VPN: МОЗАИКА ПРИКЛАДНЫХ РЕШЕНИЙ

Турская Елена Романовна
Менеджер ОАО «ЭЛВИС+»
Сетевой журнал
№12.2000

Современный бизнес предъявляет высокие требования к системам защиты и безопасности всех информационных ресурсов.

Высокая степень мобильности и масштабируемости программных решений в области защиты относительно различных системно-технических платформ, интероперабельность используемых решений с программами и оборудованием третьих фирм, простота установки, конфигурирования и эксплуатации, возможность управления в соответствии с централизованной политикой безопасности являются важными требованиями для крупных корпораций.

Решения по защите сетевых информационных ресурсов предприятий и защите информации, передаваемой по открытым сетям, сегодня могут быть реализованы на основе сертифицированных отечественных VPN-продуктов и совместимых с ними зарубежных продуктов, реализующих технологии FW для безопасного взаимодействия с внешней средой, и токенов для аутентификации пользователей сети.

Для небольших предприятий, использующих до десятка узлов, подойдут VPN-продукты, имеющие удобный графический интерфейс и допускающие локальное конфигурирование без применения централизованного управления.

Для крупных предприятий предпочтительнее системы с центром управления, обеспечивающим оперативное управление узлами, а также PKI третьих производителей, поддерживающие создание многослойной инфраструктуры сертификатов пользователей.

По мере роста компании технология VPN позволяет легко наращивать возможности и переходить к централизованному управлению.

В статье представлены типовые решения, применимые для множества задач и зависящие прежде всего от: топологии бизнес-процессов (а не только от топологии сетей); специфики бизнес-процессов с гибко настаиваемой политикой безопасности.

В предложенных решениях может использоваться масштабируемый ряд продуктов, с возможностями:

- защиты информации независимо от средств и среды передачи (спутниковые, оптические, телефонные, радиорелейные линии);
- защиты любых приложений, не требуя их изменений;
- совершенной "прозрачности" для конечных пользователей;
- реализации масштабируемых систем защиты и их наращивания;
- защиты информационной системы от атак из внешней среды;
- гарантирования информации от перехвата и изменения не только на внешних соединениях, но и на внутренних сетях корпорации;
- использования алгоритмов криптования посредством подключения плагинов;
- аутентифицирования отдельных пользователей VPN, используя любые средства - смарт-карты, USB-устройства и т. д.

Объединение офисов в защищенную сеть

Распределенный бизнес, управляемый из нескольких офисов, нуждается не только в защите каждого из этих подразделений, но и в интеграции всех их в систему с единым информационным пространством.

Суть предлагаемого решения (схема 1) в построении периметра защищенной корпоративной сети на основе технологии VPN. Решение базируется на применении ПО VPN-Офис для сетевой защиты компьютеров сети каждого офиса и защиты от несанкционированного доступа из внешних сетей. Для защиты трафика между центральным офисом и филиалами на шлюз каждой локальной сети устанавливается VPN-Офис, скрывающий внутреннюю топологию сетей офисов.

Преимущество этого решения заключается в его масштабируемости - доступ удаленным и мобильным пользователям можно предоставлять по мере необходимости. В случае объединения с небольшим филиалом, где компьютеров немного, можно установить на каждое рабочее место ПО VPN-Клиент или на сервер, содержащий критичную информацию, - VPN-Сервер. В конкретном случае решение принимается исходя из экономической целесообразности того или иного набора продуктов.

Защищенный доступ удаленных и мобильных пользователей

Условия, складывающиеся на рынке, часто требуют присутствия представителей компании в самых отдаленных уголках. И тут для эффективного решения возникающих задач необходим не только транспорт, но и средства коммуникаций.

