AAA – Аутентификация, Авторизация, Учет

Вы вводите свое имя пользователя, свой пароль. Могут быть некоторые дополнительные факторы аутентификации. И если все это верно, вы получаете доступ к ресурсам этой системы. Этот процесс начинается с идентификации, когда вы утверждаете, что являетесь конкретным пользователем этой системы. Проверка между вашим именем пользователя, паролем и другими факторами аутентификации называется **аутентификацией**. Это доказывает, что мы действительно те, кем себя называем, потому что знали секретный пароль.

Теперь, когда мы определили, кто мы, нам теперь нужно определить, какой у нас тип доступа. И это делается через **авторизацию**. Если мы входим в отдел отгрузки и приема, то у нас должен быть доступ к системам, которые должны быть доступны только для отгрузки и получения, и у нас не должно быть доступа к информации, которая может быть в отделе финансов.

И конечно, все системы безопасности должны иметь журнал **(учет)** того, что именно произошло. Поэтому нам нужно знать, во сколько кто-то вошел в систему, сколько данных могло быть отправлено или получено и во сколько. Этот человек вышел из системы. Мы называем всю эту систему структурой AAA. И это относится к аутентификации, авторизации и учету.

Рассмотрим практический пример использования AAA, собираемся на примере входа на VPN-сервер. В этом случае это будет брандмауэр или VPN-концентратор посередине. Ты на одной стороне того концентратора, и нужно использовать AAA, чтобы получить доступ к внутреннему файловому серверу.

Так что начнем с нашего клиента в интернете. И зайдем в VPN-концентратор, который подсказывает нам войти. Итак, мы предоставим имя пользователя и пароль и отправим эту информацию на концентратор VPN. В самом концентраторе нет никакой информации ни об именах пользователей, ни о паролях, ни об аутентификационных факторах, ни о чем другом. И в большинстве организаций вся эта информация хранится на центральном сервере. И мы называем это сервером AAA.

Этот сервер AAA будет получать запрос от концентратора VPN, спрашивая, соответствует ли имя пользователя, пароль и другая предоставленная информация какому-либо типу пользователей в базе данных. И если совпадение верно, оно отправляет обратно информацию в концентратор и сообщает, что эти учетные данные одобрены. В этот момент концентратор знает, что мы действительно являемся тем человеком, за которого себя выдаем, и это позволяет нам получить доступ к внутреннему файловому серверу.

Как специалист по безопасности вы будете отвечать за управление безопасностью на сотнях, а может быть, даже тысячах отдельных систем. И во многих случаях вы никогда не будете иметь физического доступа или даже не сможете увидеть, где могут быть эти системы, потому что они могут находиться в любой точке мира.

Итак, теперь возникает вопрос: как мы можем проверить, что компьютер, пытающийся подключиться к нашей сети, является компьютером, которому разрешено находиться в нашей сети? Этот компьютер сам по себе явно не может набрать пароль, чтобы доказать, кто это может быть. И в большинстве случаев вам, вероятно, все равно не захочется хранить пароль на одной из своих систем в полевых условиях. Так как же вы действительно можете подтвердить, что этой системе разрешено находиться в нашей внутренней сети? Как нам обеспечить дополнительную аутентификацию?

Во многих случаях мы используем сертификат, который мы помещаем на это устройство с цифровой подписью. И мы проверяем эту аутентификацию во время процесса входа в систему. Это позволяет любому, кому необходимо предоставить эту проверку, подтвердить, что это действительно ноутбук, принадлежащий компании. (спец центр сертификации в окружении компании)

Теперь мы помещаем этот сертификат на ноутбук и каждый раз, когда хотим выполнить аутентификацию, мы можем использовать этот сертификат в качестве фактора аутентификации и проверить, действительно ли он был подписан центром сертификации в цифровом виде. Таким образом, как часть вашей инфраструктуры безопасности, у вас будет центр сертификации. Сам этот центр сертификации имеет собственный сертификат, подписанный корневым центром сертификации. У нас также есть ноутбук в полевых условиях. И мы ранее создали сертификат устройства только для этой машины. И он подписан CA.

Как только мы узнаем сертификат CA и сертификат устройства, мы сможем сравнить эти два сертификата. И мы видим, что сертификат нашего устройства был подписан центром сертификации, которому мы доверяем нашу инфраструктуру безопасности. Теперь, когда мы прошли процесс аутентификации, как мы разрешаем тому устройству иметь доступ к ресурсам внутри нашей сети? Мы бы сделали это, используя модель авторизации. И есть много различных моделей авторизации на выбор.

Обычно они определяются ролями, организациями, атрибутами и многими другими типами характеристик. Допустим, у вас вообще не было модели авторизации. Мы бы создали ряд прав и разрешений, где пользователь имеет права доступа к ресурсу. Проблема в том, что это не очень хорошо масштабируется.

Возьмем пример кого-нибудь из отдела отгрузки и приема. Это тот, кому нужен доступ к большому количеству систем, к большому количеству данных. И мы создадим отдельные права и разрешения, чтобы каждый раз, когда этот человек войдет в систему, нам нужно было предоставить ему права на все, что ему нужно для их повседневной деятельности.

Если это единственный человек, занимающийся доставкой и получением, это относительно простой процесс. Но что, если вы входите в более крупную организацию, в судоходстве и приемке которой находятся десятки или сотни человек? Вы можете видеть, что будет сложно взять каждую учетную запись пользователя и вручную настроить права и разрешения для каждого отдельного ресурса, к которому ему нужен доступ. Ресурсов в данном случае всего три. Но представьте, если бы ресурсов было десятки или сотни. Вам нужно будет настроить их для десятков или сотен пользователей.

Теперь вы можете понять, почему это будет очень сложно масштабировать. Чтобы иметь возможность масштабироваться, нам нужно будет использовать модель авторизации. Иногда вы услышите, что это называется абстракцией, которая позволяет нам отделить пользователей от информации, к которой они пытаются получить доступ. Это значительно упрощает процесс администрирования такого большого количества пользователей или большого количества ресурсов. И мы можем поддерживать очень, очень большую инфраструктуру, просто используя очень простой набор абстракций.

Вот как бы это сработало. У нас был бы один и тот же пользователь в доставке и получении, и мы добавим их в группу под названием "Доставка и получение". Первоначально мы создали эту группу таким образом, чтобы любой, кто добавлен в группу доставки и получения, имел доступ к созданию этикетки доставки, отслеживанию доставки, просмотру ежемесячных отчетов об отправке, имел доступ к контактной информации клиента и всему, что вам понадобится при доставке. и получение.