FORTINET

SD-WAN В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Повышение гибкости бизнеса без ущерба для безопасности сети

ИССЛЕДОВАНИЕ

АННОТАЦИЯ

Большинство организаций так или иначе вступило на путь цифровой трансформации (DX). Этот процесс предусматривает внедрение новых способов вывода продуктов и услуг на рынок и предоставления преимуществ клиентам. Однако в то же время цифровая трансформация ставит новые задачи перед сотрудниками отделов эксплуатации сетей. Распределение важных бизнес-служб по разным облакам чревато ухудшением производительности, особенно в филиалах.

В связи с этими тенденциями растущая популярность технологии программно-конфигурируемой глобальной сети (SD-WAN) не вызывает ни малейшего удивления. К сожалению, SD-WAN может служить ярким примером парадоксального характера цифровой трансформации: революционная технология может вывести бизнес на новый уровень, однако ее внедрение приводит к появлению новых векторов атак, а с ними и серьезных рисков для организаций. Поэтому развертывание SD-WAN, как и другие мероприятия в рамках парадигмы цифровой трансформации, требует одновременной модернизации системы безопасности (SX): переосмысления устаревших принципов, выхода за пределы центров обработки данных, интеграции архитектуры безопасности и внедрения функций централизованного отслеживания и управления.

Цифровая трансформация способствует переносу сервисов в облака, что приводит к перегрузке традиционных сетевых архитектур и побуждает организации к переходу на SD-WAN.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОПРЕДЕЛЯЕТ ПОВЕСТКУ ДНЯ

Пожалуй, в настоящее время наиболее важной ИТ-тенденцией в мире бизнеса является цифровая трансформация. Она способствует повышению гибкости и масштабируемости организаций, что во многих отраслях является серьезным конкурентным преимуществом.[1] В процессе цифровой трансформации компании полностью переходят на цифровые технологии и становятся «гиперподключенными, адаптивными, интеллектуальными и гибкими благодаря тесной интеграции технологий с новыми операционными процессами, политиками и организациями, оказывающими поддержку в процессе реализации новаторских инициатив».[2]

Каждая организация адаптирует процесс цифровой трансформации к своим потребностям, однако практически во всех случаях он характеризуется повышением роли гибридной облачной архитектуры. Таким образом, перед сотрудниками отдела эксплуатации сетей встает задача совмещения существующих локальных ресурсов и многочисленных внешних облачных сетей, а также обеспечения их доступности и производительности независимо от местонахождения пользователей.

SD-WAN УДОВЛЕТВОРЯЕТ ТРЕБОВАНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ К СЕТЕВЫМ ПОДКЛЮЧЕНИЯМ

По мере переноса сервисов в облака становится все более очевиден тот факт, что «традиционные сетевые архитектуры... не рассчитаны на обработку нагрузок, с которыми сталкиваются организации, ориентированные на облачные вычисления».[3] Это привело к стремительному распространению другой ключевой технологии цифровой трансформации — SD-WAN. Слово «стремительный» здесь не просто фигура речи: согласно исследованию IHS Markit, 74 % организаций в 2017 г. занимались тестированием решений SD-WAN, и многие из них запланировали развертывание этих решений на следующий год.[4]

Решения SD-WAN обеспечивают высокоэффективный доступ к облачным приложениям для пользователей, занятых в подразделениях организации. Это способствует беспрецедентному повышению гибкости и степени автоматизации сетей филиалов. Перечислим преимущества этой технологии:

1. **Непосредственный доступ к облаку.** SD-WAN не требует обратной передачи трафика — перенаправления облачного трафика и трафика филиалов через центр обработки данных. Это обеспечивает непосредственный доступ к важным облачным сервисам для всех пользователей независимо от их местонахождения.
2. **Повышение производительности приложений.** Решение SD-WAN можно настроить для определения приоритетности важного бизнес-трафика и услуг в реальном времени, таких как IP-телефония (VoIP), и выбора наиболее эффективного маршрута. Наличие нескольких вариантов передачи трафика способствует снижению показателя потери пакетов в связи с перегрузкой каналов и задержкой, обусловленной большим объемом трафика. Перечисленные преимущества повышают производительность и делают пользование приложениями более удобным.[5]
3. **Повышение гибкости бизнеса.** Чтобы расширить традиционную сеть WAN, планировщик сети в течение недель и даже месяцев разрабатывает план развертывания дополнительных каналов многопротокольной коммутации по меткам (MPLS). Теперь в этом нет необходимости. Кроме того, задача обеспечения надлежащей производительности сетей многочисленных филиалов больше не препятствует внедрению других инициатив цифровой трансформации.
4. **Экономия средств.** Решение SD-WAN обеспечивает эффективное перенаправление трафика по нескольким каналам, в том числе не только существующим каналам MPLS, но и интернет-подключениям общего пользования при помощи LTE и широкополосной технологии.[6] Это способствует снижению расходов на выделение новых каналов MPLS.

