Вопросы и ответы по безопасности беспроводных устройств Cisco Aironet

Содержание

Введение

Этот документ отвечает на о большинство часто задаваемых вопросов (FAQ) о безопасности беспроводной связи Cisco Aironet.

Общие вопросы

Вопрос. . Какова потребность в Безопасности беспроводной связи?

О. В Проводной сети данные остаются в кабелях, которые подключают конечные устройства. Но Беспроводные сети передают и получают данные через широковещание радиочастотных сигналов в воздух. Из-за широковещательной природы, которую используют WLAN, существует большая угроза хакеров или злоумышленники, которые могут обратиться или повредить данные. Для облегчения этой проблемы все WLAN требуют добавления:

1. Проверка подлинности пользователя для предотвращения неавторизованный доступа к сетевым ресурсам.
2. Конфиденциальность данных для защиты целостности и конфиденциальности передаваемых данных (также известный как шифрование).

Вопрос. . Каковы другие методы аутентификации, которые определяет стандарт 802.11 для Беспроводных локальных сетей?

О. Стандарт 802.11 определяет два механизма проверки подлинности клиентов Беспроводной локальной сети:

1. Открытая проверка подлинности
2. Аутентификация с общим ключом

Также существует два других обычно используемых механизма:

1. Основанная на SSID аутентификация

2. Аутентификация с использованием MAC-адреса

Вопрос. . Что такое Открытая аутентификация?

О. Открытая аутентификация является в основном алгоритмом фиктивной проверки подлинности, что означает, что нет никакой проверки пользователя или машины. Открытая аутентификация позволяет любое устройство, которое размещает запрос аутентификации в точку доступа (AP). Открытая аутентификация использует передачу открытого текста, чтобы позволить клиенту связываться к AP. Если никакое шифрование не включено, никакое устройство, которое знает, SSID WLAN может получить доступ в сеть. Если Протокол WEP включен на AP, Ключ WEP становится средством управления доступом. Устройство, которое не имеет корректного Ключа WEP, не может передать данные через AP, даже если аутентификация успешна. Ни один не может такое устройство дешифровать данные, которые передает AP.

Вопрос. . Какие шаги Открытая аутентификация включает для клиента для соединения с AP?

1. Клиент отправляет тестовый запрос к AP.
2. AP передают тестовые ответы обратно.
3. Клиент оценивает ответы AP и выбирает лучший AP.
4. Клиент передает запрос аутентификации к AP.
5. AP подтверждает аутентификацию и регистрирует клиента.
6. Клиент тогда отправляет запрос ассоциации к AP.
7. AP подтверждает ассоциацию и регистрирует клиента.

Вопрос. . Каковы преимущества и недостатки Открытой аутентификации?

О. Вот преимущества и недостатки Открытой аутентификации:

Преимущества: Открытая аутентификация является основным механизмом аутентификации, который можно использовать с Беспроводными устройствами, которые не поддерживают сложные алгоритмы аутентификации. Аутентификация в спецификации 802.11 ориентирована на подключение. Дизайном требования проверки подлинности позволяют устройствам получать Быстрый доступ к сети. В таком случае можно использовать Открытую аутентификацию.

Недостатки: Открытая аутентификация не предоставляет способа проверить, является ли клиент допустимым клиентом и не клиентом - хакером. Если вы не используете Шифрование WEP с Открытой аутентификацией, никакой пользователь, который знает, SSID WLAN может обратиться к сети.

Вопрос. . Что такое Проверка подлинности с общим ключом?

О. Проверка подлинности с общим ключом работает подобная Открытой аутентификации с одним основным различием. При использовании Открытой аутентификации с Ключом шифрования WEP Ключ WEP используется, чтобы зашифровать и дешифровать данные, но не используется в опознавательном шаге. В Проверке подлинности с общим ключом Шифрование WEP используется для аутентификации. Как Открытая аутентификация, Проверка подлинности с общим ключом требует, чтобы у клиента и AP был тот же Ключ

WEP. AP, который использует Проверку подлинности с общим ключом, передает Пакет текста запроса клиенту. Клиент использует локально настроенный Ключ WEP для шифрования текста запроса и ответа с запросом последующей аутентификации. Если AP может дешифровать запрос аутентификации и получить исходный текст запроса, AP отвечает ответом на аутентификацию, который предоставляет доступ клиенту.

