ЗАЩИТА КАНАЛОВ СВЯЗИ БАНКА: 7 РЕШЕНИЙ ВАЖНЫХ ЗАДАЧ

■ **Христофор ГАЗАРОВ**,
технический директор
«С-Терра СиЭсПи»

Крупные отечественные банки имеют разветвленную инфраструктуру, в которую входят филиалы, отделения, дополнительные офисы, банкоматы, мобильные сотрудники. Эти объекты отличаются количеством автоматизированных рабочих мест (АРМ), размерами и сложностью локальной вычислительной сети (ЛВС), типом и пропускной способностью каналов связи. В зависимости от этих характеристик для защиты каналов связи разного типа объектов удобнее и выгоднее использовать разные по характеристикам и стоимости VPN-продукты.

ЦОД И ВЫСОКОСКОРОСТНЫЕ КАНАЛЫ СВЯЗИ

При том объеме информации, который обрабатывают банковские приложения, невозможно обойтись без создания ЦОД. Для выполнения требований отказоустойчивости, резервирования и непрерывности сервисов создаются резервные ЦОД. И здесь возникает **первая задача**: высокоскоростная передача данных между основным и резервным ЦОД. Эта функциональность необходима крупным банкам не только для своевременной репликации данных, но и для оперативного доступа к удаленным системам хранения данных (СХД), быстрой выгрузки резервных копий и т.д.

Как правило, ЦОД соединены волоконно-оптическими каналами с пропускной способностью 10 Гб/с и выше. Традиционно для защиты такого канала используется целый набор VPN-шлюзов с распараллеливанием потока, резервированием и балансировкой нагрузки. Если возможности распараллеливания трафика нет, то можно установить на периметрах ЦОД по одному (или по два — для резервирования) VPN-шлюзу высокой производительности, например, С-Терра Шлюз 7000 на серверной аппаратной платформе Intel-архитектуры.

ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА

Зачастую все информационные сервисы и бизнес-приложения разворачиваются в ЦОД на базе виртуальной инфраструктуры. В таком случае возникает **вторая задача**: защита виртуальной среды. Необходимо обеспечить не только безопасность обрабатываемой информации, но и защиту элементов управления виртуальной инфраструктурой.

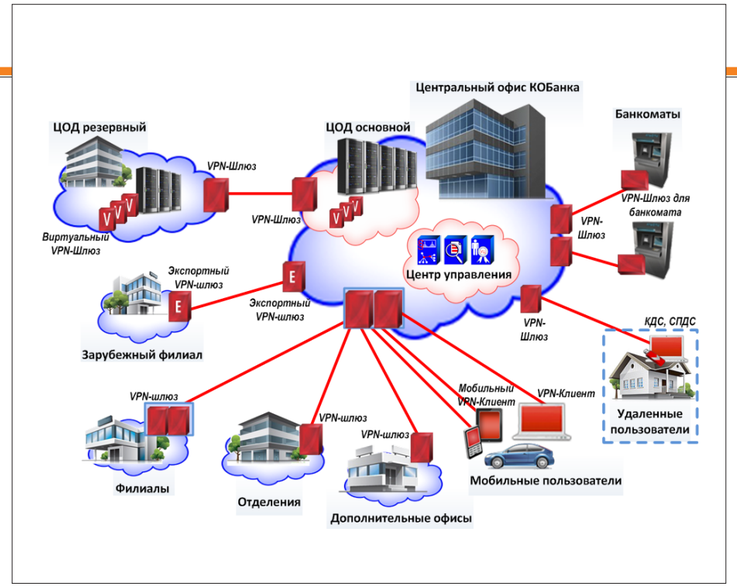
Удобнее всего в данном случае применять VPN-шлюз, который непосредственно интегрируется в виртуальную среду, то есть Виртуальный VPN-шлюз. С его помощью можно обеспечить как безопасную связь с территориально распределенными офисами, так и защищенный удаленный доступ сотрудников. Более того, Виртуальный шлюз позволяет защитить также трафик внутри виртуальной среды, обеспечив безопасный информационный обмен между сотрудниками банка.

Сегодня на рынке представлен единственный сертифицированный ФСБ России и ФСТЭК России Виртуальный шлюз (компании «С-Терра СиЭсПи»), с помощью которого можно решить все поставленные задачи. Благодаря наличию в нем функционала сертифицированного межсетевого экрана, есть возможность выделения нескольких зон безопасности с разными категориями доступа внутри виртуальной среды.

УДАЛЕННЫЕ РАБОЧИЕ МЕСТА

В современном обществе потребитель привык, что банк «всегда под рукой». Во всех торговых центрах установлены банкоматы, а в некоторых даже организованы небольшие офисы, где готовы выдать кредит на значительную покупку. При создании такого удаленного офиса банку нужно решить **третью задачу** — сделать обмен информацией с главным офисом и центральной базой данных безопасным, даже в условиях, когда системного администратора и/или специалиста по ИБ нет рядом.

