ПОСТРОЕНИЕ КОРПОРАТИВНЫХ ЗАЩИЩЕННЫХ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Андрей Березин, anber@elvis.ru ,
Сергей Петренко,s.petrenko@confident.spb.ru

Конфидент №1, 2001г.

Сегодня широкое распространение получила реализация корпоративных систем информационной безопасности на основе одного из самых грамотных и экономически выгодных решений - с помощью технологии защищенных виртуальных частных сетей Virtual Private Network (VPN). Результаты анализа существующего спроса на предложения в области безопасности компьютерных сетей свидетельствуют о том, что технологии построения виртуальных защищенных частных сетей (VPN) являются остро востребованными и привлекают все больше внимания со стороны специалистов. Причина такого интереса заключается в том, что VPN технологии действительно позволяют не только существенно сократить расходы на содержание предприятием выделенных каналов связи с удаленными подразделениями (филиалами) и мобильными сотрудниками, но и реально повысить безопасность обмена конфиденциальной информацией.

ВВЕДЕНИЕ

Исторически, под одним термином VPN понимаются две достаточно большие и независимые группы совершено различных по своим целям, задачам и применяемым техническим решениям информационных технологий:

- технологии обеспечения гарантированного уровня транспортного обслуживания (качества сервиса) для корпоративного трафика, транспортируемого через публичные сети;
- технологии обеспечения необходимых гарантий информационной безопасности, (главным образом, конфиденциальности и целостности) корпоративных данных, передаваемых через публичные сети.

К первой группе VPN-технологий относятся такие специализированные технологии управления качеством обслуживания как RSVP, DiffServ, MPLS, а также некоторые базовые технологии построения публичных сетей со встроенными элементами поддержки QoS (Frame relay и ATM).

Вторая группа VPN-технологий выполняет функции авторизации абонентов корпоративных сетей и функции криптографической защиты передаваемых данных. Как правило, технологии этой группы представляет собой различные реализации механизма инкапсуляции стандартных сетевых пакетов канального (PPTP, L2F, L2TP) сетевого (SKIP, IPSec/IKE) и вышележащих уровней модели OSI/ISO (SOCKS, SSL/TLS).

ОЧЕВИДНО, ЧТО ДЛЯ ПОСТРОЕНИЯ "НАСТОЯЩЕЙ" ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ НЕОБХОДИМА ИНТЕГРАЦИЯ УКАЗАННЫХ ДВУХ ГРУПП VPN-ТЕХНОЛОГИЙ, ЧТО НА ПРАКТИКЕ НЕ ВСЕГДА ВОЗМОЖНО, ОСОБЕННО ПРИМЕНИТЕЛЬНО К VPN-ТЕХНОЛОГИЯМ ПЕРВОЙ ГРУППЫ. VPN-ТЕХНОЛОГИИ ВТОРОЙ ГРУППЫ, НАОБОРОТ, РАЗВИВАЮТСЯ БОЛЕЕ БЫСТРЫМИ ТЕМПАМИ И, ПО ЭТОЙ ПРИЧИНЕ, УЖЕ СЕГОДНЯ КОРПОРАТИВНЫЕ РАСПРЕДЕЛЕННЫЕ КОРПОРАЦИИ МОГУТ ИХ ИСПОЛЬЗОВАТЬ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. О VPN-ТЕХНОЛОГИЯХ ЭТОЙ ГРУППЫ И ПОЙДЕТ РЕЧЬ В ДАННОЙ СТАТЬЕ.

ПРОБЛЕМЫ КОРПОРАТИВНОГО ЗАКАЗЧИКА

Построение VPN для распределенных компаний даже с небольшим количеством удаленных (5-10) подразделений (филиалов), как правило, является достаточно трудоемкой задачей, сложность которой обуславливается следующими основными причинами:

- значительная *гетерогенность* используемых аппаратно-программных платформ;
- *разнообразие* существующих задач (защищенный обмен между головным офисом и филиалами, офисом и мобильными или удаленными сотрудниками, сегментами внутренней сети компании);
- необходимость построения *централизованной системы управления* всей корпоративной VPN;
- *узкая полоса пропускания* и откровенно плохое качество существующих каналов связи, особенно с региональными подразделениями и т.д.

Сложности построения корпоративных VPN усугубляются еще и тем, что, как правило, корпоративные заказчики предъявляют к VPN достаточно жесткие требования к:

- *масштабируемости* применяемых технических решений;
- *интегрируемости* с уже существующими средствами;
- *легальности используемых алгоритмов и решений*;
- *пропускной способности* защищаемой сети;
- *стойкости* применяемых криптоалгоритмов;
- *унифицируемости* VPN решения;
- *общей совокупной стоимости* построения корпоративной VPN.

