АСПЕКТЫ, КОТОРЫЕ НЕОБХОДИМО РАССМОТРЕТЬ В ХОДЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВА ЗАЩИТЫ SD-WAN

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время организации испытывают сложности, связанные со стоимостью, производительностью и гибкостью традиционных глобальных сетей (WAN). Взрывной рост количества общедоступных облачных служб (годовой прирост за 2017 г. составил 28,6 %)[1] вынуждает организации искать более эффективное сетевое решение, которое поддерживает обработку распределенного трафика удаленных расположений и филиалов.

Перечислим некоторые из проблем, с которыми сталкиваются организации, использующие традиционные сети WAN.

- Высокая совокупная стоимость владения (TCO)
- Длительные циклы выделения ресурсов
- Падение производительности вследствие роста объема облачного трафика
- Недостаточные устойчивость и избыточность
- Отсутствие подключений, учитывающих особенности приложений

В целях более эффективного управления инвестициями в сети WAN организации внедряют новое решение, оптимальное для распределенных сетей филиалов. **Программно-конфигурируемые сети WAN (SD-WAN)** отличаются повышенной производительностью, адаптивностью, эксплуатационной гибкостью и экономичностью. Однако не все решения SD-WAN в равной степени эффективны.

[1] «Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017», IDC, 6 ноября 2017 г.

01 ПРОБЛЕМЫ, СВОЙСТВЕННЫЕ ТРАДИЦИОННЫМ РЕШЕНИЯМ WAN

Производительность традиционных сетей WAN ограничена, так как в подобных сетях применяются дорогостоящие цепи, к примеру, цепи многопротокольной коммутации по меткам (MPLS). Распределенные организации все шире используют облачные приложения, поэтому увеличивается и потребность в ресурсе пропускной способности сети. Требования к производительности растут, что приводит к повышению стоимости обслуживания традиционных инфраструктур WAN, а также усложнению их развертывания и администрирования. О наличии проблемы свидетельствуют следующие сведения, **полученные в ходе опроса, который был проведен компанией Gartner в 2016 г. на конференции, посвященной центрам обработки данных: «На 6 респондентов, которые отозвались о сети WAN в своей организации как о «нестабильной, медленной, ненадежной или слишком дорогостоящей», приходится только 1 респондент, готовый охарактеризовать корпоративную сеть как экономичную и гибкую»**[2].

[2] Gartner, Market Guide for WAN Edge Infrastructure, Эндрю Лернер (Andrew Lerner), Нил Рикард (Neil Rickard), март 2017 г.

Высокая совокупная стоимость владения

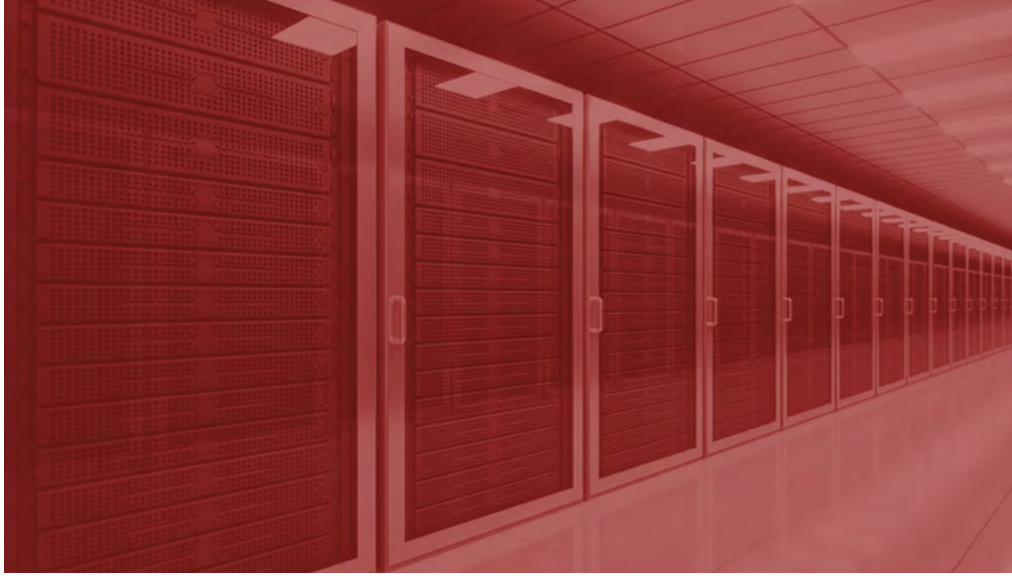
- Традиционным решениям WAN свойственна **высокая стоимость пропускной способности**. Для поддержания межсайтовых подключений и надлежащего качества услуг в таких сетях используются дорогостоящие цепи MPLS, развертывание которых к тому же занимает много времени. Это затрудняет расширение бизнеса и препятствует повышению производительности.
- Отметим и такую проблему, как **сложность инфраструктуры**. Применение изолированных функций безопасности и сетевых функций приводит к увеличению количества элементов, что затрудняет отслеживание их состояния. Эту проблему усугубляет управление при помощи интерфейса командной строки (CLI). Работа с интерфейсом CLI требует значительных затрат времени на отслеживание управления журналами, повышает вероятность возникновения ошибок, связанных с человеческим фактором, и снижает общую производительность персонала.