Вопрос. . Какие шаги Проверка подлинности с общим ключом включает для клиента для соединения с AP?

1. Клиент отправляет тестовый запрос к AP.
2. AP передают тестовые ответы обратно.
3. Клиент оценивает ответы AP и выбирает лучший AP.
4. Клиент передает запрос аутентификации к AP.
5. AP передает ответ на аутентификацию, который содержит незашифрованный текст запроса.
6. Клиент шифрует текст запроса с Ключом WEP и передает текст к AP.
7. AP сравнивает незашифрованный текст запроса с зашифрованным текстом запроса. Если аутентификация может дешифровать и получить исходный текст запроса, аутентификация успешна.

Проверка подлинности с общим ключом использует Шифрование WEP во время процесса связывания клиента.

Вопрос. . Каковы преимущества и недостатки Проверки подлинности с общим ключом?

O. В Проверке подлинности с общим ключом клиент и AP обмениваются текстом запроса (открытый текст) и зашифрованная проблема. Поэтому этот тип аутентификации уязвим для атаки по перехвату и возможному изменению передаваемых данных. Хакер может слушать незашифрованную проблему и зашифрованную проблему, и извлечь Ключ WEP (общий ключ) из этой информации. Когда хакер знает Ключ WEP, целый механизм аутентификации поставился под угрозу, и хакер может обратиться к сети WLAN. Это - главный недостаток с Проверкой подлинности с общим ключом.

Вопрос. . Что такое Аутентификация с использованием MAC-адреса?

O. Несмотря на то, что стандарт 802.11 не задает Аутентификацию с использованием MAC-адреса, сети WLAN обычно используют этот способ аутентификации. Следовательно, большинство поставщиков Беспроводного устройства, включая Cisco, поддерживает Аутентификацию с использованием MAC-адреса.

В Аутентификации с использованием MAC-адреса клиенты аутентифицируются на основе их MAC-адреса, MAC-адреса клиентов проверены против списка MAC-адресов, сохраненных локально на AP или на внешнем сервере проверки подлинности. Проверка подлинности MAC является более сильным механизмом обеспечения безопасности, чем Открытое и Проверки подлинности с общим ключом, которые предоставляет 802.11. Эта форма проверки подлинности далее уменьшает вероятность неавторизованных устройств, которая может обратиться к сети.

Вопрос. . Почему проверка подлинности MAC не работает с Защищенным

доступом по протоколу Wi-Fi (WAP) в программном обеспечении Cisco IOS версии 12.3 (8) JA2?

O. Единственный уровень безопасности для проверки подлинности MAC должен проверить MAC-адрес клиента против списка разрешенных MAC-адресов. Это считают очень слабым. В более ранних Cisco IOS Software Release вы могли настроить проверку подлинности MAC и WPA для шифрования информации. Но потому что сам WPA имеет MAC-адрес, который проверяет, Cisco решила не позволить данный тип конфигурации в более поздних Cisco IOS Software Release и решила только улучшить характеристики безопасности.

Вопрос. . Я могу использовать SSID в качестве метода для аутентификации беспроводных устройств?

O. Идентификаторы наборов сервисов (SSID) являются уникальным, чувствительным к регистру, алфавитно-цифровым значением, которое WLAN используют в качестве сетевого имени. SSID - механизм, который позволяет логическое разделение беспроводных локальных сетей. SSID не предоставляет функций конфиденциальности данных, и при этом SSID действительно не аутентифицирует клиента на AP. Значение SSID передано как открытый текст в Сигналах-маяках, Тестовых Запросах, Тестовых ответах и других типах кадров. Eavesdropper может легко определить SSID с использованием анализатора пакетов беспроводной локальной сети 802.11, например, Sniffer Pro. Cisco не рекомендует использовать SSID в качестве метода для обеспечения сети WLAN.

Вопрос. . Если я отключаю широковещание SSID, я могу достигнуть усиленной безопасности на сети WLAN?

O. При отключении широковещания SSID SSID не передается в сообщениях Маяка. Однако другие кадры такой как, Тестовые Запросы и Тестовые Ответы все еще имеют SSID в открытом тексте. Таким образом, вы не достигаете улучшенной Безопасности беспроводной связи при отключении SSID. SSID не разработан, ни предназначен для использования как механизм обеспечения безопасности. Кроме того, при отключении широковещательных сообщений SSID можно встретиться с проблемами с совместимостью Wi-Fi для смешано-клиентских развертываний. Поэтому Cisco не рекомендует использовать SSID в качестве режима безопасности.

