ciena
Experience. Outcomes.

ОПИСАНИЕ ТЕХНОЛОГИИ

Защита облака

Упрощение системы безопасности между ЦОД с помощью шифрования на уровне 1

Для защиты интеллектуальной собственности и конфиденциальных документов, а также во избежание крупных штрафов и потери дохода из-за утечки данных крайне важно обеспечить безопасность информации конфиденциального характера и особо важных сведений. Порой бывает сложно выбрать, какие данные защищать и каким образом это делать. Физическая структура центра обработки данных включает в себя различные уровни материальных средств защиты для ограничения несанкционированного доступа. Кроме того, в самом ЦОД для обеспечения безопасности могут использоваться брандмауэры, антивирусное ПО и системы обнаружения вторжений. Однако зачастую стоит только данным покинуть безопасную среду ЦОД, об их защите забывают.

Волоконно-оптические сети, связывающие центры обработки данных, часто считаются защищенными от атак, но игнорирование коммуникаций между ЦОД приводит к появлению уязвимостей, когда конфиденциальные данные передаются из одного ЦОД на устройство или приложение в другом ЦОД. Данные могут проходить через неконтролируемые организацией каналы и подвергаться рискам и угрозам.

Необходимо защитить приложения и данные компаний не только внутри ЦОД, но и во время передачи между центрами. Разработка, реализация и масштабирование системы безопасности внутри ЦОД могут оказаться сложной задачей. Шифрование на уровне приложения поможет защитить соединение между ЦОД. Шифрование на пакетном уровне также может помочь, но у каждого типа есть свои сложности. Еще одним, более привлекательным вариантом является шифрование сетевых данных на низшем сетевом уровне — оптическом. Массовое шифрование на оптическом уровне обеспечивает масштабируемость архитектуры, упрощает проектирование и эксплуатацию, защищая все данные при передаче между ЦОД или в облаке.

Важность защиты сетей между ЦОД

В ходе недавнего исследования выяснилось, что в ближайшие два года примерно одна из четырех организаций может столкнуться с масштабной утечкой данных [1]. Затраты, связанные с утечками, могут исчисляться миллионами долларов, поскольку необходимо выявить и уведомить всех потерпевших, а также оплатить все соответствующие судебные издержки и

Шифрование на уровне 1 включает:

- полную пропускную способность без заторов;
- шифрование на скорости передачи со сверхнизкими задержками для надежной защиты коммуникаций между ЦОД;
- решения, которые легко развертываются и эксплуатируются без дополнительных устройств для шифрования;
- гибкое шифрование без привязки к протоколу для различных услуг.

1 Ponemon Institute, 2017 Cost of Data Breach Study (Анализ стоимости утечек данных в 2017 г.), отчет по исследованию Ponemon Institute (июнь 2017 г.), 1–2.

сборы за осуществление распорядительных функций. Кроме того, утечка данных может повлечь за собой потерю дохода и отток клиентов, а также испортить репутацию компании.

Требования по выявлению брешей в системе безопасности и уведомлений о них постоянно ужесточаются на законодательном уровне. В зависимости от типа передаваемых данных или документов может понадобиться их шифрование в соответствии с правовыми нормами. При возникновении угроз раскрытия конфиденциальных данных компании могут столкнуться с серьезными штрафами, что повлияет на общую рентабельность.

Новое понимание безопасности

С точки зрения безопасности в организациях должен действовать подход, который предполагает, что утечки могут и будут происходить. Нецелесообразно думать, что средства защиты предотвратят атаки злоумышленников на сеть. Вместо этого компаниям следует исходить из того, что нарушители уже в сети или скоро проникнут в нее. Такой тип мышления позволит создать средства для постоянной защиты данных вместо того, чтобы пытаться разработать неуязвимую систему или беспокоиться о защите информации, когда целостность системы уже нарушена. Например, организации могут зашифровать данные, передаваемые по сети, чтобы злоумышленники не смогли их прочитать даже в случае перехвата.

Успешная атака требует соблюдения ряда условий. Система должна быть уязвима, например по причине ненадежного ПО, для которого не были применены исправления системы безопасности. Она должна иметь какую-либо ценность для злоумышленника и быть доступна. В таком случае утечка возможна — если у нарушителя есть соответствующие инструменты и навыки.