Развертывание облаков и отслеживание их состояния

- Традиционные сети WAN **не обеспечивают отслеживание состояния облаков на надлежащем уровне**, так как они поддерживают только контроль на уровне пакетов и маршрутизации. Об отслеживании на уровне приложений речи не идет.
- Кроме того, традиционные сети WAN нередко создают **«узкие места»**, что негативно сказывается на производительности пользователей и бизнес-операций. Особенно актуальной эта проблема становится в условиях роста потребности в доступе к облачным приложениям. Перенаправление трафика через центр обработки данных увеличивает время его нахождения в сети и приводит к повышению задержки. Также следует отметить, что **трафик традиционных сетей WAN не является интеллектуальным**, поэтому такие сети не поддерживают выделение для трафика соответствующего широкополосного канала при помощи политики.

Безопасность центров обработки данных

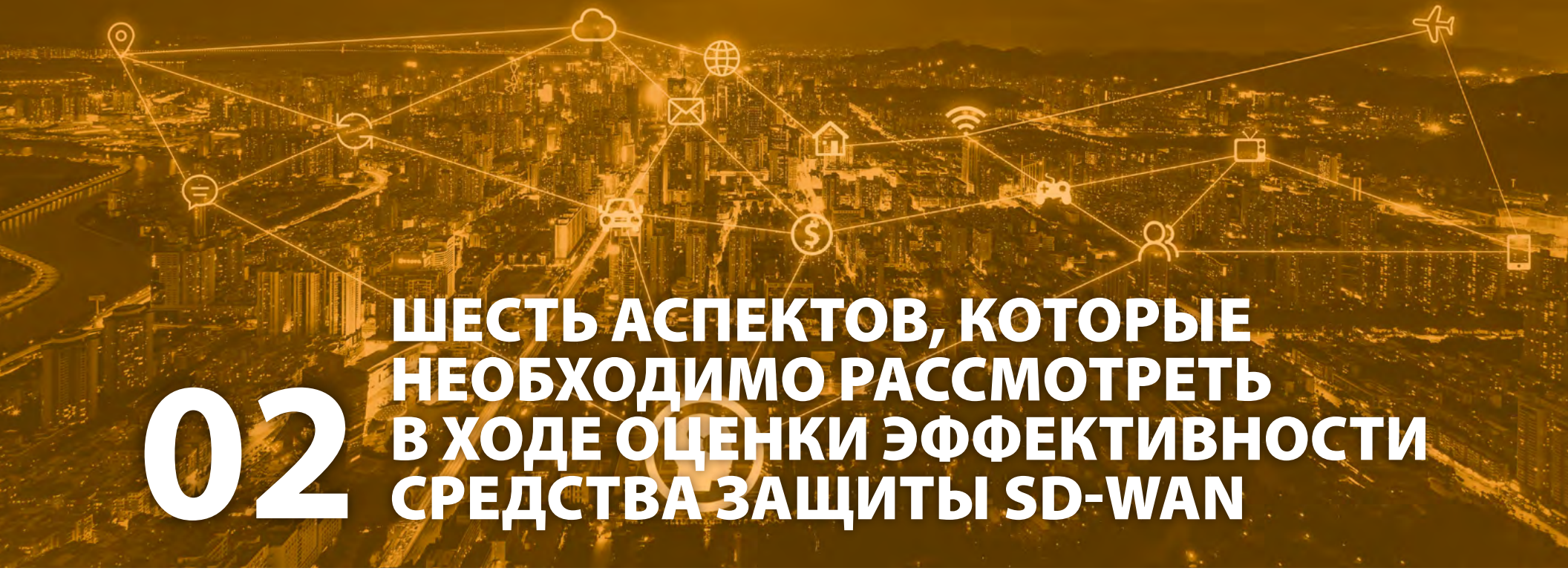
- Частные подключения MPLS, которые используются большинством традиционных сетей WAN, поддерживают централизованное обеспечение безопасности. Звездообразная форма сетевой архитектуры позволяет проверять и фильтровать трафик, проходящий через сеть. Этот подход предусматривает поступление трафика в центр обработки данных (эта процедура называется «обратной передачей трафика»). Проверка трафика обеспечивает его безопасность, однако **сказывается на производительности**.