Вопрос. . Чем уязвимости найдены в безопасности 802.11?

O. Главные уязвимости безопасности 802.11 могут быть суммированы следующим образом:

- Слабая аутентификация только для устройства: Устройства клиента аутентифицируются, не пользователи.
- Слабое шифрование данных: Протокол WEP был доказан неэффективным как средство зашифровать данные.
- Никакая целостность сообщения: значение проверки целостности (ICV) было доказано неэффективным как средство гарантировать целостность сообщения.

Вопрос. . Что роль 802.1x является аутентификацией в WLAN?

O. Для адресации к недостаткам и Уязвимости безопасности в первоначальных способах

аутентификации, которую стандарт 802.11 определяет, система аутентификации 802.1X включена в проект для улучшений безопасности MAC - уровня 802.11. Исследовательская группа i (TGi) IEEE 802.11 в настоящее время разрабатывает эти усовершенствования. Платформа 802.1X предоставляет уровню соединения расширенную проверку подлинности, обычно замеченную только в более высоких уровнях.

Вопрос. . Каковы три объекта, которые определяет платформа 802.1x?

O. Платформа 802.1x требует, чтобы эти три логических объекта проверили устройства на сети WLAN.

1. **Соискатель** — соискатель находится на клиенте Беспроводной локальной сети и также известен как клиент EAP.
2. **Средство проверки подлинности** — средство проверки подлинности находится на AP.
3. **Сервер проверки подлинности** — сервер проверки подлинности находится на сервере RADIUS.

Вопрос. . Когда я использую систему аутентификации 802.1x, как происходит аутентификация беспроводного клиента?

O. Когда беспроводной клиент (клиент EAP) становится активным, беспроводной клиент аутентифицируется или с открытой или разделенной аутентификацией. 802.1x работает с открытой аутентификацией и запускается после того, как клиент успешно связывается к AP. Станция клиента может связаться, но может передать трафик данных только после успешной аутентификации 802.1x. Вот шаги в аутентификацию 802.1x:

1. AP (Средство проверки подлинности), настроенное для 802.1x, запрашивает идентичность пользователя от клиента.
2. Клиенты отвечают его идентичностью в предусмотренном периоде времени.
3. Если идентичность пользователя присутствует в своей базе данных, сервер проверяет идентичность пользователя и начинает аутентификацию с клиента.
4. Сервер передает сообщение об успешном завершении к AP.
5. Как только клиент аутентифицируется, сервер вперед ключ шифрования к AP, который используется для шифрования трафика, передаваемого и от клиента.
6. В шаге 4, если идентичность пользователя не присутствует в базе данных, сервер отбрасывает аутентификацию и передает сообщение об ошибках к AP.
7. AP передает это сообщение клиенту, и клиент должен аутентифицироваться снова с корректными учетными данными.

Примечание: В течение аутентификации 802.1x, AP просто вперед сообщения аутентификации к и от клиента.

Вопрос. . Каковы другие варианты EAP, которые я могу использовать с системой аутентификации 802.1x?

О. 802.1x определяет процедуру для аутентификации клиентов. Тип EAP, используемый в платформе 802.1x, определяет тип учетных данных и метода проверки подлинности, используемого в обмене 802.1x. Платформа 802.1x может использовать любой из этих вариантов EAP:

- EAP-TLS — Transport Layer Security расширяемого протокола аутентификации
- EAP-FAST — Гибкая аутентификация EAP через Защищенный Туннель
- SIM EAP — EAP Subscriber Identity Module
- LEAP Cisco — легковесный расширяемый протокол аутентификации
- PEAP EAP — EAP защищенный расширяемый протокол аутентификации
- EAP-MD5 — алгоритм Дайджеста сообщения EAP 5
- OTP EAP — EAP вовремя пароль
- EAP-TTLS — EAP туннелировал Transport Layer Security

Вопрос. . Как я выбираю метод EAP 802.1x из других доступных вариантов?

О. Большая часть важного фактора, который необходимо рассмотреть, - совместим ли метод EAP с существующей сетью или нет. Кроме того, Cisco рекомендует выбрать метод, который поддерживает обоюдную проверку подлинности.

