СПЕЦИФИКАЦИЯ

Высокоемкие модули шифрования на скорости передачи

для 6500 Packet-Optical Platform

Будучи разработано для обеспечения конфиденциальности данных в процессе передачи, решение Ciena 6500 Packet-Optical Platform обеспечивает экономичное гибкое шифрование на скорости передачи 10G, 100G и 200G без привязки к конкретному протоколу. Оно сочетает в себе удобство эксплуатации и администрирования, позволяя легко реализовать стратегию защиты данных для услуг Ethernet, Fibre Channel, SONET/SDH и OTN.

Решение Ciena WaveLogic Encryption — это проверенная на практике технология шифрования, развернутая на множестве платформ в глобальном масштабе, и надежность передового решения 6500, которое успешно используется более чем 600 операторов в разных странах мира. Это решение упрощает развертывание шифрования, интегрируя его функционал непосредственно в сетевой элемент транспортной сети, упрощая структуру сети и устраняя необходимость в управлении отдельными решениями шифрования для различных приложений.

Высоконадежное сертифицированное решение

Функция шифрования в рамках многоуровневого подхода Ciena к обеспечению безопасности с гарантией конфиденциальности, целостности и доступности данных в сети непрерывно действует в решении Ciena WaveLogic Encryption, обеспечивая высочайший уровень безопасности, поскольку весь трафик постоянно шифруется. Может показаться, что возможность включения/отключения шифрования повысила бы гибкость решения, но на практике это может привести к случайной передаче важного трафика по сети в незашифрованном виде. Решение проходит внешнюю проверку и независимую сертификацию силами третьей стороны, что гарантирует его реализацию с использованием стандартного ядра и алгоритмов AES. Соответствуя высочайшим стандартам безопасности, включая сертификацию по общим критериям и FIPS, это решение обеспечивает сертифицированный FIPS механизм шифрования AES-256 с использованием стандартных механизмов аутентификации стандартов (например, сертификатов X.509), что позволяет упростить органичную интеграцию с существующими корпоративными PKI.

Возможности и преимущества

- Решение шифрования со сверхнизким уровнем задержки на скорости передачи для обеспечения надежных и прозрачных комплексных коммуникаций
- Независимое от протокола шифрование, способное обеспечить гибкость для поддержки разнообразных услуг
- Защита всех важных данных в процессе обработки посредством совместимого с FIPS решения шифрования AES256
- Два разных набора 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 в инфраструктурах под управлением оператора или предприятия при помощи специального встроенного инструмента
- Проверенное на практике решение шифрования, широко используемое по всему миру в сетях финансовых, коммунальных, медицинских, военных и правительственных организаций

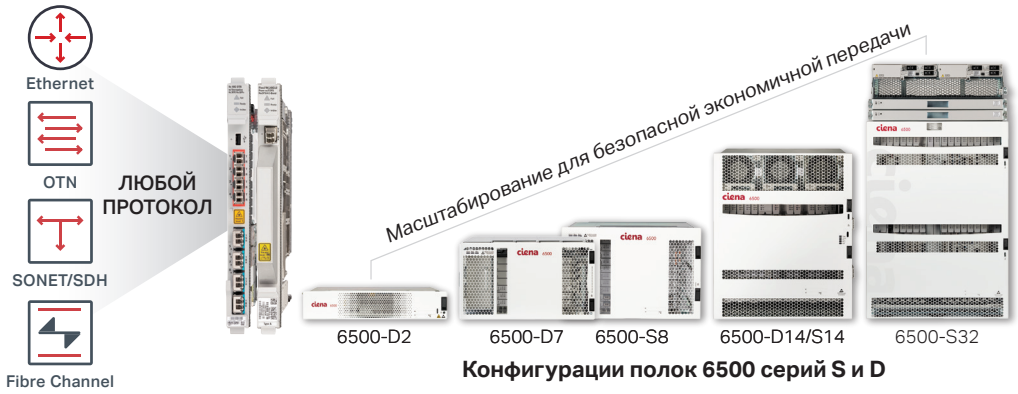

Рис. 1. Решение WaveLogic Encryption 6500 без привязки к протоколу с возможностью масштабирования в соответствии с вашими требованиями к сети

Непревзойденная гибкость

Решение 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. Клиенты могут развертывать дифференцированные варианты услуг со сверхмалой задержкой и несколькими способами защиты маршрутов и оборудования.