- В силу самой своей сущности традиционные сети WAN **не имеют прямого доступа к Интернету** при помощи общедоступных ссылок, что ограничивает производительность и препятствует расширению использования таких облачных служб, как приложения «Программное обеспечение как услуга» (SaaS).
- Некоторые организации делают выбор в пользу приобретения отдельных сетевых решений и решений безопасности. **Изолированные устройства с отдельными консолями управления** не поддерживают **комплексное отслеживание элементов сети**. Кроме того, такой подход усложняет операции и делает их более времязатратными.

Устойчивость/непрерывность бизнес-процессов

- Функции отработки отказа сетей WAN для MPLS (сети 4G/3G) **не отличаются надежностью**. Организации не могут добиться **устойчивости**, необходимой для успешного ведения коммерческой деятельности. Простои препятствует выполнению бизнес-операций и чреваты падением производительности.



02 ШЕСТЬ АСПЕКТОВ, КОТОРЫЕ НЕОБХОДИМО РАССМОТРЕТЬ В ХОДЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВА ЗАЩИТЫ SD-WAN

С учетом вышеперечисленных проблем, сопряженных с применением традиционных сетей WAN, организации нуждаются в более простой и экономичной инфраструктуре, которая лучше приспособлена к задачам внедрения облачных технологий.

В отличие от традиционных архитектур WAN **программно-конфигурируемые глобальные сети (SD-WAN)** поддерживают динамическое распределение трафика по нескольким расположениям, а также автоматически реагируют на изменение политик приложений, что повышает производительность. В свою очередь, такой подход способствует большей гибкости и экономичности по сравнению с традиционными сетевыми решениями.

Согласно прогнозу компании Gartner, «в течение ближайших двух лет 25 % организаций внедрят сети SD-WAN»[3]. Однако между продуктами разных поставщиков, представленными на рынке, существует множество отличий — от функциональности до принципов развертывания и управления, от эффективности отслеживания до соотношения цены и производительности.

Ниже перечислены шесть ключевых преимуществ, которые должны учитывать руководители в ходе подбора корпоративного решения SD-WAN.

[3] Gartner, Market Guide for WAN Edge Infrastructure, Эндрю Лернер (Andrew Lerner), Нил Рикард (Neil Rickard), март 2017 г.

1. ВНЕДРЕНИЕ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

По данным компании IDC, темп ежегодного увеличения количества облачных служб составляет 28,6 %[4]. Это приводит к росту числа корпоративных облаков. Средняя современная организация уже использует около 30 разных корпоративных приложений SaaS.[5]

Еще больше усложняет ситуацию тот факт, что специалисты, занимающиеся приобретением и администрированием приложений SaaS, как правило, не являются руководителями в ИТ-сфере. Согласно прогнозу на 2017 г., специалисты по закупкам потратят больше средств на приобретение приложений (150,7 млрд долл. США), чем ИТ-специалисты (64,7 млрд долл. США)[6].