Для того чтобы защитить трафик в этих условиях, нужно обеспечить аутентификацию пользователя на сервере приложений, работу в централизованной автоматизированной банковской системе, подпись документов, работу с локальными USB-устройствами (токен, принтер, сканер, видеокамера и т.п.). Для этих целей удобно использовать в качестве рабочего места защищенный бездисковый тонкий клиент российского производства (помним про импортозамещение) с интегрированным программно-аппаратным средством построения доверенного сеанса (СПДС). Неплохим примером такого оборудования является комплект доверенного сеанса С-Терра КДС, обеспечивающий защиту от НСД, шифрование канала связи с центральным офисом или с ЦОД, где установлен С-Терра Шлюз требуемой производительности. При этом для организации удаленного доступа можно использовать терминальные решения разных производителей.



БАНКОМАТЫ

Мы уже упоминали в нашей статье о широком распространении банкоматов. Остановимся подробнее на этом вопросе. Следующая, **четвертая задача**, с которой сталкивается крупный банк,— это защита каналов передачи данных от банкоматов. Для ее решения необходимо либо установить небольшой недорогой VPN-шлюз внутри корпуса банкомата, либо, если позволяет регламент обслуживания, установить VPN-клиент в операционную систему встроенного в банкомат компьютера. В обоих случаях необходимо иметь возможность удаленного обновления, как программного обеспечения средства защиты, так и ключей для шифрования трафика. Для выполнения такого рода задач хорошо подойдут шлюз безопасности на компактной аппаратной платформе С-Терра Шлюз 100В, либо программный продукт С-Терра Клиент.

МОБИЛЬНЫЕ УСТРОЙСТВА

Пятая задача, которую нельзя обойти вниманием — доступ к внутренним информационным ресурсам банка с мобильных устройств. Это особая разновидность удаленного доступа. Топ-менеджеры, администраторы ИТ и ИБ, много разъезжающие сотрудники банка нуждаются в оперативной связи с центральным офисом и ЦОД. Для этого применяются MDM-системы, позволяющие определять политики безопасности одновременно для различных групп пользователей, а защита трафика осуществляется с помощью мобильного VPN-клиента. Конечно, нежелательно вмешиваться в операционную систему (Android, Windows, iOS), установленную производителем гаджета. Поэтому лучше предпочесть VPN-клиент, не требующий взлома ОС для установки, например, С-Терра Клиент-М для ОС Android 4.x (опробованы на ряде смртфонов Samsung и Yota) или С-Терра Клиент для Windows 8.x (опробованы на планшетах с Intel-процессорами), которые к тому же протестированы на совместимость с MDM решениями разных производителей (в частности Citrix XenMobile) и позволяют хранить параметры защищенных соединений на Radius-сервере.

ЗАРУБЕЖНАЯ ФИЛИАЛЬНАЯ СЕТЬ

В случае наличия у крупного банка зарубежного филиала возникает **шестая задача** — необходимость создания шифрованного канала связи с ним. По российскому законодательству в таких случаях необходимо получить разрешение ФСБ на экспорт СКЗИ. Но в большинстве случаев на обычное СКЗИ, используемое банком, получить такое разрешение проблематично. Необходим специализированный продукт в экспортном исполнении с соответствующим сертификатом ФСБ. Такой уникальный экспортный вариант шлюза безопасности на российской криптографии (CSP VPN Gate E) есть в линейке продуктов С-Терра. Его эксплуатация официально допускается как на территории РФ, так и за её пределами.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Большое многообразие средств защиты, используемых в крупном банке, требует создания центра управления. Это **седьмая задача**. Часто для ее решения даже выделяют отдельный сегмент, в котором собирают все необходимые системы управления. Для контроля, мониторинга, обновления настроек VPN-продуктов С-Терра, о которых мы говорили выше, разработана специализированная централизованная система управления С-Терра КП, в одном сегменте с которой удобно расположить SIEM-систему (например, протестировано с HP ArcSight), куда VPN-продукты С-Терра посылают свои сообщения (Syslog, SNMP).

О ВАЖНОМ!

В условиях политики импортозамещения мы все чаще говорим о необходимости перехода на решения отечественных производителей, соответствующие национальным стандартам безопасности. Наступает период, когда и финансово-кредитные организации задумываются о том, как удобнее заменить западные алгоритмы защиты каналов связи на российские, тем более, что аналогов на российском рынке достаточно. Например, продукты компании «С-Терра СиЭсПи», соответствующие всем требованиям российского законодательства и обеспечивающие эффективную реализацию комплексной системы защиты каналов передачи данных российского банка.