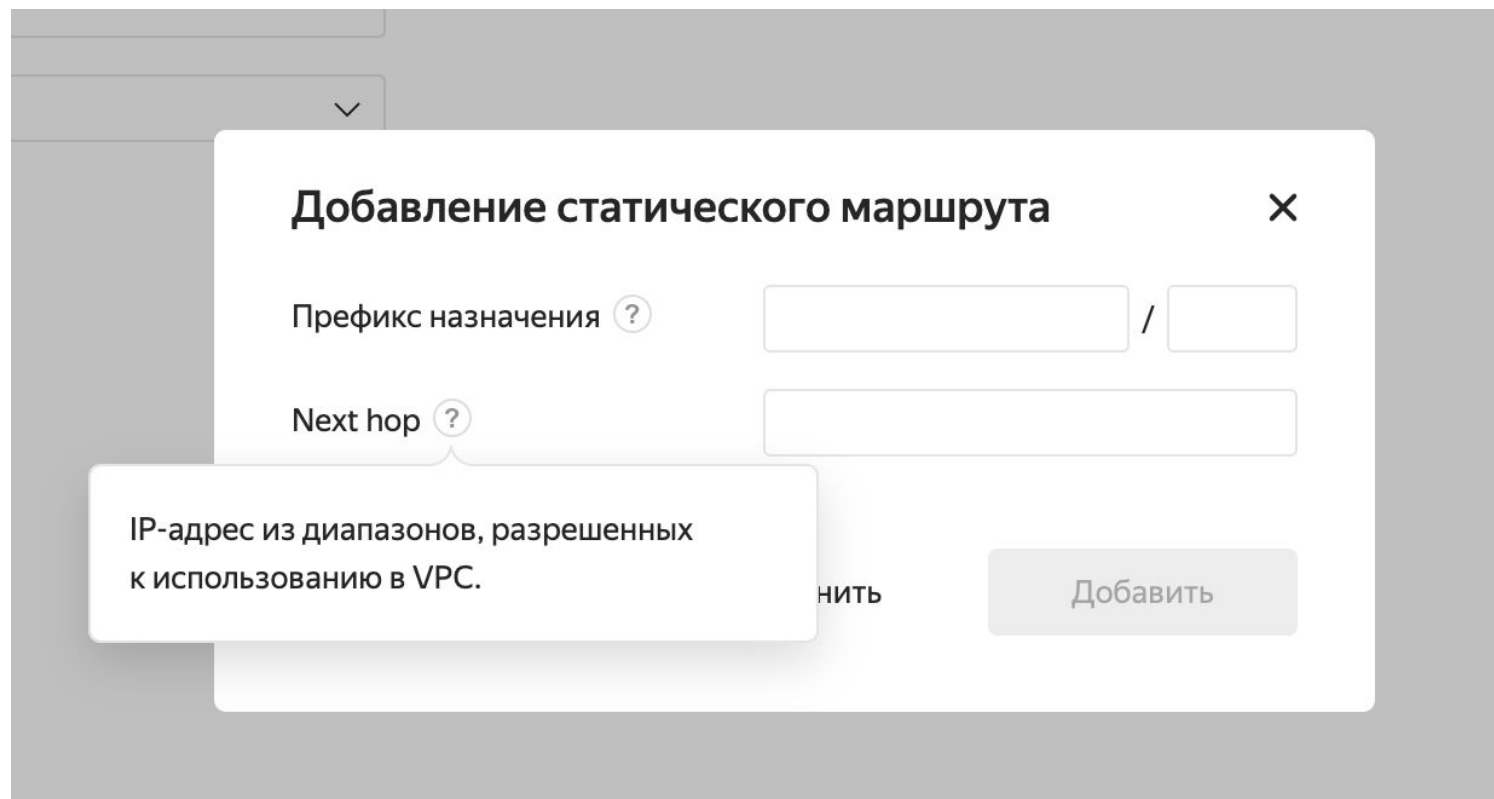
* Required

- Egress Only Internet Gateway
- Gateway Load Balancer
- Endpoint
- Instance
- Internet Gateway
- NAT Gateway
- Network Interface
- Outpost Local Gateway
- Peer Connection

Routing Tables

- есть главная, распространяющаяся на весь VPC;
- есть дополнительные для каждой подсети;
- можно заводить свои, влияющие на одну или множество выбранных подсетей.

Routing Tables



Добавление статического маршрута ×

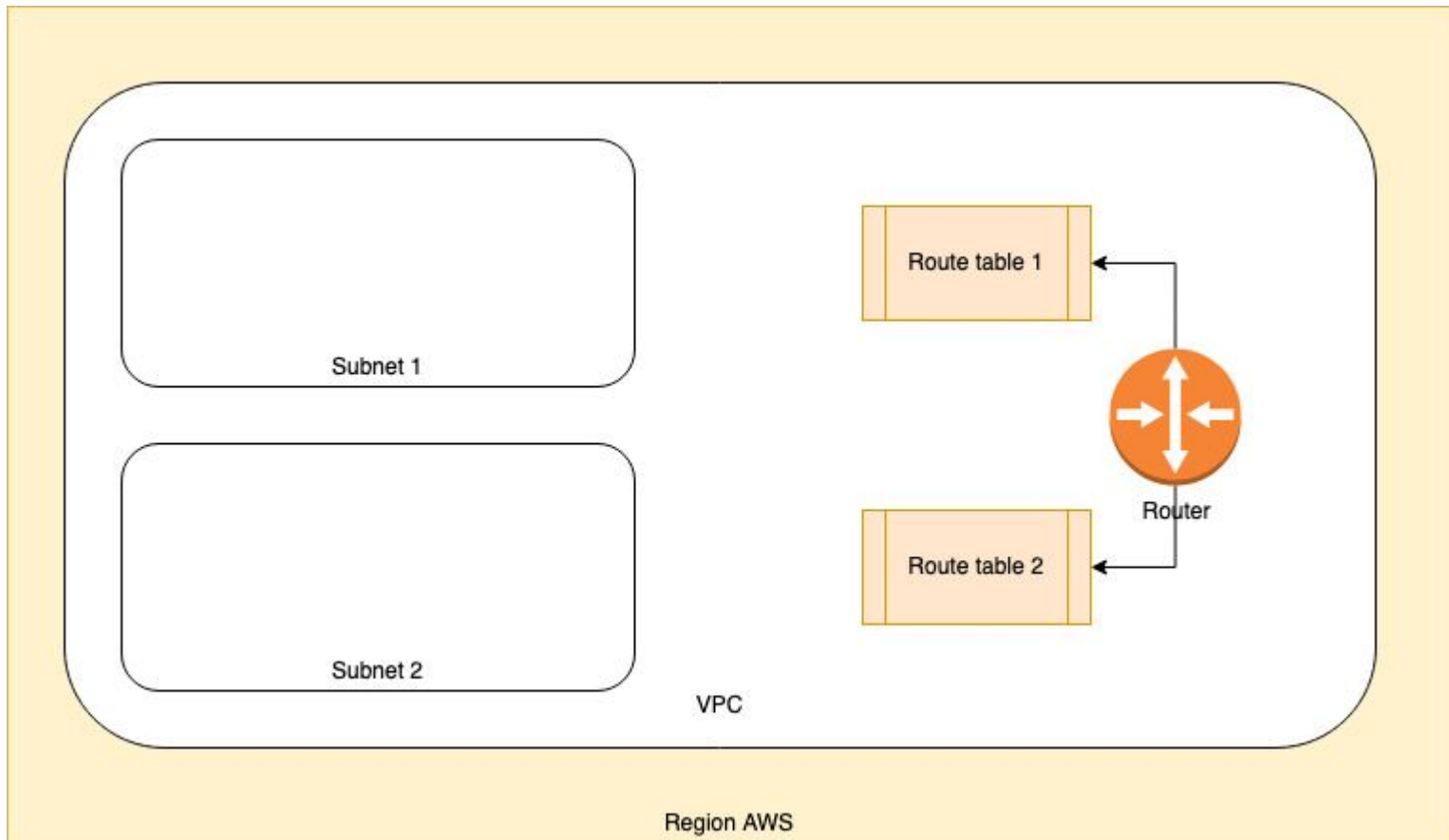
Префикс назначения (?) /

Next hop (?)

IP-адрес из диапазонов, разрешенных к использованию в VPC.

Отменить Добавить

Routing Tables





Network ACL

отсутствует в ЯО

Network ACL

- Дополнительный слой контроля трафика между подсетями.
- Поддерживает как разрешающие, так и запрещающие правила.
- Трафик подсети (Subnet) может регулироваться только одной Network ACL.
- Применяется первое правило в цепочке, под которое попал трафик (как в iptables).
- По умолчанию, создается default Network ACL при создании VPC и разрешает все.
- При создании своего (Custom) NACL по-умолчанию все запрещено

Network ACL

В правиле указывается:

- приоритет,
- protocol,
- port,
- source/destination
- разрешаем или запрещаем этот трафик.

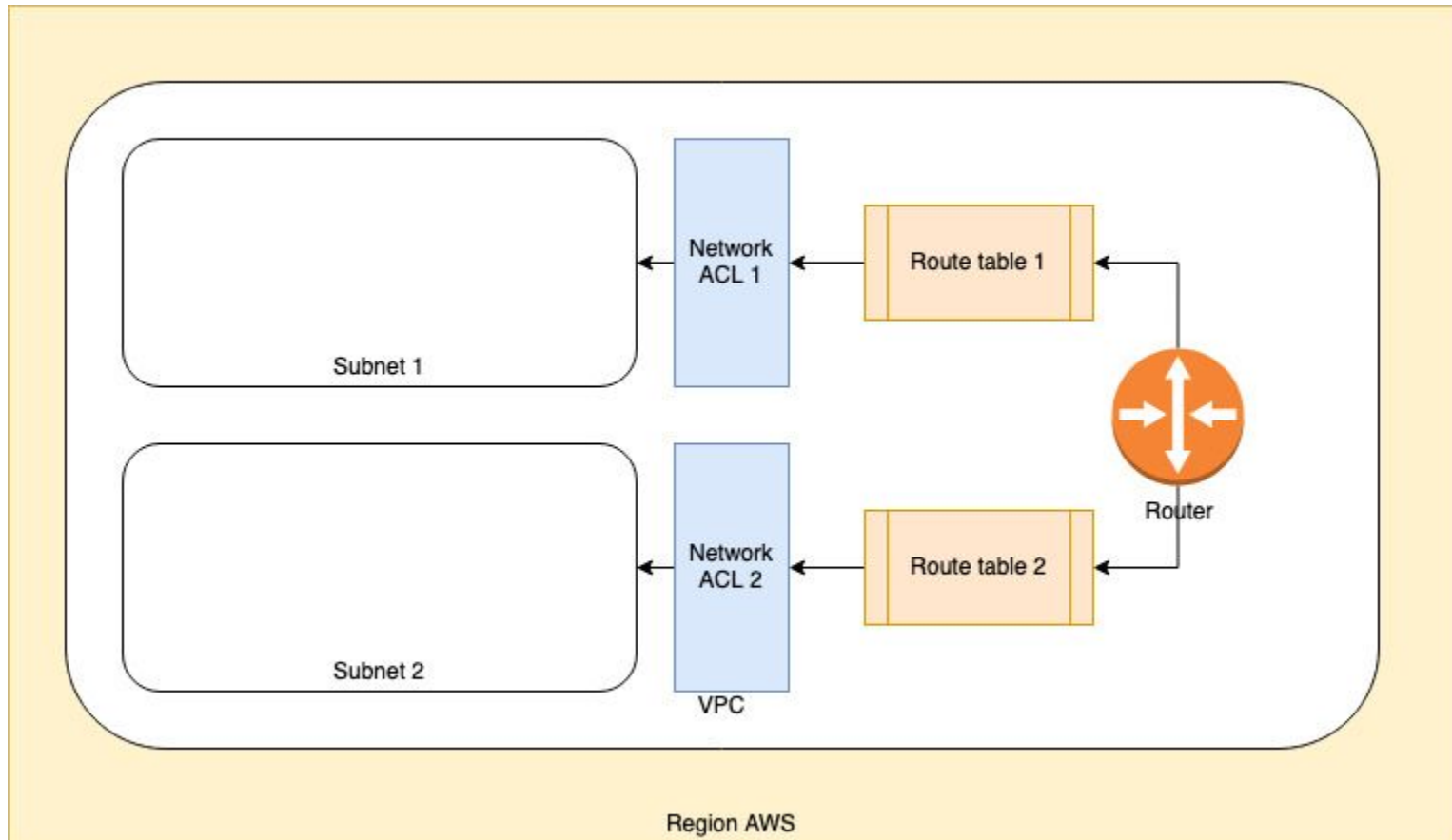
Правила применяются от меньшего числа к большему.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic ▼	All ▼	All	0.0.0.0/0	Allow ▼	<button>Remove</button>
*	All traffic ▼	All ▼	All	0.0.0.0/0	Deny ▼	

Add new ruleSort by rule number

Необходимо отдельно настраивать обратные правила – **Stateless**.