В условиях сохранения тенденции к росту количества активных облачных приложений наиболее целесообразным для организаций выходом является развертывание технологии SD-WAN, которая позволяет внедрять дополнительные приложения SaaS без ущерба для производительности сети и конечных пользователей. В частности, благодаря возможности прямого доступа к Интернету при помощи удаленных сетей технология SD-WAN не требует обратной передачи трафика облачных приложений в центры обработки данных. Это способствует существенному снижению задержки и потери пакетов.

[4] «Worldwide Public Cloud Services Revenue Growth Remains Strong in the First Half of 2017», IDC, 6 ноября 2017 г.
[5] Нирав Шах (Nirav Shah) и Билл МакДжи (Bill McGee), «Empowering Distributed Enterprises with Secured SD- WAN», Fortinet, по состоянию на 16 декабря 2017 г.
[6] «Technology Purchases from Line of Business Budgets Forecast to Grow Faster Than Purchases Funded by the IT Organization» IDC, 23 марта 2017 г.

Технология SD-WAN обладает очевидными преимуществами для организаций самой разной направленности, однако ее потенциал является наивысшим в следующих сферах.

- **Здравоохранение.** Как правило, в состав учреждений здравоохранения входит большое количество удаленных расположений, на территории которых находятся пользователи, нуждающиеся в доступе к службам SaaS. Эти службы используются для ведения электронных медицинских карт (EMR) и расчетно-финансовых операций, оказания медицинских услуг и реализации других функций. Для работы этих служб необходимо выделение значительной пропускной способности, поэтому традиционные сети WAN не способны адаптироваться к растущим требованиям облачных служб, применяющихся в расширенных инфраструктурах здравоохранения. Надежное решение SD-WAN поддерживает гибкое и доступное выделение пропускной способности в соответствии с потребностями медицинских работников в доступе к облачным приложениям. Это способствует улучшению состояния пациентов и сохранению конфиденциальности частной медицинской информации.
- **Розничная торговля.** Современные торговые сети реализуют товар как через оффлайновые торговые точки, так и через Интернет, поэтому они активно используют комплексные наборы облачных инструментов электронной коммерции, предназначенные для согласования всех аспектов коммерческой деятельности — от инвентаризации товаров до обработки платежей и анализа данных клиентов. В ассортименте удаленных торговых точек могут быть представлены сотни и даже тысячи товаров, поэтому предприятия розничной торговли широко применяют сети SD-WAN в целях повышения производительности сетевых приложений, обрабатывающих огромные массивы данных, которые поступают от распределенных точек, в том числе в период пика продаж.
- **Промышленное производство.** Как и организации розничной торговли, современные производственные предприятия используют большое количество согласованно работающих приложений SaaS в целях повышения эффективности управления различными операциями на разных производственных площадках и даже в разных странах. Некоторые из этих операций являются жизненно важными и выполняются в суровых условиях. Это означает, что ограничение производительности сетевых приложений недопустимо и чревато серьезными последствиями. Надежное решение SD-WAN поддерживает гибкое и экономичное выделение пропускной способности для реализации таких функций, как автоматизированное управление поставками, международная торговля и регулирование производственных процессов, направленное на обеспечение безопасности сотрудников и достижение оптимального уровня производительности.

2. УЧЕТ ОСОБЕННОСТЕЙ ПРИЛОЖЕНИЙ

Статичность традиционной инфраструктуры WAN накладывает существенные ограничения на производительность приложений в рамках распределенной среды. Решение SD-WAN должно поддерживать актуальную в настоящее время функцию **комплексного отслеживания приложений**, благодаря которой администраторы получают возможность выполнять мониторинг и управление шаблонами трафика, заниматься балансировкой пропускной способности и масштабировать производительность всех элементов распределенной сети. В этом случае сеть SD-WAN получает актуальные сведения обо всех приложениях и оптимизирует их работу за счет интеллектуальной маршрутизации и определения приоритетов на основании потребности в пропускной способности сети и количества пользователей, работающих с приложением. В число сведений о каждом приложении входят данные о его состоянии и потребности в ресурсах.

