Андрей ШПАКОВ
ведущий инженер отдела технического консалтинга ООО «С-Терра СиЭсПи»

КАКОЙ VPN ВЫБРАТЬ?

СРАВНЕНИЕ ТЕХНОЛОГИЙ И ПРОТОКОЛОВ ЗАЩИЩЕННОГО ДОСТУПА

VPN является неотъемлемой частью всех систем информационной безопасности, в том числе тех, которые обеспечивают защиту информационных систем финансовых организаций. Эта технология является самым простым, понятным и доступным способом безопасно объединить территориально распределенные площадки и надежно защитить информацию при передаче по сетям общего пользования.

Существует множество сценариев применения VPN: организация взаимодействия между удаленными офисами, подключение удаленных сотрудников или клиентов, подключение банкоматов, доступ к ЦОД-ам, в которых сосредоточены ресурсы информационных систем банка. Кроме задачи обеспечения взаимодействия, в ряде случаев, VPN позволяет сформировать четкий периметр защиты и обеспечить доступность сегментов информационной системы.

Однако, прежде чем приступить в выбору конкретного поставщика решения, нужно и важно понимать, какие технологии VPN существуют и каково различие между ними.

ПРОПРИЕТАРНЫЕ ПРОТОКОЛЫ

Все протоколы для передачи данных разделяются на две категории.

Первая категория, о которой пойдет речь — проприетарные (закрытые) протоколы и технологии, являющиеся интеллектуальной собственностью отдельных компаний. Преимущества такого подхода в том, что технология может быть относительно быстро доработана под требования производителя оборудования или желание конкретного заказчика. Однако, есть и ряд минусов.

Во-первых, для заказчика велика вероятность стать объектом исследований и технических доработок за свои же деньги. Для того, чтобы снизить риск появления архитектурных ошибок, необходимо максимально полно отработать новую технологию с привлечением как можно более широкого круга экспертов. К сожалению, база заказчиков российских вендоров, использующих проприетарные протоколы, не всегда позволяет это сделать. К слову, зарубежные лидеры ИТ рынка не идут путем создания проприетарных протоколов. Они развивают функциональные возможности общепринятых протоколов, открывают доступ к своей технологии и делают ее публичной, доступной для других производителей.

Во-вторых, существенным недостатком является то, что нестандартный дизайн продукта и недокументированное поведение устройств могу поставить заказчика в зависимость от поставщика продуктов. Если качество сервиса или услуг перестанет устраивать заказчика, переход с проприетарного протокола на другой может быть крайне затратным, либо вообще невозможным без полной перестройки системы безопасности. В лучшем случае заказчик сможет рассчитывать на использование б/у аппаратных платформ, на которые можно будет поставить новое программное обеспечение. Специалисты компании «С-Терра СиЭсПи» уже имели опыт установки своего VPN-шлюза на платформы компании Stonesoft (которая хоть и использовала стандартные протоколы, но, как известно, прекратила активную деятельность на рынке сетевой безопасности в России).

В-третьих, любой нестандартный дизайн создает проблемы при поиске неисправности или неправильной работе устройств. Необходимо иметь в штате людей, знающих особенности поведения как стандартного оборудования, так и специфику работы технологий конкретного производителя.

И в-четвертых, нужно учитывать тот факт, что проприетарный протокол имеет минимальные шансы для получения совместимости с другими производителями.

ПУБЛИЧНЫЕ ПРОТОКОЛЫ

Вторая категория — это публичные (или стандартные) протоколы, которые могут применяться в оборудовании, произведенном различными вендорами. Описание этих технологий приводится в специальных документах (Request for Comments, RFC) организации инженерного совета Интернета (Internet Engineering Task Force, IETF). Их создают и дополняют лучшие эксперты отрасли. Для VPN из публичных протоколов наиболее часто используются IPsec и SSL в различных вариациях.

