WPA2 на защите беспроводных сетей Wi-Fi

WPA2 обеспечивает самый высокий уровень защиты данных и контроль доступа в беспроводную сеть для корпоративных (WPA2-Enterprise) и индивидуальных пользователей (WPA2-Personal).

WPA2 (Wireless Protected Access ver. 2.0) – это вторая версия набора алгоритмов и протоколов обеспечивающих защиту данных в беспроводных сетях Wi-Fi. Как предполагается, WPA2 должен существенно повысить защищенность беспроводных сетей Wi-Fi по сравнению с прежними технологиями. Новый стандарт предусматривает, в частности, обязательное использование более мощного алгоритма шифрования AES (Advanced Encryption Standard) и аутентификации 802.1X.

На сегодняшний день для обеспечения надежного механизма безопасности в корпоративной беспроводной сети необходимо (и обязательно) использование устройств и программного обеспечения с поддержкой WPA2. Предыдущие поколения протоколов - WEP и WPA содержат элементы с недостаточно сильными защитой и алгоритмами шифрования. Более того, для взлома сетей с защитой на основе WEP уже разработаны программы и методики, которые могут быть легко скачаны из сети Интернет и с успехом использованы даже неподготовленными хакерами-новичками.

Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise). В режиме WPA2-Personal из введенной открытым текстом парольной фразы генерируется 256-разрядный ключ PSK (PreShared Key). Ключ PSK совместно с идентификатором SSID (Service Set Identifier) используются для генерации временных сеансовых ключей PTK (Pairwise Transient Key), для взаимодействия беспроводных устройств. Как и статическому протоколу WEP, протоколу WPA2-Personal присуще определенные проблемы, связанные с необходимостью распределения и поддержки ключей на беспроводных устройствах сети, что делает его более подходящим для

применения в небольших сетях из десятка устройств, в то время как для к орпоративных сетей оптимален WPA2-Enterprise .

В режиме WPA2-Enterprise решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль, аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации. Точка доступа или беспроводной контроллер проводят мониторинг подключений и направляют аутентификационные запросы на соответствующий сервер аутентификации (как правило, это сервер RADIUS). Базой для режима WPA2-Enterprise служит стандарт 802.1X, поддерживающий аутентификацию пользователей и устройств, пригодную как для проводных коммутаторов, так и для беспроводных точек доступа.