ОПИСАНИЕ ТЕХНОЛОГИИ

Решения Wavelogic Encryption

Непрерывная защита всех данных при передаче

Безопасность стала важной корпоративной проблемой. Согласно отчету Thales Data Threat Report за 2020 год[1], 49 % компаний по всему миру на каком-то этапе своего развития становились жертвами нарушения безопасности данных. Гораздо больше остальных пострадали предприятия, работающие в сфере здравоохранения, финансирования, образования и государственного управления.

Утечки данных не только подвергают опасности данные ваших клиентов, но и снижают прибыльность вашего бизнеса. Результаты глобального исследования Ponemon[2] показали, что приблизительно 25 500 документов подвергаются опасности при каждой утечке данных. Таким образом, стоимость одной утечки может достигать нескольких миллионов долларов, и это без учета ущерба от потери доверия клиентов. Кроме того, это исследование показало, что средний ущерб от утечки данных в 2019 году в США составил 8,19 млн долларов. Это значение варьируется в зависимости от отрасли: например, в отрасли здравоохранения ущерб от утечки каждого документа вдвое выше среднего показателя.

Но даже в этих условиях объем сетевого трафика растет. Требования к пропускной способности увеличиваются, и потребность в масштабировании сетей для поддержки растущих мощностей и снижения эксплуатационной сложности становится все более насущной. Изощренность и частота нарушений данных растет, и уже ни одна организация не может похвастаться стопроцентной защитой от атак злоумышленников, пытающихся получить доступ к важной конфиденциальной информации. Современным высокоемким сетям недостаточно высокой пропускной способности. Они требуют наличия стратегии безопасности для защиты всех важных данных, как при хранении, так и при передаче в городских сетях, региональных сетях, сетях дальней передачи и подводных сетях по всему миру.

Будучи разработано для современных высокоемких безопасных сетей, решение Ciena WaveLogic Encryption™ обеспечивает экономичное масштабируемое шифрование со сверхнизкой задержкой без привязки к конкретному протоколу на базе распространенного решения 6500 Packet-Optical Platform. Решение поддерживает семейство высокоемких компактных модульных транспортных устройств Ciena Waveserver®, обеспечивающих экономически эффективные и безопасные приложения для соединений ЦОД (DCI). Непрерывное шифрование предлагает удобство эксплуатации и администрирования, позволяя легко реализовать стратегию защиты данных на основе ведущей в отрасли когерентной

Преимущества

- Совместимое с FIPS решение шифрования со сверхнизким уровнем задержки для обеспечения надежных и прозрачных комплексных коммуникаций
- Масштабирование с программируемой когерентной технологией WaveLogic для гибкого шифрования на скорости передачи от 100G до 400G
- Независимое от протокола шифрование, способное обеспечить гибкость для поддержки разнообразных услуг
- Усовершенствованная защита с использованием двух разных наборов ключей для аутентификации и шифрования данных с ротацией ключей шифрования за считанные секунды
- Органичная интеграция в инфраструктуры открытых ключей (PKI) на предприятиях с использованием аутентификации на основе сертификата X.509
- Безопасное управление функционалом «шифрование как услуга» для конечного пользователя при помощи специального встроенного инструмента
- Проверенное на практике решение шифрования, широко используемое по всему миру в сетях финансовых, юридических, медицинских, военных, коммунальных и правительственных организаций

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Ponemon, IBM study: Cost of a Data Breach 2020: https://www.ibm.com/security/data-breach

технологии WaveLogic для обеспечения не имеющей аналогов гибкости и производительности первого в отрасли когерентного решения 100G/400G с шифрованием на скорости передачи.

Технология шифрования

Шифрование — это процесс преобразования информации с использованием алгоритма, в результате которого воспользоваться этой информацией можно только при наличии специального криптографического ключа. По сути этот процесс блокирует сеть, шифруя данные. Они становятся непригодными для использования злоумышленником, получившим к ним доступ, поскольку расшифровать их можно только при наличии правильного ключа.

