Как бороться с прослушкой оптических каналов связи?

Александр ВЕСЕЛОВ,
руководитель
отдела технического
консалтинга,
ООО «С-Терра СиЭсПи»

Наиболее универсальное и действенное средство защиты конфиденциальной информации – шифрование. Компания «С-Терра СиЭсПи» предлагает надежное и высокопроизводительное сертифицированное решение для шифрования трафика ВОЛС на канальном уровне.

Когда в начале 80-х годов прошлого века миру информационных технологий были предложены волоконно-оптические линии связи (ВОЛС), они воспринимались не только как высокоскоростные и механически надежные, но и как наиболее защищенные с точки зрения возможного подключения к ним для тайного «снятия» информации. В то время думали, что считать информацию с такого канала невозможно, поскольку электромагнитных волн он не излучает.

На самом деле защищенность ВОЛС иллюзорна. Яркий пример актуальной угрозы – так называемые прищепки для съема данных с оптических каналов (скажем, между ЦОДами). Для осуществления атаки злоумышленникам не требуется проникать во внутреннюю инфраструктуру объекта, они прослушивают канал связи. Это позволяет перехватить пользовательский трафик, трафик репликации данных, переезд виртуальных машин и т.п.

Подобная атака была предпринята в аэропорту Франкфурта еще в далеком 2000 г. Тогда было обнаружено подключение к трем главным линиям компании Deutsche Telekom. Когда именно «прищепка» была установлена и в течение какого времени производился перехват, не сообщается. Стоят «прищепки» сегодня всего несколько сотен долларов. Они уже не роскошь и широко используются киберпреступниками. Gartner называет проблемы безопасности одним из важнейших трендов в индустрии ЦОДов на 2016 г.

Ответвитель-прищепка FOD 5503

Чего ожидаем от средств безопасности?

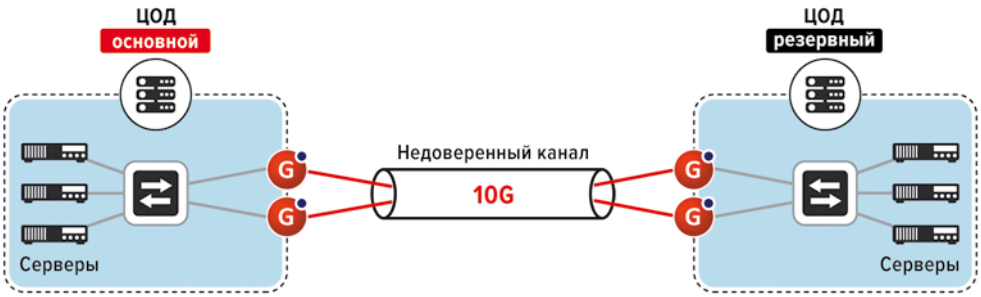
Для защиты ВОЛС принимаются организационные и технические меры. Основная организационная мера – постоянное наблюдение за волокном – применима только на небольших расстояниях, например между двумя соседними зданиями в контролируемой зоне. Физическая защита или наблюдение на более протяженном участке экономически неэффективны, а иногда просто невозможны, скажем, при использовании городских подземных коммуникаций.

Технические меры – это мониторинг уровня сигнала и шифрование трафика. Мониторинг очень важен, он позволяет обнаружить ослабление уровня сигнала по вине злоумышленника или по другим причинам. По этому факту можно оперативно принять меры – переключиться на другой канал, прекратить передачу конфиденциальной информации, отправить на предполагаемое место неисправности технических специалистов. Все это значимые аспекты политики информационной безопасности, но по сути они не защищают информацию от перехвата и попадания в чужие руки. Это, скорее, обнаружение инцидента и реагирование на него. Наиболее универсальным методом, обеспечивающим конфиденциальность и целостность трафика при передаче, является шифрование. На нем остановимся подробнее.

Для шифрования трафика используются средства криптографической защиты информации (СКЗИ). Основные требования, которые следует предъявлять к решению по криптозащите высокопроизводительного канала связи:

- Надежность. Если данное требование не выполняется, то зачем вообще нужна такая система защиты?
- Высокая производительность. Решение должно быть не просто «высокопроизводительным» на некоем синтетическом оптимальном трафике, но обеспечивать требуемое качество сервиса для реального трафика, который может включать в себя пакеты разной длины, разного приоритета, разного назначения – IP-телефонию, видеоконференцсвязь и т.д.
- Масштабируемость. По мере роста ЦОДа, увеличения количества потребителей сервиса решение должно легко подстраиваться под изменяющиеся требования бизнеса плавным наращиванием мощностей системы информационной безопасности, а не полной ее заменой.
- Отказоустойчивость. Система должна выполнять свои функции, даже если часть ее вышла из строя.
- Прозрачность для приложений. Безопасность – это сервис для бизнеса, а не наоборот. Цель решения – обеспечить высокий уровень защиты, не ухудшая при этом качество предоставляемого сервиса.
- Централизованное управление и мониторинг. Позволяет снизить эксплуатационные расходы, обнаруживать проблемы на ранней стадии и легко получать полную информацию о состоянии системы.
- Соответствие законодательству. Если в информационной системе обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные),