В этом случае необходимо дополнить корпоративную сеть защищенными мобильными рабочими местами для перемещающихся сотрудников и обеспечить их доступ к сети компании по защищенному каналу. Другими словами, защищенный периметр корпоративной сети должен иметь возможность, "растягиваясь", проходить сквозь любые IP-сети общего доступа, оставаясь при этом таким же надежным, как если бы никто из сотрудников не покидал офисов, т. е. обеспечивая установленный уровень конфиденциальности и целостности.

При установке на входном шлюзе сети программного средства VPN-Офис или на корпоративном сервере (почтовом, баз данных, www-сервере) ПО VPN-Сервер, а на мобильном рабочем месте - VPN-Клиент, пользователь получает доступ к необходимым ресурсам компании по защищенному каналу независимо от местонахождения и способа подключения к Интернету.

Представленное на схеме 2 решение дает возможность получить доступ из любой точки мира, в том числе и с помощью мобильного телефона. Отличительная особенность этого решения заключается в возможности устанавливать защищенную связь с пользователями, имеющими изменяющиеся IP-адреса, по сертификату пользователя.

Благодаря аутентификации по паролю или смарт-карте, допускающей в VPN определенного пользователя, в случае кражи или потери компьютера посторонний не получит доступа к информации. Вся информация о пользователе, включая его сертификат и присвоенную ему конфигурацию VPN, хранится не в компьютере, а на смарт-карте. После того как смарт-карта вынута, эта информация уничтожается, и остается "голое" ПО, не позволяющее войти в VPN.

Система централизованного управления средствами защиты

Современная парадигма стратегии бизнеса предполагает не только тенденцию к использованию электронной коммерции (e-commerce), но и переход к реализации концепции электронного бизнеса (e-business). При этом принципиальным моментом является интеграция существующих и традиционных информационных ресурсов Интернет.

Применяемые для решения этих задач средства безопасности предполагают использование ключей шифрования (симметричного или асимметричного). Чем изощреннее система защиты, чем больше пользователей у информационной системы, тем сложнее управлять всеми необходимыми ключами системы, распределять и обновлять их.

Даже когда число пользователей информационной системы, имеющей все основные компоненты подсистемы защиты, не превышает сотни, реализовать все необходимые операции по управлению ключами без помощи специальных программных средств практически невозможно. Более того, ряд современных технологий информационной защиты неприменимы без компьютерной поддержки всех необходимых операций по управлению ключами. Именно поэтому одна из проблем в области сетевой информационной безопасности заключается в управлении средствами защиты, в частности, с помощью генерации ключей, их распределения, обновления, а также конфигурирования средств защиты.

Комплексные продукты VPN позволяют получить наиболее эффективное решение и обеспечить:

- централизованное управление и определение политики безопасности для всей системы;
- единую защищенную инфраструктуру (безопасность на сетевом и прикладном уровнях, PKI, аутентификацию, систему протоколирования и аудита);
- создание единых решений по безопасности для всех филиалов, дочерних и зависимых компаний;
- возможность наращивания инфраструктуры безопасности.

В рамках корпоративной политики безопасности генерация ключей осуществляется, как правило, в центральном аппарате, а конфигурирование средств защиты - на региональном уровне.

Создание системы централизованного управления средствами защиты (схема 3) базируется на использовании средств управления центра сертификации.

Центр сертификации предназначен для генерации ключей (секретных и соответствующих открытых), включая главный ключ центра сертификации. ПО центра сертификации представляет собой базу данных, где хранятся ключи и сертификаты вместе с данными об их владельце и ведется регистрационный журнал, включающий все действия по администрированию продукта. Центр сертификации устанавливается на выделенный компьютер с ОС Windows NT. В процессе генерации открытый ключ оформляется в виде сертификатов X.509 с информацией о его владельце, организации, отделе, идентификационном номере и т.п. Для гарантии подлинности производится подпись сертификатов главным ключом центра сертификации.

Главный секретный ключ хранится в локальной базе данных сертификационного центра и выдается на внешний носитель только в случае замены рабочего места сертификации или создания резервной копии базы данных.