Encryption Testing and Certification
Загрузить информационный материал

Шифрование высочайшего уровня

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).

Рис. 2. 4x10G OTR с модулем шифрования

Шифрование на скорости передачи 10G

Операторы могут без чрезмерных затрат предложить зашифрованные услуги 10G, используя однослотовый оптический транспондер (OTR) 4x10G с модулем шифрования, обеспечивающим шифрование на скорости передачи 40G с использованием четырех отдельных линейных портов без привязки к конкретному протоколу. Соответствующий требованиям FIPS 140-2 уровня 3 модуль обеспечивает повышенную защиту всей важной информации от физической фальсификации путем обнуления (установки нулевого значения для всех данных при обнаружении любой физической фальсификации криптографического модуля — даже если сама плата не подключена в полке).

Программируемое шифрование WaveLogic Encryption на скорости передачи 100G или 200G

Решение Ciena WaveLogic Encryption использует ведущую в отрасли когерентную технологию WaveLogic для реализации высокоемкого гибкого настраиваемого решения шифрования на базе нового линейного модуля WaveLogic 3 (WL3) Extreme. Благодаря сочетанию возможностей WL3 и дополнительных модуляций с расширенным подавлением линейных и нелинейных искажений, WL3 Extreme обеспечивает максимальную

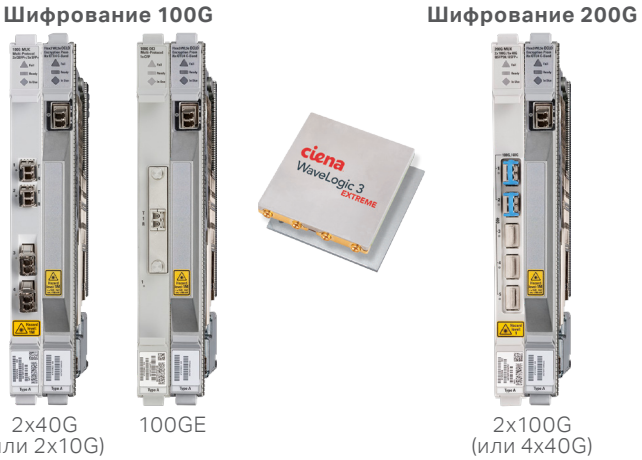

Рис. 3. Примеры программируемого шифрования на скорости передачи 100G или 200G с линейным модулем WL3 Extreme

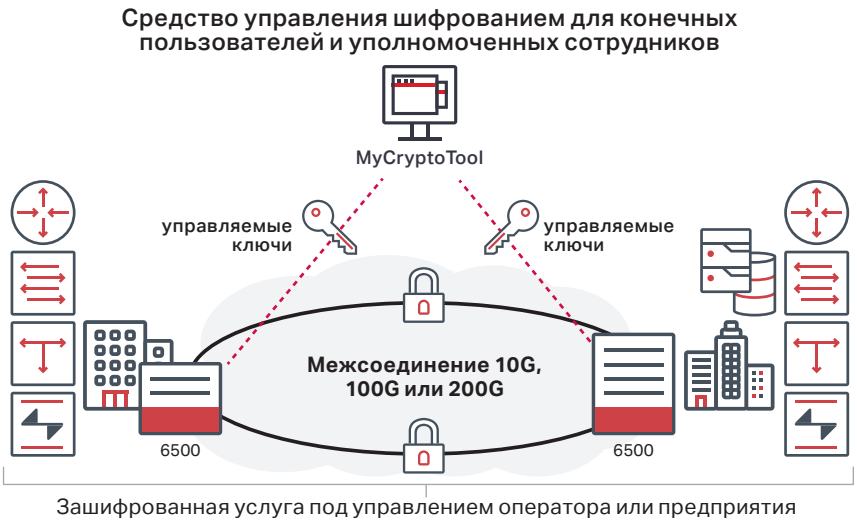

Рис. 4. Специальный интерфейс управления шифрованием MyCryptoTool

Data Security with Optical Encryption
Загрузить инфографику

производительность всех когерентных сетевых решений. Это передовое решение отвечает всем требованиям инфраструктуры — от городских сетей до сетей дальней передачи. Оно обеспечивает программируемую модуляцию для реализации шифрования 100G с модуляцией QPSK и шифрования 200G с модуляцией 16QAM — впервые в отрасли.

