



Пришло время отказаться от маршрутизаторов в филиалах

4 преимущества системы защиты SD-WAN

Число организаций, которые отказываются от маршрутизаторов в филиалах и переходят к системе защиты SD-WAN, неуклонно растет. Эта система лучше совместима с облачными технологиями и повышает удобство использования сети. Средства защиты SD-WAN не только проще в управлении, но и способствуют упрощению операций WAN в целом.

Корпоративные средства защиты SD-WAN обеспечивают более эффективное использование унифицированных коммуникаций и важных приложений SaaS, упрощают пользователям в филиалах доступ к облачным ресурсам и создают возможности для взаимодействия. Перечислим четыре ключевых преимущества безопасного SD-WAN по сравнению с устаревшими архитектурами маршрутизации филиалов.

1. Улучшенная адаптируемость приложений.

Маршрутизаторы работают по принципу передачи пакетов. В связи с этим они не поддерживают тщательное отслеживание приложений. Большинство организаций используют облачные приложения и сервисы, поэтому невозможность идентификации важных приложений и применения протоколов, обеспечивающих потребность в определенном объеме пропускной способности и подключениях, чревата неудобствами для пользователей.

Решения SD-WAN поддерживают все функции традиционных маршрутизаторов, в том числе расширенную маршрутизацию и подключения WAN. Помимо традиционных функций маршрутизации, решения SD-WAN:

- Идентифицируют приложения и выбирают оптимальные маршруты при помощи технологии динамического выбора пути в целях обеспечения стабильного качества обслуживания.
- Идентифицируют приложения и создают соглашения об уровне обслуживания для тысяч приложений, таких как O365 и Salesforce.com, и унифицированных коммуникаций.
- Обеспечивают точную идентификацию и маршрутизацию бизнес-приложений за счет ежедневного обновления.



Средства защиты SD-WAN просты в управлении и способствуют упрощению операций WAN в целом.

2. Удобство масштабирования, значительное снижение капитальных и эксплуатационных расходов.

Скорость подключений MPLS и передаваемые объемы данных определены заранее. Это дорогостоящие подключения, и неожиданный рост трафика, обусловленный ростом количества высокоскоростных подключений объединенных коммуникаций или обработкой большого объема данных, может создать неудобства для всех пользователей. Развертывание новых маршрутизаторов в филиалах не спасает ситуацию — это такой же дорогостоящий и затратный процесс.

При помощи решений SD-WAN клиенты могут перейти от подключений MPLS к широкополосным (DSL, 4G/5G, Ethernet). Во многих случаях такое решение способствует снижению эксплуатационных расходов на 40%. Технология SD-WAN обеспечивает безопасное динамическое масштабирование сетей десятков тысяч филиалов, слаженное взаимодействие с существующими физическими и облачными инфраструктурами и удаленное устранение неполадок, что позволяет отказаться от дорогостоящих услуг квалифицированных специалистов. Кроме того, безопасный SD-WAN объединяет в общую инфраструктуру целый ряд специализированных продуктов, в том числе маршрутизаторов, межсетевых экранов и средств оптимизации WAN, что снижает капитальные расходы.

3. Удобство управления и оркестрации.

Процедуры установки, обновления и обслуживания маршрутизаторов филиалов нередко сложны, даже если эти устройства позиционируются как высокоавтоматизированные. Настройка конфигурации требует навыков работы с интерфейсом командной строки маршрутизатора. В силу сложности этой процедуры сотрудники филиалов редко могут выполнить ее самостоятельно.

Управление безопасным SD-WAN централизовано, благодаря чему новые сервисы и политики ориентированы на взаимодействие с приложениями. Конфигурации подключений и компонентов безопасности, а также изменения политик оперативно распространяются по всей расширенной сети WAN, что устраняет необходимость в настройке и администрировании каждого устройства или службы по отдельности. Также централизованная система защиты SD-WAN поддерживает анализ производительности приложений как в прошлом, так и в режиме реального времени, благодаря чему специалисты получают возможность оперативно устранять неполадки и улучшать ключевые показатели производительности, к примеру, среднее время отклика.

4. Интегрированные сетевые функции и функции обеспечения безопасности.

Сетевые функции и функции обеспечения безопасности маршрутизаторов филиалов нельзя назвать интегрированными. Подключение MPLS можно дополнить технологией раздельного туннелирования для обеспечения прямого доступа к Интернету, но при этом управление подключениями при помощи маршрутизаторов филиалов становится невозможным. Они не поддерживают сверхбыстрое переключение трафика на оптимальный канал или альтернативный маршрут во избежание разрыва соединений, неспособны устранить проблемы передачи данных и обеспечить динамическую буферизацию джиттера. Также маршрутизаторы не решают задачу активного регулирования трафика с целью снижения нагрузки. Что еще хуже, из-за неэффективности защиты маршрутизаторов подключения, отличные от MPLS, создают дополнительные риски для организации.

Важно отметить, что большинство решений SD-WAN также нельзя отнести к полностью защищенным, несмотря на то, что наличие полностью интегрированной системы безопасности является одним из важнейших факторов надлежащей работы подключений SD-WAN. В качестве примера интегрированного решения можно привести межсетевой экран следующего поколения (NGFW), который включает такие компоненты, как IPS, Web Filtering, проверка SSL и защита от вредоносного ПО. Сеть SD-WAN без полностью интегрированной системы безопасности превращается в еще один проводник для вредоносного ПО и атак киберпреступников.

Для создания эффективной платформы необходимы инструменты, рассчитанные на взаимодействие в рамках единой системы. В идеале все элементы должны работать на базе одной операционной системы и поддерживать управление из одного окна. В этом случае все транзакции поддаются отслеживанию и проверке, решения обмениваются сведениями об угрозах и аномальном поведении, что обеспечивает максимальную защищенность. В составе такой интегрированной системы сетевые функции и подключения SD-WAN не просто тесно связаны с функциями безопасности платформы, а слиты с ними воедино.

Рекомендации по переходу на следующий этап

Недостаточно понимать необходимость отхода от традиционной стратегии WAN на базе маршрутизаторов. Важно правильно подобрать полнофункциональную систему защиты SD-WAN, которая охватывает все возможные сценарии использования. В этом случае ваше новое развертывание SD-WAN будет не только обеспечивать все потребности организации, но и адаптироваться к быстро изменяющимся требованиям.