Не трудно заметить, что большинство из перечисленных выше требований находятся в явном противоречии друг с другом. Поэтому, как правило, на практике приходится либо пренебрегать некоторыми из перечисленных требований, либо строить комбинированные VPN на базе существующих решений:

- VPN на базе сетевых операционных систем;
- VPN на базе маршрутизаторов;
- VPN на базе межсетевых экранов (МЭ);
- VPN на базе специализированного программного обеспечения.

Каждое из упомянутых решений имеет свои достоинства и недостатки, которые рассмотрим на примере наиболее часто встречающихся в России VPN продуктов.

ВАРИАНТЫ ПОСТРОЕНИЯ VPN

Построение VPN на базе сетевой ОС, является достаточно удобным и дешевым средством создания инфраструктуры защищенных виртуальных каналов. Сегодня в России наибольшее распространение среди сетевых операционных систем (ОС), позволяющих стоить VPN штатными средствами самой ОС, получила Windows NT.

По мнению специалистов, данное решение является оптимальным для построения VPN внутри локальных сетей (localnet-VPN) или домена Windows NT, а также для построения intranet- и externet-VPN для небольших компаний для защиты некритичной для их бизнеса информации. В то же время крупный бизнес вряд ли доверит свои секреты этому решению, поскольку многочисленные испытания VPN, построенных на базе Windows NT показали, что используемый в этой ОС протокол PPTP имеет достаточно большое количество уязвимостей:

- применение функции хеширования паролей и протокола аутентификации CHAP;
- ограниченность протокола шифрования в одноранговых сетях (MPPE);
- открытость для атаки на этапе конфигурации соединения и атак типа "отказ в обслуживании";
- недостаточная проработанность вопросов обеспечения безопасности в данной ОС и др.

Поэтому в своей новой ОС - Windows 2000 - компания Microsoft сделала ставку на реализацию более современного протокола IPSec (см. далее). Однако, результаты первых независимых тестов, показали на присутствие серьезных проблем с безопасностью и этой ОС.

Построение VPN на базе маршрутизаторов. В России безусловным лидером на этом рынке является компания Cisco Systems.

Построение VPN каналов на базе маршрутизаторов компании Cisco осуществляется средствами самой ОС, начиная с версии Cisco IOS 12.x. Если на пограничные маршрутизаторы Cisco других отделений компании установлена данная ОС, то имеется возможность сформировать корпоративную VPN, состоящую из совокупности виртуальных защищенных туннелей типа "точка-точка" от одного мартшутизатора к другому (см. рис.1). Как правило, для шифрования данных в канале "по умолчанию" используется американский криптоалгоритм DES (Data Encryption Standard) с длиной ключа 56 бит.

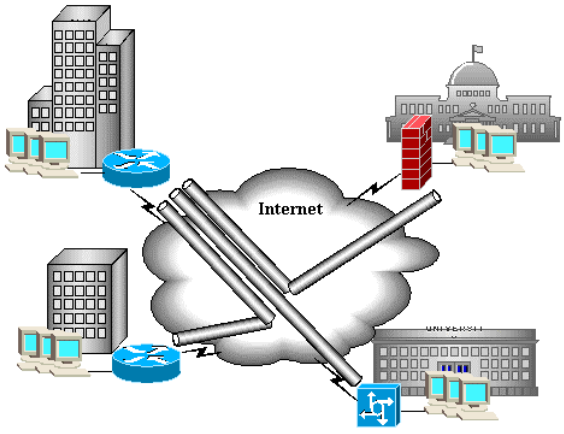


Рис.1. Типовая схема построения корпоративной VPN на базе маршрутизаторов Cisco.

Сравнительно недавно в прайс-листах российских дилеров появился новый продукт компании - Cisco VPN client, который позволяет стоить защищенный соединения "точка-точка" между рабочими станциями (в т.ч. и удаленными) и маршрутизаторами Cisco, что делает возможным построение internet- и localnet-VPN.

Для организации VPN туннеля маршрутизаторы компании Cisco в настоящее время используют протокол канального уровня L2TP. Этот протокол обеспечивает инкапсулирование протоколов сетевого уровня (IP, IPX, NetBEUI и др.) в пакеты канального уровня (PPP) для передачи по сетям, поддерживающим доставку дейтаграмм в каналах "точка-точка". Основным преимуществом L2TP является его независимость от транспортного уровня, что позволяет использовать его в гетерогенных сетях. Достаточно сильным качеством L2TP является его поддержка в ОС Windows 2000, что в принципе позволяет строить комбинированные VPN на базе продуктов Microsoft и Cisco. Однако, "канальная природа" L2TP протокола является причиной его существенного недостатка: для гарантированной передачи защищенного пакета через составные сети все промежуточные маршрутизаторы должны поддерживать этот протокол, что, очевидно, достаточно трудно гарантировать. Видимо, по этой причине компания Cisco сегодня обратила более пристальный взгляд на продвижение более современного VPN протокола - IPSec.