3. ИНТЕЛЛЕКТУАЛЬНАЯ МАРШРУТИЗАЦИЯ

Сущность интеллектуальной маршрутизации заключается в **автоматическом определении приоритетов в ходе маршрутизации приложений** с выделением пропускной способности сети в зависимости от приложения и пользователя. Интеллектуальная маршрутизация поддерживает динамический выбор оптимального подключения WAN с учетом обстоятельств и условий конкретного соглашения об уровне обслуживания. Благодаря этому организации могут назначать приоритет для приложений в зависимости от их важности, времени суток и других факторов.

В отличие от традиционных служб WAN на основе MPLS, для которых свойственны дорогостоящие подключения ограниченной производительности, технология SD-WAN предоставляет упрощенную замену традиционным маршрутизаторам WAN и работает с разными каналами передачи данных WAN (MPLS, Интернет, LTE и т. д.). Решения SD-WAN поддерживают интеллектуальное распределение трафика между несколькими широкополосными подключениями в целях повышения эффективности сети и ее адаптации к условиям распределенной компании. Интеллектуальная маршрутизация позволяет в полной мере использовать преимущества подключений SD-WAN.

4. ИНТЕГРИРОВАННЫЕ ФУНКЦИИ БЕЗОПАСНОСТИ И ОБЕСПЕЧЕНИЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

В связи с отказом от централизованного подхода к защите, предусматривающего обратную передачу сетевого трафика в центры обработки данных, переход от подключений MPLS к широкополосным интернет-подключениям прямого доступа требует внедрения дополнительных средств безопасности корпоративной инфраструктуры. Это особенно важно в свете тенденций к увеличению количества и сложности кибератак.

Сети WAN не соответствуют современным требованиям к производительности и безопасности распределенных сетей. По данным компании Gartner, в настоящее время «программно-конфигурируемые сети WAN (SD-WAN) оснащаются функциями защиты сетевого периметра, однако более 90 % поставщиков решений SD-WAN не занимаются разработкой средств защиты на постоянной основе. Это вызывает у клиентов сомнения в надежности встроенных функций безопасности»[7]. В связи с этим клиенты прибегают к внедрению дополнительных технологий защиты, что чревато повышением затрат на развертывание и совокупной стоимости владения, а также создает опасные уязвимости между изолированными сетевыми технологиями и технологиями безопасности. Согласно прогнозам, в ближайшие годы объем корпоративного трафика с шифрованием SSL превысит 50 %[8]. Эта тенденция требует внедрения функций тщательной проверки зашифрованного трафика на наличие скрытого вредоносного ПО без ущерба для производительности сети.

[7] Gartner, Four Architectures to Secure SD-WAN, Бьерн Мюнх (Bjarne Munch), Грег Янг (Greg Young), октябрь 2017 г.
[8] Нирав Шах (Nirav Shah) и Билл МакДжи (Bill McGee), «Empowering Distributed Enterprises with Secured SD-WAN», Fortinet, по состоянию на 16 декабря 2017 г.

Наличие **межсетевого экрана следующего поколения (NGFW)** — это ключевой фактор безопасности прямого доступа к Интернету при помощи архитектуры SD-WAN. Использование межсетевого экрана следующего поколения значительно сокращает подверженность расширенной сети рискам. Для эффективной защиты сетей SD-WAN особенно важны следующие функции межсетевого экрана.