Есть много способов шифрования данных на основе различных стандартов, определяющих требования к шифрованию вспомогательных продуктов и ключей, и реализации процесса сертификации в среде сетевого оборудования. Существует целый ряд стандартных алгоритмов шифрования, включая передовой стандарт шифрования (AES) с ключами различного масштаба (на 56, 128 и 256 бит), разработанный Национальным институтом стандартов и технологий (NIST). Эти стандарты представлены в публикациях федерального стандарта обработки информации (США). Например, алгоритм шифрования AES-256 был опубликован как FIPS 197. NIST не ограничивается публикациями алгоритмов (FIPS 197 и др.). NIST также публикует стандарты, координирующие требования к криптографическим модулям, включая как аппаратные, так и программные компоненты (в FIPS 140-2).

Для сертификации решений по шифрованию используются другие аналогичные платформы. Еще одним важным международным стандартом для сертификации компьютерной безопасности являются Общие критерии оценки защищенности информационных технологий (CC) (ISO/IEC 15408). Общие критерии предоставляют средства, обеспечивающие выполнение процесса спецификации, реализации и оценки сетевого устройства, например элемента оптической сети, надлежащим образом в соответствии со стандартом. В Германии BSI, федеральное ведомство по вопросам информационной безопасности, проводит сертификацию систем безопасности, в том числе по общим критериям. Сертификаты BSI по общим критериям используются в качестве основы для местной сертификации, что позволяет сэкономить время и деньги. Этот набор стандартов и процессов сертификации гарантирует поставщикам услуг и конечным пользователям, что данное решение шифрования соответствует установленным требованиям, и это подтверждается успешным прохождением строгого лабораторного тестирования и результатами рассмотрения на основе стандартов.

Обеспечение безопасности современных сетей

Шифрование широко используется сегодня для защиты данных как при хранении, так и при передаче. По данным доклада Ponemon, посвященного новейшим подходам

Рис. 1. Шифрование передаваемых данных является частью целостной стратегии обеспечения безопасности

к шифрованию, лишь 13 процентов респондентов по всему миру не имеют какой-либо стратегии шифрования.[3] Организации любого масштаба, независимо от отрасли, идут на многое, стремясь обеспечить защиту информации в своих ЦОД от несанкционированного доступа. Негативное влияние утечек данных и связанный с ними ущерб нельзя игнорировать. Их последствия для организации могут оказаться очень серьезными: от ухудшения репутации до судебного преследования, наложения крупных штрафов и оттока большей части клиентов.

Для защиты данных, хранящихся на защищенных серверах, базах данных, маршрутизаторах и коммутаторах, наиболее часто сегодня используется управление доступом пользователей на основе учетных данных. В современных сетях Webscale, однако, большие объемы важнейших данных значительную часть времени находятся в процессе передачи, поскольку ресурсоемкие коммуникации реализуются за пределами ЦОД, в среде крупных сетей. Поэтому универсальный подход к обеспечению безопасности ИТ должен предусматривать шифрование передаваемых данных в рамках целостной стратегии обеспечения безопасности (см. рис. 1). Шифруя данные, покидающие защищенные частные облака, операторы предотвращают их несанкционированный перехват при передаче в сети с различными уровнями безопасности.

Многие организации уже реализовали шифрование передаваемых данных в рамках своей стратегии обеспечения безопасности. Особое внимание, как правило, уделялось шифрованию передаваемых данных на уровне 2 и выше. Это неплохой вариант для низкоскоростных ИТ-приложений, не предъявляющих высокие требования к длительности операций и объемам данных. В масштабе всего предприятия, однако, он используется редко. При этом он, как правило, используется только для шифрования данных IP-приложений. Эта модель развертывания решения шифрования весьма громоздка и требует значительных затрат (см. рис. 2). В большинстве случаев она требует наличия автономных устройств шифрования на базе протоколов, существенно увеличивая при этом длительность задержек, снижая пропускную способность приложений и эффективность использования ресурсов полосы пропускания. Кроме того, управление ключами шифрования и аутентификация являются трудоемкими

