Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11. Специфика России.

Максим Филиппов
Менеджер проектов компании
ОАО «Элвис-Плюс»
<maxim@elvis.ru>

«Предупрежден, значит вооружен»
А.В.Суворов

Настоящая статья - это попытка сделать обзор текущего состояния безопасности беспроводных сетей с целью ответа на вопрос: возможно ли уже сегодня построить корпоративную беспроводную сеть, устраивающую собственника сети с точки зрения обеспечения требуемого уровня безопасности, а также в соответствии с требованиями законодательства РФ и руководящих документов в области защиты информации?

Технологии беспроводных сетей широко используется во всем мире, привлекая внимание пользователей относительно невысокими экономическими затратами и простотой развертывания, удобством использования и гибкой архитектурой. Бесспорным лидером на рынке беспроводных сетей, является оборудование, отвечающее спецификациям семейства стандартов 802.11. Поэтому в дальнейшем при употреблении термина «беспроводные сети», будем иметь в виду сети, построенные на оборудовании, совместимом со стандартами семейства 802.11.

Одним из основных сегментов рынка оборудования беспроводных сетей является решение для так называемых «офисных или корпоративных» сетей. Характерная особенность такого решения - создание непрерывной зоны покрытия в пределах офисного здания. Данное решение часто требует размещения достаточно большого количества точек доступа. И в таком случае, актуальной становится задача мониторинга и управления беспроводной сетью. Следовательно, уже на этапе проектирования необходимо заложить в решение использование средств централизованного управления и мониторинга состояния сети, что в дальнейшем позволит существенно снизить совокупную стоимость владения системой (ТСО). В дальнейшем мы не будем возвращаться к вопросам ТСО, - это тема отдельной статьи и отдельного обсуждения.

Другим основным вопросом при построении беспроводных сетей, безусловно, является вопрос обеспечения требуемого уровня безопасности информации, циркулирующей в сети. В первую очередь, причина остроты вопроса в используемой среде передачи данных – радиоэфире. В отличие от обычных сетей, в которых информация передается по проводам, осуществить перехват информации в радиоэфире намного проще – достаточно иметь комплект оборудования, аналогичный комплекту оборудования абонента беспроводной сети. Поэтому в спецификации стандартов 802.11 особое внимание уделено вопросам безопасности - определен протокол обеспечения безопасности беспроводных сетей WEP (Wired Equivalent Privacy).

Безусловно, вопрос обеспечения безопасности, поставленный в этой статье далеко нетривиален, но с чего-то надо начинать… И чтобы подступиться к решению этого вопроса, давайте определим доступные нам меры и средства, позволяющие сделать беспроводную сеть как можно более безопасной. Итак, нам необходимо:

- ✓ ***Уменьшить зону радиопокрытия (разумеется, до минимально приемлемой). В идеале, зона радиопокрытия сети не должна выходить за пределы контролируемой территории.***
- ✓ ***Изменить пароль администратора, установленный по умолчанию***
- ✓ ***Активизировать фильтрацию по MAC-адресам***
- ✓ ***Запретить широковещательную рассылку идентификатора сети (SSID)***
- ✓ ***Изменить идентификатор сети (SSID), установленный по умолчанию***
- ✓ ***Периодически изменять идентификатор сети (SSID)***
- ✓ ***Активизировать функции WEP***
- ✓ ***Периодически изменять WEP-ключи***
- ✓ ***Установить и настроить персональные МЭ и антивирусные программы у абонентов беспроводной сети***
- ✓ ***Выполнить соответствующие настройки фильтрации трафика на телекоммуникационном оборудовании и межсетевых экранах***
- ✓ ***Обеспечить резервирование оборудования, входящего в состав беспроводной сети***
- ✓ ***Обеспечить резервное копирование ПО и конфигураций оборудования***
- ✓ ***Осуществлять периодический мониторинг состояния защищенности беспроводной сети с помощью специализированных средств анализа защищенности для беспроводных сетей (см. например, www.iss.net, www.wildpackets.com или www.sniffer.com).***

Все эти методы защиты сегодня можно реализовать на оборудовании практически любого производителя, представленного на рынке беспроводных сетей стандарта 802.11 и имеющего логотип Wi-Fi[1].

