Шифрование: сценарии использования

Владимир Воротников, *руководитель отдела интеграционных решений ООО "С-Терра СиЭсПи"*

В современном мире ценность информации высока как никогда. Подтверждением тому служит целый ряд успешных компаний, весь бизнес которых строится на том или ином виде обработки информации. Вместе с ростом ценности информации возрастают и потенциальные убытки от ее потери или несанкционированного доступа к ней. Система защиты данных из опциональной части информационной системы превращается в ее неотъемлемый атрибут. Одним из способов защиты данных является их шифрование. Само по себе шифрование не является ценностью, но это чрезвычайно важный элемент различных систем и протоколов безопасности. В данной статье пойдет речь о сценариях использования шифрования в одной из самых распространенных областей его применения – в построении виртуальных частных сетей (VPN).

Новые технологии передачи и хранения данных требуют новых подходов к обеспечению безопасности. К примеру, распространение облачных технологий привело к появлению новых угроз и, как следствие, к внедрению новых способов защиты.

Базовый сценарий – защита передаваемых данных

Чаще всего данные между географически удаленными объектами передаются через каналы общего пользования. Даже если провайдер может предоставить вам персональный выделенный канал, это все равно не означает его полной защищенности. Да и услуга эта стоит недешево, особенно если вам нужно соединить локальные сети не в рамках одного города, а распределенные по всей стране. Поэтому провайдерский канал почти всегда является недоверенным, и для защиты данных, которые циркулируют в этом канале, требуются дополнительные меры. Это базовый сценарий использования шифрования. В классическом варианте для его реализации используются VPN-шлюзы и VPN-клиенты. Современные условия требуют, чтобы криптографические функции, встроенные в эти продукты, работали прозрачно, то есть таким образом, чтобы пользователи сетей передачи данных не замечали этого. Такого эффекта можно добиться, используя в VPN-продуктах механизмы QoS, приоритизацию трафика, технологию плавного перестроения криптографических туннелей Smooth Rekeying, а также различные механизмы обеспечения отказоустойчивости. Собственно, шифрование при этом должно обладать высокой производительностью, поддержкой современных криптографических стандартов и быть одобрено регуляторами отрасли (ФСТЭК РФ, ФСБ РФ). В полной мере всем перечисленным требованиям отвечают шлюзы и клиенты безопасности "С-Терра" со встроенным криптографическим модулем ST и интегрированным межсетевым экраном.

Помимо этого, шлюзы безопасности со встроенной криптографической библиотекой ("С-Терра Шлюз" с криптографией ST) обладают целым рядом преимуществ. Кроме более привлекательной стоимости, бесспорным плюсом является то, что на использование VPN-продукта требуется только одна лицензия. Это снижает затраты на поддержку системы, количество разрешительных документов и позволяет спокойно работать в течение всего срока действия сертификатов регуляторов на сам продукт.

Не только филиальные сети требуют защиты. Для эффективного функционирования бизнеса бывает чрезвычайно удобно, а зачастую и жизненно необходимо наличие сотрудников, работающих с корпоративными данными удаленно. Но одновременно это может стать и угрозой безопасности. Дистанционные сотрудники работают с корпоративной сетью не

Таблица. Продукты ООО "С-Терра СиЭсПи"

Продукты	Назначение	Возможности
С-Терра Шлюз	Создание VPN, защита трафика, МЭ, защита подсетей, защищенный удаленный доступ	IPSec, шифрование и имитозащита, Radius, PKI, мониторинг SNMP, туннелирование, QoS, RRI-балансировка нагрузки, маскирование топологии, фильтрация и маркирование трафика и т.д.
С-Терра Клиент	Безопасный удаленный доступ к корпоративной сети, МЭ	IPSec, шифрование и имитозащита, PKI, фильтрация, туннелирование и маркирование трафика, интеграция с Radius и т.д.
С-Терра Клиент-М	Безопасный удаленный доступ с Андроид устройств	IPSec, шифрование и имитозащита, PKI, Radius, туннелирование, совместимость с MDM-системами
СПДС "ПОСТ"	Защищенный удаленный доступ к ресурсам корпоративной сети	Обеспечение целостности и изоляции программной среды клиента, строгая аутентификация, шифрование и имитозащита трафика, поддержка PKI, IKE, пакетная фильтрация, и т.д.
С-Терра Виртуальный Шлюз	Работа в виртуальной среде, защита периметра облака и взаимодействия виртуальных машин.	Полноценный шлюз безопасности, поддержка VMware ESX, Xen, Hyper-V, KVM и др.