3 Ponemon, Thales e-Security research report: 2018 Global Encryption Trends Study; апрель 2018 г.; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

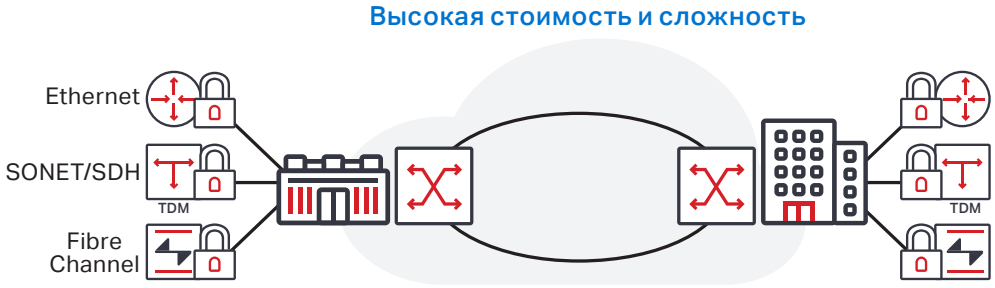

Рис. 2. Традиционное протокольное шифрование в мультисервисной сети

задачами, а диагностировать сеть становится еще труднее ввиду наличия множества независимых устройств. Этот подход недостаточно эффективен в отношении реализации стратегии защиты передаваемых данных. Риск несанкционированного подключения к кабельной системе для доступа к данным обычно не учитывается в корпоративной стратегии обеспечения безопасности, но он, тем не менее, вполне реален. Волоконно-оптические кабели, как правило, легкодоступны, поскольку какая-либо охрана для них не предусмотрена. Любой злоумышленник, обладающий нужными инструментами, может к ним подключиться и незаметно собирать нужные данные — несколько дней, месяцев и даже лет. Развертывание решения шифрования транспортного уровня безостановочно защищает все передаваемые данные, обеспечивая безопасность каждого бита данных.

Безопасность данных с оптическим шифрованием
Загрузить инфографику

WaveLogic Encryption

Ciena WaveLogic Encryption входит в состав многоуровневого решения Ciena для обеспечения конфиденциальности, целостности и доступности данных в сети. Ciena WaveLogic Encryption — это проверенная на практике технология шифрования, развернутая на множестве платформ в глобальном масштабе, и надежность передового решения 6500 Packet-Optical Platform, которое успешно используется более чем 600 операторов в разных странах мира. Кроме того, функционал Ciena WaveLogic Encryption предусматривает поддержку стекируемых систем взаимосвязи Ciena Waveserver и Waveserver Ai, обеспечивая шифрование на скорости передачи до 1,2 Тбит в корпусе 1RU в рамках простых приложений DCI в стеках и стойках.

Простота развертывания

Решение WaveLogic Encryption упрощает развертывание шифрования, интегрируя его функционал непосредственно в сетевой элемент транспортной сети. Такой подход упрощает структуру сети и устраняет необходимость в управлении отдельными решениями шифрования для различных приложений (см. рис. 3). Упрощает он и управление решением шифрования, используя специальный инструмент для аутентификации и управления ключами с удобной интеграцией в текущие корпоративные инфраструктуры закрытых ключей (PKI).

Платформа 6500 характеризуется высочайшей гибкостью, поэтому клиенты могут выбрать оптимальный размер полки в соответствии со своими требованиями к емкости, площади и питанию, обеспечивая экономичную передачу зашифрованных услуг. Другим важным преимуществом решения является его независимость от протоколов и поддержка широкого спектра гибких клиентов для работы с разнообразными приложениями в организациях, уделяющих особое внимание вопросам безопасности (включая Ethernet, SONET/SDH, Fibre Channel и OTN).