Вопрос. . Что такое локальная EAP-аутентификация?

О. Локальный EAP является механизмом, в котором WLC действует как сервер проверки подлинности. Учетные данные пользователя сохранены локально на WLC для аутентификации беспроводных клиентов, который действует как процесс бэкэнда в удаленных офисах, когда выключается сервер. Учетные данные пользователя могут быть получены или из локальной базы данных на WLC или от внешнего Сервера LDAP. LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2 и PEAPv1/GTC являются другие Аутентификации eap, поддерживаемые локальным EAP.

Вопрос. . Что такое LEAP Cisco?

О. Легковесный расширяемый протокол аутентификации (LEAP) является патентованным методом Cisco аутентификации. LEAP Cisco является типом проверки подлинности 802.1X для беспроводных локальных сетей (WLAN). LEAP Cisco поддерживает сильную обоюдную проверку подлинности между клиентом и сервером RADIUS через пароль входа как общий секретный ключ. LEAP Cisco предоставляет динамичный для каждого пользователя, для каждого сеанса ключи шифрования. LEAP является наименее сложным методом для развертывания 802.1x и требует только сервера RADIUS. См. LEAP Cisco для получения информации о LEAP.

Вопрос. . Как работает EAP-FAST?

О. EAP-FAST использует алгоритмы с симметричным ключом для достижения туннелируемого процесса проверки подлинности. Установка туннеля полагается на учетные данные для защищенного доступа (PAC), что EAP-FAST может настраиваться и управляться динамично EAP-FAST через аутентификацию, авторизацию и учет (AAA) (такую

как сервер Cisco Secure Access Control Server [ACS] v. 3.2.3). Со взаимно аутентифицируемым туннелем EAP-FAST предлагает защиту от подборов пароля по словарю и man-in-the-middle уязвимостей. Вот фазы EAP-FAST:

EAP-FAST не только снижает риски от пассивных подборов пароля по словарю и атак по перехвату и возможному изменению передаваемых данных, но также и включает безопасную аутентификацию на основе в настоящее время развертываемой инфраструктуры.

- Этап 1: Установите взаимно аутентифицируемый туннель — Клиент и PAC использования AAA-сервера, чтобы аутентифицировать друг друга и установить безопасный туннель.
- Этап 2: Выполните аутентификацию клиента в установке туннеля — Клиент передает имя пользователя и пароль, чтобы аутентифицировать и установить политику авторизации клиента.
- Дополнительно, Фаза 0 — аутентификация EAP-FAST нечасто использует эту фазу, чтобы позволить клиенту быть динамично настроенным с PAC. Эта фаза генерирует учетные данные доступа для каждого пользователя надежно между пользователем и сетью. Фаза 1 аутентификации использует эти учетные данные для каждого пользователя, известные как PAC.

См. EAP-FAST Cisco для получения дополнительной информации.

Вопрос. . Есть ли документы о cisco.com, которые объясняют, как настроить EAP в сети WLAN Cisco?

O. См. Аутентификацию eap с сервером RADIUS для получения информации о том, как настроить Аутентификацию eap в сети WLAN.

См. Защищенное Примечание к приложению EAP для получения информации о том, как настроить аутентификацию PEAP.

См. Аутентификацию LEAP с Локальным сервером RADIUS для получения информации о том, как настроить Аутентификацию LEAP.

Вопрос. . Что другие механизмы шифрования обычно используются в беспроводных сетях?

O. Вот обычно используемые схемы шифрования, используемые в беспроводных сетях:

- WEP
- TKIP
- AES

AES является методом аппаратного шифрования, тогда как шифрование WEP и TKIP обработано на микропрограммном обеспечении. С обновлением микропрограммного обеспечения устройства WEP могут поддержать TKIP, таким образом, они совместимы. AES является самым безопасным и самым быстрым методом, тогда как WEP наименее безопасен.

Вопрос. . Что такое Шифрование WEP?

