Ключевые сетевые тренды на 2021 г.

Компания Cisco представила исследование на тему глобальных сетевых трендов о тенденциях, которые руководители сетевых и ИТ-служб должны учитывать в рамках обеспечения бесперебойной работы своей организации. Пять наиболее значительных сетевых трендов на 2021 г. касаются таких направлений, как штат сотрудников, рабочие места, нагрузки на сеть и ИТ-операции. В большей степени это связано с тем, что за период пандемии мир изменился очень сильно. Инструменты и решения, ускоряющие цифровую трансформацию, стали играть еще более важную роль.

Тренд 1: Обеспечение безопасности для удаленных сотрудников

В условиях «новой нормальности» ИТ-отделы сталкиваются с новыми требованиями, включая необходимость расширять возможности для удаленной работы, а также предоставлять сотрудникам доступ к корпоративным сервисам и приложениям с домашних систем. При этом обеспечение безопасности становится все более важной задачей. Для усиления защищенности Cisco рекомендует придерживаться нескольких простых правил.

• Используйте VPN: это по-прежнему является одним из самых эффективных и быстрых способов усилить защиту как сотрудников, так и корпоративных сетей в целом.

• Используйте многофакторную аутентификацию (MFA) для защиты приложений. Такой подход позволяет идентифицировать каждого пользователя, прежде чем разрешить доступ в сеть или к конфиденциальным приложениям и данным.

• Настройте периферийный сервис безопасного доступа (SASE), чтобы обеспечить защищенный доступ в многооблачной среде. Это поможет защититься от Internet-угроз независимо от типа удаленного подключения, устройства с которого осуществляется подключение и используемого облачного сервиса.

Тренд 2: Обеспечение безопасного возвращения в офис

Очевидно, что работа в офисе после пандемии потребует нововведений. Многие компании уже развивают такие решения, как видеоконференцсвязь и геолокация на основе Wi-Fi, внедряют сервисы мониторинга соблюдения социальной дистанции, совершенствуют автоматизацию рабочих мест и даже начинают использовать роботов. Для реализации этих нововведений потребуется современная интеллектуальная сетевая инфраструктура. Cisco рекомендует учитывать следующие аспекты:

• нагрузочное тестирование сети: если сеть не работала в течение нескольких недель. Не факт, что она по-прежнему может предоставлять необходимые проводные и беспроводные услуги;

• автоматизация безопасного доступа на основе идентификации: организациям необходима возможность управления, защиты и сегментации подключений, независимо от местонахождения пользователей;

• обеспечение безопасности сотрудников с помощью аналитики на основе геопозиционирования. Мониторинг рабочего места за счет использования Wi-Fi, оповещение и аналитика помогут защитить здоровье и безопасность сотрудников.

Тренд 3: Использование многооблачной стратегии для повышения устойчивости бизнеса

В условиях пандемии ИТ-руководители используют облачные сервисы для повышения устойчивости бизнеса. Однако в будущем все активнее будет внедряться модель мультиоблака, то есть распределение приложений, рабочих нагрузок и данных между локальными ЦОД и поставщиками общедоступных облаков. Такой подход позволяет снижать затраты, повышать гибкость, усиливать защиту от возможных сбоев.

В этих условиях организациям необходима проактивная сетевая стратегия работы с несколькими облачными системами. При создании такой стратегии важно опираться на следующие три основных принципа:

• оптимизация нагрузки на сеть: внедрение облачной операционной модели для упрощения политик, безопасности и управления нагрузками на сеть и услугами в локальных центрах обработки данных, разрозненных облаках и других вычислительных средах;

• использование программно-определяемой глобальной сети (SD-WAN) и SASE для обеспечения постоянного безопасного мультиоблачного (включая SaaS) доступа для пользователей и устройств в корпоративных и общедоступных сетях из кампуса, филиала, дома или в дороге;

• фокус на безопасность: снижение рисков, связанных с пользователями, устройствами и приложениями, распределенными в нескольких облаках и других вычислительных средах.

Тренд 4: Автоматизация сетевых операций

Пандемия вызвала изменения в отношении числа клиентов, моделей трафика приложений и новых сетевых сервисов таких, как электронное обучение, видеоконференции, виртуальные мероприятия, удаленное обслуживание, автоматизация процессов и др. И сегодня половина сетевых специалистов считает автоматизацию сети критически важным требованием. В связи с этим предлагается применять следующий пошаговый подход.

• Автоматизируйте повторяющиеся административные задачи, чтобы снизить административную нагрузку и улучшить соответствие требованиям в каждом домене.

• Автоматизируйте процесс подключения к сети, адаптацию и сегментацию для защиты групп распределенных пользователей и устройств от кибератак.

• Автоматизируйте сетевые политики в корпоративном ЦОД с помощью сегментации, ориентированной на приложения, которая защищает приложения и данные, а также отслеживает нагрузки на сеть.

• Автоматизируйте политику за пределами ЦОД в облаке с помощью облачной операционной модели, которая обеспечивает согласованную политику приложений для локальных и гибридных облачных сред.

• Автоматизируйте сквозную сегментацию на основе политик для нескольких доменов, чтобы установить согласованную сквозную модель доступа на базе подхода zero-trust (никому не доверять).

Тренд 5: Использование сетевой аналитики на базе искусственного интеллекта (ИИ)

При совершении сетевых операций не только из традиционной корпоративной сети, но и за ее пределами, необходимы инструменты, повышающие прозрачность работы сетей и предоставляющие максимум сетевой аналитики. Лучшие помощники в этой области — системы сетевой аналитики и обеспечения безопасности на базе ИИ. Они помогают достичь следующих результатов.

• Автоматическое обнаружение проблем внутри сети и между доменами.

• Быстрое устранение проблем. Автоматическое сопоставление всех сетевых событий позволяет оперативно выявлять первопричины проблем и избегать их в будущем.

• Автоматизированное управление политиками: выявляйте устройства, приложения и тенденции их использования для своевременного обновления политик.

• Повышение надежности: выявляйте закономерности и тенденции и предоставляйте контекстную аналитическую информацию, которая ускоряет проактивные корректирующие и предупреждающие действия.

• Сравнительный анализ: предоставление сведений и аналитики, которые помогают администраторам сети сравнивать производительность своей сети с глобальными, отраслевыми или региональными показателями.

Http://www.cisco.ru