Открытые сертификаты переносятся на корпоративный сервер сертификатов в виде файлов по сети или на магнитных носителях.

Сервер сертификатов предназначен для автоматического предоставления сертификатов открытых ключей удаленным узлам, на которых установлены программные продукты VPN-Офис, VPN-Сервер и VPN-Клиент. Сертификаты передаются по CDP-протоколу после запроса со стороны удаленного узла. VPN-Сервер сертификатов устанавливается на сервер с операционной системой Windows NT.

На сервере сертификатов ведется собственный регистрационный журнал, где отмечается время и характер совершаемых в процессе работы действий (например: вход в Сервер сертификатов и выход из него, регистрация, выдача и маркировка сертификата как скомпрометированного и т. д.). При просмотре журнала возможно определение отображаемых событий. VPN-Сервер сертификатов дополнительно может получать сертификаты от узлов, на которых установлены продукты VPN-Офис и VPN-Клиент, по протоколам CDP и LDAP.

Центр управления предназначен для подготовки администратором безопасности терминальных пакетов для продуктов VPN-Корпоративный клиент и конфигураций для продуктов VPN-Персональный клиент соответственно.

Терминальные пакеты могут быть защищены посредством электронно-цифровой подписи центра сертификации, которая переносится на центр управления при помощи дискеты или токена.Терминальный пакет содержит следующие компоненты и настройки для работы ПО VPN-Корпоративный клиент:

- сертификаты центра сертификации, локальный сертификат пользователя с его секретным ключом, открытые сертификаты партнеров по взаимодействию;
- защищенные и незащищенные соединения с заданными параметрами;

- CDP-запросы для получения открытых сертификатов партнеров по взаимодействию. При этом обеспечивается автоматическое получение сертификата с сервера сертификатов во время загрузки корпоративного клиента;
- определение токена в качестве носителя локального сертификата, что позволяет хранить секретный ключ пользователя на внешнем носителе (дискета, смарт-карта, токен, удовлетворяющий стандарту PKCS №11).

Защита почтовой системы

Одним из распространенных сервисов в корпоративных распределенных сетях является электронная почта. Как правило, именно с нее начинается развитие информационных систем. В условиях корпораций, имеющих разветвленную сеть филиалов и дочерних предприятий, целостность и безопасность электронного почтового обмена и его конфиденциальность - первейшая задача обеспечения информационной безопасности.

Существенно, что данная задача должна решаться в условиях территориальной распределенности подсетей, почтовых серверов и пользователей, в том числе находящихся вне периметра корпоративной сети и имеющих доступ к корпоративной почте из сетей общего доступа. Конфиденциальность передачи сообщений, а также идентификация и аутентификация пользователей - вот наиболее часто встречающиеся требования.

Для создания системы защищенного почтового обмена внутри распределенной корпоративной сети используется решение, которое заключается в установке VPN-продуктов как на почтовые серверы организации, так и на персональные компьютеры. Комплексные VPN-продукты экономически наиболее эффективны, имеют тонкие возможности индивидуальной настройки, просты в эксплуатации и масштабируемы до произвольного числа пользователей. При необходимости могут быть учтены любые требования по использованию тех или иных методов шифрования и защиты данных и информации.

Преимущество подобного решения перед специализированными защищенными почтовыми системами: - полная прозрачность для пользователей: им не надо при отправке письма заниматься выбором ключей для шифрования. Почтовые серверы компании, размещенные в различных местах распределенной интрасети, могут быть защищены программным средством VPN-Сервер, а рабочие места пользователей - продуктом VPN-Клиент.

На схеме 4 один из почтовых серверов (внешний) располагается в так называемой демилитаризованной зоне (ДМЗ), доступной внешним по отношению к корпоративной сети абонентам, что обеспечивает возможность безопасной работы абонентов с другими почтовыми серверами "вне корпоративной сети". Для защиты подсетей, расположенных за шлюзом, от неавторизованного доступа из открытых сетей устанавливается ПО VPN-Офис.