Новый подход с непрерывным шифрованием

Шифрование в среде решений Ciena WaveLogic Encryption ведется непрерывно, весь трафик шифруется постоянно, обеспечивая высочайший уровень защиты данных. Может показаться, что возможность включения/отключения

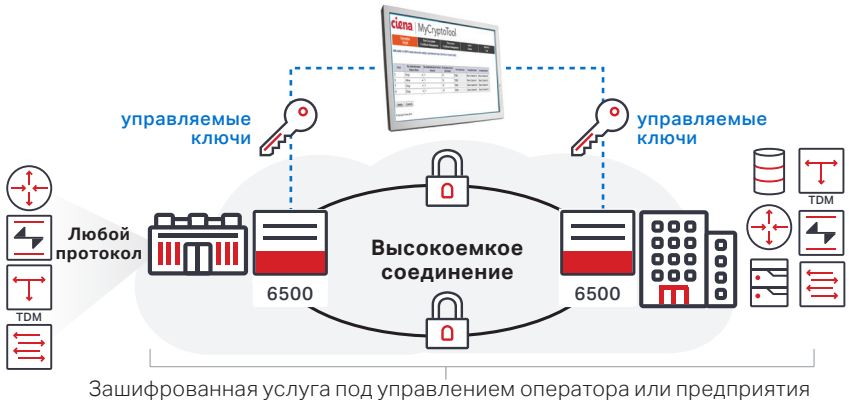

Рис. 3. Решение Ciena 6500 WaveLogic Encryption

шифрования повысила бы гибкость решения, но на практике это может привести к случайной передаче важного трафика по сети в незашифрованном виде. Операторы могут использовать дифференцированную инфраструктуру, которая постоянно защищает все передаваемые данные в городских сетях, региональных сетях, подводных сетях и сетях дальней передачи по всему миру. Кроме того, операторы могут увеличить доход и сохранить свою клиентскую базу, предлагая дифференцированные соглашения об уровне обслуживания для зашифрованных услуг со сверхнизкими задержками и рядом вариантов защиты маршрутов и оборудования.

Шифрование высочайшего уровня

Решение Ciena WaveLogic Encryption проходит внешнюю проверку и независимую сертификацию силами третьей стороны, что гарантирует его реализацию с использованием стандартных отраслевых алгоритмов и передовых функций обеспечения защиты, включая сертификацию по общим критериям и FIPS. Оно работает на базе сертифицированного FIPS ядра шифрования AES-256 со стандартными механизмами аутентификации (например, сертификаты X.509), обеспечивая эффективную интеграцию в текущую инфраструктуру закрытых ключей (PKI) предприятия. Кроме того, аппаратные и программные компоненты криптографических модулей 6500 отвечают требованиям FIPS 140-2 и сертификации BSI в соответствии с Общими критериями оценки защищенности информационных технологий, гарантируя поставщикам услуг и конечным пользователям, что данное решение шифрования соответствует всем аспектам настоящей комплексной оценки, включая алгоритмы шифрования, ключевые механизмы обмена и аутентификацию пользователей.

Для повышения эффективности защиты при аутентификации и шифровании данных используются два разных независимых набора ключей, интервал ротации ключей шифрования при этом составляет несколько секунд. Сеансовые ключи шифрования данных AES-256 согласовываются и сменяются каждую секунду, независимо на каждом линейном порту, не оказывая какого-либо влияния на трафик и пропускную способность. Вмешательство пользователя при этом не требуется. Операторы могут развернуть новое поколение алгоритмов криптографии на основе открытых ключей с поддержкой криптографии на основе эллиптических кривых (ECC), которая обеспечивает гораздо более безопасную стратегию шифрования (по сравнению с системами криптографии на основе открытых ключей первого поколения).