Назовем комплекс вышеперечисленных мер защиты «начальным» уровнем, ниже которого опускаться категорически нельзя при проектировании корпоративной беспроводной сети.

Допустим, весь комплекс мер реализован, но, увы, учитывая известные технические и технологические проблемы протокола WEP[2], и как следствие, низкий уровень сложности взлома подобной сети, беспроводную сеть с «начальным» уровнем безопасности лучше всего рассматривать как далеко небезопасную сеть. И, как следствие, точки доступа такой сети (даже при использовании WEP) не следует соединять с внутренней проводной сетью, - они должны находиться по внешнюю сторону от межсетевого экрана. Таким образом, обрабатывать конфиденциальную информацию в сети с описанным выше начальным уровнем безопасности нельзя.

Чтобы исправить ситуацию, некоторые производители (например, Agere Systems, D-Link, US Robotics,), с целью улучшения базового уровня защищенности, предлагают использовать более длинные ключи шифрования протокола WEP - 128, 152 или даже 256 бит. Но это часто приводит к отсутствию совместимости с оборудованием стандарта 802.11 других производителей. Кроме того, с точки зрения злоумышленника, трафик протокола WEP представляет из себя набор исходных данных для решения задачи

---

[1] (www.wi-fi.com): Для сертификации оборудования беспроводных сетей на совместимость создана организация WECA (Wireless Ethernet Compatibility Alliance), присваивающая знак совместимости Wi-Fi (Wireless Fidelity) оборудованию, построенному в соответствии со спецификациями семейства стандартов 802.11 и прошедшему соответствующие тесты. На сегодня в альянс входит 207 компаний. Начиная с марта 2000 года, успешно прошли испытания и получили соответствующий сертификат Wi-Fi 611 продуктов.

[2] Более детально описание уязвимостей протокола WEP см. на http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

криптоанализа типа «вскрытие с использованием выбранного ключа»[3]. А учитывая то, что злоумышленнику известен алгоритм смены ключей, определенный протоколом WEP, на решение этой задачи он затратит несколько часов[4]. После чего нам обеспечено несанкционированное подключение к нашей беспроводной сети. Мало того, заменить MAC-адрес своей карты доступа на MAC-адрес карты доступа легального пользователя, для злоумышленника не составит особого труда, а нам станет фактически не возможно обнаружить подобный взлом. Увеличение длинны ключа даже до 256 бит, лишь увеличивает количество пакетов, которые должен прослушать злоумышленник (например, используя анализаторы пакетов AirMagnet или AiroPeek), и время, необходимое злоумышленнику для криптоанализа.

Поточный шифр RC4, лежащий в основе WEP-шифрования и разработанный американцем Рональдом Райвестом в 1987 году, получил широкое распространение благодаря удачному сочетанию криптографической стойкости и высокого быстродействия. Уязвимости реализации протокола RC-4 в WEP изучаются криптографами достаточно давно[5]. По мнению многих экспертов необходимо заменить криптографический инструментарий протокола WEP на более прочный.

Итак, осознание проблем протокола WEP пришло не вчера, поэтому уже сегодня на рынке есть решения, позволяющие сделать использование протокола WEP более безопасным. Например:

- Использование некоторых протоколов стандарта 802.1x (о них речь пойдет ниже), позволяет решить проблему динамической смены ключей шифрования для беспроводных устройств.
- Протокол MIC (Message Integrity Check) позволяет защитить WEP-пакеты от их изменения и подделки, в процессе передачи.
- Протокол TKIP (Temporal Key Integrity Protocol), также разработаный с целью улучшения ситуации с безопасностью протокола WEP, предполагает использование уникальной ключевой последовательности для каждого устройства, а также обеспечивает динамическую схему ключа каждые 10 000 пакетов. Однако, также как и WEP, протокол TKIP использует для шифрования криптографический алгоритм RC4. Отметим, что для использования протокола TKIP нет необходимости отказываться от имеющегося оборудования 802.11, достаточно лишь обновить программное обеспечение (разумеется, если производитель реализовал поддержку этого протокола).