В ТО ЖЕ ВРЕМЯ ТЕХНОЛОГИЯ SD-WAN МОЖЕТ НЕСТИ В СЕБЕ УГРОЗУ СЕТЕВОЙ БЕЗОПАСНОСТИ

В эпоху цифровой трансформации сложно усомниться в преимуществах сетевой архитектуры SD-WAN. Однако технология SD-WAN также имеет серьезные недостатки. Каждое расположение с поддержкой SD-WAN и локальным доступом в Интернет представляет собой новый вектор атак и уязвимое место системы корпоративной сетевой безопасности. Это усугубляет существующие проблемы, так как еще до внедрения SD-WAN наблюдалась тенденция к меньшей защищенности сетей филиалов по сравнению с сетями главных офисов.

74 % организаций в 2017 г. занимались тестированием решений SD-WAN. Многие из них запланировали развертывание этих решений на следующий год.[7]

Разумеется, многие другие технологии цифровой трансформации также способствуют появлению новых векторов атак, и внедрение новых решений в первую очередь блокируют именно аспекты безопасности.[8] Успешное развертывание любой инициативы цифровой трансформации, в том числе технологии SD-WAN, должно сопровождаться модернизацией системы безопасности.

МОДЕРНИЗАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЕСПЕЧИВАЕТ ЗАЩИТУ В ПРОЦЕССЕ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ SD-WAN

Модернизация системы безопасности предусматривает переосмысление принятых принципов корпоративной безопасности, в том числе стратегии защиты периметра, эффективность которой неуклонно падает по мере развертывания новых облачных служб. Также эта модель несовместима с решениями SD-WAN. Кроме того, разработка стратегии модернизации системы безопасности должна идти параллельно с составлением плана цифровой трансформации, а не «задним числом». Специалисты по планированию и развертыванию должны подвергать каждую инициативу цифровой трансформации анализу с точки зрения безопасности.

К моменту выбора наиболее подходящего решения SD-WAN следует подготовить соответствующую стратегию безопасности, поэтому важно, чтобы в процессе анализа альтернатив участвовали и сотрудники отдела управления сетью, и специалисты по сетевой безопасности. Как правило, два упомянутых отдела функционируют независимо друг от друга, а в некоторых случаях еще и конкурируют.[9] Однако следующие проблемы безопасности, связанные с внедрением SD-WAN, можно решить лишь при условии сотрудничества специалистов из разных сфер:

- Противодействие новым угрозам, появляющимся в связи с цифровой трансформацией и внедрением инфраструктуры SD-WAN[10]
- Предотвращение распространения проникшего в сеть вредоносного ПО[11]
- Компенсация нехватки квалифицированных специалистов по ИТ-безопасности в удаленных филиалах
- Развертывание функций отслеживания и централизованного управления всеми компонентами корпоративной сети

Технология SD-WAN должна сопровождаться модернизацией системы безопасности — переосмыслением принятых принципов корпоративной безопасности, в том числе стратегии защиты периметра.

КЛЮЧЕВЫМ ЭТАПОМ МОДЕРНИЗАЦИИ СИСТЕМЫ БЕЗОПАСНОСТИ ЯВЛЯЕТСЯ ИНТЕГРАЦИЯ

Недавнее исследование показало, что на протяжении последних двух лет среднестатистической организации пришлось столкнуться с 20 кибератаками, из которых четыре привели к негативным последствиям — потере данных, простоям и нарушению требований.[12] В частности, это обусловлено тем, что в среднем обнаружение атаки может занять более шести месяцев (197 дней). В течение этого периода злоумышленники могут свободно перемещаться внутри корпоративной сети.[13] Большинство подобных случаев связано с продвинутыми угрозами, разработанными специально для обхода традиционных мер защиты. Необдуманное внедрение технологии SD-WAN и других инициатив цифровой трансформации может усугубить проблему киберугроз.