O. WEP обозначает Безопасность, аналогичная защите проводных сетей. WEP используется, чтобы зашифровать и дешифровать информационные сигналы та передача между устройствами WLAN. WEP — это дополнительная функция IEEE 802.11, которая позволяет предотвратить раскрытие и изменение транзитных пакетов, а также обеспечивает контроль доступа для сети. WEP делает канал WLAN таким же безопасным, как проводной канал. Поскольку стандарт задает, WEP использует алгоритм RC4 с 40-разрядным или 104-разрядным ключом. RC4 является симметричным алгоритмом, так как использует один ключ для шифрования и расшифровки данных. При включении WEP все радиостанции получают ключи. Ключ используется для скремблирования данных перед передачей в эфир. Если станция получает пакет, который не был скремблирован правильным ключом, она отклоняет пакет и никогда не доставляет его хосту.

См. дополнительные сведения о настройке WEP в документе Настройка WEP (Wired Equivalent Privacy).

Вопрос. . Что такое Ротация (широковещательных) ключей? Какова частота обращения широковещательного ключа?

O. Ротация (широковещательных) ключей позволяет AP генерировать самый лучший случайный ключ группы. Ротация (широковещательных) ключей периодически обновляет всех клиентов, способных к управлению ключами. При включении широковещательного вращения Ключа WEP AP предоставляет динамический широковещательный Ключ WEP и изменяет ключ в интервале, который вы устанавливаете. Ротация (широковещательных) ключей является превосходной альтернативой к TKIP, если ваша беспроводная локальная сеть поддерживает беспроводные клиентские устройства не-Cisco или устройства, которые вы не можете обновить к последним версиям микропрограммного обеспечения для устройств клиента Cisco. См. Включение и Отключение Ротации (широковещательных) ключей для получения информации о том, как настроить функцию ротации (широковещательных) ключей.

Вопрос. . Что такое TKIP?

O. TKIP обозначает Протокол временной целостности ключа. TKIP был представлен для адресации к недостаткам в Шифровании WEP. TKIP также известны как Хэширование ключа WEP и первоначально назвали WEP2. TKIP является временным решением, которое решает ключевую проблему повторного использования WEPs. TKIP использует алгоритм RC4 для выполнения шифрования, которое совпадает с WEP. Основное различие от WEP - то, что TKIP изменяет временный ключ каждый пакет. Временный ключ изменяет каждый пакет, потому что изменяется значение хеш-функции для каждого пакета.

Вопрос. . Могут устройства, которые используют взаимодействуют TKIP с устройствами то Шифрование WEP использования?

O. Преимущество с TKIP состоит в том, что WLAN с существующими основанными на WEP AP и радио могут обновить к TKIP через простые микропрограммные исправления. Кроме того, оборудование только для WEP все еще взаимодействует с поддерживающими TKIP устройствами тот WEP использования.

Вопрос. . Что такое Message Integrity Check (MIC)?

O. MIC является еще одним усовершенствованием для адресации к уязвимостям в

Шифровании WEP. MIC предотвращает разрядно-зеркально отраженные атаки на зашифрованные пакеты. Во время разрядно-зеркально отраженной атаки злоумышленник перехватывает зашифрованное сообщение, изменяет сообщение и затем повторно передает измененное сообщение. Получатель не знает, что сообщение повреждено и не легитимное. Для решения этой проблемы функция MIC добавляет поле MIC к беспроводному кадру. Поле MIC предоставляет проверку целостности кадра, которая не уязвима для тех же математических недостатков как ICV. MIC также добавляет поле порядкового номера к беспроводному кадру. AP отбрасывает кадры, принятые не в порядке.

Вопрос. . Что такое WPA? Как WPA 2 отличается от WPA?

O. WPA – это стандартный способ обеспечения безопасности Wi-Fi Alliance, учитывающий уязвимые места в сетях WLAN. WPA обеспечивает улучшенную защиту данных и контроль доступа к системам WLAN. WPA обращается ко всем известным уязвимостям Протокола WEP в исходной реализации безопасности IEEE 802.11 и приносит непосредственное решение по обеспечению безопасности сетей WLAN и на предприятии и на малом офисе, домашнем офис (SOHO) среды.

