

МОДЕРНИЗАЦИЯ ИНФРАСТРУКТУРЫ WAN С ПОМОЩЬЮ FORTIGATE SD-WAN

Предприятия вливаются в процесс цифровой трансформации с целью повышения производительности и ускорения темпов развития бизнеса. Ключевым компонентом цифровой трансформации является перемещение инфраструктуры или служб в облако, что позволяет предприятиям незамедлительно приступить к работе. «Предприятиям необходимо модернизировать свою архитектуру WAN для поддержки новых инициатив цифрового бизнеса и адаптации общедоступных облачных служб, доля которых выросла на 86 % в период с 2014 по 2018».¹ При переходе к облаку происходит обратная передача трафика из филиалов в облако, что снижает производительность приложений. Обратная передача облачного трафика может не только увеличивать задержку, но и создавать проблемы безопасности. 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».² Gartner рекомендует «выбирать поставщиков решений SD-WAN, которые могут предложить надежные системы проверки подлинности устройств и контроллеров, средства авторизации и управления доступом».³

Когда администраторы анализируют плюсы и минусы традиционных решений WAN, становится очевидно, что необходимо срочно менять инфраструктуру на более простую и экономичную, которая лучше приспособлена к задачам внедрения облачных технологий. Решение SD-WAN обеспечивает эффективную маршрутизацию сетевого трафика из филиалов в облако, главные офисы или другие подразделения. Оно предоставляет филиалам прямой доступ к облачным приложениям за счет динамического использования широкополосных подключений, тем самым повышая производительность сети и снижая затраты. Решение SD-WAN использует подход, ориентированный на приложения, благодаря чему предприятия могут максимизировать пропускную способность для важных бизнес-приложений и повысить эффективность инвестиций.

FORTIGATE SD-WAN

Средство защиты SD-WAN можно использовать с межсетевым экраном следующего поколения FortiGate. Компания Fortinet признана лидером по результатам исследования Gartner Magic Quadrant, посвященного корпоративным межсетевым экранам.⁴ По данным IDC, решение FortiGate также занимает лидирующую позицию по общему количеству ежегодных поставок систем безопасности по всему миру.⁵ FortiGate объединяет функции межсетевого экрана NGFW и SD-WAN в одном решении, повышающем эффективность и безопасность WAN. Ниже перечислены основные компоненты FortiGate SD-WAN.

■ Учет особенностей приложений

В традиционных сетях WAN предприятиям сложно поддерживать качество и удобство работы пользователей в приложениях. Традиционная инфраструктура WAN использует пакетную маршрутизацию и не учитывает особенности приложений. Система FortiGate SD-WAN помогает клиентам отслеживать приложения, используемые в корпоративной сети, для принятия более взвешенных решений при создании политик SD-WAN. Компания Fortinet имеет обширную базу данных, которая

позволяет идентифицировать более 3000 отдельных приложений. FortiGate SD-WAN может идентифицировать даже облачные приложения с зашифрованным трафиком, начиная с момента передачи первого пакета.

■ Контроллер путей WAN

Учет особенностей приложений предоставляет возможности для интеллектуальной расстановки 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. Решение FortiGate SD-WAN предоставляет подробные сведения о маршрутах WAN (такие как задержки, джиттер и потери пакетов). Используя эти данные, технология многопутевой маршрутизации выполняет автоматическое переключение на другой самый оптимальный доступный канал (при неудовлетворительных показателях основного маршрута). Все механизмы автоматизации являются встроенными и пользователю не нужно вносить никаких изменений. Такой подход снижает сложность и повышает производительность приложений. Компания Gartner рекомендует клиентам «опробовать решения SD-WAN на филиалах для уменьшения сложности парка устройств, транспортной нагрузки на сеть WAN и стоимости оборудования».⁶

■ Безопасность межсетевого экрана NGFW и соответствие требованиям

Уникальное преимущество компании Fortinet заключается в том, что она предлагает систему безопасности SD-WAN, которая обеспечивает высокоуровневую защиту корпоративной сети с помощью одного комплексного решения. Кроме того, компания Fortinet является единственным поставщиком решения SD-WAN, чей межсетевой экран следующего поколения (NGFW) получил статус «Рекомендовано» от NSS Labs. Система FortiGate SD-WAN предлагает следующие возможности.

- Проверка SSL и защита от угроз для отслеживания и устранения вредоносного ПО.
- Служба Web filtering обеспечивает безопасность в Интернете и снижает сложность за счет устранения необходимости в отдельном устройстве SWG.
- Туннели IPsec VPN с высокой пропускной способностью и масштабируемостью обеспечивают непрерывное шифрование трафика и гарантируют его конфиденциальность.
- Отслеживание активности угроз в режиме реального времени для оценки рисков, выявления потенциальных проблем и их устранения. Мониторинг правил и политик межсетевого экрана и автоматизированное выполнение проверок на соответствие требованиям.
- **Управление из одного окна и развертывание в автоматическом режиме**
Когда предприятия внедряют решение SD-WAN, очень важно иметь возможность беспрепятственно реализовать новую технологию и иметь правильные инструменты для управления этой технологией. Администрирование FortiGate SD-WAN осуществляется с помощью единой удобной и универсальной консоли управления, которая называется

FortiManager. Она оснащена функциями для удаленного управления и оркестрации как облачными системами, так и размещенными на хосте. Это мощное решение поддерживает управление тысячами распределенных расположений. Устройства FortiGate полностью готовы к эксплуатации. В FortiManager можно указать сведения об устройствах и настроить централизованные политики и устройства FortiGate будут автоматически обновляться до последней конфигурации политики.