Интегрируя линейный модуль WL3 Extreme в один из клиентских интерфейсов, операторы получают возможность развернуть решение в соответствии с собственными требованиями к передаче трафика услуг на скорости 10G, 40G или 100G. По мере роста требований этот линейный модуль WL3 Extreme 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.

Простой подход к управлению шифрованием

Решение Ciena WaveLogic Encryption включает MyCryptoTool — специальный интерфейс управления шифрованием, предназначенный для распределенного управления сетью, которое позволяет конечному пользователю (уполномоченному сотруднику) независимо управлять параметрами безопасности и аварийными сигналами операторских или корпоративных услуг 10G, 100G или 200G. Удобный интерфейс MyCryptoTool в защищенном режиме подключается к криптографическому модулю платы и обеспечивает взаимную аутентификацию, гарантируя запрет доступа всем пользователям, за исключением уполномоченного персонала.

Решение Ciena WaveLogic Encryption сочетает в себе высокую степень гибкости и безопасности с удобной эксплуатацией и управлением для реализации экономичного, независящего от протоколов решения шифрования со сверхмалой задержкой на скорости 10G/100G/200G без привязки к конкретному протоколу. Оно способно обеспечить защиту практически любых современных коммуникационных приложений Webscale.

Wire-speed Encryption Solution — описание технологии
Загрузить сейчас

Техническая информация

Печатная плата	4x10G OTR с шифрованием	Линейный модуль WaveLogic 3 Extreme с шифрованием
Системные требования	Работает на любом шасси 6500 серий S и D	Работает на любом шасси 6500 серий S и D (за исключением 6500-D2)
Формат порта **Поддерживаемые клиентом интерфейсы**	OC-192/STM-64 10GbE LAN, 10GbE WAN FC400, FC800, FC1200 OTU2, OTU2e	OC-192/STM-64 10GbE LAN, 10GbE WAN, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
Поддерживаемые линейные интерфейсы	OTU2 OTU2e	Когерентный 100G (QPSK); 1xOTU4 Когерентный 200G (16QAM); 2xOTU4
Варианты защиты	Защита линии 1+1 Защита оборудования и клиента 1+1	Защита линии 1+1 Защита оборудования и клиента 1+1
Режимы FEC	RS-8 FEC, UFEC и OFF в соответствии со стандартом G.709	Прогр. FEC
Характеристики окружающей среды Рабочая температура Относительная влажность Высота	 От +5 °C до +40 °C От -5 °C до +55 °C краткосрочно — 6500-D2/D7/S8/D14/S14 От -5 °C до +50 °C краткосрочно — 6500-S32 От 5 % до 85% (без конденсации) 4000 м	
Физические характеристики	288 мм (В) x 25 мм (Ш) x 237 мм (Г)	
Функции безопасности	• Криптографическое решение на основе алгоритма AES-256 (сертификат NIST) • Алгоритмы на основе эллиптических кривых (ECC) • Согласование ключей по протоколу Диффи-Хелмана (включая эллиптические кривые) • Поддержка сертификата X.509 для аутентификации • Поддержка списка отозванных сертификатов (CRL) • Прозрачная ротация ключей AES-256 каждую секунду • Защита TLS с интерфейсом взаимной аутентификации для управления шифрованием • Поддержка аутентификации Radius • TACACS+AAA • Поддержка SNMPv3	
	• Сертификаты RSA 2048 бит • Сертификаты ECC	• Сертификаты ECC
Сертификаты	• Общие критерии профиля защиты сетевых устройств • BSI (Федеральное управление по информационной безопасности, Германия) • FIPS 140-2, уровень 3 — сертификат №2379, 2635 • FIPS 197 — AES-256 — сертификат №2963, 2964, 3599, 3600 • IBM GDPS • EMC, Brocade	• Общие критерии профиля защиты сетевых устройств • BSI (Федеральное управление по информационной безопасности, Германия) • FIPS 140-2, уровень 2 — сертификат №2697, 2843 • FIPS 197 — AES-256 — сертификат №3601, 3602, 4231, 4232, 5241 • IBM GDPS • EMC, Brocade

Обратитесь в Ciena уже сегодня