1. Шифрование WPA-PSK, WPA

WPA и WPA2 (Wi-Fi Protected Access) — представляет собой обновлённую программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии защиты беспроводной Wi-Fi сети WEP. Плюсами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратном, так и на программном уровнях. На данный момент WPA и WPA2 разрабатываются и продвигаются организацией Wi-Fi Alliance. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). Стоит заметить, что в WPA2 поддерживается шифрование в соответствии со стандартом AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования), который имеет ряд преимуществ над используемым в WEP RC4, например гораздо более стойкий криптографический алгоритм.

Большим плюсом при внедрении WPA является возможность работы технологии на существующем аппаратном обеспечении Wi-Fi.

Некоторые отличительные особенности WPA:

усовершенствованная схема шифрования RC4 обязательная аутентификация с использованием EAP. система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

Wi-Fi Alliance даёт следующую формулу для определения сути WPA:

WPA = 802.1X + EAP + TKIP + MIC

Видно, что WPA, по сути, является суммой нескольких технологий.

Как упомянуто выше, в стандарте WPA используется Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ в сеть. Для этого права пользователь проходит проверку по специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена. База зарегистрированных пользователей и система проверки в больших сетях, как правило, расположены на специальном сервере (чаще всего RADIUS).

Следует отметить, что WPA имеет упрощённый режим. Он получил название Pre-Shared Key (WPA-PSK). При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть. Даже не принимая во внимание тот факт что WEP, предшественник WPA, не обладает какими-либо механизмами аутентификации пользователей как таковыми, его ненадёжность состоит, прежде всего, в криптографической слабости алгоритма шифрования. Ключевая проблема WEP заключается в использовании слишком похожих ключей для различных пакетов данных.

TKIP, MIC и 802.1X (части уравнения WPA) усилили шифрование передаваемых данных в сетях, использующих WPA.

TKIP отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в TKIP используется специальная иерархия ключей и методология управления ключами, которая убирает излишнюю предсказуемость, которая использовалась для несанкционированного снятия защиты WEP ключей.

Сервер аутентификации, после получения сертификата от пользователя, использует 802.1X для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динами-

ческой генерации ключей шифрования данных, которые в свою очередь используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

2. Настройка параметров IP-камер

IP-камера — цифровая видеокамера, особенностью которой является передача видеопотока в цифровом формате по сети Ethernet и TokenRing, использующей протокол IP. Являясь сетевым устройством, каждая IP-камера в сети имеет свой IP-адрес. В отличие от аналоговых камер, при использовании IP-камер, после получения видеокадра с ПЗС (англ. CCD) или КМОП (англ. CMOS) матрицы камеры, изображение остаётся цифровым вплоть до отображения на мониторе.

Как правило, перед передачей, полученное с матрицы изображение сжимается с помощью покадровых (MJPG) или потоковых (MPEG-4, H.264) методов видеосжатия. Специализированные IP-камеры чаще осуществляют передачу видео в несжатом виде.

В качестве протокола транспортного уровня в IP-камерах могут использоваться протоколы: TCP, UDP и другие протоколы транспортного уровня модели OSI. Распространена возможность электропитания IP-камер через PoE.

Первый парамерт, с которым нужно определиться - это "Максимальный битрейт". Здесь есть 2 пути.

1. камера подключается к серверу сбора видеопотоков

2. камера сама является сервером предоставляющим видеопотоки клиентам.

В первом случае у камеры будет только 1 клиент, во втором сколько угодно. Отсюда, для первого случая bitrate можно выставить максимальным. Для второго случая, когда сама камера выступает в роли сервера и нужно на неё завести максимальное количество клиентов нужно параметр выбирать как можно меньше.

Bitrate можно назвать ключевым параметром, если его не будет хватать для передачи видео с заданным разрешением, fps, качеством и I Frame Rate, то возможны проблемы. Например если будет испотльзоваться udp, который используется по умолчанию, то будут теряться кадры и ffmpeg будет давать сбои. Ffmpeg1 будет продолжать работать, но будет выводить ошибки передачи. Если будет использован tcp, то ошибок не будет, но изображение будет кратковременно замирать, не все кадры будут доходить до сервера. Замирания можно наблюдать через web интерфейс камеры. Эти явления нежелательны, так как можно потерять важные кадры события.

Параметры настройки видео камеры нужно задавать так, чтобы скорость обмена между IP камерой и сервером не превышала заданный bitrate. Скорость обмена можно смотреть например через Windows диспетчер задачь или на сервере, через

```
# systat -ifstat 1
```

.

Задаваемые параметры всецело зависят от решаемой задачи. Если нужно получать поток для целей видеонаблюдения, или для трансляции живого видео потребителям, то параметры могут различаться весима существенно.

После bitrate следует обратить внимание на параметр 'Интервал I кадра' или I Frame Interval. Это интервал между ключевыми кадрами. Например, знаение 50 означает, что только каждый 50й кадр будет ключевым, остальные разностные, содержащие информацию только о разнице между текущим и предыдущим изображением. Ключевой кадр полный и содержит всю информацию о текущем снимке. Т.е. если fps = 10, то ключевой кадр будет передаваться раз в 5 секунд. Если I Frame Interval = 1, то каждый кадр будет ключевым.