Программируемое шифрование на скорости передачи от 100G до 400G

Для обеспечения требований современных высокоемких коммуникаций решение Ciena WaveLogic Encryption использует ведущую в отрасли когерентную технологию WaveLogic для реализации высокоемких, гибких и настраиваемых решений шифрования. Благодаря сочетанию возможностей WaveLogic 3 и дополнительных модуляций с расширенным подавлением линейных и нелинейных искажений WaveLogic 3 Extreme обеспечивает максимальную производительность всех когерентных сетевых решений. Это передовое решение впервые в отрасли обеспечивает программируемую модуляцию для поддержки шифрования на скорости передачи 100G с модуляцией QPSK, шифрования на скорости передачи 150G с модуляцией 8QAM и шифрования на скорости передачи 200G с модуляцией 16QAM. WaveLogic Ai работает на базе лучшей в своем классе платформы WaveLogic 3 и использует усовершенствованное оптимизированное ядро с поддержкой передачи 400G, существенно повышающее экономическую эффективность передачи данных. Эта новая технология позволяет в два раза увеличить емкость на канал, в три раза увеличить расстояние передачи при эквивалентной емкости и в четыре раза повысить плотность услуг.

На базе решения 6500 операторы могут интегрировать линейный модуль WaveLogic 3 Extreme с шифрованием в один из клиентских интерфейсов, чтобы развернуть решение в соответствии с собственными требованиями к передаче трафика услуг на скорости 10G, 40G или 100G. По мере роста требований в рамках модульной структуры с наращиванием емкости этот линейный модуль можно запрограммировать для передачи зашифрованного трафика на скорости 200G путем простого добавления дополнительной клиентской платы. Кроме того, операторы могут развернуть высокоемкие услуги с шифрованием в среде сети, используя возможности гибридной матрицы 6500 с поддержкой OTN и пакетной передачи, тем самым увеличивая эффективность сетевых ресурсов.

С помощью Waveserver операторы могут реализовать сертифицированное FIPS шифрование 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. Программируемая модуляция позволяет Waveserver оптимизировать пропускную способность линии шифрования на скорости передачи для каждого конкретного приложения или задачи, обеспечивая две длины волны 100, 150 или 200 Гбит/с. Для работы с приложениями на базе безопасных соединений сверхвысокой емкости операторы могут развернуть Waveserver Ai, чтобы обеспечить емкость шифрования до 1,2 Тбит/с в корпусе 1RU с возможностью поддержки трех модулей трафика, каждый из которых обеспечивает шифрование до 400 Гбит/с. Waveserver и Waveserver Ai обеспечивают надежную защиту данных при передаче со сверхнизкой задержкой в городских сетях, региональных сетях и сетях дальней передачи.

Шифрование 6500 на скорости передачи 10G

Операторы могут экономично предоставлять зашифрованные услуги 10G, используя оптический транспондер 4x10G с модулем шифрования. Однослотовый модуль обеспечивает для зашифрованных услуг

High-capacity Wire-speed Encryption Modules
Загрузить спецификацию

емкость на уровне 40G посредством четырех различных независимых от протоколов зашифрованных линейных портов 10G, благодаря чему пользователи получают возможность воспользоваться преимуществами упрощенной структуры сетей с интегрированным функционалом шифрования в любом варианте шасси 6500. Этот модуль предлагает повышенную безопасность за счет своей структуры, сертифицированной по 3 уровню FIPS 140-2, обеспечивая защиту от физической фальсификации плат с поддержкой обнуления. Это гарантирует удаление всей важной информации при обнаружении любой физической фальсификации криптографического модуля путем установки нулевого значения для всех данных, даже если сама плата не подключена в полке.

Простой подход к управлению шифрованием

Лучшее в своем классе решение обеспечения безопасности транспортного уровня требует упрощенного подхода к управлению интегрированными средствами шифрования. Отделение управления шифрованием от управления транспортом придает дополнительную гибкость инфраструктуре, находящейся в ведении оператора или предприятия. В обоих случаях важно, чтобы у конечного пользователя как у «хозяина» данных оставались механизмы полного контроля над параметрами защиты шифруемого контента, выпуском новых ключей и сертификатов с учетом собственной политики безопасности, а также сквозной прослеживаемостью всех предупреждений и журналов, связанных с безопасностью.

