Как и многие компании в настоящее время, мы также попросили своих сотрудников работать из дома, чтобы обезопасить их здоровье. В результате, характеристики нашего сетевого трафика резко изменились. Эти изменения вызваны рядом проблем, связанных с эксплуатацией и безопасностью сети.

Предположительно, существует большое количество других компаний, которые испытывают такую же ситуацию. В этой статье мы хотели бы поделиться нашим опытом и тремя наиболее важными проблемами, которые мы наблюдали. В данной ситуации для нас было важно убедиться, что все сотрудники Flowmon могут оставаться на связи и могут комфортно продолжать свою работу из дома.

1. Безопасная и достаточная пропускная способность VPN

VPN - это готовое решение для обеспечения удаленного подключения. Однако изменилось то, что вместо нескольких удаленных пользователей внезапно подключаются все. Но VPN не был готов к такой емкости. Для нас это означало, что регулярный трафик в будние дни вырос в десять раз по сравнению с обычным. Хотя для более крупных компаний это увеличение может быть совершенно другим, применяемые принципы могут быть одинаковыми.

Начните с проверки структуры трафика; сколько емкости вы используете и в каком объеме нуждаетесь с точки зрения количества одновременно работающих пользователей и пропускной способности сети.

Если количество пользователей превысило допустимое число, обратитесь к поставщику и посмотрите, поможет ли обновление лицензии.

Если вы ограничены пропускной способностью из-за недостатка аппаратных ресурсов, уточните у своего поставщика, сможете ли вы получить обновление в ближайшее время.

У некоторых из вас может оказаться дополнительный сервер с большим количеством ресурсов, и при желании вы можете использовать его для VPN, например, с помощью OpenVPN для доступа к сетевому трафику. Особенно в такой ситуации, когда вы находитесь под давлением, обратите внимание на безопасность и следуйте рекомендациям, таким как включение двухфакторной аутентификации для VPN.

Насколько позволяет ваша политика безопасности, вы можете настроить клиентские станции для прямой маршрутизации Интернет-трафика, разгрузив некоторую пропускную способность VPN, с некоторыми ограничениями.

Наконец, попросите своих сотрудников воздерживаться от использования сервисов большого объема; например, YouTube или Netflix.

2. Управление использованием Uplink

В зависимости от того, как вы настроили VPN, вы увидите увеличение или уменьшение использования uplink в Интернете. В Flowmon мы используем множество облачных приложений (Google Suite, Salesforce и т. д.), к которым пользователи получают доступ прямо из дома. Это означало, что использование нашей компанией Интернет-связи снизилось. На самом деле, многим нашим пользователям вообще не нужен VPN-доступ. Это преимущество современной, облачной компании.

Однако, если ваши сотрудники используют uplink чаще, чем обычно, свяжитесь с вашим провайдером. Многие сейчас предлагают хорошие скидки. Кроме того, вы всегда можете ограничить службы, которые вы разрешаете использовать, например, блокировать потоковые приложения. Учитывая тенденцию к превышению масштаба uplink, это не может быть проблемой для большинства организаций.

3. Минимизируйте риски, связанные с использованием личных устройств

Разрешение вашим сотрудникам работать на своих личных устройствах из дома порождает некоторые серьезные проблемы безопасности. Как правило, вы не контролируете эти устройства, и политики безопасности становятся неэффективными. Если это ваш случай, рассмотрите следующие предложения:

Контролируйте трафик правильно. Вы должны выполнять обычный ежедневный мониторинг, как вы привыкли, но с особым вниманием к узлам VPN и трафику VPN. Но, как и много раз в прошлом, недоброжелатели могут быть очень креативными, когда дело доходит до использования глобальных социальных проблем. Вредоносная программа под названием Emotet использует глобальную чрезвычайную ситуацию для поиска новых жертв. Таким образом, в дополнение к заботе о нашем здоровье, в кибер-мире стоит также следить за аномалиями и избегать рисков кибербезопасности.

Ограничьте доступ и изолируйте пользователей - предоставьте пользователям доступ только к тем данным и услугам, которые им необходимы в их роли. Если вы используете приложения SaaS, это не должно быть проблемой.

Ищите другие способы обеспечения безопасности коммуникаций. Одним из вариантов может быть использование служб терминалов, когда пользователь подключается с незащищенного персонального устройства через VPN к, скажем, серверу Windows через RDP. Этот сервер находится под вашим контролем и безопасен. Удаленный рабочий стол может быть не лучшим с точки зрения пользовательского опыта, но он гораздо менее рискован и довольно прост в настройке и использовании.

Это некоторые рекомендации, основанные на нашем опыте. Мы надеемся, что вы нашли их полезными.

Если вам нужна помощь в адаптации к изменениям, которые на вас влияют, обратитесь в службу поддержки по адресу **support@flowmon.com**.