НУЖНО УЧИТЫВАТЬ ТОТ ФАКТ, ЧТО ПРОПРИЕТАРНЫЙ ПРОТОКОЛ ИМЕЕТ МИНИМАЛЬНЫЕ ШАНСЫ ДЛЯ ПОЛУЧЕНИЯ СОВМЕСТИМОСТИ С ДРУГИМИ ПРОИЗВОДИТЕЛЯМИ

SSL (TLS)

Это семейство протоколов предназначено для обеспечения удаленного клиентского доступа и ориентировано на конкретные пользовательские приложения. Существует несколько вариантов использования SSL (TLS):

Бесклиентский режим. В этом режиме используется односторонняя аутентификация сервера на клиентской стороне. При этом пользователю не требуется устанавливать специализированное клиентское ПО для защиты трафика, а достаточно иметь на АРМ-е только криптопровайдер. Работа в таком режиме возможна только с Web-приложениями, причем в российских реалиях есть привязка к не самому популярному браузеру Internet Explorer. Такой режим работы подходит, например, для ограниченного перечня сценариев защищенного доступа к web-порталу.

Клиентский режим. Если требуется обеспечить доступ к какому-либо другому приложению, используется специальный SSL (TLS)-клиент. В этом режиме есть возможность использовать двухстороннюю аутентификацию.

Одним из главных преимуществ протокола является отсутствие или минимальная необходимость персональной настройки клиента. Однако, в случае если на рабочую станцию будет установлено новое ПО или появится новый сервис, к которому требуется доступ, пользователь должен будет добавить эти параметры в настройки клиента.

Также нужно учитывать особенность, что стандартный SSL работает на уровне приложения и не может защитить трафик от сетевого оборудования или от сегментов сети. Решить эту задачу может протокол DTLS, но он тоже имеет клиент-серверную модель и слабо распространен среди российских производителей.

IPsec

IPsec работает на более низком уровне модели OSI, и для его работы не требуется поддержка со стороны приложений. Он отлично подходит для создания защищенных соединений как между филиалами в территориально распределенной сети, так и для организации защищенного удаленного доступа.

За счет работы протокола на сетевом уровне, для работы VPN не требуется вносить изменения в ПО на рабочих местах. Все пользовательские приложения работают «прозрачно» и не знают про существование VPN. Протокол всегда осуществляет двухстороннюю аутентификацию.

При реализации удаленного доступа требуется персонализированная настройка клиента для каждой конкретной рабочей станции. При этом клиент защищает все сетевые взаимодействия между АРМ-ом и удаленной сетью. Следовательно, необходимость наличия на рабочих местах пользователей средств защиты от несакционируемого доступа к АРМ является более актуальной, чем в случае SSL.

IPsec является самым известным протоколом для построения VPN и продолжает развиваться. Появилась вторая версия протокола распространения ключей IKE, стек протоколов является частью стандарта IPv6.

РЯД РОССИЙСКИХ ПРОИЗВОДИТЕЛЕЙ, В ТОМ ЧИСЛЕ КОМПАНИЯ «С-ТЕРРА СИЭСПИ», ОБЕСПЕЧИЛИ СОВМЕСТИМОСТЬ СВОИХ СЕРТИФИЦИРОВАННЫХ РЕШЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ ПРОТОКОЛА IPsec

Кроме вышеперечисленного, у стандартных протоколов IPsec и SSL (TLS) есть определенные преимущества именно в российских реалиях. Речь идет про деятельность технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) в области выработки рекомендаций по использованию единообразных узлов замены и параметров эллиптических кривых в российских ГОСТах по криптографии, а также их использование в протоколах передачи данных. Эта деятельность уже принесла свои плоды — ряд российских производителей, в том числе компания «С-Терра СиЭсПи», обеспечили совместимость своих сертифицированных решений при использовании протокола IPsec. Безусловно, если бы применялись проприетарные протоколы, таких результатов невозможно было бы достичь. Хотя такие процессы не происходят быстро, у заказчиков появляется перспектива исполнения заветной мечты — появления технической совместимости различных сертифицированных VPN-решений между собой.

Использование стандартных протоколов в разных областях (Syslog, SNMP, Netflow и т.д.) позволяет объединять продукты в единую систему. Например, такая практика является общепринятой при решении задач мониторинга и построения SIEM-систем.

ДЕЛАЕМ ВЫВОДЫ

При выборе стандартного протокола заказчик должен определиться с желаемым сценарием использования. Если ему достаточно защиты лишь отдельных сервисов и важна простота настройки — SSL (TLS), при необходимости полной сетевой связности между объектами — его выбор IPsec.

* * *

Вместе с тем, необходимо помнить, что помимо протокола передачи данных, в каждом решении есть большое количество разных технологий и особенностей. Поэтому стоит оценивать и сравнивать продукты в целом, в зависимости от поставленной задачи.