Теперь обратимся к вопросам обеспечения безопасного информационного взаимодействия пользователей беспроводной сети с ресурсами корпоративной сети. Для решения этой задачи, нам потребуются реализовать авторизацию пользователей беспроводной сети (в протоколе WEP проверка аутентичности пользователя не реализована совсем), а также использовать более сильные методы защиты, способные обеспечить требуемый уровень конфиденциальности и целостности информации. Один из таких методов –

- ✓ ***установка сервера контроля доступа, использующего протоколы стандарта EAP/802.1x[6] (LEAP; PEAP; EAP-TLS; EAP-TTLS), с целью усиленной аутентификации абонентов беспроводной сети.***

---

[3] Брюс Шнайер. Прикладная криптография, 2-е издание: протоколы, алгоритмы, исходные тексты на языке Си.Под редакцией П.В. Семьянова. М., Триумф, 2002

[4] См. например AT&T Labs Technical Report TD-4ZCPZZ "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP" (доступно на http://www.cs.rice.edu/~astubble/wep/)

[5] См. например Scott R. Fluhrer, Itsik Mantin, Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4. (доступно на www.cs.umd.edu/~waa/class-pub/rc4_ksaproc.pc)

[6] EAP (Extensible Authentication Protocol) - расширяемый протокол аутентификации позволяет проводить аутентификацию на основе: одноразовых паролей (OTP - one-time passwords), токенов, цифровых сертификатов, смарт-карт, протокола Kerberos. Стандарт 802.1x определяет инкапсуляцию EAP во фреймы сети. Протокол EAP определен в RFC №2284 (см. www.ietf.org/rfc/rfc2284.txt).

Остановимся более подробно на этом методе. Стандарт 802.1x в нашем случае определяет взаимодействие клиента беспроводной сети с сервером доступа на этапе авторизации абонента в системе. Схема авторизации пользователя в беспроводной сети показана на рисунке 1.

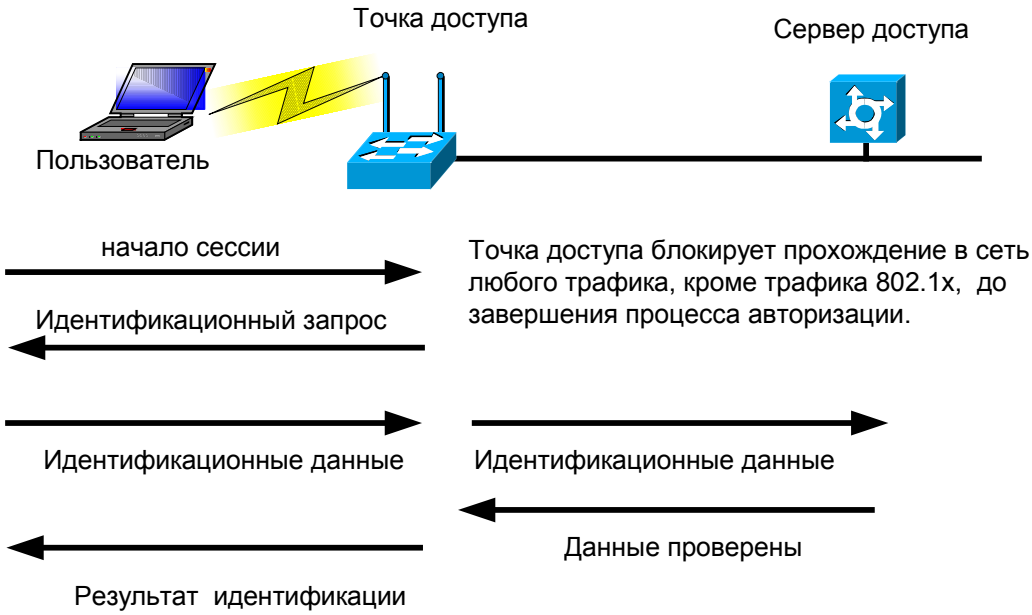


Рис.1 Схема авторизации 802.1x

Наиболее популярные серверы доступа на сегодняшний день - Cisco Secure Access Control Server и Internet Authentication Service (IAS). Последний встроен в операционную систему Microsoft Windows 2000.

