AWS

Amazon Virtual Private Cloud

это сервис, который дает возможность запускать ресурсы AWS в определяемой пользователем логически изолированной виртуальной сети. Это позволяет полностью контролировать среду виртуальной сети, в том числе выбирать собственный диапазон IP-адресов, создавать подсети, а также настраивать таблицы маршрутизации и сетевые шлюзы.

Amazon VPC features

IP-адресация
С помощью IP-адресов ресурсы VPC взаимодействуют друг с другом и с ресурсами, расположенными в Интернете. Amazon VPC поддерживает как протокол адресации IPv4, так и IPv6. В VPC можно создать подсети, предназначенные только для IPv4, только для IPv6 или с «двойным стеком», а затем запускать инстансы Amazon EC2 в пределах этих подсетей.

Flow Logs
Мониторинг журналов потоков VPC, доставляемых в Amazon Simple Storage Service (Amazon S3) или Amazon CloudWatch, обеспечивает операционный контроль сетевых зависимостей и моделей трафика, выявление аномалий и предотвращение утечки данных и устранение неполадок сетевых подключений и проблем конфигурации.

Network Access Analyzer
С помощью Network Access Analyzer можно проверить, отвечает ли сеть в AWS требованиям сетевой безопасности и другим нормативным требованиям. Network Access Analyzer позволяет указать необходимые требования к сетевой безопасности и нормативные требования, а также способен выявить непреднамеренный доступ к сети, которая им не соответствует

Reachability Analyzer
Этот инструмент для анализа статических конфигураций позволяет анализировать и выполнять отладку доступности сети при подключении ресурсов в VPC между собой.

Traffic Mirroring
Зеркалирование трафика дает возможность копировать сетевой трафик из сетевого интерфейса инстансов Amazon EC2 и отправлять его на внеполосные устройства обеспечения безопасности и мониторинга для углубленной проверки пакетов.

IP Address Manager (IPAM)
С помощью IPAM легче планировать, отслеживать и проверять IP-адреса для рабочих нагрузок AWS. IPAM автоматизирует IP-адресацию для Amazon VPC, позволяя больше не использовать собственные приложения для планирования или приложения на базе электронных таблиц.

Network Access Control List
это необязательный уровень безопасности VPC, который действует как брандмауэр, контролирующий входящий и исходящий трафик одной или нескольких подсетей.

Ingress Routing
Эта возможность позволяет направлять входящий и исходящий трафик, проходящий через шлюз Интернета или шлюз виртуальной частной сети, в интерфейс конкретного инстанса Amazon EC2.

Security Groups
Группы безопасности действуют в качестве брандмауэра для связанных инстансов Amazon EC2 и контролируют входящий и исходящий трафик на уровне инстанса.