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

BIS-КОММЕНТАРИЙ

Одно из ключевых направлений безопасности, обозначенных в статье,— это катастрофоустойчивость. Речь идет о наличии резервного ЦОД, который территориально удален от основного ЦОД и взаимодействует с ним по защищенному каналу связи. Развеем некоторые мифы, касающиеся защиты так называемых «толстых» каналов.

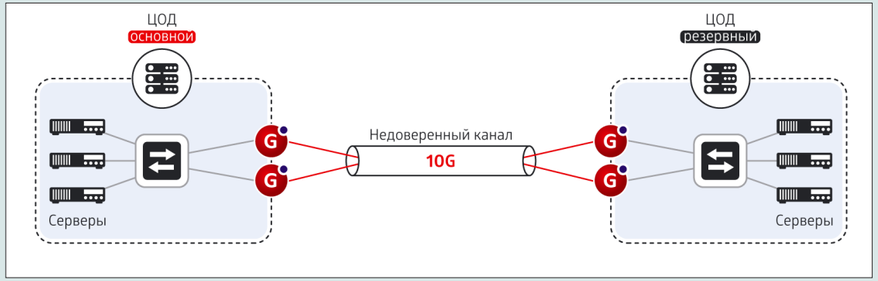
Миф № 1: Оптические каналы связи защищать не требуется. Традиционно считается, что к волоконно-оптической линии связи (ВОЛС) подключиться и перехватить трафик довольно сложно. Но эта информация давно устарела, оборудование для «съема» данных вполне доступно по цене и удобно в использовании. Например, «прищепка» FOD 5503 стоит порядка 35 тысяч рублей.

Защититься от подобных угроз можно организационными и/или техническими мерами. Организационные меры — это постоянный контроль за волокном. Но на практике это применимо только на небольших расстояниях, например, между двумя соседними зданиями в контролируемой зоне. Если речь идет о катастрофоустойчивости, то физическая защита или наблюдение неэффективны с экономической точки зрения, а иногда просто невозможны, скажем, при использовании городских подземных коммуникаций.

Технические меры — это, в основном, шифрование. Оно может быть реализовано на международных криптоалгоритмах или на отечественных ГОСТ. Если речь идет об информации, подлежащей обязательной защите в соответствии с законодательством, то требуется применять именно криптоалгоритмы ГОСТ. При этом средства криптографической защиты информации (СКЗИ) должны быть сертифицированы ФСБ России.

Реальность № 1: Любые каналы связи, в том числе и оптические, защищать необходимо. Лучше это сделать с применением сертифицированных криптосредств.

Миф № 2: Шифровать канал 10Гб/с ГОСТом невозможно. Поддержка ГОСТ-шифрования, высокая производительность и сертификация — теперь сочетание этих трех понятий стало возможным. Применение комбинированного преобразования ESP_GOST-4M–IMIT в соответствии с рекомендациями ТК26 и оптимизация сетевого стека позволили в новом продукте С-Терра Шлюз 10G получить производительность шифрования 10Гб/с на смешанном трафике. Решение на основе высокопроизводительного шлюза многократно проверено как в лаборатории, так и в пилотных проектах заказчиков на различных генераторах трафика.



VPN-Шлюз, который шифрует данные в соответствии с ГОСТ со скоростью 10 Гбит/с

Реальность № 2: VPN-Шлюз, который шифрует данные в соответствии с ГОСТ со скоростью 10 Гбит/с — это реальность.

Миф № 3: Российские разработки ненадежны. СКЗИ, необходимые для защиты 10G канала, можно разделить на две части — аппаратную и программную. Аппаратные платформы в основном выбираются зарубежные, с наработкой на отказ в десятки тысяч часов. Но стоит обратить внимание и на отечественные устройства (Kraftway, Depo), практически не уступающие по качеству и надежности (справедливости ради, отметим, что компоненты этих аппаратных платформ все же не российского производства).

Программную часть средств защиты лучше предпочесть российскую, которая тщательно проверяется как производителем, так и регулятором ИБ. Во время разработки производитель учитывает задачу связи ЦОДов и закладывает механизмы отказоустойчивости в продукт. В нашем случае, например, это масштабирование с балансировкой нагрузки на любом коммутаторе, поддерживающем агрегированный канал.

Реальность № 3: За последнее время российские компании сделали огромный шаг вперед в сфере надежности и отказоустойчивости сетевых средств защиты и во многом не уступают западным аналогам.