Развертывая SD-WAN в процессе цифровой трансформации, организации должны позаботиться о модернизации системы безопасности. Трафик начинает идти в обход центра обработки данных, что требует расширения архитектуры сетевой безопасности с сохранением ее комплексного характера. Безопасная стратегия развертывания SD-WAN предусматривает интеграцию системы безопасности с сетью и включение многосайтовой распределенной корпоративной среды в сферу ее охвата. Такой подход обеспечивает централизованное отслеживание и управление, автоматизацию процессов безопасности, динамический обмен данными об угрозах и надежность сети.

На протяжении последних двух лет среднестатистической организации пришлось столкнуться с 20 кибератаками.

Обнаружение вторжения может занять до шести месяцев. Это означает, что традиционная парадигма безопасности потерпела крушение, а организациям угрожают серьезные риски — от хищения данных и атак с использованием вредоносного ПО до простоев в работе.

МОДЕРНИЗАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ СПОСОБСТВУЕТ РЕАЛИЗАЦИИ ПРЕИМУЩЕСТВ SD-WAN

Благодаря технологии SD-WAN организации получают возможность повысить эффективность сетей филиалов. ИТ-специалистам и руководителям по безопасности необходимо помнить следующее:

- Для многих организаций внедрение SD-WAN является важнейшим этапом цифровой трансформации.
- Технология SD-WAN обладает неоспоримыми преимуществами: она открывает филиалам доступ к облачным сервисам, повышает производительность приложений и гибкость бизнеса, а также снижает затраты.
- Во многих случаях SD-WAN создает новые уязвимости и может стать слабейшим звеном в корпоративной системе безопасности.
- Эффективную защиту в процессе внедрения и эксплуатации SD-WAN может обеспечить только модернизация системы безопасности.
- Залогом безопасности SD-WAN является интеграция.

[1] Майкл Кригсман (Michael Krigsman), «Digital transformation and the CIO: Everything you need to know today», ZDNet, 25 мая 2018 г.

[2] Benson Chan, «Digital transformation reimagines everything», Strategy of Things, 7 сентября 2017 г.

[3] Келли Ахуджа (Kelly Ahuja), «A digital-first enterprise needs SD-WAN», Network World, 7 июня 2018 г.

[4] Энди Патрицио (Andy Patrizio), «Enterprises are moving to SD-WAN beyond pilot stages to development», Network World, 7 мая 2018 г.

[5] Ли Дойл (Lee Doyle), «How does SD-WAN manage real-time network performance?», TechTarget SearchSDN, 9 января 2018 г.

[6] «Traditional WANs vs Next Gen SD-WAN», Infosecurity, 12 декабря 2017 г.

[7] Энди Патрицио (Andy Patrizio), «Enterprises are moving to SD-WAN beyond pilot stages to development», Network World, 7 мая 2018 г.

[8] «Security Implications of Digital Transformation Report», Fortinet, 26 июля 2018 г.

[9] Эрин О'Малли (Erin O'Malley), «Driving the Convergence of Networking and Security», SecurityWeek, 15 мая 2018 г.

[10] Стив Гарсон (Steve Garson), «Warning: security vulnerabilities found in SD-WAN appliances», Network World, 28 ноября 2017 г.

[11] Ли Дойл (Lee Doyle), «What are the options for securing SD-WAN?», Network World, 12 июля 2018 г.

[12] «Security Implications of Digital Transformation Report», Fortinet, 26 июля 2018 г.

[13] «Advanced Threats in Financial Services and Retail: A Study of North America & EMEA», Ponemon Institute, 28 мая 2015 г.

FORTINET В РОССИИ
Пресненская набережная
10, блок С
123317 Москва
Тел: +7 495 937 80 50
Эл. адрес: russia@fortinet.com

ГЛАВНЫЙ ОФИС
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
США
Тел.: +1.408.235 7700
www.fortinet.com/sales

ОТДЕЛ ПРОДАЖ В EMEA
905 rue Albert Einstein
06560 Valbonne
Франция
Тел.: +33 4 8987 0500

ОТДЕЛ ПРОДАЖ В APAC
300 Beach Road 20-01
The Concourse
Сингапур 199555
Тел.: +65 6513 3730

ЛАТИНСКАЯ АМЕРИКА
ГЛАВНЫЙ ОФИС
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Тел.: +1 954 368 9990

1 апреля, 2019 1:47 ПП
253349-0-1-RU
wp-sdwan-in-the-age-of-digital-transformation-a4