- **Комплексное решение**, которое сочетает сетевые функции и функции безопасности на базе одного устройства, повышает эффективность защиты распределенной среды, упрощает управление и снижает инвестиционные затраты.
- Функция **проверки SSL**, предназначенная для защиты распределенной сети от вредоносного ПО и других угроз, скрытых в зашифрованном веб-трафике. Функция проверки SSL поддерживает просмотр зашифрованных сеансов и пакетов, выявление угроз и их блокировку.
- Функция **Web Filtering**, которая является первой линией защиты организаций от сетевых атак за счет блокировки доступа к взломанным сайтам и сайтам с вредоносным или неприемлемым содержимым.
- Функция **IPsec VPN с высокой пропускной способностью**, которая относится к числу важнейших составляющих средства защиты развертываний SD-WAN. Благодаря архитектуре безопасности интернет-протокола (IPsec) два или несколько узлов могут безопасно обмениваться данными за счет проверки подлинности и шифрования каждого IP-пакета в рамках сеанса связи по виртуальной частной сети (VPN).
- **Функции проверки на соответствие требованиям и составления отчетов** обеспечивают соблюдение отраслевых стандартов и предписаний, а также снижают риск убытков, связанных с выплатой штрафов и судебных издержек. Межсетевой экран следующего поколения должен быть оснащен функциями составления отчетов, которые отслеживают активность угроз в режиме реального времени. Эти функции обеспечивают оценку рисков, выявление потенциальных проблем и их устранение. Кроме того, межсетевой экран должен поддерживать мониторинг правил и политик, а также автоматизированное выполнение проверок на соответствие требованиям.

5. ПОДДЕРЖКА НЕСКОЛЬКИХ ШИРОКОПОЛОСНЫХ ПОДКЛЮЧЕНИЙ

Как уже говорилось в разделе, посвященном интеллектуальной маршрутизации, контроллер SD-WAN должен одновременно обслуживать несколько широкополосных подключений (Интернет, MPLS, LTE и т. д.) в целях обеспечения прямого доступа к интернет-подключениям общего пользования. Технология SD-WAN не ограничена особенностями работы операторов и каналов передачи данных, поэтому созданные по новой технологии подключения больше не зависят от механизмов MPLS и ненадежных функций отработки отказа сети 4G/3G, применение которых чревато остановкой коммерческой деятельности. Технология SD-WAN в качестве резервного ресурса задействует интернет-подключение общего пользования, благодаря чему она отличается **повышенной устойчивостью и избыточностью**, что предотвращает падение производительности и сбои.

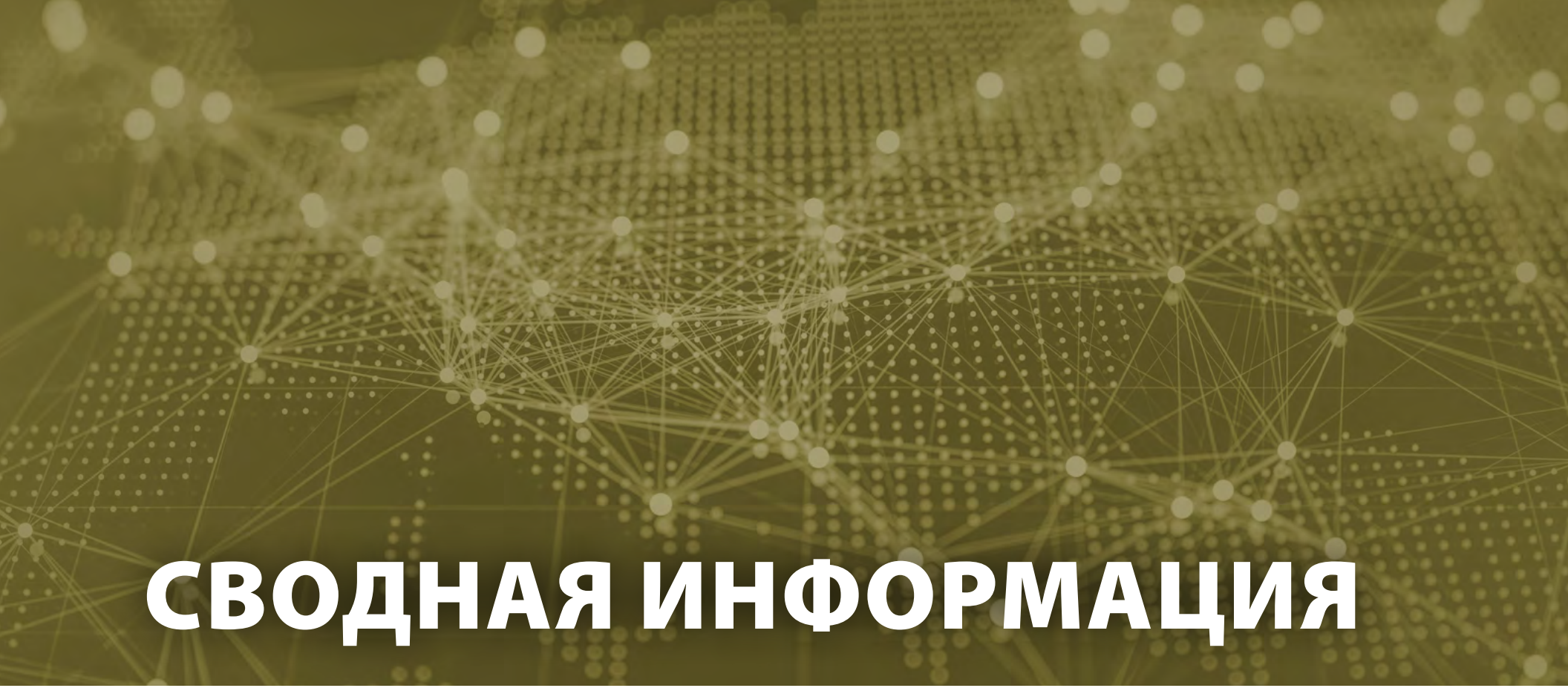
6. СОВОКУПНАЯ СТОИМОСТЬ ВЛАДЕНИЯ

Необходимость замены дорогостоящих подключений MPLS более экономичными вариантами, такими как интернет-подключения общего пользования или стандарт долговременного развития (LTE), обусловлена распространением общедоступных широкополосных подключений. По сравнению с традиционными сетями WAN новые технологии способствуют существенному снижению эксплуатационных затрат.

Кроме того, технология SD-WAN благодаря возможности администрирования функций безопасности и сетевых функций **из одного окна** снижает сложность структуры и упрощает управление. За счет этого специалисты

по безопасности могут сократить временные затраты на управление различными сетевыми компонентами, выполнение операций безопасности и корреляцию событий.

Также ваше решение SD-WAN должно поддерживать **развертывание в автоматическом режиме**. Эта функция повышает эффективность развертывания сетей филиалов. Организации получают возможность реализовать потенциал развития благодаря автоматизации, которая обладает следующими преимуществами: быстрое выделение ресурсов, упрощенная процедура конфигурации, автоматическая проверка подлинности, централизация мониторинга и поддержки. Развертывание в автоматическом режиме экономит значительное количество времени по сравнению с процедурами интеграции сетей филиалов в традиционную среду WAN, требующими привлечения специалистов.



СВОДНАЯ ИНФОРМАЦИЯ

Традиционные сети WAN больше не являются эффективным вариантом для современных распределенных компаний. В качестве решения значительных проблем, связанных с подключениями и обеспечением безопасности, организации выбирают переход на технологию SD-WAN. Компания Gartner сообщает, что «к 2018 г. более 40 % инициатив по модернизации периферийных инфраструктур WAN будут строиться на применении средств vCPE или SD-WAN в противовес традиционным маршрутизаторам»[9].

[9] Gartner, Market Guide for WAN Edge Infrastructure, Эндрю Лернер (Andrew Lerner), Нил Рикард (Neil Rickard), март 2017 г.

В настоящее время на рынке представлено множество разных решений SD-WAN. Задача вице-президентов ИТ-отделов — дать продуманную оценку каждому средству. Для этого можно воспользоваться нашим материалом «Шесть аспектов, которые необходимо рассмотреть». Средство защиты сетей SD-WAN Fortinet соответствует всем описанным в данном документе требованиям и сочетает современные функции SD-WAN с надежными технологиями безопасности. Это решение следующего поколения, оснащенное функциями защиты и сетевыми функциями, которые повышают эффективность работы сети без ущерба для безопасности.

www.fortinet.com

154319-A-0-EN