Не вдаваясь в технические подробности реализации конкретных протоколов стандарта 802.1x, необходимо отметить следующие важные моменты:

- Данная схема требует установки на стороне клиента специализированного программного обеспечения – так называемого «сапликанта». По умолчанию поддержка механизма аутентификации по протоколу 802.1x встроена в операционную систему Windows XP и доступна для установки в виде отдельного пакета для операционной системы Windows 2000 (видимо, войдет в состав пакета обновлений Service Pack #4). Сапликант также может поставляться вместе с драйверами оборудования доступа к беспроводной сети.
- Ряд протоколов стандарта 802.1x используют в своей работе цифровые сертификаты формата X.509. Так, протокол PEAP для проверки пользователем сервера доступа использует сертификат сервера доступа, а протоколы EAP-TLS и EAP-TTLS для взаимной авторизации используют сертификаты X.509 как сервера доступа, так и клиента. Отметим, что существует возможность взаимодействия сервера доступа и внешнего хранилища цифровых сертификатов, например, по протоколу LDAP.

В связи с тем, что стандарт 802.1x относительно молод, сегодня еще можно столкнуться с такими «неприятными» моментами как:

- реализации различными производителями одного и того же протокола не совместимы друг с другом;
- отсутствие сапликантов для некоторых типов клиентских устройств доступа к беспроводной сети.

Но несмотря на все эти неприятные моменты, можно констатировать что реализованный различными производителями набор протоколов стандарта 802.1x (LEAP; PEAP; EAP-TLS; EAP-TTLS), позволяет уже сегодня выбрать и реализовать способ авторизации, устраивающий собственника беспроводной сети.

Мы понимаем, что в нашей сети могут присутствовать различные категории пользователей (абонентов). И вполне естественно, что мы захотим предоставить этим различным категориям пользователей различные права по доступу к тем или иным ресурсам. Простейший пример представлен в Таблице 1.

Таблица 1.

Абоненты беспроводной сети	**Доступ к конфиденциальной информации**	**Доступ к публичной информации (в т.ч. Internet)**
Сотрудник	+	+
Гость	-	+
Злоумышленник	-	-

Очевидно, что после аутентификации абонента беспроводной сети ему будет необходимо присвоить соответствующую его категории политику безопасности. Одной из возможных реализаций подобного подхода является:

- ✓ **Использование технологии, определенной стандартом 802.1q и позволяющей поместить авторизованных абонентов беспроводной сети в различные VLAN с определенной ранее политикой безопасности для каждого из этих VLAN-ов (в зависимости от типа абонента).**

Итак, используя в дополнение к методам базового уровня защиты, средства усиленной аутентификации по протоколу 802.1x и средства улучшения защищенности протокола WEP, уже сегодня можно достигнуть приемлемого уровня защиты информации, циркулирующей в беспроводной сети.

К сожалению, сегодня предложить вышеописанные решения может довольно узкий круг компаний. В первую очередь - это лидеры рынка оборудования для беспроводных сетей. Причем безусловным законодателем мод на рынке решений для обеспечения безопасности беспроводных сетей является компания Cisco Systems.

Отметим также, что реализация средств защиты в популярных операционных системах может существенно «подтянуть» уровень безопасности для беспроводных сетей, отчасти сняв эту «головную боль» с производителей оборудования. Но вопрос совместимости реализаций конкретных протоколов различными производителями остается открытым.