WPA 2 – это следующее поколение систем безопасности Wi-Fi. WPA 2 – это совместимая с Wi-Fi Alliance улучшенная версия одобренного стандарта IEEE 802.11i. WPA 2 выполнен на основе рекомендованного Национальным институтом стандартов и технологий (NIST) алгоритма шифрования AES (улучшенного стандарта шифрования) с использованием режима счетчика и протокола CCMP. Режим счетчика AES – это блочный шрифт, за раз шифрующий 128 битовый блок данных при помощи 128 битового ключа шифрования. WPA2 предлагает более высокий уровень безопасности, чем WPA. WPA 2 создает новые ключи сеанса при каждом сопоставлении. Ключи шифрования, что использование WPA2 для каждого клиента в сети является уникальным и определенным для того клиента. В итоге каждый пакет, посылаемый в эфир, зашифрован при помощи уникального ключа.

И WPA1 и WPA2 могут использовать или TKIP или шифрование CCMP. (Это истинно, что некоторые точки доступа и некоторые клиенты ограничивают комбинации, но существует четыре возможных сочетания). Различие между WPA1 и WPA2 находится в информационных элементах, которые помещены в сигналы-маяки, кадры ассоциации и кадры четырехстороннего квитирования. Данные в этих информационных элементах являются в основном тем же, но используемый идентификатор является другим. Основное различие в ключевом квитировании - то, что WPA2 включает начальную группу, вводят четырехстороннее квитирование, и первое квитирование ключа группы пропущено, тогда как WPA должен сделать это дополнительное квитирование для отправки начальных ключей группы. Смена ключа ключа группы происходит таким же образом. Квитирование происходит перед выбором и использованием набора шифров (TKIP или AES) для передачи датаграмм пользователя. Во время WPA1 или квитирования WPA2, определен набор шифров для использования. После того, как выбранный, набор шифров используется для всего трафика пользователя. Таким образом WPA1 плюс AES не является WPA2. WPA1 обеспечивает (но часто ограниченная клиентская сторона), или TKIP или шифр AES.

Вопрос. . Что такое AES?

O. AES обозначает Расширенный стандарт шифрования. AES предлагает много усиленного шифрования. AES использует алгоритм Rijndael, который является блочным шифром с 128-, 192-, и 256-разрядная ключевая поддержка и намного более силен, чем RC4. Для устройств WLAN для поддержки AES аппаратные средства должны поддержать AES вместо WEP.

Вопрос. . Какие методы аутентификации поддерживаются сервером Microsoft Internet Authentication Service (IAS)?

O. IAS поддерживает эти протоколы аутентификации:

- Протокол аутентификации пароля (PAP)
- Протокол проверки пароля Shiva (SPAP)
- Протокол аутентификации по квитированию вызова (CHAP)
- Протокол квитирования с аутентификацией Microsoft (MS-CHAP)
- Версия протокола 2 Квитирования с аутентификацией Microsoft (MS-CHAP v2)
- CHAP дайджеста 5 сообщения протокола расширенной проверки подлинности (CHAP EAP-MD5)
- Transport Layer Security EAP (EAP-TLS)
- Защищенный MS-CHAP EAP v2 (PEAP-MS-CHAP v2) (также известный как PEAPv0/EAP-MSCHAPv2)

Когда Пакет обновления Сервера Windows 2000 4 установлен, IAS TLS PEAP в Сервере Windows 2000 поддерживает PEAP-MS-CHAP v2 и TLS PEAP. Для получения дополнительной информации обратитесь к Методам аутентификации для использования с IAS.

Вопрос. . Как VPN внедрена в беспроводной среде?

O. VPN является механизмом безопасности уровня 3; беспроводные механизмы шифрования внедрены на Уровне 2. VPN внедрена по 802.1x, EAP, WEP, TKIP и AES. Когда механизм Уровня 2 существует, VPN добавляет издержки к реализации. В местах как общие хот-споты и отели, где никакая безопасность не внедрена, VPN была бы полезным решением внедрить.

Устранение проблем и часто задаваемые вопросы дизайна

Вопрос. . Есть ли какие-либо оптимальные методы для развертывания безопасности беспроводной связи в LAN беспроводных сетей для развертывания вне зданий?

O. См. Оптимальные методы Для Безопасности Беспроводных сетей для развертывания вне зданий. Этот документ предоставляет сведения об оптимальных методах безопасности для развертывания LAN беспроводных сетей для развертывания вне зданий.

Вопрос. . Я могу использовать Windows 2000 или сервер 2003 с Active Directory для сервера RADIUS для аутентификации беспроводных клиентов?

O. Windows 2000 или сервер 2003 с Active Directory могут работать как сервер RADIUS. Для получения информации о том, как настроить этот сервер RADIUS, необходимо связаться с Microsoft, потому что Cisco не поддерживает конфигурацию Windows Server.