Решение шифрования Ciena 6500 WaveLogic Encryption включает MyCryptoTool — специальный интерфейс управления шифрованием, предназначенный для распределенного управления сетью, который позволяет конечному пользователю (уполномоченному сотруднику) независимо управлять параметрами безопасности и аварийными сигналами операторских или корпоративных

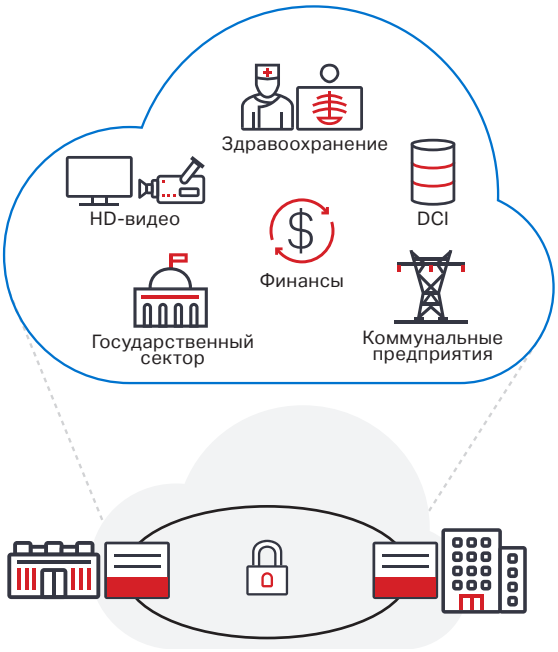

Рис. 4. Примеры основных приложений WaveLogic Encryption

сетей. Удобный интерфейс MyCryptoTool в защищенном режиме подключается к криптографическому модулю платы и обеспечивает взаимную аутентификацию, гарантируя запрет доступа всем пользователям, за исключением уполномоченного персонала. В случае приобретения криптографически защищенной услуги у поставщика услуг последний будет управлять каналами, их подготовкой и администрированием, а также мониторингом их производительности, как и в случае других услуг, но обзора и контроля над параметрами шифрования иметь не будет. Такой подход также можно использовать, если решение шифрования развертывается и управляется двумя различными группами в рамках одного предприятия или государственного органа.

Ключевые области применения

Решения Ciena WaveLogic Encryption разработаны специально для защиты критически важных данных при передаче во всех современных ресурсоемких приложениях. Наибольшую эффективность они, в частности, обеспечивают в следующих средах:

- среды соединения корпоративных ЦОД с высокоемкими хранилищами и средствами передачи зашифрованного трафика;
- правительственные учреждения и организации, требующие сертифицированных безопасных высокоскоростных коммуникаций между различными объектами;
- медицинские приложения с высокими требованиями к качеству и задержкам для безопасного и эффективного удаленного взаимодействия;
- приложения на основе управляемых услуг;
- приложения с высокими требованиями к задержкам при передаче, например приложения видеосвязи высокого разрешения и финансовые приложения для торговли, требующие безопасного транспортного решения со сверхнизкой задержкой;
- коммунальные предприятия, стремящиеся защитить свои коммуникационные инфраструктуры.

Заключение

По мере популяризации услуг передачи важных данных по волоконно-оптическим сетям подход к обеспечению безопасности ИТ в современных высокоемких коммуникациях должен предусматривать не только защиту серверов и шифрование хранимых данных, но и надежное шифрование данных при передаче. Решение Ciena WaveLogic Encryption сочетает в себе высокую степень гибкости и безопасности с удобной эксплуатацией и управлением для реализации экономичных масштабируемых решений шифрования на скорости передачи для непрерывной защиты всех передаваемых данных — в локальных сетях, в сетях дальней передачи и в подводных сетях.