Управление политикой безопасности осуществляется с помощью программного средства VPN-Центр управления.

Каждый корпоративный почтовый пользователь - это объект почтовый клиент. Все они определяются списком идентификаторов - сертификатов открытых ключей.

Все закрытые корпоративные почтовые серверы образуют другую защищенную группу - защищенные почтовые серверы. Почтовый сервер, размещенный в ДМЗ, - это третий защищенный объект - внешний почтовый сервер.

Объект Интернет определен как полное адресное пространство сети Интернет за исключением IP-адресов, используемых в корпоративной сети.

Вся политика безопасности корпоративной сети может быть представлена в виде таблицы. На основе таблицы определены файлы конфигурации для всех продуктов VPN, загружаемые администратором безопасности во все точки корпоративной сети по каналам связи.

Следует отметить, что одним из преимуществ такого решения является отсутствие необходимости каких-либо изменений в настройках системы при изменении любым из пользователей его физического месторасположения и соответствующего изменения точек входа в корпоративную систему, в том числе и при изменении IP-адреса. Это решение легко расширяется при увеличении числа пользователей простым добавлением продукта VPN-Клиент.

Защита прикладных распределенных систем

Корпорации, как правило, приобретают либо создают собственные прикладные распределенные информационно-аналитические системы для поддержки большого количества разнообразных задач. Это бухгалтерские и финансовые системы, системы документооборота. Пользователями таких систем являются соответствующие профессиональные подразделения, насчитывающие десятки, сотни и даже тысячи сотрудников, распределенных между офисами, филиалами и дочерними компаниями.

Такие системы часто содержат критичную для бизнеса корпораций информацию, потеря, искажение и даже несанкционированное раскрытие которой могут привести к колоссальным потерям и даже краху бизнеса. Кроме того, необходимость управлять работой большого количества сотрудников требует ведения управленческой отчетности, и особенную важность приобретает возможность идентификации, аутентификации и авторизации пользователей систем. Возникает целый ряд требований к корпоративной информационной системе с точки зрения информационной защиты.

В этих случаях для защиты информационных систем организации, распределенных по некоторому количеству предприятий и соединенных различными каналами связи (радиорелейными, оптоволоконными, через Интернет, Ethernet и т.п.), а также для организации доступа ограниченного круга пользователей к определенным ресурсам можно предложить решение.

Элементы систем, содержащие критичную информацию, а также рабочие места пользователей, работающих с этой информацией, выделяются в отдельные виртуальные защищенные от постороннего доступа подсети (например, подсети информационно-аналитической системы руководства и бухгалтерской системы, см. схему 5).

Для защиты передачи критичной информации в системах, работающих по принципу клиент - сервер, на соответствующие рабочие места устанавливаются программные средства VPN-Клиент, а на серверы - VPN-Сервер. Такое решение подойдет для защиты любой системы, реализованной по технологии клиент - сервер. Суть этого решения заключается в выделении внутренних периметров в корпоративной сети путем построения отдельных VPN, топология которых отвечает топологии бизнес-процессов, а не топологии сетей предприятия.

Применение для защиты сегментов сети продукта VPN-Офис позволяет дополнительно скрывать от внешнего мира структуру защищенного сегмента. Для внешнего наблюдателя данный сегмент виден в качестве одного IP-адреса, независимо от того, сколько компьютеров в сегменте. Этот вариант решения позволяет защитить "чувствительные" к угрозам информационные ресурсы не только от внешних угроз, но и от атак изнутри, со стороны "нелояльного персонала".