Network ACL





Security Groups

Стадия Preview в ЯО

Security Groups

Security Groups – это как firewall, описывают, какой трафик куда «может ходить» в подсети. По умолчанию все запрещено.

Чтобы security group применилась к инстансу, ее нужно явно указать при создании инстанса.

Каждая VPC имеет default security group, разрешающая любой трафик между ec2-инстансами. Дополнительные сервисы в VPC, например, EKS или RDS, требуют создания дополнительных правил, чтобы к ним мог начать ходить трафик.

Security Groups

В правиле для входящего трафика указывается protocol, port и source. Правило для исходящего трафика отличается только тем, что вместо source указывается destination.

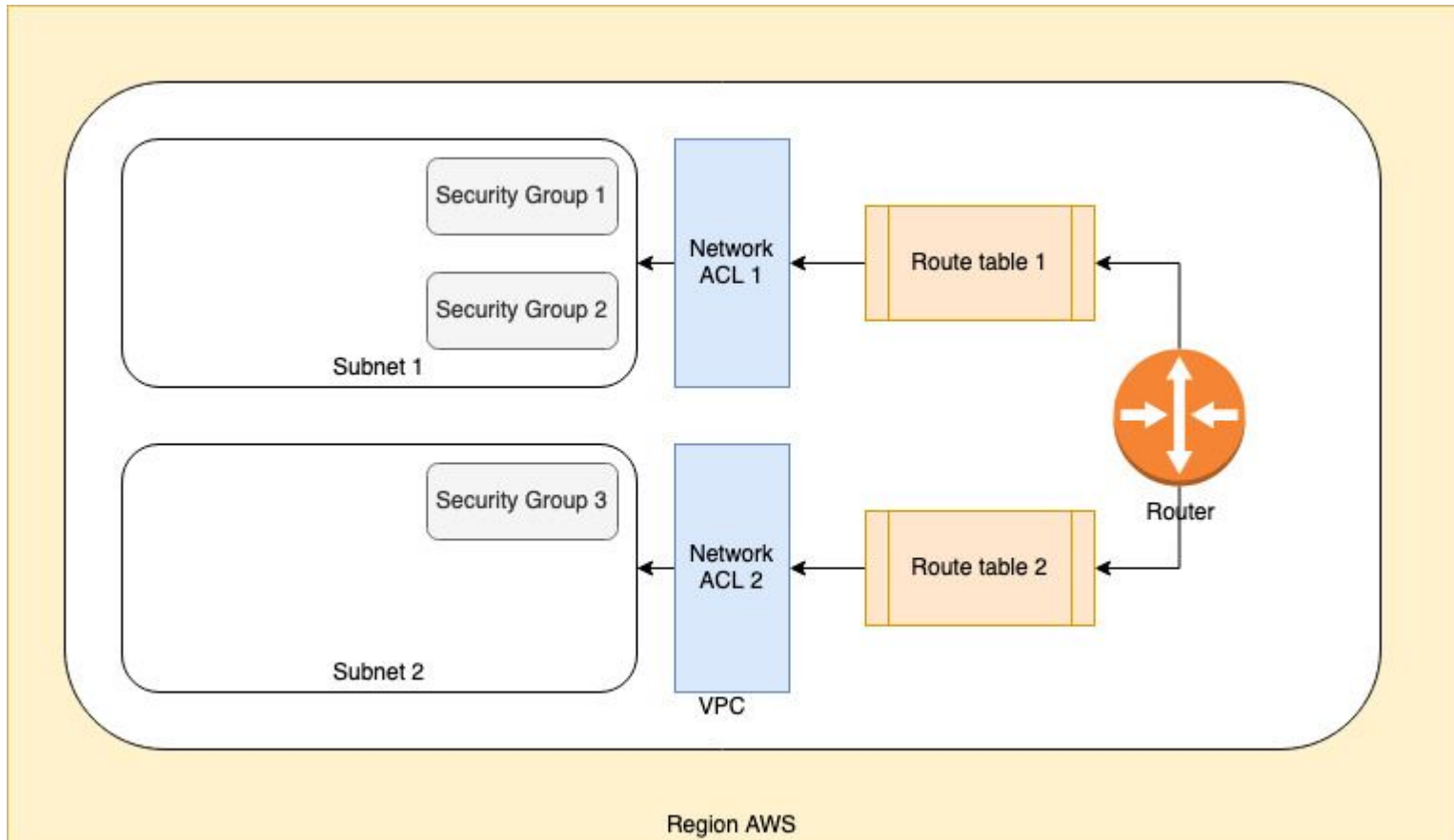
Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
SSH ▼	TCP	22	Custom ▲ Custom Anywhere My IP	<input type="text" value=""/> sg-05d38a24e11cd1033 ✕	<input type="text" value=""/> <input type="button" value="Delete"/>
<input type="button" value="Add rule"/>					

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

При создании правила, обратное для сессии не требуется – **StateFull**.

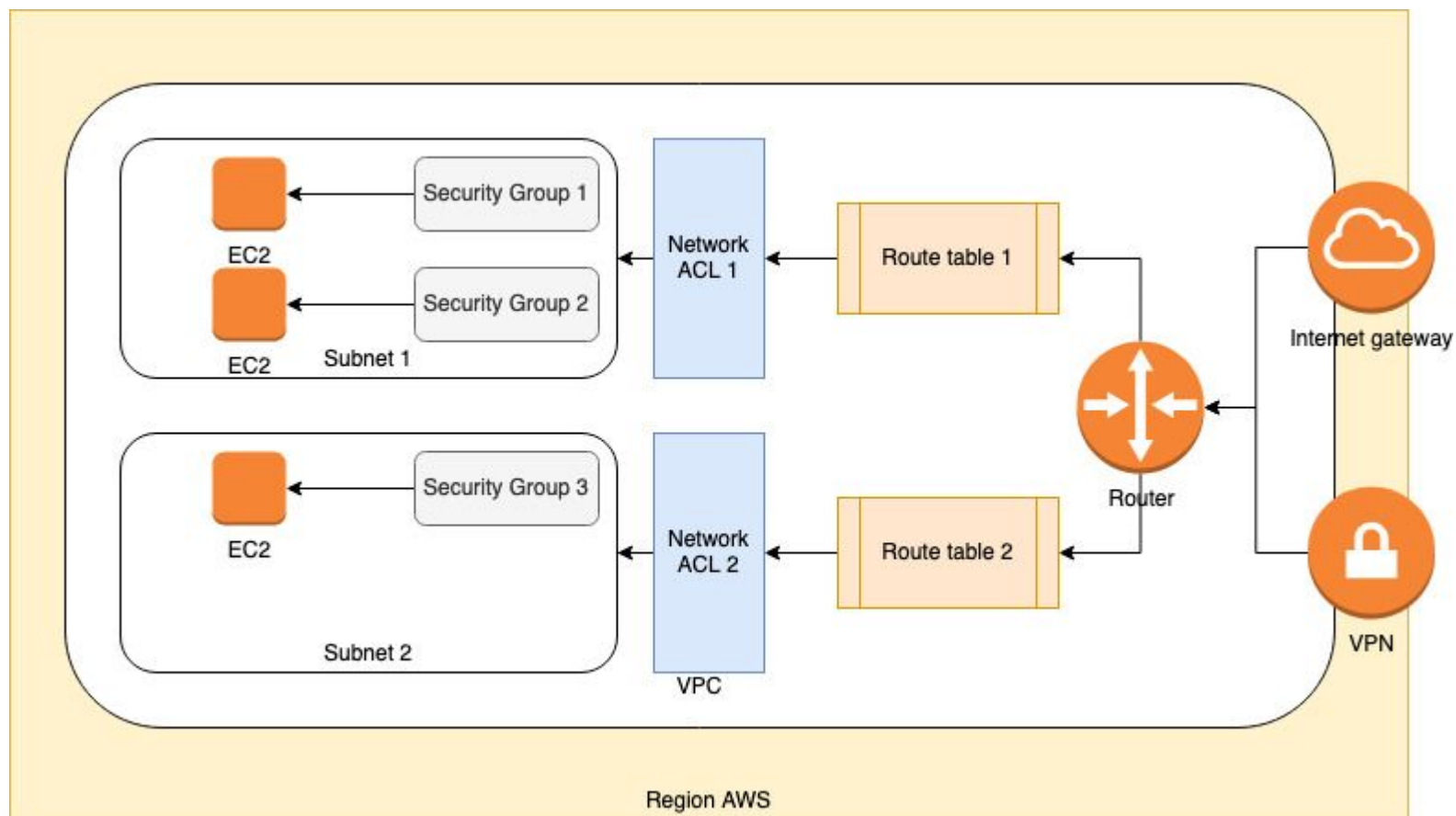
Security Groups



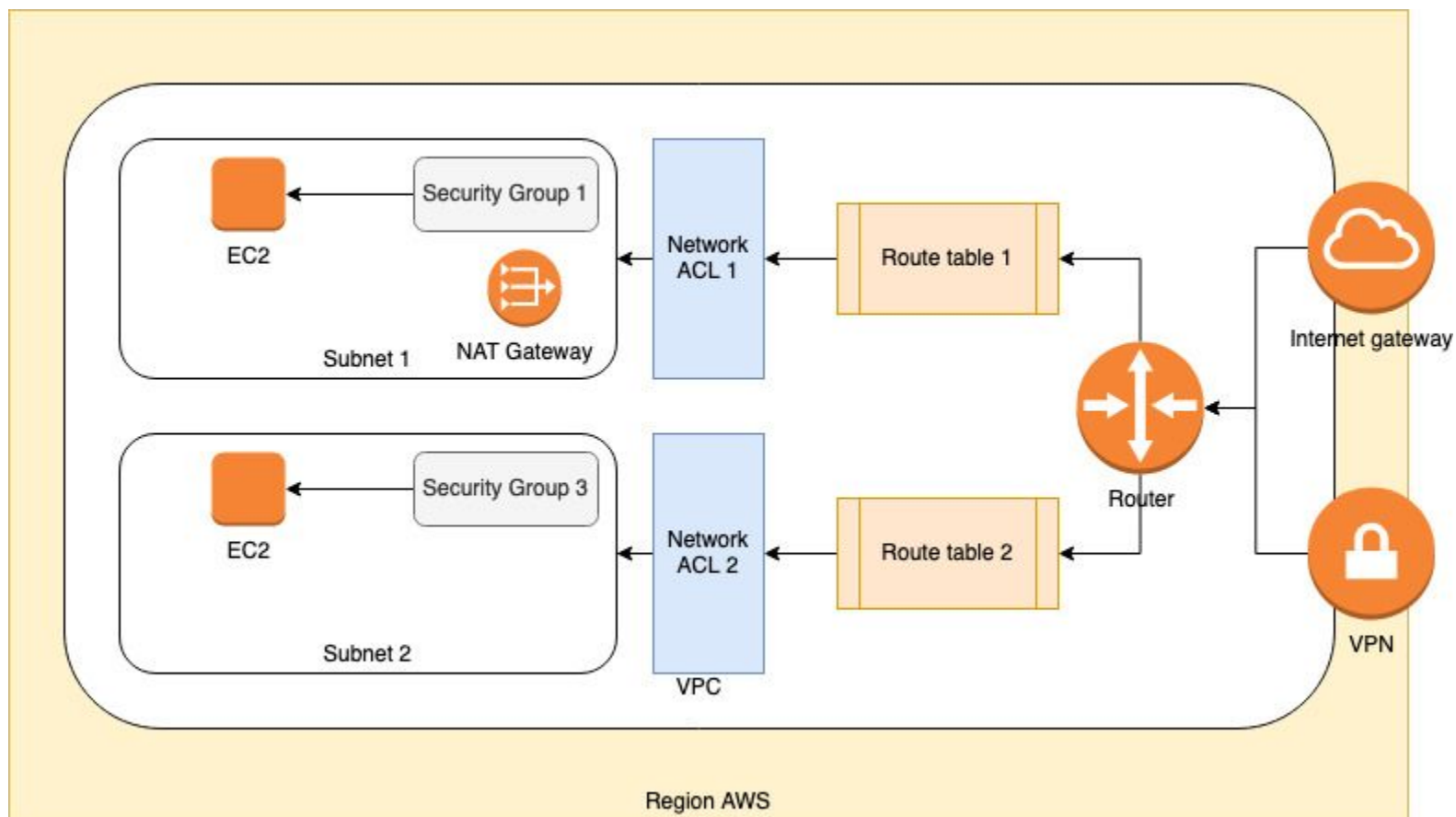
Сравнение Security Group и Network ACL

Security group	Network ACL
Регулирует трафик инстанса в подсети.	Регулирует трафик подсетей.
Только разрешающие правила.	Разрешающие и запрещающие правила.
Обратный трафик разрешен независимо от правил.	Обратный трафик должен быть явно разрешен.
Для принятия решения учитываются все правила.	Для разрешения трафика правила применяются поочередно, согласно своему номеру приоритета.
Применяется к инстансу только, если указана при создании.	Применяется ко всем инстансам в подсети.