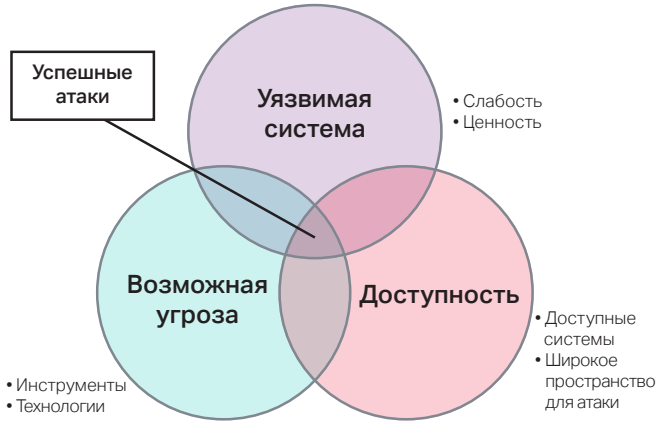

Рис. 1. Компоненты успешной атаки

Разработка стратегии защиты в компаниях должна выполняться в три этапа: выявление активов, определение границ доступа и осознание угроз. Компании должны знать, какие активы содержат важные данные и конфиденциальные документы, а также как осуществляется их защита и доступ к ним. Информация в базе данных может храниться в безопасности благодаря защите самой базы данных, но при экспорте и передаче по сети данные могут подвергаться угрозам. Например, если специалист отдела кадров экспортирует данные в Excel для составления отчета, резервные копии электронной таблицы, которые перемещаются из одного ЦОД в другой без применения шифрования, теряют защиту.

Сетевое шифрование для комплексной стратегии безопасности

Являясь частью комплексной стратегии безопасности, защита всех данных между ЦОД, включая облако, становится невероятно важной. Ни одна область сети не должна восприниматься как полностью защищенная от атак. Кроме того, нецелесообразно пренебрегать передаваемыми данными. Для обеспечения конфиденциальности данных компании должны применять комплексный подход к защите ИТ, который включает в себя эффективное масштабируемое средство для защиты данных, проходящих через облако.

Как правило, ИТ-компании понимают под безопасностью средства защиты на предприятии, к которым относятся такие элементы, как физическая охрана на точках входа в ЦОД и ограниченный доступ к серверам и оборудованию. Брандмауэры, системы предотвращения вторжений, полное шифрование дисков, повышение надежности приложений и баз данных, элементы управления доступом на основе ролей и другие защитные средства обеспечивают безопасность и шифрование для хранилищ критически важных данных. Но когда данные пересекают эти границы защиты или передаются между ЦОД, они теряют защиту. Еще больше усложняет проблему то, что при передаче данных по сторонним сетям или сетям различных поставщиков услуг компания не имеет полного контроля над ними для обеспечения безопасности.

Шифрование можно применять для защиты данных при их передаче между ЦОД, но тогда придется рассмотреть множество решений. У каждого из них есть свои преимущества и недостатки. При этом идеальное решение должно быть легким в развертывании и управлении, высокомасштабируемым и эффективным.

Защита на уровне приложений или сетевой инфраструктуры?

При внедрении решения шифрования ИТ-компании либо пытаются защитить уровень приложений, либо используют средства шифрования, встроенные в сетевую инфраструктуру. Защита на уровне приложений требует обеспечения безопасности как для хост-устройства, так и для приложения, поэтому большинство инфраструктур защиты на уровне приложений располагаются в ЦОД. Кроме того, такие решения, как протокол TLS для защиты каналов связи между приложениями (например, веб-браузерами или почтовыми клиентами) и серверами, обычно не