Попробуем заглянуть в будущее, чтобы понять, каких перемен следует ожидать в области защиты беспроводных сетей в ближайшее время. Вот два основных момента, которые должны поставить точку вместо вопросительного знака в вопросе «Использование беспроводных сетей безопасно?»:

- На смену WEP в конце 2003 года должен прийти стандарт 802.11i, который объединит в себе системы усиленной аутентификации, динамической смены ключей, управления ключами, проверки подлинности пакетов и т.д. Вместо WEP-шифрования планируется использовать AES (Advanced Encryption Standart – криптографический протокол Rijndael). Однако, это, в свою очередь, потребует разработки новых, более дорогих базовых наборов микросхем, а значит и дополнительных затрат от пользователей на обновление оборудования;
- Значительно улучшится ситуация с совместимостью решений различных производителей в области безопасности беспроводных сетей. Так, уже сейчас организация WECA опубликовала спецификацию Wi-Fi Protected Access (WPA), призванную внести ясность в вопрос совместимость решений в области безопасности различных производителей и определяющую использование протокола TKIP и протоколов аутентификации стандарта 802.1x. Сертификация

оборудования на соответствие спецификации Wi-Fi Protected Access начнется уже в первом квартале 2003 года, а к моменту утверждения стандарта 802.1i выйдет новая версия этой спецификации - Wi-Fi Protected Access 2, которая будет удостоверять соответствие решений различных производителей стандарту 802.1i и их интероперабельность.

А теперь вспомним, что мы живем в России, а значит, весь приведенный обзор архитектуры безопасности для беспроводных сетей будет не полным, если мы не остановимся именно на российской специфике использования средств защиты информации и средств криптографической защиты информации. Какие же требования накладывает законодательство на пользователей этих технологий в России?

Необходимо заметить, что за последнее время в России в области защиты информации сделано очень много. Появились соответствующие нормативные и руководящие документы, регламентирующие процесс защиты. Консалтинговые компании проводят аудит безопасности корпоративных сетей. Образованы органы по аттестации информационных систем. Страховые компании предлагают услуги по страхованию информационных рисков. Но, к сожалению, приходится констатировать, что всем этим новомодным услугам еще только предстоит завоевывать популярность на Российском рынке. Возможно, что все эти процессы, наконец, создадут прецеденты реальной юридической ответственности за разглашение конфиденциальной информации, а также ответственности организаций, проектирующих и внедряющих СОБИ (систему обеспечения безопасности информации), выдающих заключения (аттестаты соответствия) о соответствии построенной СОБИ требованиям руководящих документов**.**

Но вернемся к нашей теме. Как было сказано выше, одной из базовых технологий защиты информации в беспроводных сетях является криптография. Сегодня в России для защиты конфиденциальной информации мы ЛЕГИТИМНО можем использовать только сертифицированные ФАПСИ средства криптографической защиты информации. Именно для ЗАЩИТЫ. Надеяться на то, что позиция России по вопросу использования на ее территории «чужой» криптографии изменится, не стоит– право любого государства определять, как использовать криптографию. С другой стороны, ограничения, действующие на вывоз «сильной» криптографии из США, никто не снимал. Не менее иллюзорны надежды на то, что мы когда либо увидим реализацию российского криптоалгоритма в оборудовании зарубежных производителей.

Оптимальное решение этих проблем видится в использовании технологии защищенных частных виртуальных сетей (VPN):

- ✓ **Внедрение технологии VPN для обеспечения конфиденциальности и целостности информации, циркулирующей в беспроводной сети, в соответствии с требованиями российского законодательства и руководящих документов ФАПСИ и Гостехкомиссии.**

Производители оборудования при построении беспроводных сетей с максимальным уровнем защищенности рекомендуют использовать VPN решения на базе семейства протоколов IPSec: например, VPN решения российских производителей органично вписываются в архитектуру SAFE – архитектуру защищенных сетей, построенных на базе оборудования Cisco Systems.