На серверы информационной системы, содержащие корпоративную информацию, устанавливаются программные средства VPN-Сервер, а на рабочие места пользователей, работающих с критичной информацией, - VPN-Клиент. Решение может быть усилено системой аутентификации пользователей, исключая доступ к критичной информации неавторизованных пользователей, это особенно актуально при работе с финансовой информацией. На АРМ, входящих в систему, не содержится информации о ключах, сертификатах, конфигурации VPN, что также усиливает систему безопасности.

Решение для электронной коммерции B2B

Системы электронной коммерции между предприятиями (B2B) имеют свои особенности:

- определенное количество пользователей системы (в отличие от систем B2C);
- крупные объемы заказов и, как следствие, высокая чувствительность к атакам и надежности связи;
- большое разнообразие прикладных протоколов (не только HTTP);
- повышенные требования к безопасности.

В настоящее время ведется разработка и внедрение множества различных систем для коммерции. На схеме 6 показана реализация защиты для системы типа B2B.

Для защиты сервера с ПО любой прикладной системы B2B устанавливается продукт VPN-Сервер, а на клиентскую часть системы, размещаемой у бизнес-партнера, - VPN-Клиент. Продукт VPN-Офис гарантирует сокрытие топологии внутренней сети и ее защиту от внешних атак из Интернета, от неавторизованного доступа извне.

Использование комплексных VPN-продуктов позволяет строить систему защиты для сети в целом, и это выгодно отличает их от специализированных VPN-продуктов, обеспечивающих защиту для отдельных классов приложений. Так, для аутентификации и защиты потоков данных в ряде известных программных продуктов используется протокол SSL (Secure Socket Layer), недостатком которого является его "привязанность" к определенному типу приложений, а, значит, неспособность удовлетворить разнообразные требования к системе защиты, предъявляемые крупными корпорациями и Интернет-провайдерами.

Если ИС защищена отдельными продуктами средств защиты информации (шифрование, электронная цифровая подпись), то VPN все равно нужна, поскольку только она защитит систему от сетевых атак, в частности DoS. Система, основанная только на SSL, не обеспечивает такой полной защиты, как продукты VPN. VPN будет "пускать" в сеть только пакеты, подписанные на допущенных к системе сертификатах.

Следует отметить еще одно свойство, принципиально важное для электронной системы B2B, - развитые средства аутентификации пользователей:

- с помощью пароля;
- с помощью устройств SecurID;
- с помощью смарт-карт (или других токен-устройств, дискет), поддерживающих стандартный интерфейс PKCS №11.

Без введения пароля или предъявления внешнего носителя (токена), подтверждающего право доступа, нельзя получить доступ ни к какой информации, кроме той, что открыта для всех пользователей.

Решение для торговой компании

Развитие российского потребительского рынка предопределило быстрый рост числа частных торговых организаций и значительное расширение их сетей. Необходимость внедрения современных способов торговли, повышения уровня обслуживания и оперативности сделали актуальным вопрос о комплексной автоматизации магазинов и включении их в системы электронных платежей, которая, в свою очередь, делает актуальным вопрос защиты информации.

Представленная схема 7 эффективно решает эту проблему, обеспечивая доступность, конфиденциальность и целостность информации в любое время, невзирая на сетевые атаки.

Набор средств, представленных в данном решении, позволяет построить двухуровневую систему защиты, в которой построен общий периметр защиты, отделяющий ресурсы компании от внешнего мира, а внутри него выделена и функционирует отдельная информационная система с повышенными требованиями к защите. Для торговой компании, имеющей несколько баз и магазинов, а также мобильный персонал (менеджеры по закупкам или продажам), нужно установить следующие компоненты:

- на каждом сервере системы управления поставками - ПО VPN-Сервер для обеспечения защищенного обмена информацией между серверами;
- на компьютеры, имеющиеся в магазинах и у мобильных или удаленных сотрудников, - ПО VPN-Клиент для защищенного обмена с серверами и с системами обеспечения офисной деятельности баз и головного офиса;
- в головном офисе, на каждой торговой базе и в каждом магазине - ПО VPN-Офис для объединения их в единую корпоративную защищенную сеть.