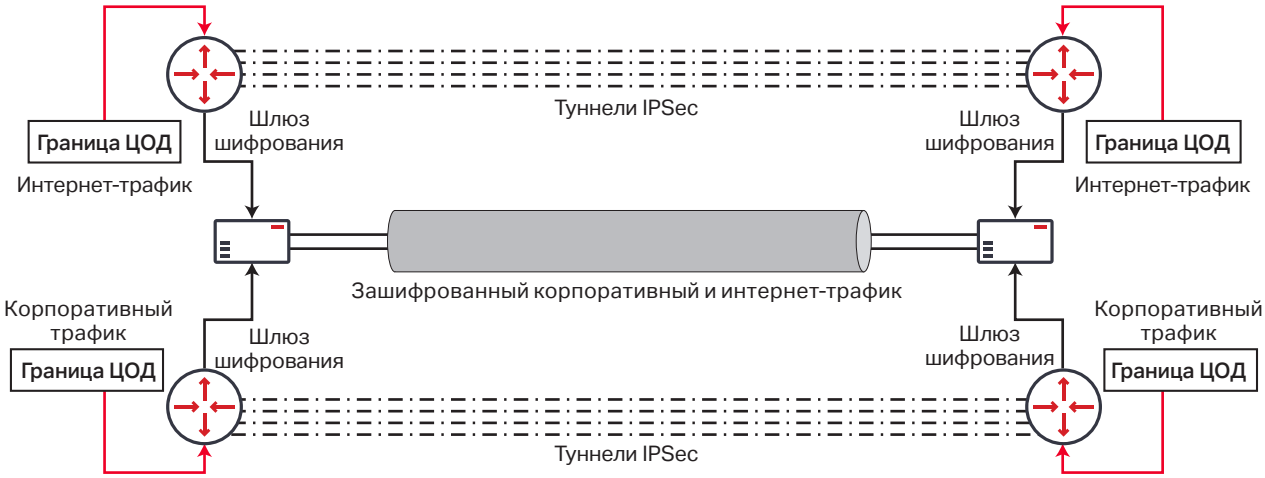

Рис. 2. Защита всего трафика на пакетном уровне с наложением (логическое представление)

предназначены для обеспечения безопасности на уровне «приложение — приложение» при передаче данных через облако или между ЦОД. Создание общей инфраструктуры безопасности на уровне «приложение — приложение» для множества центров обработки данных может быть сложным, поэтому организации часто выбирают сетевую инфраструктуру.

При использовании сетевой инфраструктуры возникают свои трудности, и защита сети на уровне инфраструктуры может чрезвычайно усложнить сетевую архитектуру. Объем трафика между ЦОД весьма велик, из-за чего система защиты всего трафика между различными соединениями 100G+ может оказаться громоздкой в эксплуатационном плане и сложной в разработке и масштабировании.

Можно использовать наложение зашифрованных шлюзов VPN для защиты трафика на пакетном уровне (рис. 2). В таком случае потребуется специализированное дорогостоящее оборудование для шлюзов шифрования на всех каналах, требующих защиты. Эта модель ограничивает трафик до одной пары IP-адресов источника и точки назначения, причем внешняя информация о заголовках IPsec недоступна промежуточным маршрутизаторам для многоскачковых трасс. Метод наложения не предусматривает возможности использования различных типов трафика, а также нарушает трассы со множеством маршрутов с равными метриками (ECMP) и группами агрегации каналов (LAG). Кроме того, он плохо поддается масштабированию и увеличивает задержки. Поскольку требования к пропускной способности ужесточаются, а потоки данных становятся более ячеистыми, для зашифрованных шлюзов необходимо использовать высокоскоростные порты, что существенно повышает стоимость.

К основным недостаткам наложения зашифрованных шлюзов VPN для защиты облака относят:

- сложность сетевой архитектуры, разработки и технического обеспечения;
- необходимость специальных навыков для работы с трафиком внутри ЦОД и управления им;
- неэффективность масштабирования;
- появление дополнительной задержки между ЦОД;
- снижение общей пропускной способности пакетной передачи из-за шифрования пакетного уровня;
- сложные процессы мониторинга, устранения неполадок и управления;
- высокую стоимость оборудования для зашифрованных шлюзов.

Как было отмечено ранее, из-за увеличения потоков трафика для шлюзов шифрования требуются порты с более высокой скоростью. Архитектура на основе пакета плохо масштабируется, а устройства шифрования становятся громоздкими, дорогостоящими и с трудом обеспечивают полную пропускную способность в зашифрованных каналах между ЦОД. Чтобы устранить эту проблему и сократить затраты на специализированное оборудование для зашифрованных шлюзов при более высоких нагрузках трафика, можно попробовать выполнить профилирование трафика. После этого его при необходимости разделяют между зашифрованными и незашифрованными трассами посредством зашифрованных или незашифрованных шлюзов (рис. 3). Таким образом можно попытаться облегчить масштабирование на зашифрованном шлюзе, передавая трафик, который необходимо зашифровать, на зашифрованный шлюз, и выгружая остальной трафик на незашифрованные шлюзы.

Рис. 3. Профилирование трафика для снижения стоимости шлюза шифрования (логическое представление)

Однако профилирование трафика также имеет свои сложности. Бывает непросто точно определить, какой трафик необходимо зашифровать. Немногие организации знают свои данные достаточно хорошо, чтобы точно разделить их, а неверное определение трафика может поставить конфиденциальные данные под угрозу. Назначение и параметры приложений часто обновляются, и если профиль трафика не соответствует этим изменениям, это может привести к передаче конфиденциальных данных по незащищенным маршрутам.

К основным недостаткам профилирования трафика с помощью зашифрованных и незашифрованных шлюзов относят:

- сложность сетевой архитектуры, разработки и технического обеспечения;
- необходимость специальных навыков для работы с трафиком внутри ЦОД и управления им;
- высокую вероятность появления ошибок при профилировании трафика (зашифрованного и незашифрованного);
- необходимость соблюдать единообразие профилей приложений и трафика, а также выполнять синхронизацию, поскольку области применения приложений со временем меняются;
- сложность разработки и развертывания обычных/незашифрованных и зашифрованных экземпляров маршрутизации на сетевом оборудовании;
- появление дополнительной задержки между ЦОД;
- снижение общей пропускной способности пакетной передачи из-за шифрования пакетного уровня;
- высокую стоимость оборудования для зашифрованных шлюзов.

Масштабировать профилирование трафика такого рода до глобального уровня чрезвычайно сложно, со временем его обслуживание усложняется. Профили трафика для новых и существующих приложений и источников данных необходимо постоянно обновлять для обеспечения надлежащей защиты трафика. Успешное профилирование трафика требует тесного непрерывного взаимодействия между разработчиками приложений, специалистами по безопасности, а также системными и сетевыми администраторами.

Оба метода шифрования на пакетном уровне имеют свои недостатки в виде сложного масштабирования и развертывания. К счастью, существует другой способ снижения сложности и оптимизации масштабирования — шифрование передаваемого трафика на оптическом уровне.

Шифрование на оптическом уровне: простой и надежный подход

Вместо расходования ресурсов на профилирование и разделение трафика для защиты только конфиденциальных данных организации все чаще обращаются к решениям для шифрования на оптическом уровне, которые легко развертываются и при этом защищают все данные. Именно это обеспечивает шифрование на уровне 1 (оптическом уровне). В данном случае выполняется шифрование всей полезной нагрузки OTN с защитой всех сообщений, заголовков и данных, начиная с верхнего уровня коммуникаций (рис. 4).

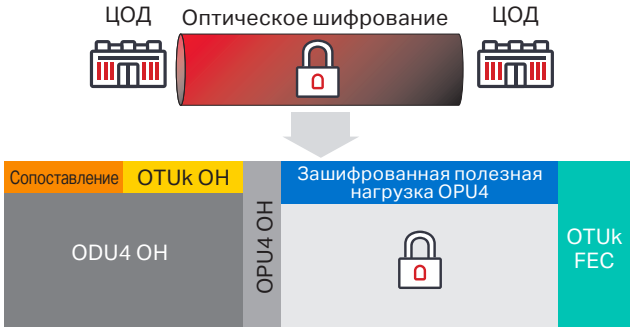

Рис. 4. Защита ВСЕГО трафика с помощью шифрования на уровне 1

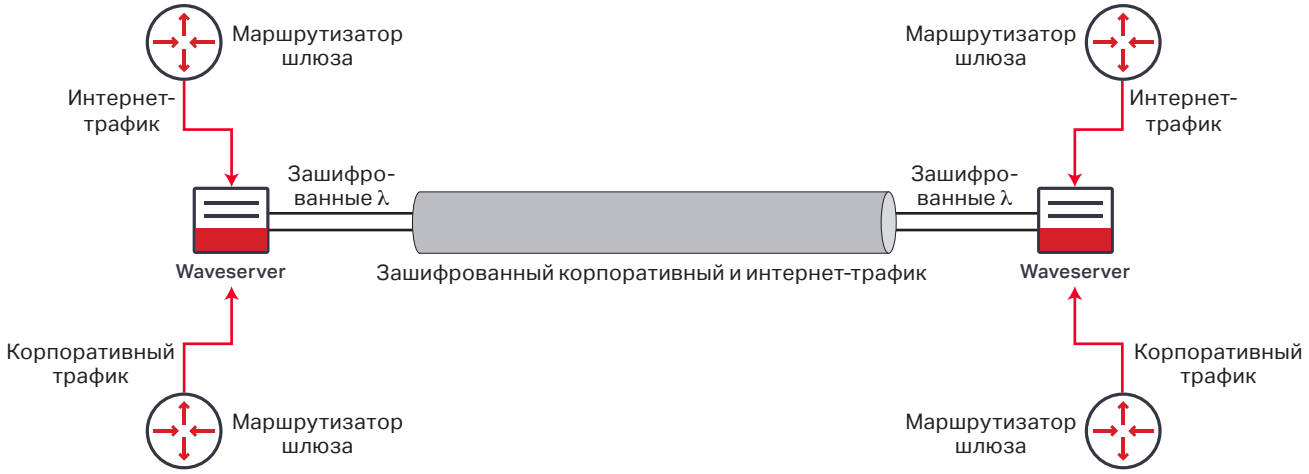

Рис. 5. Защита всего трафика на оптическом уровне (логическое представление)

Шифрование на оптическом уровне упрощает сетевую архитектуру (рис. 5). Маршрутизаторы шлюзов передают трафик непосредственно транспортному устройству (в данном случае Waveserver®) для массового шифрования. Дорогостоящие шлюзы шифрования не нужны. Кроме того, не требуется профилировать трафик, чтобы определить области для шифрования. *Весь трафик, покидающий ЦОД, шифруется на скорости передачи с полной пропускной способностью.*

Шифрование на уровне 1 имеет следующие преимущества.

- **Не требуются дополнительные VPN для шифрования трафика.** Поскольку при шифровании на уровне 1 шифруется весь трафик, нет необходимости профилировать его для передачи на зашифрованные или незашифрованные сети VPN. Все коммуникации защищены.
- **Минимальная задержка.** При шифровании на уровне 1 задержка составляет несколько нано- или микросекунд, в то время как решения более высокого уровня, такие как IPsec или шифрование на уровне приложений, могут привести к задержке в сотни миллисекунд.
- **Полная пропускная способность.** Шифруется только полезная нагрузка транспортного уровня, поэтому пропускная способность пакетного уровня в маршрутизаторах и коммутаторах не меняется. Решения для шифрования на уровне 1 со скоростью передачи обеспечивают полную пропускную способность при шифровании трафика.
- **Простота проектирования, создания и эксплуатации.** Решения для шифрования на уровне 1 встраиваются в те же оптические транспортные системы, которые обеспечивают передачу DWDM в городской или магистральной сети, дополнительные устройства шифрования не требуются.
- **Многопротокольная поддержка.** Уровень 1 обеспечивает поддержку различных типов трафика, включая Ethernet, IP, SONET/SDH, Fibre Channel и другие, сокращает количество необходимых устройств шифрования и имеет улучшенную поддержку протоколов по сравнению с ограниченными одним протоколом (IP) решениями, такими как IPSec.

Переход к шифрованию на уровне 1 обеспечивает простое решение для защиты облака. Оно позволяет выполнять массовое шифрование для всех данных, передаваемых по защищенному каналу. Другим преимуществом шифрования на уровне 1 является возможность его использования в качестве средства глобального контроля на нижнем уровне. Организации в сфере безопасности при необходимости могут разрабатывать решения для шифрования на верхнем уровне для обеспечения соответствия правовым нормам или в рамках всестороннего плана защиты. Если при этом возникнут угрозы на верхнем уровне, данные будут зашифрованы на оптическом уровне. Компании могут либо разработать комплексный план защиты, либо внедрить шифрование на уровне 1 в качестве средства глобального контроля в зависимости от того, на какой стадии развития находится их глобальная политика безопасности.

Решение Ciena WaveLogic Encryption

Ciena предлагает решение для шифрования на уровне 1 для защиты данных посредством алгоритмов шифрования AES-256 вместо передачи данных по незащищенным каналам. Кроме того, если злоумышленник получит доступ к физической среде и попытается подключиться к волоконной линии, все данные будут зашифрованы и недоступны для использования.

Ciena WaveLogic Encryption — это простое в развертывании решение для оптического шифрования на скорости передачи, встроенное в сетевое оборудование для оптического транспорта. Используемый подход не требует постоянного контроля: шифрование всегда включено, что гарантирует непрерывную защиту передаваемых данных. Благодаря этому исключаются человеческие ошибки, из-за которых конфиденциальные данные могут передаваться по сети в незашифрованном виде.

Ciena предоставляет соответствующий стандартам FIPS механизм шифрования AES-256 с поддержкой новейших алгоритмов криптографии на основе открытых ключей, включая криптографию на основе эллиптических кривых (ECC). Решение WaveLogic Encryption доступно на базе пакетной оптической платформы Ciena 6500 Packet-Optical Platform и семейства наращиваемых систем межсоединений Ciena Waveserver. В нем используются когерентные интерфейсы WDM, которые можно запрограммировать для обеспечения шифрования на скорости передачи при различных линейных скоростях, включая 100G QPSK, 150G 8QAM, 200G 16QAM и 400G с одной несущей.

Благодаря платформе Ciena 6500 операторы могут использовать универсальную плату на основе мукспондера для шифрования на уровне 10G или подключить к клиентской интерфейсной плате линейный модуль 100G/200G с шифрованием для обеспечения соответствия определенным требованиям в отношении трафика. С помощью Waveserver операторы могут развертывать решения для шифрования AES-256 на скорости передачи с производительностью до 400 Гбит/с, используя только одно стойко-место, с возможностью поддержки различных клиентов (10GE, 40GE и 100GE) на одном устройстве. Решение Waveserver Ai, оптимизированное для клиентских интерфейсов 100GE, позволяет операторам развертывать решения с производительностью шифрования до 1,2 Тбит/с на одном стойко-месте.

Возможность программирования на стороне линии, встроенная в когерентный транспорт Ciena, позволяет операторам оптимизировать производительность линии в соответствии с любыми требованиями приложений и защищать передаваемые данные в городской, региональной или магистральной сети. Это обеспечивает надежное соединение между ЦОД, независимо от расстояния или базовой системы фотонных линий.

Платформу 6500 и Waveserver можно развернуть для защиты облака без тех сложностей, которые возникают при использовании решений более высокого уровня на основе приложений или IP-инфраструктур. По мере популяризации услуг передачи конфиденциальных данных по волоконно-оптическим сетям и ужесточения законов и норм по защите данных подход к обеспечению безопасности ИТ в современных облачных коммуникациях должен предусматривать не только защиту серверов и шифрование хранимых данных, но и надежное шифрование данных при передаче.

Шифрование без проблем — Узнать больше.

Заключение

Реализация комплексного плана защиты может оказаться сложной задачей, особенно при использовании коммуникаций уровня «приложение — приложение» между центрами обработки данных. Организации часто выбирают сетевую инфраструктуру для развертывания средств по защите данных, передаваемых между ЦОД. Однако шифрование сети на уровне 3 может оказаться дорогостоящим и плохо масштабируемым. К счастью, простое в развертывании шифрование на оптическом уровне обеспечивает надежную защиту первого уровня. Оно не требует привязки к протоколу и поддерживает различные типы трафика. Решение обеспечивает шифрование на скорости передачи без снижения пропускной способности при больших нагрузках, при этом дополнительные задержки практически не возникают. Шифрование на уровне 1 — это экономичный способ защиты данных, передаваемых между ЦОД. Решение Ciena WaveLogic Encryption сочетает в себе высокую степень гибкости и надежности с простотой эксплуатации и управления. Оно обеспечивает экономичное, высокопроизводительное шифрование на скорости передачи для постоянной защиты коммуникаций между ЦОД как в локальных сетях, так и в сетях дальней передачи.

Посетите сообщество Ciena
Получите ответы на свои вопросы