то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами – ФСБ России и ФСТЭК России. За нарушения предусмотрена административная ответственность, причем в этом году Государственная Дума одобрила законопроект, увеличивающий максимальный размер штрафа за использование несертифицированных средств связи с 40 до 300 тыс. руб.



Структурная схема решения

Обгоняя «Сапсан»

В 2012 г. впервые в России компании Cisco и «С-Терра СиЭсПи» представили высокопроизводительное решение с шифрованием на канальном уровне. Решение было модульным: коммутатор-балансировщик Cisco и сертифицированные шлюзы безопасности С-Терра. Модульная структура позволила обеспечить и масштабируемость, и отказоустойчивость. Прямо с демонстрационного стенда решение отправилось к крупному заказчику из топливно-энергетической отрасли для защиты его ЦОДа в процессе переезда.

К 2016 г. аналогичные продукты вслед за «С-Терра СиЭсПи» начали предлагать многие компании – поставщики решений инфобезопасности. За это время решение С-Терра для ЦОДов было серьезно усовершенствовано. Архитектура осталась прежней, но теперь вместо стандартного шлюза безопасности используется специализированный – С-Терра Шлюз 10G. Его производительность на смешанном трафике составляет 10 Гбит/с, что в 10 раз превышает показатели предыдущей версии. В типовом случае это позволяет сократить количество шлюзов безопасности с 16 пар устройств до двух пар. В результате решение стало не таким громоздким, занимает меньше места в стойках, потребляет меньше электроэнергии и требует меньше ресурсов охлаждения. Кроме того, уменьшение количества аппаратных платформ существенно снижает итоговую стоимость – как стоимость закупки, так и общую стоимость владения.

Один из наших заказчиков обеспечил защищенную миграцию своего ЦОДа из Москвы в Санкт-Петербург. Расстояние между старым и новым ЦОДами более 700 км. Скоростной поезд «Сапсан» преодолевает его за 4 часа, а трафик, зашифрованный на оборудовании «С-Терра СиЭсПи», – за несколько миллисекунд.

Новое решение может быть масштабировано для более широких каналов связи и повышения отказоустойчивости по стандартным сценариям. Еще одним его преимуществом является функционирование на канальном уровне, которое обеспечивает прозрачную работу сервисов внутри шифрованного туннеля. Улучшенное централизованное управление облегчает обслуживание. Поддерживается интеграция с системами мониторинга заказчика.

В продуктах С-Терра, применяемых в решении, используются отечественные криптоалгоритмы, соответствующие ГОСТу. Продукты сертифицированы в ФСБ России как СКЗИ по классам КС1, КС2, КС3 и как межсетевой экран 4-го класса, а также во ФСТЭК России (МЭ3, НВД3, ОУД4). Это позволяет обеспечить надежную защиту и выполнить требования законодательства.

Распространение ВОЛС – закономерный этап развития инфраструктуры ЦОДов. Одновременно с этим объемы передаваемых данных возрастают, как возрастает и доля конфиденциальной информации. Все эти факторы не остаются без внимания злоумышленников. После подключения к линии связи они могут нарушить конфиденциальность и целостность передаваемой информации. Потенциальный ущерб от подобных атак недооценивать нельзя.

Защита ВОЛС необходима. В некоторых случаях можно обойтись организационными мерами, но наиболее универсальным и действенным способом является шифрование.

Компания «С-Терра СиЭсПи» предлагает проверенное и не имеющее аналогов по производительности сертифицированное решение с шифрованием по алгоритмам, отвечающим ГОСТу, производительностью 10 Гбит/с и более. Еще одна ключевая его характеристика – соответствие российскому законодательству.

Подобное решение – вещь не дешевая. Но в случае инцидента наличие у посторонних лиц резервной копии какого-либо критически важного сервера может заставить пересмотреть взгляды на необходимость и стоимость защиты. Ведь помимо прямых материальных потерь могут быть и другие – например, огласка в СМИ факта успешной атаки и утечки данных клиентов может поставить крест на дальнейшем развитии бизнеса.

Решение на базе С-Терра Шлюз 10G – своеобразный комплекс из подушек безопасности – современный и проверенный инструмент, с помощью которого можно предотвратить нежелательные последствия и обеспечить целостность и сохранность самого дорогого...