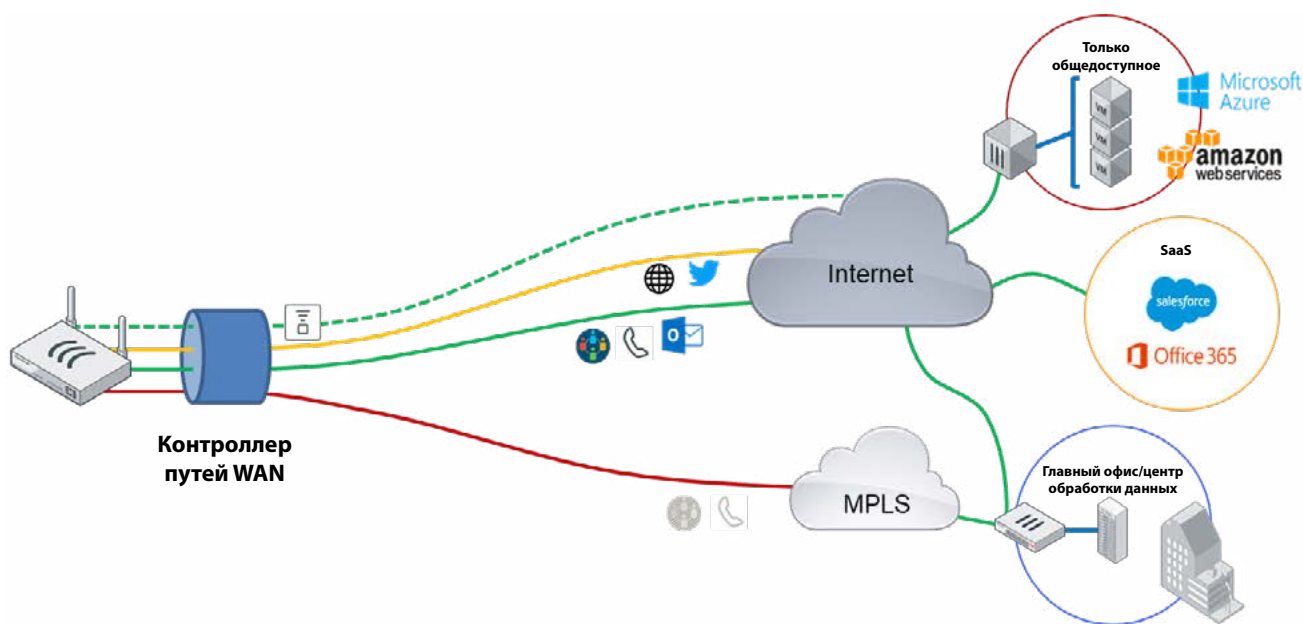
■ Совокупная стоимость владения

Необходимость замены дорогостоящих подключений MPLS более экономичными вариантами обусловлена распространением общедоступных широкополосных подключений. С решением Fortinet, которое не зависит от каналов передачи данных, предприятия могут использовать всю доступную пропускную способность, используя два из этих подключений в режиме «активный-активный». FortiGate SD-WAN объединяет лучшие функции безопасности и возможности SD-WAN в одном решении.

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. В настоящее время на рынке представлено множество разных решений SD-WAN. Задача вице-президентов ИТ-отделов — дать продуманную оценку каждому средству. Gartner рекомендует клиентам «не принимать стратегических решений на основе данных в изолированной, разрастающейся сети WAN, отделенной от сетевой группы».⁷

Решение FortiGate SD-WAN сочетает в себе 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.



Справочные материалы:

^{1,6,7} Gartner, «Market Guide for WAN Edge Infrastructure», Эндрю Лернер (Andrew Lerner), Нил Рикард (Neil Rickard), март 2017 г.

^{2,3} Gartner, «Four Architectures to Secure SD-WAN», октябрь 2017 г.

⁴ Исследование Gartner Magic Quadrant, посвященное корпоративным межсетевым экранам, Адам Хилс (Adam Hils), Джереми Д'Хойн (Jeremy D'Hoinne) и Раджприт Каур (Rajpreet Kaur), июль 2017 г.

Заявление об ограничении ответственности компании Gartner

Компания Gartner не занимается продвижением каких-либо поставщиков, продуктов и услуг, упомянутых в исследовании, и не дает пользователям технологий рекомендации по выбору только поставщиков, получивших наивысшую оценку или отнесенных к иной категории. В исследованиях Gartner приведены мнения специалистов исследовательской организации Gartner, которые не должны рассматриваться как констатация факта. Компания Gartner отказывается от обязательств по всем гарантиям в части настоящего исследования, как явным, так и подразумеваемым, в том числе гарантиям коммерческого качества и пригодности для целевого использования.

⁵ IDC Worldwide Security Appliances Tracker, апрель 2017 г. (на основе ежегодных поставок товара).



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

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

ОТДЕЛ ПРОДАЖ В АТР
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

Fortinet
Смоленская площадь 3,
Регус, офис 610,
121099 Москва
Тел.: +7 (499) 955-24-99