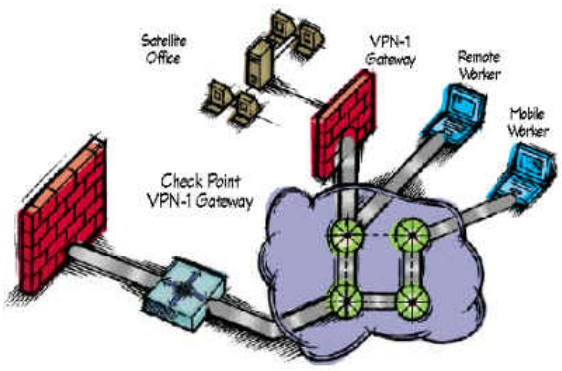
Сегодня IPSec является одним из самых проработанных и совершенных Интернет-протоколов в плане безопасности. В частности, IPSec обеспечивает аутентификацию, проверку целостности и шифрование сообщений на уровне каждого пакета (для управления криптографическими ключами IPSec использует протокол IKE, хорошо зарекомендовавший себя в своей более ранней версии Oakley). Кроме того, работа протокола на сетевом уровне является одним из стратегических преимуществ IPSec, поскольку VPN на его базе работают полностью прозрачно как для всех без исключения приложений и сетевых сервисов, так и для сетей передачи данных канального уровня. Также IPSec позволяет маршрутизировать зашифрованные пакеты сетям без дополнительной настойки промежуточных маршрутизаторов, поскольку сохраняет стандартный IP-заголовок, принятый в IPv4. И, наконец, тот факт, что IPSec включен в качестве неотъемлемой части в будущий Интернет протокол IPv6, делает его еще более привлекательным для организации корпоративных VPN.

К сожалению, IPSec присущи и некоторые недостатки: поддержка только стека TCP/IP и довольно большой объем служебной информации, который может вызвать существенное снижение скорости обмена данными на низкоскоростных каналах связи, пока, к сожалению, имеющих в России наибольшее распространение.

Возвращаясь к построению корпоративных VPN на базе маршрутизаторов, отметим, что основной задачей этих устройств является маршрутизация трафика, а значит, криптообработка пакетов является некоторой дополнительной функцией, требующей, очевидно, дополнительных вычислительных ресурсов. Другими словами, если ваш маршрутизатор имеет достаточно большой запас по производительности, то ему вполне можно "поручить" и формирование VPN.

Построение VPN на базе межсетевых экранов. Немалое количество специалистов по информационной безопасности считают, что построение VPN на базе МЭ является единственным оптимальным решением для обеспечения комплексной безопасности корпоративной информационной системы от атак из открытых сетей. Действительно, объединение функций МЭ и VPN шлюза в одной точке под контролем единой системы управления и аудита является решением не только технически грамотным, но и удобным для администрирования. В качестве примера рассмотрим типовую схему построения корпоративной VPN на базе популярного в России программного продукта компании CheckPoint Software Technologies - CheckPoint Firewall-1/VPN-1.

МЭ CheckPoint Firewall-1 позволяет в рамках единого комплекса построить глубокоэшелонированный рубеж обороны для корпоративных информационных ресурсов. В состав такого комплекса входит как сам CheckPoint FW-1, так и набор продуктов для построения корпоративной VPN - CheckPoint VPN-1, средства обнаружения вторжений RealSecure, средства управления полосой пропускания FloodGate и т.д.



Подсистема построения VPN на базе CheckPoint FW-1 включает в себя программные продукты VPN-1 Gateway и VPN-1 Appliance, предназначенные для построения intranet-VPN; VPN-1 SecureServer, предназначенный для защиты выделенных серверов, а также VPN-1 SecuRemote и VPN-1 SecureClient - для построения internet/externet/localnet-VPN (см. рис. 2). Для шифрации трафика в каналах CheckPoint Firewall-1 использует известные криптоалгоритмы DES, CAST, IDEA, FWZ и др.

Рис.2. Типовая схема корпоративной VPN на базе CheckPoint FW-1/VPN-1

Весь продуктовый ряд CheckPoint VPN-1 реализован на базе открытых стандартов (IPSec), имеет развитую систему аутентификации пользователей, поддерживает взаимодействие с внешними системами распределения открытых ключей (PKI), позволяет стоить централизованную систему управления и аудита и т.д. Поэтому не удивительно, что продукция данной компании занимает 52% мирового рынка VPN, согласно последнему исследованию Dataquest.