Центр управления VPN позволяет администратору безопасности системы определять, устанавливать и изменять политику безопасности для всей системы в целом и для ее отдельных частей.

Все пользователи системы из числа персонала магазинов и менеджеры по продажам могут быть объединены с помощью списка персональных сертификатов в одну виртуальную группу пользователей "Продавцы".

Другая виртуальная защищенная группа может быть объединена под названием "Информационные серверы", с локализацией IP-адресов серверов и их сертификатов.

Адресное пространство головного офиса, за исключением IP-адреса информационного сервера, выделено в защищенную группу "Головной офис". Аналогично группируются адреса баз и магазинов, имеющих свои собственные локальные сети. Группы "Головной офис", "База 1", "База 2" и т.д., "Магазин 1", "Магазин 2" и т.д. дополнительно объединены в защищенную группу "Компания".

Конкретное приложение торговой системы использует HTTP-протокол для обеспечения доступа с рабочего места пользователя к информационным серверам. Комбинация информации о TCP-портах при взаимодействии серверов по протоколу TCP обозначена понятием "Информационный сервис".

Web-сервер для открытого доступа определен как объект "Витрина", объект "Интернет" определен как полное адресное пространство сети Интернет, исключая IP-адреса корпоративных пользователей.

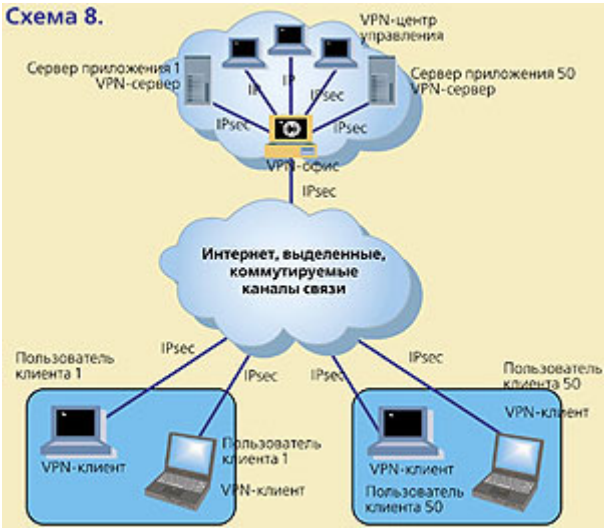
Сотрудники, занимающиеся модификацией "Витрины", определены как объект "Операторы".

Достоинством такого решения является то, что каждый сотрудник или продавец, имеющий персональный идентификатор, в любом из магазинов или с удаленного рабочего места имеет доступ в защищенном режиме к информационным серверам со своего персонального компьютера.

Решение для сервис-провайдеров информационных услуг

Стремительно развивающийся рынок коммуникаций предоставляет новые возможности и услуги, в частности услуги по аренде различных приложений, избавляющих потребителей от затрат на приобретение дорогостоящего ПО, дополнительного оборудования и техническую поддержку того и другого. Обращение к программам по каналам "живой" оперативной связи с поставщиками программных услуг ASP (application service provider) очень привлекательно, ему сопутствуют и некоторые проблемы. Важнейшая из них - необходимость обеспечить должный уровень защиты информации каждого клиента, а также устойчивость системы к попыткам внешнего вмешательства.

Эта проблема также решаема с помощью программных продуктов VPN, обеспечивающих защиту от всего спектра сетевых атак и позволяющих провайдеру предоставить клиентам высокое качество сервиса.



Для защиты рабочего места каждого клиента устанавливается продукт VPN-Клиент, для основных и резервных серверов приложений - VPN-Сервер, для собственной интрасети компания-провайдер может использовать продукт VPN-Офис.

Представленное на схеме 8 решение обеспечивает надежное разделение систем клиентов, т. е. система Клиента А (приложение, информация, пользователи) изолированы от системы Клиента В с ее ресурсами посредством защищенных связей.