Вопрос. . Мой узел собирается мигрировать от открытой беспроводной сети (350 и AP серии 1200) к сети PEAP. Я хотел бы иметь обоих, которые ОТКРЫТЫЙ SSID (SSID, настроенный для Открытой аутентификации) и SSID

PEAP (SSID, настроенный для Аутентификации PEAP), работает на тот же AP в то же время. Это дает нам время для миграции клиентов на SSID PEAP. Существует ли способ одновременно разместить Открытый SSID и SSID PEAP на том же AP?

O. AP Cisco поддерживают VLAN (только уровень 2). Это - фактически единственный способ достигнуть того, что вы хотите сделать. Необходимо создать две VLAN, (собственный компонент и другая VLAN). Затем у вас могут быть Ключ WEP для одного и никакой Ключ WEP для другого. Таким образом, можно настроить одну из VLAN для Открытой аутентификации и другой VLAN для аутентификации PEAP. См. Использование VLAN с Беспроводным оборудованием Cisco Aironet, если вы хотите понять, как настроить VLAN.

Обратите внимание на то, что необходимо настроить коммутаторы для dot1Q, и для предают земле Маршрутизацию виртуальной локальной сети, коммутатор L3 или маршрутизатор.

Вопрос. . Я хочу установить свой VxWorks AP Cisco 1200 года, чтобы сделать, чтобы пользователи беспроводной связи аутентифицировались на концентраторе VPN Cisco 3005. Какая конфигурация должна присутствовать на AP и клиентах для выполнения этого?

O. Нет никакой определенной конфигурации, необходимой на AP или клиентах для этого сценария. Необходимо реализовать все конфигурации на концентраторе VPN.

Вопрос. . Я развертываю AP AG Cisco 1232. Я хотел бы знать самый безопасный метод, который я могу развернуть с этим AP. У меня нет AAA-сервера, и мои единственные ресурсы являются AP и доменом Windows 2003. Я знаком с тем, как использовать статические 128-разрядные ключи WEPs, нешироковещательный SSID и ограничения MAC-адреса. Пользователи главным образом работают с рабочими станциями Windows XP и некоторыми PDA. Какова самая безопасная реализация для этой настройки?

O. Если у вас нет сервера RADIUS как ACS Cisco, можно настроить AP как локальный сервер RADIUS для LEAP, EAP-FAST или проверки подлинности MAC.

Примечание: Очень важный момент, который необходимо рассмотреть, - хотите ли вы использовать своих клиентов с LEAP или EAP-FAST. Если так, у ваших клиентов должна быть утилита для поддержки LEAP или EAP-FAST. Утилита Windows XP только поддерживает PEAP или EAP-TLS.

Вопрос. . Аутентификация PEAP отказывает с ошибкой "EAP-TLS или аутентификацию PEAP, подведенную во время подтверждения связи SSL". В чем причина?

O. Эта ошибка может произойти из-за идентификатора ошибки Cisco CSCee06008 (только зарегистрированные клиенты). PEAP отказывает с ADU 1.2.0.4. Обходной путь для этой проблемы должен использовать последнюю версию ADU.

Вопрос. . У меня могут быть WPA и аутентификация Локального MAC - адреса на том же SSID?

О. AP Cisco не поддерживает аутентификацию локального MAC - адреса и Ключ Pre-share Защищенного доступа по протоколу Wi-Fi (WPA-PSK) в тех же идентификаторах наборов сервисов (SSID). При включении аутентификации локального MAC - адреса с WPA-PSK WPA-PSK не работает. Эта проблема возникает из-за того, что при аутентификации локального MAC удаляется строка настройки, содержащая пароль WPA-PSK ASCII.

Вопрос. . У нас в настоящее время есть три настройки AP беспроводных сетей Cisco 1231 с Шифрами 128-разрядное Шифрование WEP для нашего VLAN для передачи данных. Мы не передаем SSID. У нас нет отдельного сервера RADIUS в нашей среде. Кто-то смог определить Ключ WEP через программное средство сканирования и использовал программное средство в течение нескольких недель для мониторинга нашего беспроводного трафика. Как мы можем предотвратить это и сделать сеть безопасной?