Exposure mode (Выдержка) Задаёт режим работы электронного затвора камеры. В режиме "Автоматически камера сама задаёт выдержку в зависимости от освещённости объекта, регулируя световой поток на матрицу. Тем самым общая яркость картинки будет оптимальной. Не стоит изменять значение по умолчанию этого параметра, если только у вас не установлен объектив с автоматической диафрагмой (В большинстве IP камер диафрагма отсутствует, её роль выполняет электронный затвор). При необходимости можно вручную установить постоянную выдержку - 1/50, 1/100, 1/250, 1/500, 1/1000, 1/2000, 1/4000, 1/100000 В этом случае следует учитывать, что при изменении освещённости объекта, изображение может стать слишком тёмным или слишком пересвеченным, так как камера уже не управляет этим параметром.

3. Управление полосой пропускания VPN-трафика на ZyWALL 5/35/70

VPN-трафик зашифровывается перед передачей через Интернет. Таким образом, лучше всего воспользоваться функцией управления полосой пропускания VPN-трафика уже после его дешифрации. Адреса источника и назначения тогда будут соответствовать локальному и удаленному адресам правил стадии 2 (Phase 2) VPN-туннеля. Можно использовать эту информацию для настройки правила управления полосой пропускания.

Рассмотрим пример, в котором используются два ZyWALL 5. Нужно настроить функцию управления полосой пропускания (Bandwidth Management) на входящий трафик (из WAN в LAN), ограничивающий VPN-трафик от удаленной стороны.

1. Необходимо зайти в настройки ZyWALL5 A через веб-конфигуратор. Выберите раздел SECURITY - VPN и настройте VPN-правило для создания туннеля с ZyWALL5 B.

2. Далее следует настроить соответствующее VPN-правило на ZyWALL5 B и затем в веб-конфигураторе ZyWALL5 A зайдите в меню ADVANCED - BW MGMT. Например, настроим управление полосой пропускания из WAN в LAN, выбрав класс LAN.

3. На закладке Class Setup, выберите LAN в поле Interface следует выбрать Add Sub-Class для создания подкласса для VPN-трафика.

4. Установить подкласс для контроля VPN-трафика от удаленной подсети в локальную сеть. Можно установить ZyWALL для контроля трафика основанный на сервисах FTP или SIP проходящих через VPN-туннель по определенному типу трафика. В нашем примере управление полосой пропускания используется для всего трафика.

5. Можно проверить в реальном времени работу управления полосой пропускания на закладке Monitor. Для этого следует направить трафик из удаленной подсети в локальную сеть за ZyWALL5 A и убедиться, что статистика по использованию трафика отображается на этом экране.

6. Если статистика текущего использования для подкласса VPN отображается в правом столбце (Current Usage) на закладке Monitor, то настройка управления полосой пропускания для VPN произведена правильно.

4. Интерфейс командной строки в коммутаторах ZyXEL

Command Line Interface - интерфейс командной строки, разновидность текстового интерфейса между человеком и компью тером, в котором инструкции компью теру даются в основном путём ввода с клавиатуры текстовых строк (команд). Также известен под названием консоль

Управление сетевыми коммутаторами ZyXEL осуществляется через Web- интерфейс и интерфейс командной строки (CLI – Command Line Interface). Интерфейс командной строки доступен через коммуникацион - ную программу (например , HyperTerminal), а также через сетевые протоколы **telnet** и **ssh** (защищенный командный интерпретатор). Интерфейс командной строки через коммуникационную программу является полезным средством настройки коммутатора, если тот недоступен по сети (отсутствует информация об IP- адресах

на интерфейсе Management и остальных портах). В этом случае осуществляется подключение компьютера к коммутатору через выбранный последовательный порт, производится запуск программы HyperTerminal с параметрами: битовая скорость – 9600 бит/с, бит в слове – 8, четность – Нет, стоповый бит – 1, управление потоком – Нет) и ввода логина admin, пароля 1234. В зависимости от версии микропрограммы и модели устройства запустится либо привилегированный , либо непривилегированный режим управления. Режимы внешне отличаются символом перед вводом команды ('#'– привилегированный или '>'– непривилегированный). Переключение между режимами управления осуществляется с помощью команд **enable** (переход из '>' в '#') и с помощью команды **disable** (переход из '#' в '>'). Сброс текущей конфигурации осуществляется командой **erase running-config** . После этого IP- адрес для управления коммутатором на интерфейсе Management устанавливается 192.168.0.1, а через рабочие порты он доступнен по адресу 192.168.1.1. При этом IP- адрес на интерфейсе Management задается командой **ip address**. Для сохранения конфигурации используется команда **write memory**.

Команда **show hardware-monitor** показывает аппаратные измерения: температуру, напряжение, скорости вращения вентиляторов. Если на коммутаторе моргает красный светодиод ALM, с помощью этой команды Вы всегда сможете узнать причину неисправност.

Некоторые другие команды

- **show hardware-monitor**
  show ip
- **show running-config**
- **ping**
- **traceroute**