В итоге, можно сказать, что построение VPN на базе МЭ выглядит вполне грамотным и сбалансированным решением. Однако, ему тоже присущи некоторые недостатки. Прежде всего, это высокая стоимость такого решения в пересчете на одно рабочее место корпоративной сети и достаточно высокие требования к производительности МЭ даже при умеренной ширине полосы пропускания выходного канала связи. Очевидно, что вопросу производительности МЭ должно уделяться повышенное внимание при построении VPN, поскольку фактически вся нагрузка по криптообработке трафика ложится на МЭ. Причем даже в том случае, когда мы хотим объединить в localnet-VPN двух клиентов локальной сети.

ПОСТРОЕНИЕ КОРПОРАТИВНЫХ VPN В РОССИЙСКИХ УСЛОВИЯХ

До сих пор мы говорили о различных вариантах построения корпоративных VPN на базе продуктов исключительно западных производителей, поскольку, к сожалению, сетевые ОС и маршрутизаторы в России не производятся, а МЭ с функциями VPN начали появляться только недавно. Однако, при всех своих технологических преимуществах западные VPN продукты имеют один общий недостаток, который в некоторых случаях может обесценить все имеющиеся достоинства. Речь идет о тех случаях, когда построение корпоративной VPN необходимо увязывать с положениями существующего сегодня в РФ законодательства.

Одним из неотъемлемых и, пожалуй, базовых элементов любого VPN продукта является наличие в нем средств (модулей, аппаратных устройств и т.д.), осуществляющих криптографическое преобразование (шифрацию) данных. Вопросы применения криптографии во всех развитых странах мира подвержены достаточно жесткому законодательному регулированию со стороны государства. Как правило, регулирование это касается трех сторон применения криптографии:

- сертификация средств криптографической защиты информации (СКЗИ);
- лицензирование деятельности организаций и предприятий, связанной с производством, распространением, эксплуатацией и т.д. СКЗИ;
- экспортно-импортные ограничения на СКЗИ.

Цель такого регулирования достаточно проста: для обеспечения собственной безопасности любому государству необходимо в максимальной степени обеспечить контроль за циркулирующей в компьютерных сетях информации, причем желательно не только в своих национальных сетях и не только своей информации. Так, например, большинство имеющихся на российском рынке западных VPN продуктов поставляются с криптоалгоритмом симметричного шифрования DES с длиной ключа 56 бит. В таблице 1. приведены ориентировочные расчеты времени и материальных средств, которые необходимо затратить на взлом этого алгоритма методом "грубой силы", т.е. путем полного перебора всех возможных ключей с использованием как стандартных компьютеров, так и специализированных криптоаналитических аппаратных средств.

Таблица 1.Сравнительный анализ трудоемкости взлома криптоалгоритма DES с длиной ключа 56 бит

№	Тип атакующего	Бюджет атакующего	Средства атаки	Время проведения успешной атаки
1	Хакер	до $500	ПК	Несколько десятков лет
2	Небольшие фирмы	до $10 тыс.	FPGA	18 месяцев
3	Корпоративные департаменты	до $300 тыс.	FPGA ASIC	19 дней 3 дня
4	Большие корпорации	до $10 млн.	FPGA; ASIC; суперЭВМ	13 часов 6 минут
5	Специализированные агентства	?	?	?

Примечание: Данные взяты из книги А.А.Петрова: "Компьютерная безопасность. Криптографические методы защиты", М., 2000

Характерно, что для приобретения СКЗИ с более криптостойким алгоритмом TripleDES с длиной ключа 168 бит иностранным компаниям необходимо получать специальное разрешение со стороны Государственного департамента США.

Российское законодательство также имеет ряд законодательных актов и инициатив, призванных регулировать использование СКЗИ на территории РФ. Отметим кратко те положения, которые прямо относятся к построению VPN:

1. Деятельность организаций и предприятий, связанная с проведением работ (производство, реализация, эксплуатация и т.д.) в области защиты информации, подлежит обязательному лицензированию ФАПСИ и ФСБ. Лицензирование деятельности в области защиты информации и работ, связанных с созданием средств защиты информации (СЗИ) осуществляется Гостехкомиссией и ФАПСИ в рамках их компетенции.

2. Организация сертификации СЗИ и СКЗИ, в том числе и импортного производства, возложена на Гостехкомиссию и ФАПСИ при Президенте РФ. При этом органы ФАПСИ могут проводить сертификацию только средств криптографии и шифрования (СКЗИ). Сертификацию СЗИ, не использующих методы криптографии и шифрования, организует Гостехкомиссия РФ.

3. Обязательной сертификации подлежат СЗИ и СКЗИ, в том числе и иностранного производства, предназначенные для использования в информационных системах с обработкой информации, представляющей государственную тайну.

4. Государственным организациям, предприятиям и банкам, а также предприятиям, работающим по государственному заказу, и предприятиям и организациям при их информационном взаимодействии с ЦБ РФ, запрещено использование СЗИ и СКЗИ, не имеющих сертификатов государственного образца.

5. Ввоз-вывоз СКЗИ может быть разрешен таможенными органами только на основании соответствующего разрешения ФАПСИ после проведения необходимой технической экспертизы. Это в первую очередь требует обязательного проведения технической экспертизы СЗИ при пересечении границы РФ на предмет их отнесения к шифровальным средствам.

Из всего вышесказанного можно сделать следующий вывод: проектировщикам корпоративных VPN в некоторых случаях придется серьезным образом обратить внимание на отечественных производителей VPN-продуктов.

VPN ПРОДУКТЫ РОССИЙСКИХ ПРОИЗВОДИТЕЛЕЙ

Всех российских производителей VPN-продуктов можно разделить на две группы: компании, предлагающие VPN-продукты, разработанные на базе известных мировых стандартов, и компании, предлагающие VPN-продукты на основе собственных разработок. Для сведения читателя, вторая группа на сегодня выглядит более многочисленной.

Как правило, для построения корпоративной VPN более предпочтительным выглядит выбор в пользу VPN продуктов из первой группы, т.е. реализующие известные и всесторонне изученные мировые стандарты. Интерес к таким продуктам еще более повышается, если они реализуют сильные отечественные криптографические алгоритмы, такой, например, как (кстати, совершенно открытый) криптоалгоритм ГОСТ 28147-89 с длиной ключа 256 бит.

Среди отечественных производителей VPN продуктов указанной группы наибольшую известность и распространенность на сегодня имеют, пожалуй, два: криптографический комплекс "Шифратор IP-пакетов" (ШИП) производства МО ПНИЭИ и продуктовая линейка программных продуктов серии ЗАСТАВА от компании ЭЛВИС+. Поскольку указанные продукты являются специализированными VPN продуктами, набор предоставляемых ими функциональных возможностей в некоторый случаях даже шире, чем у рассмотренных ранее западных конкурентов, а криптостойкость используемых криптоалгоритмов, безусловно, многократно превышает соответствующие параметры поставляемых в Россию западных функциональных аналогов.

А) Криптографический комплекс ШИП

КК ШИП представляет собой отдельное программно-апаратное устройство (криптошлюз), осуществляющее сквозное шифрование всего исходящего из локальной сети трафика на базе реализации протокола SKIP (Simple Key management for Internet Protocol).

В КК ШИП входят следующие продукты:

- Непосредственно сам программно-аппаратный комплекс "ШИП", который осуществляет защиту данных, предаваемых между узлами сети в соответствии с ГОСТ 28147-89;
- Центр управления ключевой структурой (ЦУКС), который используется для периодической смены ключей шифрования (для чего используется стандартная служба DNS), аудита работы VPN и др.
- Для построения internet-VPN служит программный комплекс "Игла-П", который устанавливается непосредственно на рабочую станцию (ноутбук) удаленного пользователя, а также может самостоятельно выступать в качестве криптомаршрутизатора.

Схема организации корпоративной VPN на базе КК "ШИП" показана на рис. 3.

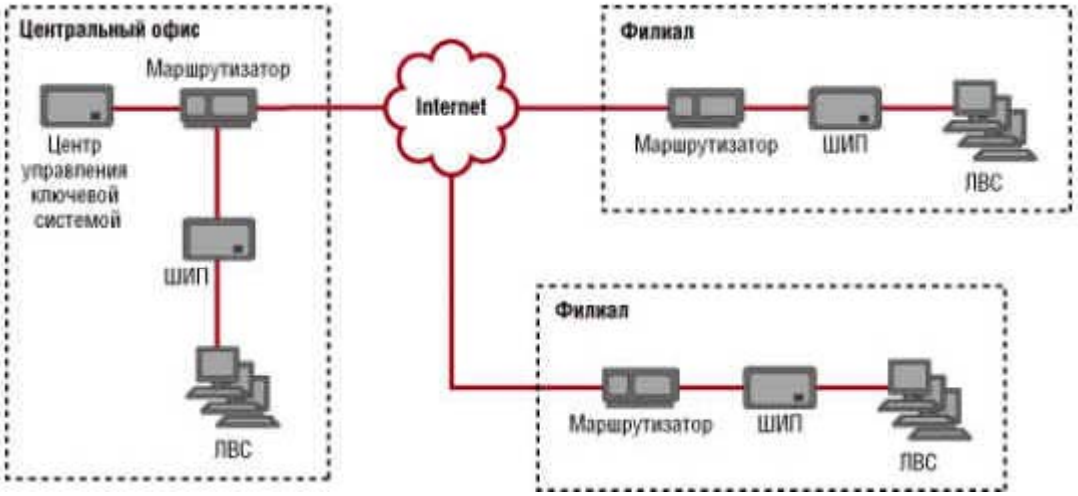


Рис.3. Типовая схема включения КК "ШИП"