Каждая группа пользователей конкретного "Клиента" определена списком их публичных сертификатов и названа "Пользователи клиента №n". Аналогично каждая пара приложений основного и резервного серверов приложений для конкретного клиента определяется их публичными сертификатами и IP-адресами как "Сервер приложений №n".

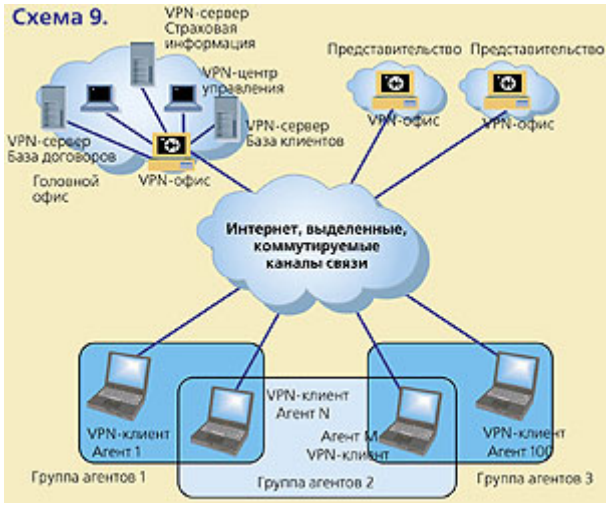
В результате образовано, например, 50 объектов: "Пользователи клиента № 1"... "Пользователи клиента №50", а также 50 соответствующих им объектов: "Сервер приложения № 1"... "Сервер приложения № 50".

Политика безопасности системы описывается набором правил. Администратору безопасности не требуется определять ее для каждого отдельного элемента системы, достаточно определить глобальную политику для набора бизнес-объектов: "Пользователь клиента №n" и "Сервер приложений №n". Дополнительная особенность решения: на его основе компания-провайдер может обеспечить своим корпоративным пользователям возможность прозрачной поддержки мобильных пользователей без снижения уровня защиты и сервиса независимо от их географического положения.

Эффективность, расширяемость и надежность решения позволяет компании-провайдеру обеспечивать поддержкой быстро растущий контингент клиентов при невысокой численности персонала администраторов.

Решение для защиты информационных ресурсов финансовых организаций

Это решение (схема 9) интересно для компаний, имеющих территориально разнесенные представительства и значительное количество постоянно перемещающихся агентов (брокеров, продавцов, консультантов и т.п.).



Для защиты головного офиса и представительств, имеющих локальные сети, устанавливается ПО VPN-Офис. В головном офисе серверы со специальными приложениями (база данных клиентов, база договоров, информация о страховании) защищены ПО VPN-Сервер. Персональные компьютеры агентов защищены ПО VPN-Клиент.

Защита периметра с большим количеством мобильных пользователей и удаленных представительств сочетается с жестким разграничением доступа определенных агентов к соответствующим серверам и системам.

Серверы, работающие с базой клиентов, страховой информацией и базой договоров, определяются их IP-адресами и сертификатами в качестве объектов, называемых "База клиентов", "Страховая информация", "База договоров".

Группа агентов, которым разрешен доступ к Базе клиентов, определена как защищенный групповой объект "Группа агентов 1" и задана списком персональных сертификатов этих агентов. Аналогично определены защищенные групповые объекты для агентов, которым разрешен доступ к серверам "Страховая информация" и "База договоров". Заметим, что группы агентов являются пересекающимися множествами, т. е. агент X может включаться в любой групповой объект или в несколько одновременно, получая соответствующие права доступа.

Адресное пространство IP головного офиса, за исключением IP-адресов "Базы клиентов", "Страховой информации" и "Базы договоров", формирует защищенный объект "Головной офис". IP-адреса всех представительств образуют групповой защищенный объект "Представительства".