Есть еще один аргумент в пользу использования технологии VPN для защиты информации, циркулирующей в беспроводной сети. Создав на базе VPN продуктов внешнюю защитную оболочку, собственник приобретает уверенность в том, что он защищен не только от известных уязвимостей встроенных протоколов защиты беспроводных сетей, но и от тех, которые могут появиться в дальнейшем. И самое главное – использование VPN решения на базе протокола IPSec российских производителей позволяет придать всей системе защиты легитимность, поскольку появляется

возможность использовать сертифицированные ФАПСИ и Гостехкомиссией России продукты.

Не смотря на то, что сама по себе технология защищенных частных виртуальных сетей способна обеспечить жесткую авторизацию пользователя по его цифровому сертификату формата X.509, ее не следует рассматривать как альтернативу решениям на базе протокола 802.1x. Это взаимодополняющие решения. Поскольку средства VPN обеспечивают защиту на сетевом уровне, а использование решений на базе протокола 802.1x позволяет предотвратить несанкционированный доступ к беспроводной сети на более раннем этапе. Подобное решение позволяет построить многоэшелонированную защиту: авторизуя пользователей по протоколу 802.1x мы убеждаемся, что имеем дело с легальным пользователем нашей беспроводной сети, а реализуя дополнительную авторизацию средствами VPN мы убеждаемся, что допускаем к работе с конфиденциальными ресурсами пользователей, которые имеют на это право. Кроме этого, использование функций межсетевого экранирования на устройстве VPN-шлюз, позволит нам назначать различные права доступа внутри группы пользователей, имеющих доступ к конфиденциальной информации. Необходимо также заметить, что сам протокол 802.1x имеет ряд уязвимостей к атакам типа «man-in-the-middle» и «session hijacking»[7]. Поэтому, не лишним будет повторить: использование технологии VPN позволяет создать внешнюю защитную оболочку беспроводной сети передачи данных.

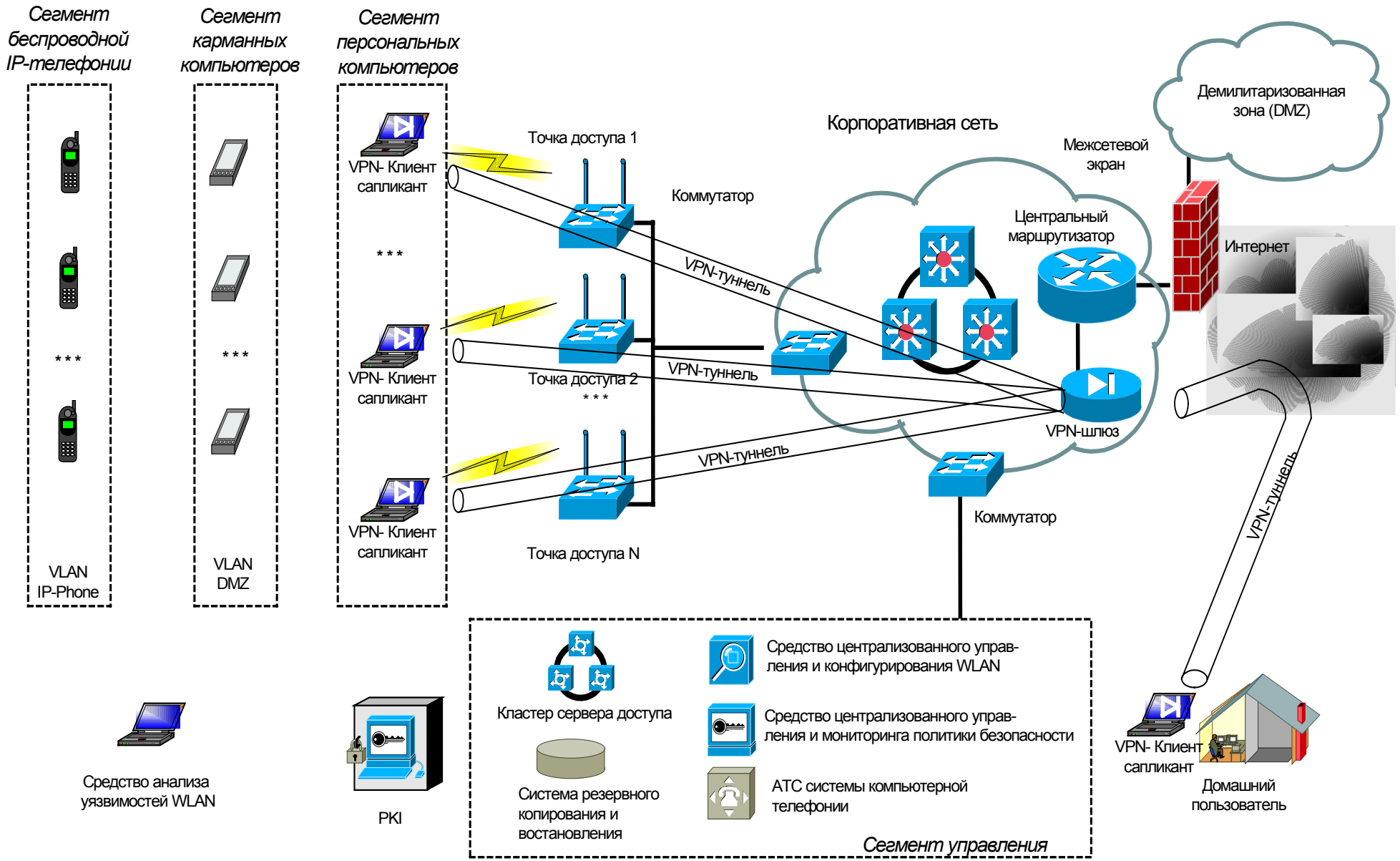
Как всегда, вопрос обеспечения требуемого уровня безопасности и вопрос удобства и простоты использования находятся на разных чашах весов. Посмотрим, что является «платой» в случае использования технологии VPN:

1. Снижение общей пропускной способности сети. По опыту нашей компании, в случае использования в протоколах семейства IPSec сертифицированных криптоядер, снижение производительности составит ориентировочно от 20 до 30%.
2. В случае использования карманных компьютеров (PDA) и/или беспроводных IP-телефонов найти VPN агента и криптографическое ядро для этих аппаратных платформ, достаточно проблематично. Поэтому, на данном этапе будет правильным применить к этим устройствам доступа политику безопасности, исключающую их взаимодействие с конфиденциальными ресурсами в корпоративной сети.
3. Увеличение общей стоимости (включая и TCO) решения.

Теперь, обсудив все основные вопросы, давайте, наконец, посмотрим как может выглядеть архитектура защищенной сети передачи данных с учетом всего вышесказанного – см. рисунок 2.

[7] См. Arunesh Mishra, William A. Arbaugh «An Initial Security Analysis of the IEEE 802.1x Standart» (доступно на http://www.cs.umd.edu/~waa/1x.pdf)

Рисунок 2. Схема защенного беспроводного сегмента корпоративной сети



Хотелось бы добавить, что в этой статье не рассмотрен весьма важный вопрос – вопрос интеграции подсистемы безопасности беспроводной сети в корпоративную СОБИ, но по своей значимости он, безусловно, заслуживает отдельной статьи.

Итак, основной вывод из всего вышесказанного: процесс построения любой из подсистем обеспечения безопасности информации достаточно сложный и трудоемкий, тем более в области беспроводных сетей. Причина тому – отсутствие устоявшихся стандартов в области безопасности, поддерживаемых всеми производителями. Но уже сейчас можно сказать, что технологии сегодняшнего дня позволяют построить в России корпоративную беспроводную сеть, приближающуюся по уровню безопасности к обычным проводным сетям и полностью соответствующую требованиям руководящих документов Гостехкомиссии и ФАПСИ. Главное - уделить должное внимание вопросам создания системы защиты информации беспроводной сети уже на этапе проектирования и пилотных испытаний и, естественно, не ошибиться с выбором Исполнителя.