О. Если хакер перехватывает достаточно пакетов и в состоянии получить два или больше пакета с тем же Вектором инициализации (IV), статический ключ WEP уязвим для этой проблемы и может быть получен.

Существует несколько способов предотвратить возникновение этой проблемы:

1. Используйте динамические Ключи WEP.
2. Используйте WPA.
3. Если вы имеете только адаптеры Cisco, включаете На Пакетный Ключ и MIC.

Вопрос. . Если у меня есть два других WLAN, оба настроенные для Защищенного доступа по протоколу Wi-Fi (WAP) - Предобщий ключ (PSK), предварительные общие ключи могут быть другими на WLAN? Если они являются другими, это влияет на другой WLAN, настроенный с другим предварительным общим ключом?

О. Значение WPA-PSK должно быть на WLAN. При изменении одного WPA-PSK он не должен влиять на другой WLAN, который настроен.

Вопрос. . В моей среде я использую главным образом Pro/Беспроводной Intel, Гибкая аутентификация через защищенное туннелирование для расширяемого протокола аутентификации (EAP-FAST) и сервер Cisco Secure Access Control Server (ACS) 3.3 связанных к учетным записям Windows Active Directory (AD). Проблема состоит в том, когда пароль пользователя собирается истечь, Windows не побуждает пользователя изменять пароль. В конечном счете учетная запись истекает. Существует ли решение заставить Windows побудить пользователя изменять пароль?

О. Функция устаревания пароля Cisco Secure ACS позволяет вам вынудить пользователей изменить свои пароли под один или больше этих условий:

- После заданного номера дней (правила возраста по дате)
- После заданного номера входов в систему (правила возраста использованием)
- Первоначально новый пользователь входит (правило изменения пароля)

Для получения дополнительной информации о том, как настроить Cisco Secure ACS для этой функции, обратитесь к Включению Устаревания пароля для Базы данных пользователей CiscoSecure.

Вопрос. . Когда входы пользователя в систему в беспроводном использовании LEAP они заставляют свой сценарий регистрации подключать сетевые диски. Однако с помощью Защищенного доступа по протоколу Wi-Fi (WAP) или WPA2 с аутентификацией PEAP, сценарии регистрации не работают. И клиентом и точкой доступа является Cisco, как RADIUS (ACS). Почему сценарий регистрации не работает на RADIUS (ACS)?

О. Аутентификация компьютера является обязательной для сценариев регистрации для работы. Это позволяет пользователям беспроводной связи получить доступ к сети для загрузки сценариев перед входами пользователя в систему на.

Для получения информации о том, как настроить аутентификацию компьютера с PEAP-MS-CHAPv2, обратитесь к Cisco Secure ACS Настройки для Windows v3.2 With PEAP-MS-CHAPv2 Machine Authentication.

Вопрос. . С выпуском 3.0 утилиты Cisco Aironet Desktop Utility (ADU), когда пользователь настраивает аутентификацию компьютера для Transport Layer Security расширяемого протокола аутентификации (EAP-TLS), ADU не позволяет пользователю создавать профиль. В чем причина?

О. Это вызвано тем, что идентификатора ошибки Cisco CSCsg32032 (только зарегистрированные клиенты). Если клиентскому компьютеру установили сертификат компьютера и не имеет сертификата пользователя, это может произойти.

Обходной путь должен скопировать сертификат компьютера к пользовательскому хранилищу, создать профиль EAP-TLS и затем удалить сертификат из пользовательского хранилища для аутентификации компьютера только конфигурация.

Вопрос. . Там какой-либо путь состоит в том, чтобы назначить VLAN на Беспроводной локальной сети на основе MAC-адреса клиента?

О. Нет. Это не возможно. Назначение VLAN от сервера RADIUS только работает с 802.1x, не Проверкой подлинности MAC. Если MAC-адреса аутентифицируются в сервере RADIUS (определенный как идентификатор пользователя/пароль в LEAP/PEAP), можно использовать RADIUS для продвижения VSA с проверкой подлинности MAC.

Дополнительные сведения

- Безопасность беспроводной сети
- Описание технологических решений безопасности беспроводной локальной сети
- Обзор безопасности беспроводной локальной сети

- Руководство по развертыванию EAP-TLS для беспроводных локальных сетей
- LEAP Cisco
- Настройка WEP (Wired Equivalent Privacy)
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация