Добрый день, уважаемые студенты! Я рад вас всех видеть на очередной сессии вопросов и ответов. Давайте начнем.

Вопрос: «Как расшифровывается аббревиатура “IP” в термине IP-адрес?» Ответ: IP – это Интернет-протокол (Internet Protocol), и на текущий момент существуют две версии этого протокола, это IPv4, т.е. версия четвертая, и IPv6, версия 6. В большинстве случаев во время вашей работы облачным инженером либо системным администратором, в основном вам будет встречаться протокол IPv4. Протокол IPv6 распространен намного реже, но если он вам встретится, то уже в процессе работы можно будет дополнительно его освоить и изучить, т.к. глобальных отличий от IPv4 у него нет, а есть лишь некоторые дополнительные нюансы.

Вопрос: «Откуда берутся цифры в примерах IP-адресов?» Ответ: Казалось бы, простой вопрос, но на самом деле мне и здесь есть что рассказать! Существует определенный набор спецификаций под названием RFC плюс определенный набор цифр, это такие скучные документы, опубликованные в интернете, описывающие все те технологии, которые так или иначе связаны с интернетом. Так вот, одна из них, это RFC 1918, которая описывает подробности по IP-адресам и их распределению. Дополнительно с этим документом можно ознакомиться в рамках самостоятельной работы путем обычного Google запроса, а я бы хотел ознакомить вас с определенной частью этого документа, а именно то, что согласно рекомендации этой спецификации, у нас есть три IP-range, так называемых CIDR блоков, которые рекомендуется использовать в вашей локальной сети, и это номера от 10.0.0.0 до 10.255.255.255. Как префикс вы можете здесь указывать /8 и выше. Второй  вариант, он начинается на 172., здесь все аналогично, здесь уже как рекомендация использовать префикс 12, здесь может меняться лишь только определенная часть, т.е. эта подсеть немножко меньше. Следующая рекомендация, это IP-адрес, с которым вы, скорее всего, сталкивались, когда настраивали интернет дома, либо знакомым. Это IP- range в третьей строке, начиная с 192.168.0.0 и до последней в этом range, 192.168.255.255. Этот range еще меньше, как префикс мы выбираем 16 и выше. Можете дополнительно отметить где-то у себя эти range. Как вопрос внутри реального AWS экзамена, эти range не придут, это больше для вашей будущей карьеры. Когда вы начнете работать в какой-нибудь IT-компании, вы можете обратить внимание, что в корпоративной сети, конкретно для вашего рабочего компьютера, будет дан локальный IP-адрес, относящийся к одной из следующих IP-range.

Вопрос: «Помимо упрощения инфраструктуры, будет ли использование AWS Transit Gateway более экономичным в плане финансов в сравнении с VPC peering?» Ответ: Очень хороший вопрос, он затрагивает целый ряд других подобных вопросов, связанных со сравнением решений внутри AWS между собой по цене, по качеству и многим другим факторам. Как вы знаете, внутри AWS более 200 различных сервисов, какая-то часть похожа между собой, таким образом, любое IT-решение, любую IT-инфраструктуру вы можете построить различными путями. Нет единого верного ответа. Таким образом, в случаях, когда сервисы похожи, возникает вопрос, что же лучше использовать? Что выгоднее, что дает дополнительные преимущества? На примере Transit Gateway и VPC peering я могу вам сказать, что если у вас небольшое количество VPC, и они слабо связаны между собой, т.е. нет необходимости для каждого нового VPC создавать отдельный VPC-connection между всеми из существующих VPC, в этом случае возможно выгодным будет использование VPC peering. В случае же, когда у вас большое количество VPC, связанных между собой, то рациональнее использовать AWS Transit Gateway. Это общее направление, как следует оценивать. Когда мы говорим про конкретную бизнес-задачу, вы должны учитывать, во-первых, текущее состояние вашей IT-инфраструктуры и на какой-то период в будущем, то, как она может потенциально измениться. Возможно, быть так, что на текущий момент вам выгодно использовать VPC peering, но при определенном количестве дополнительных VPC станет выгодным использовать Transit Gateway. Поэтому необходимо обязательно изучить этот вопрос как можно детальнее, разузнать у других IT-специалистов, архитекторов в вашей компании, если это кейс внутри вашей компании, уточнить возможный рост, возможное развитие текущей инфраструктуры и понимать, как она в будущем, хотя бы через 6 месяцев, изменится, как будет выглядеть. Если есть тенденция, что у вас увеличивается количество VPC, количество VPC peering растет в геометрической, либо подобной прогрессии, в этом случае, возможно, следует учесть этот момент и использовать AWS Transit Gateway. При решении подобных вопросов в последующем вам нужно будет оценивать текущее и будущее состояние инфраструктуры, учитывать все факторы, которые оплачиваются конкретно сервисами, которые вы выбираете. Эти расчеты помогут понять, какой вариант для вас лучше. Здесь нет какого-то единственно верного ответа, все зависит от вашей бизнес-задачи и вы, как облачный инженер, должны уметь правильно посчитать, проанализировать и предоставить вашему бизнесу самое релевантное и выгодное решение.

Вопрос: «Что такое firewall?» Ответ: Firewall – это понятие не относится к облачным технологиям и является общим термином, больше связанным со сферой networking, т.е. сетями. Если говорить простыми словами, firewall – это виртуальное или физическое устройство, которое по определенным правилам и алгоритмам помогает защитить ресурсы вашей сети. Если мы говорим о конкретных примерах в AWS, которые могут являться Firewall, то Security groups являются Firewall на уровне инстанса. Network ACLs является Firewall на уровне subnet. Также мы можем отнести к Firewall сервис AWS Shield, который защищает ваши VPC от DDoS-атак. То есть это достаточно общее понятие и в зависимости от конкретного случая она может видоизменяться. Но основной смысл в том, что он защищает ресурсы от внешнего трафика в вашем периметре, в вашей локальной сети.

Вопрос: «Лекция, посвященная сетям и доставке контента, была достаточно объемной и непростой для понимания. Что ожидать от следующих лекций?» Ответ: Это был достаточно ожидаемый вопрос, я специально включил его в подборку, чтобы дать вам более развернутый ответ. Хочу вас немного успокоить, не переживайте, что следующие лекции будут сложными и вам будет тяжело закончить эту дисциплину. Не волнуйтесь, на самом деле это не так. Давайте попробую объяснить. Все IT-университеты, готовящие IT-специалистов, “заточены” на выпуск разработчиков. Даже сейчас вы по себе можете представить, кем вы будете, большинство из вас представляет себя разработчиком, освоившим какой-то язык программирования. Набор дисциплин, которые преподаются в рамках вашего университета, больше используются у разработчиков. Даже если сравнить, казалось бы, такую популярную IT-специальность, как системный администратор, все равно вы ближе к разработчику. Развивая идею дальше, говоря про дисциплины, связанные с сетями, возможно, у вас была специально выделенная дисциплина, например, в моем случае, у моих знакомых специальной дисциплины именно по сетям не было. Таким образом, networking – это тема, которая является более узконаправленной, более узкоспециализированной, так же, как и облачные технологии. Поэтому совершенно нормально, что сети кажутся вам чем-то сложным и вполне ожидаемо, что эта тема будет немного сложна для вашего восприятия. Если же у вас совсем не сложилось впечатление по networking внутри AWS, я настоятельно рекомендую найти время, пересмотреть все активности ровно в том порядке, в котором рекомендуется, и попробовать усвоить материал лучше. Если снова возникли некоторые затруднения, вы всегда можете написать мне, представителю Cloud Academy в наши групповые Telegram-чаты, мы обязательно ответим вам. Самые интересные вопросы мы добавим в подборку сессии вопросов и ответов и разберем их отдельно. Последующими темами после лекции на тему Networking, будут темы, посвященные хранению данных, про вычислительные мощности в облаке, про базы данных и вопросы архитектуры. Все эти темы являются очень интересными и ожидается, что они будут намного проще для восприятия. Почему networking пришел посередине? Это рекомендуемая последовательность прохождения тем, которые вы должны знать для того, чтобы было легче освоить следующую тему. Приведу пример – после networking мы через какое-то время пройдем тему баз данных, а также пройдем тему вычислительных мощностей. Когда говорим про базы данных – это RDS, когда говорим про вычислительные мощности — это EC2. Чтобы развернуть и правильно и безопасно использовать в облаке оба ресурса, что RDS, что EC2, они должны находиться внутри VPC. Таким образом, вы не сможете правильно пользоваться этими сервисами, не зная и не ознакомившись с сетями внутри AWS. Вот почему networking пришел раньше. Все последующие темы для вас, как для условных разработчиков, являются ближе и легче для восприятия. Поэтому бояться и переживать, что следующие лекции станут еще сложнее не стоит, на самом деле это не так.

Сегодня мы разобрали самые интересные вопросы, которые были получены от вас и на этом мы завершаем сессию вопросов и ответов. Спасибо за внимание, увидимся на следующих наших активностях!