только через недоверенные провайдерские каналы (Интернет), но и часто через открытые точки доступа (в кафе, аэропортах, гостиницах и т.д.). В данном случае на помощь также приходит шифрование, которое позволяет защитить взаимодействие между устройством сотрудника, работающего вне офиса (ноутбук, планшет, смартфон), и корпоративной сетью. Для защиты удаленного доступа с такого рода устройств существуют мобильные клиенты безопасности, специально разработанные для работы под управлением различных операционных систем. Например, "С-Терра Клиент" поддерживает работу под управлением ОС Windows, включая версию 8.1, а "С-Терра Клиент-М" – под управлением ОС Android 4.x. Примечательно, что высокий уровень оптимизации шифрования ST позволяет добиться производительности, достаточной для комфортной работы даже на не очень мощных мобильных платформах. Кроме того, "С-Терра Клиент-М" не требует взлома устройства (т.е. получения прав root).

Защищенный терминальный доступ

Итак, мобильный клиент С-Терра позволяет защитить данные, передаваемые по сети. Однако это не единственный из существующих рисков. Например, работник может потерять ноутбук, на жестком диске которого будут находиться конфиденциальные данные. Кроме того, даже без физической потери устройства доступ к нему может быть получен злоумышленником удаленно. Для того, чтобы избежать подобных рисков, лучше вообще не хранить важную информацию на устройствах сотрудников, работающих дистанционно. Для решения этой задачи можно применить терминальный доступ.

Нагляднее всего продемонстрировать принцип реализации такого применения шифрования можно на примере. Устройство СПДС "ПОСТ" от компании "С-Терра СиЭсПи" позволяет загрузить со специального загрузочного носителя безопасную операционную систему и целевое приложение (терминальный клиент или Web-браузер). Целостность ОС и прикладного ПО контролируется на этапе загрузки. Обмен данными между терминальным клиентом и терминальным сервером (находящимся внутри защищенного корпоративного периметра) защищается шифрованным IPsec-туннелем. Конфиденциальные данные, с которыми работает пользователь, не сохраняются на его локальном компьютере, а остаются внутри защищаемого периметра. В результате потеря пользовательского устройства не приводит к компрометации конфиденциальных данных.

Эшелонированная защита, различные уровни доверия

Мир не делится на белый и черный, поэтому и всех пользователей, пытающихся получить доступ к информации, нельзя разделить на однозначно добропорядочных и злоумышленников. Так, например, даже добропорядочному сотруднику бухгалтерии не нужно иметь доступ к инженерным разработкам компании. Верно и обратное: простому инженеру не должны быть доступны внутренние финансовые документы компании. Зачастую защищаемую информацию нужно разделить на несколько уровней конфиденциальности. Шифрование может помочь и в этом случае. Так, например, часть корпоративных данных может шифроваться только при передаче через Интернет и быть доступна в открытом виде в локальной сети. В то время как другая информация может передаваться в зашифрованном виде и внутри локальной сети тоже. Стандартные возможности семейства протоколов IPsec, реализованные в VPN-продуктах "С-Терра", позволяют создавать эшелонированную защиту с разделением на разные уровни доверия. Более того, программный комплекс "С-Терра Клиент" позволяет строить защищенные одноранговые полносвязные топологии внутри локальной сети. Такая возможность становится особенно актуальной для защиты беспроводной (Wi-Fi) локальной сети.

Новое время и новые вызовы. Шифрование в облаке

Стремительно растет популярность средств криптографической защиты, встраиваемых непосредственно в виртуальную инфраструктуру. При этом шифруются данные, не только передаваемые за пределы облака, но и находящиеся внутри его периметра.

В качестве примера такого решения можно привести "С-Терра Виртуальный шлюз", который может работать под большинством популярных гипервизоров (VMware ESX, Xen, Hyper-V, KVM и др.) и обеспечивает надежную защиту данных, передаваемых в зашифрованном виде как между виртуальными машинами, так и за пределы облачной инфраструктуры. При этом производительность и функциональность виртуального VPN-шлюза и шлюзов на аппаратной платформе идентичны, а его важным преимуществом является гибкая масштабируемость: по мере роста облачной инфраструктуры проще наращивать мощность виртуального шлюза, чем аппаратных модулей. Важно также отметить, что "С-Терра Виртуальный шлюз" сертифицирован ФСБ РФ и ФСТЭК РФ.

Обеспечение безопасности – не место для экспериментов

Важно обратить внимание как на репутацию компании – поставщика криптографического решения, время ее присутствия на рынке информационной безопасности (компания "С-Терра СиЭсПи" уже более 10 лет успешно работает в этой отрасли), так и на соответствие продукта современным требованиям и стандартам (ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012, VKO_GOSTR3410_2012_256), а также целостность и комплексность решений. Также во избежание архитектурных проблем необходимо соблюдать лучшие мировые практики, естественно, с учетом особенностей национального законодательства.

Использование этих критериев позволит вам создать не только функциональную, но и действительно надежную систему безопасности. ●

Разработка криптографического ПО – нетривиальная задача. В отличие от обычных пользовательских программ любая, даже мельчайшая, ошибка при разработке может привести к тому, что вся система безопасности перестанет отвечать ожидаемому уровню защищенности. При этом внешне система может работать нормально. Поэтому к выбору криптографического продукта следует подойти крайне ответственно.