Общая картина работы сети



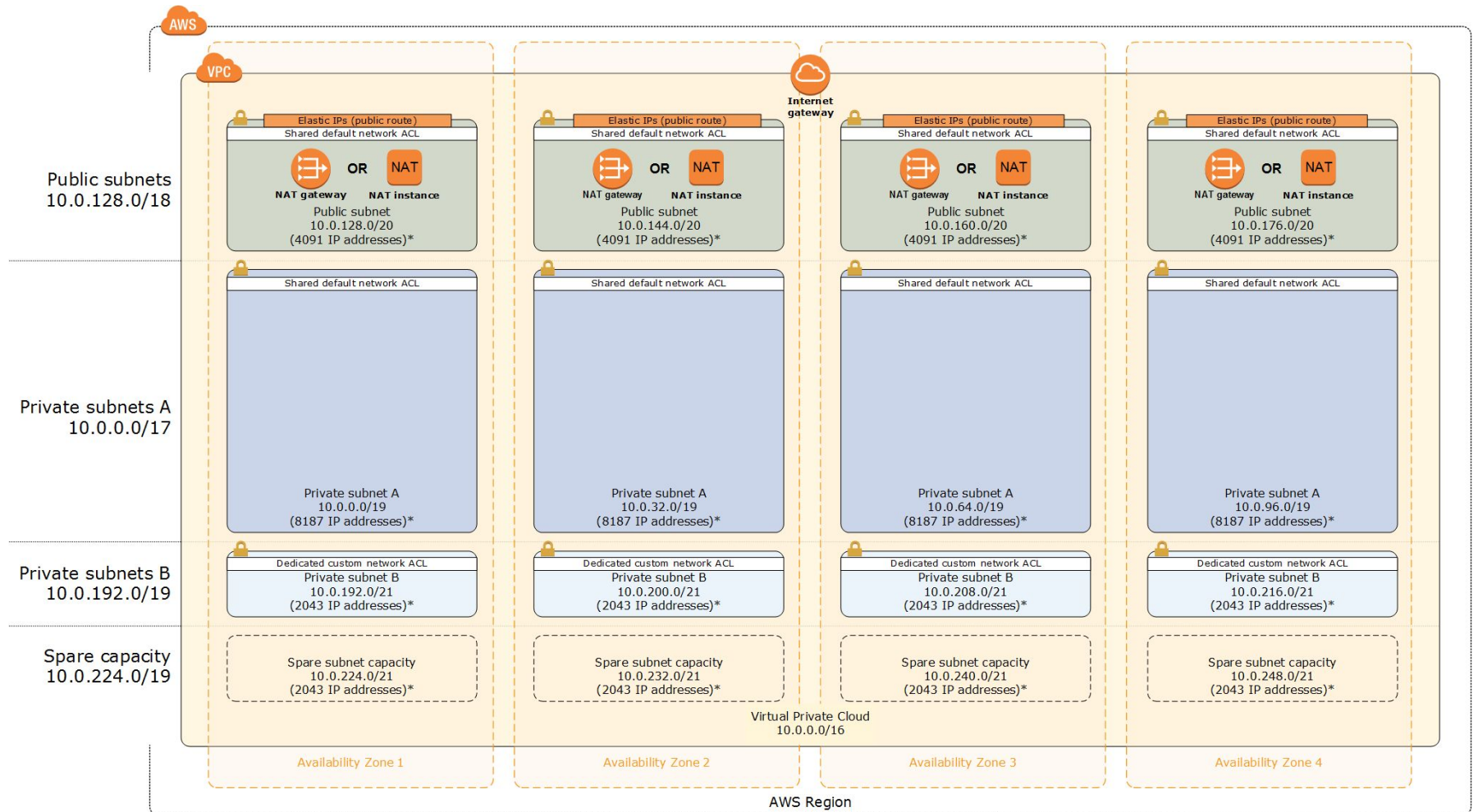
Общая картина работы сети



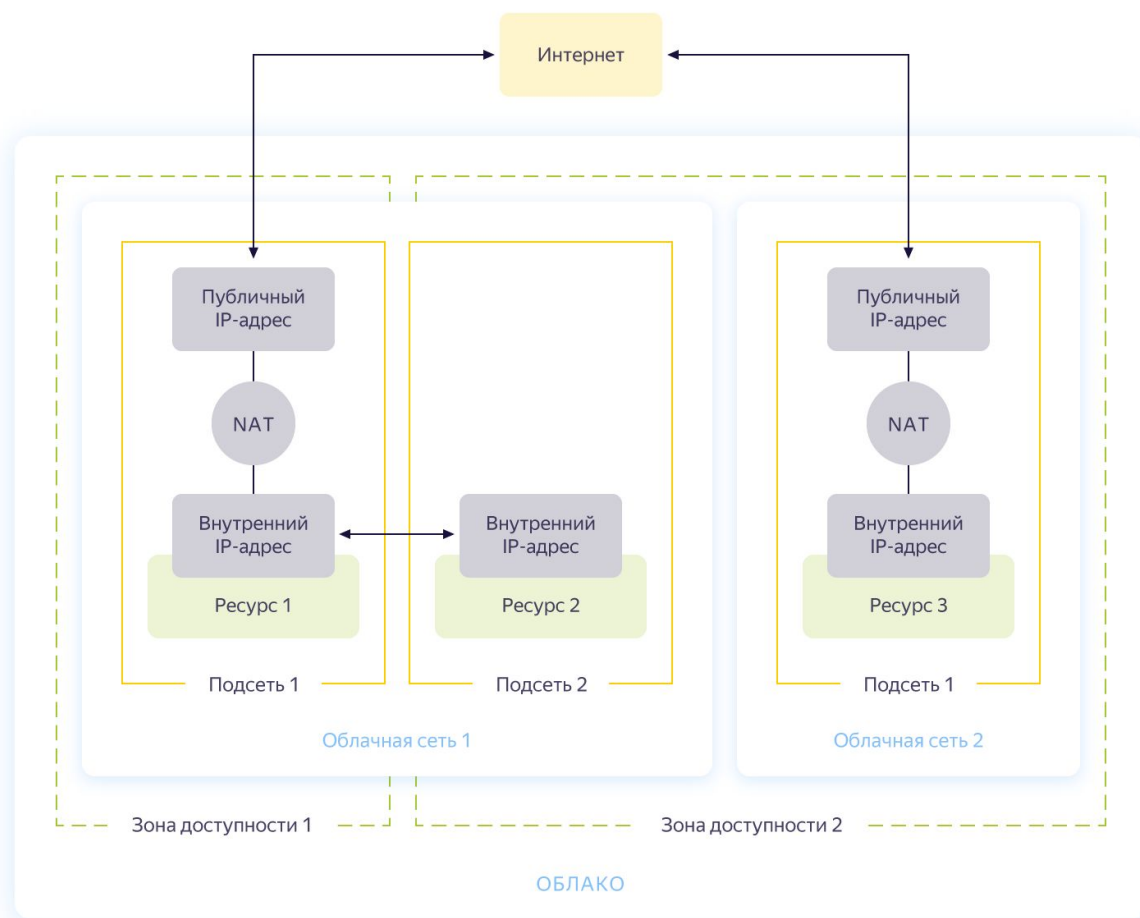


Production ready VPC

Production VPC Architecture



Production VPC Architecture



Итоги

Сегодня на занятии мы:

- поговорили о Amazon VPC;
- изучили, что бывает в подсети VPC и какие бывают виды сетей;
- узнали, что такое Security Groups и Network ACL.

Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

**Задавайте вопросы и
пишите отзыв о лекции!**

Денис Альмухаметов