



Андрей ФРОЛОВ
вице-президент,
директор по ИТ
ПАО «Почта Банк»



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

ПРАКТИЧЕСКИЙ ОПЫТ ПОСТРОЕНИЯ VPN СЕТЕЙ В БАНКАХ

Одной из особенностей нашей страны является обширная территория, которая подталкивает бизнес к созданию распределенной корпоративной сети. Банковская сфера — не исключение: региональные филиалы, дополнительные офисы, банкоматы — обязательные атрибуты большинства банков. При этом необходимо защищать их взаимодействие как между собой, так и с головным офисом

и ЦОД. Традиционно, системы защиты каналов связи строятся на основе мирового стандарта IPsec VPN с шифрованием по западным алгоритмам. Но стоит учитывать еще одну особенность нашей страны — локальное законодательство. В соответствии с отраслевым стандартом СТО БР ИББС персональные данные необходимо защищать с помощью VPN-продуктов, сертифицированных ФСБ России.

В компанию «С-Терра СиЭсПи» регулярно поступают запросы от банковских организаций на приобретение продуктов для модернизации системы защиты сети. Вместе с Андреем Фроловым, вице-президентом, директором по ИТ ПАО «Почта Банк», который является нашим заказчиком, мы рассмотрим перечень требований, предъявляемых при выборе VPN-продуктов, и продемонстрируем спектр предлагаемых решений С-Терра, удовлетворяющих этим требованиям.

ТРЕБОВАНИЕ 1. Неизменная логика работы, т.е. модернизация с минимальным изменением структуры сети.

Если новое оборудование работает по тем же протоколам, что и старое, то изменения действительно будут минимальны. Продукты С-Терра реализованы на базе протокола IPsec в соответствии с RFC, поэтому заказчик имеет возможность плавной миграции.

Андрей Фролов: Изначально мы использовали шифрование на западных алгоритмах с резервированием оборудования и каналов связи. На первом этапе мы заменили оборудование на резервном канале — установили туда С-Терра. Временно сделали этот канал основным, провели пилотное тестирование. Для нас крайне важной была возможность в любой момент без проблем вернуться к старой схеме. Вторым этапом было заменено оборудование на основном канале.

ТРЕБОВАНИЕ 2. Соответствие законодательству и отраслевым стандартам.

Защита персональных данных регламентируется Федеральным Законом № 152 «О персональных данных», Постановлением Правительства № 1119, приказом ФСБ № 378, приказом ФСТЭК № 21 и, конечно же, СТО БР ИББС.

Поэтому средства защиты информации (СЗИ) должны быть сертифицированы регуляторами — ФСБ России и ФСТЭК России, при этом уровни сертификации определяются на этапе проектирования. Продукты С-Терра поддерживают шифрование по отечественным ГОСТ-алгоритмам и сертифицированы ФСБ России как СКЗИ по классам КС1, КС2 (требование для ПДн в СТО БР), КС3, и как МЭ4 класса, а также во ФСТЭК России. Это позволяет реализовать систему защиты в соответствии с требованиями российского законодательства.

Андрей Фролов: При закупке сертифицированного оборудования мы обращали внимание не только на сам факт наличия сертификатов на момент закупки, а на наличие у поставщика дорожной карты по разработке и сертификации на 5 лет. Ведь сроки действия сертификатов составляют всего три года с возможностью продления до пяти. И этот срок редко отсчитывается от начала проекта, т.е. скорее всего в рамках обслуживания потребуются своевременное обновление до актуальной сертифицированной версии. Для продуктов С-Терра такая возможность предоставляется при использовании вендорской технической поддержки.

Также нам важно знать в каком направлении движется компания-производитель, сможем ли мы использовать их решения в других проектах. Во время общения с коллегами из компании «С-Терра СиЭсПи» мы поняли, что к нашему мнению прислушиваются, для будущих проектов продукты могут быть доработаны с учетом наших пожеланий. Для нас это важно.

ТРЕБОВАНИЕ 3. Оптимальное соотношение цена / качество / функциональные характеристики.

Для типовых объектов требуются недорогие комплекты оборудования с базовым набором функций: межсетевой экран, криптозащита, доступ в интернет и т.п. Для продуктов С-Терра это могут быть как совместные решения с крупнейшими компаниями — производителями сетевого оборудования — Cisco и Huawei, так и полностью отечественный продукт — универсальный сервисный криптомаршрутизатор Eltex ESR-ST. Это позволяет выбрать оптимальный вариант для любой задачи.

Андрей Фролов: В продуктовой линейке С-Терра нас привлекла гибкость, компания готова сотрудничать с различными производителями сетевого оборудования для выработки оптимальных для нас решений. Таким образом, удалось сформировать несколько вариантов комплектов для типовых узлов.

ТРЕБОВАНИЕ 4. Удобное обслуживание.

Оборудование необходимо администрировать, следовательно, дополнительная нагрузка будет возложена на отделы ИБ и/или ИТ. Если средства защиты имеют собственный интерфейс и логику управления, то необходимо обучение сотрудников, которое требует временных и финансовых затрат. Продукты С-Терра, наряду с собственной системой управления, могут конфигурироваться через консоль с подмножеством команд Cisco IOS, знакомых большинству сетевых инженеров.

Андрей Фролов: Нам хотелось найти продукт с интуитивно понятным интерфейсом управления, уже известным администраторам, а также с возможностью интеграции в наши системы мониторинга. В продуктах С-Терра управление реализовано в виде «cisco-like» консоли, а для мониторинга можно использовать широкий перечень параметров SNMP.

Выводы

Банк — прагматичный заказчик, который подходит к проектированию системы защиты фундаментально, рассматривая как высокоуровневые задачи, так и разбираясь в деталях работы компонентов решения. У банков есть то, что нужно злоумышленникам — деньги. Ставки слишком высоки, чтобы экономить на защите. Специфика требований отрасли — интеграция с сетевой инфраструктурой, средствами управления и мониторинга, выгодное соотношение цены и качества, а также соответствие требованиям регуляторов.

Андрей Фролов: Проектирование и внедрение любых систем, и защита каналов связи не исключение, в крупной организации процесс довольно долгий, ведь нам нужно учесть множество нюансов. Это является дополнительной проверкой производителя — он должен все время держать руку на пульсе, своевременно реализовывать новые требования, соблюдая соотношение цена-качество. С компанией «С-Терра СиЭсПи» мы работаем уже довольно давно и хорошо знаем их надежные, современные продукты, соответствующие требованиям российского законодательства.