Описание работы и опыта эксплуатации КК "ШИП" можно найти на сайте производителя.

Б) VPN продукты ЗАСТАВА

В настоящее время продуктовая линейка программных продуктов ЗАСТАВА (текущей) версии 2.5. включает в себя девять программных продуктов различного назначения, работающих под управлением ОС Windows 95/98/NT и Solaris SunSparc/Intel:

1. МЭ ЗАСТАВА (с возможностью организации VPN);
2. ЗАСТАВА - Персональный клиент;
3. ЗАСТАВА - Корпоративный клиент;
4. Центр управления ЗАСТАВА;
5. ЗАСТАВА - Сервер;
6. ЗАСТАВА - Офис;
7. Персональный центр сертификации ЗАСТАВА;
8. Корпоративный центр сертификации ЗАСТАВА;
9. Сервер сертификатов ЗАСТАВА.

Как и КК "ШИП", ЗАСТАВА версии 2.5. для организации защищенных каналов связи использует протокол SKIP. Наличие полного продуктового ряда - клиент-сервер-шлюз позволяет строить на базе ЗАСТАВЫ разнообразные VPN решения, как по функциональности, так и по стоимости. При этом защищенные каналы могут быть организованы как вне, так и внутри защищаемой ЛС (рис. 4).

Надежное и проработанные решения по управлению ключевой инфраструктурой (с использованием протоколов CDP и LDAP), а также возможность поддержки как закрытых, так и открытых соединений и совместимость с VPN-продуктами других производителей (включая Sun Microsystems и CheckPoint) тоже делает ЗАСТАВУ весьма привлекательным продуктом для построения корпоративных VPN различного масштаба: от нескольких десятков (Персональный цент сертификации) до нескольких десятков тысяч рабочих станций и серверов (Корпоративный центр сертификации).

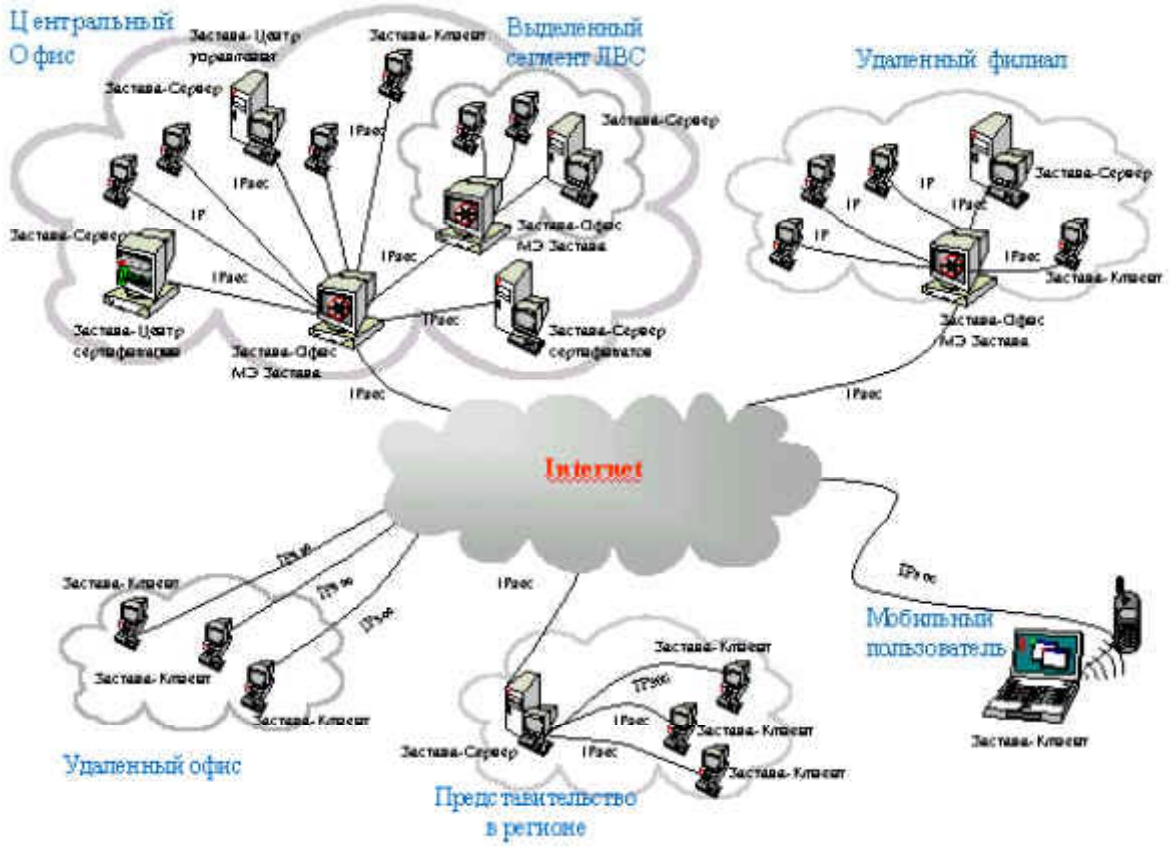


Рис.4. Схема корпоративной VPN на базе VPN продуктов ЗАСТАВА.

Нельзя не упомянуть еще одно качество ЗАСТАВЫ, которое делает эти продукты по-настоящему уникальными для российского рынка. VPN-продукты ЗАСТАВА не имеют встроенных криптоалгоритмов; все криптоалгоритмы носят внешний характер и взаимодействуют с базовым ПО через специально разработанный криптоинтерфейс. Это качество, во-первых, снимает с данного ПО экспорто-импортные ограничения, свойственные другим VPN продуктам, а во-вторых, предоставляет пользователю полную свободу выбора криптоалгоритма для построения своей VPN. При этом в рамках одной сети существует возможность построения единой VPN на базе нескольких криптоалгоритмов, поскольку ЗАСТАВА одновременно может поддерживать работу до 256 криптомодулей. В настоящее время ЗАСТАВА работает с двумя основными модулями преобразования информации: модуль кодирования информации фирмы ЛАН-Крипто , реализующий алгоритм ВЕСТА-2М - отраслевой стандарт газовой промышленности России (ОСТ 51 06 98), и криптомодуль "Cripton-Emulator" фирмы АНКАД, реализующий базовый отечественный криптоалгоритм ГОСТ 28147-89. Длина ключа в обоих алгоритмах - 256 бит, что гарантирует высокую их стойкость.

РЕКОМЕНДАЦИИ ПО ВЫБОРУ VPN ПРОДУКТОВ

Рекомендации по выбору средств построения корпоративных VPN целесообразно разделить на три группы в соответствии с организационно-правовой формой компании-заказчика и уровня секретности информации, которая будет обрабатываться в пределах проектируемой VPN:

1. Предприятия и организации (не только государственные), работающие с информацией, представляющей государственную тайну.
2. Государственные учреждения, не работающие с государственной тайной.
3. Негосударственные учреждения, желающие ограничить доступ к служебной, деловой, технической, экономической и другим видам информации, не представляющей государственной тайны.

В соответствии с вышеизложенными положениями российского законодательства для компаний первой и второй группы на сегодня нет другой альтернативы, кроме как изначально ориентироваться на отечественных производителей VPN-продуктов, имеющих соответствующие лицензии и сертификаты Гостехкомиссии и ФАПСИ. Присутствующая сегодня тенденция явно свидетельствует о том, что список таких продуктов будет постоянно расширяться. Однако, необходимо иметь в виду, что работа с информацией, представляющей государственную тайну, сопряжена с необходимостью выполнения достаточно большого объема различных организационно-технических мероприятий для удовлетворения большого количества разнообразных

требований. Как показала практика, сегодня ни один из отечественных VPN продуктов сам по себе не обеспечивает возможности защиты такого вида информации.

Из рассмотренных в рамках данной статьи VPN продуктов КК "ШИП" можно рекомендовать использовать в тех случаях, когда имеющиеся партнеры по производству/бизнесу уже работают с этим продуктом и если компания имеет надежные каналы связи для поддержки работоспособности ключевой системы.

Сертифицированные Гостехкомиссией РФ продукты ЗАСТАВА целесообразно использовать в тех случаях, когда компании необходимо одновременно обеспечить наличие как защищенных, так и открытых соединений в Интернет с удаленными подразделениями/сотрудниками. Кроме того, ЗАСТАВА представляет собой оптимальное решение также и в тех случаях, когда компания предпочитает иметь масштабируемое решение по созданию собственной ключевой инфраструктуры, способную работать с изменяющимся количеством абонентов.

Наибольшей свободой выбора обладают, очевидно, компании третьей группы, которые сегодня практически могут использовать любые VPN продукты в т.ч. и западного производства. Тут на первый план выходят такие параметры как стоимость, функциональность, качество, производительность, криптостойкость, трудоемкость обслуживания, совместимость с уже имеющимся парком оборудования и т.д. Информация табл. 2, подготовленная на базе открытых публикаций производителей, дает некоторое представление о этих параметрах.

Если попытаться дать общую рекомендацию, то, по мнению специалистов, оптимальным решением с точки зрения обеспечения информационной безопасности является построения VPN на базе МЭ. Хорошими кандидатами на эту роль являются CheckPoint FW-1/VPN-1 в случае, если необходима богатая функциональность продукта, а также Cisco PIX Firewall - если необходима большая производительность и меньшая стоимость решения. Из отечественных МЭ можно рекомендовать продукт ФПСУ-IP компании "Амикон", DataGuard компании "Сигнал-Ком", а также комплекс МЭ ЗАСТАВА с модулем построения VPN.

Довольно привлекательным решением выглядит построение корпоративной VPN на базе ЗАСТАВЫ с модулем кодирования ВЕСТА-2М, поскольку помимо хорошей масштабируемости, функциональности и высокой стойкости, это решение позволяет легко и без дополнительных затрат (путем смены криптомодуля) решить проблему легитимности применения средств преобразования информации в случае ужесточения российского законодательства в этой области.

Таблица 2. Сравнительные параметры некоторых VPN продуктов.

№	Параметр	Windows NT/2000	Cisco IOS 12.x	CheckPoint FW-1	КК "ШИП"	ЗАСТАВА 2.5
1	Страна- производитель	США	США	Израиль	Россия	Россия
2	Протокол, реализующий виртуальные туннели	PPTP/IPSec	L2TP/IPSec	IPSec	SKIP	SKIP
3	Способ реализации	программный	программный	программный	программно-аппаратный	программный
4	Поддерживаемые аппаратные платформы	Intel	Cisco	Intel, SunSPARC, HP и др.	Intel	Intel, SunSPARC
5	Поддерживаемые операционные системы	-	IOS 12.x	Windows 95/98/ NT/2000; Soliaris; Linux, HP-UX и др.	FreeBSD	Windows 95/98/NT; Soliaris
6	Аутентификация и поддержка целостности пакетов	Нет/Да	Да	Да	Да	Да
7	Поддержка внешних устройств усиленной аутентификации пользователей	Да	Нет	Да	Да	Да
8	Возможность центрального администрирования VPN	Да	Да	Да	Нет	Да

9	Используемые криптоалгоритмы (алгоритмы преобразования информации)	DES; 3DES	DES; 3DES	DES; 3DES; CAST; IDEA и др.	ГОСТ 28147-89	ГОСТ 28147-89; ВЕСТА-2М; DES; 3DES
10	Максимальная криптостойкость (длина ключа, бит)	168	168	168	256	256
11	Количество одновременно используемых криптоалгоритмов	1	1	1	1	256
12	Наличие открытого криптоинтерфейса	Да	Нет	Нет	Нет	Да
13	Ведение журнала аудита	Да	Да	Да	Да	Да
14	Максимальная производительность (АП - аппаратная платформа)	зависит от АП	250 Мб/с	зависит от АП	8 Мб/с	зависит от АП
15	Наличие клиентских; серверных; шлюзовых частей	Да Да Нет	Да Нет Да	Да Да Да	Да Нет Да	Да Да Да
16	Средства построения собственной ключевой системы	Нет	Нет	Да	Да	Да
17	Наличие сертификата Гостехкомиссии	Нет	Да, на отдельные ихзделия	Да, на партии изделий	Нет	Да на производство
18	Наличие сертификата ФАПСИ (в т.ч. на внешние криптомодули)	Нет	Нет	Нет	Да	Да
19	Поддержка внешних систем распределения ключей и сертификатов (PKI)	Да	Да	Да	Нет	Да
20	Поддержка внешних средств защиты от НСД	Да	-	Да	Аккорд	Аккорд; Dallas Lock; Secur ID

Перспективы рынка VPN продуктов

Рынок VPN продуктов постоянно расширяется, поскольку интерес к этой технологии в последнее время усиливается. Вместе с тем, информационная безопасность корпоративных сетей и применение криптографии для защиты информации при передаче по открытым каналам связи являются достаточно "тонкими" областями знаний, поэтому даже малейшая ошибка при проектировании корпоративной VPN может привести к фатальным для компании результатам. По этой причине необходимо быть особенно осмотрительным и даже скрупулезным как при выборе VPN продуктов, так и при проектировании самой VPN.
