

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Решения по обеспечению безопасности единой беспроводной сети Cisco \(UWN\)](#)

[Матрица совместимости безопасности контроллеров беспроводной LAN 2-го и 3-го уровней](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет матрицу совместимости для Уровня 2 и механизмов безопасности уровня 3, поддерживаемых на Контроллере беспроводной локальной сети (WLC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основные сведения о настройке "облегченных" точек доступа и беспроводных локальных сетей Cisco
- Основные сведения о протоколе облегченных точек доступа (LWAPP)
- Базовые знания о решениях для безопасности беспроводной связи

Используемые компоненты

Сведения в этом документе основываются на WLC Серии Cisco 4400/2100, который выполняет версию микропрограммы 7.0.116.0

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Решения по обеспечению безопасности единой

беспроводной сети Cisco (UWN)

Единая беспроводная сеть Cisco (UWN) поддерживает методы безопасности уровня 3 и Уровень 2.

- Безопасность уровня 2
- Безопасность уровня 3 (для WLAN) или безопасность уровня 3 (для Гостевой LAN)

Безопасность уровня 2 не поддерживается на Гостевых LAN.

Эта таблица приводит различный Уровень 2 и методы безопасности уровня 3, поддерживаемые на Контроллере беспроводной локальной сети. Эти методы безопасности могут быть включены от **Вкладки Безопасность на WLAN> страница Edit WLAN.**

| Механизм безопасности уровня 2 | | |
|--------------------------------|-------------------------------|--|
| Параметр | | Описание |
| Безопасность уровня 2 | Нет | Никакая безопасность уровня 2 не выбрана. |
| | WPA+WPA2 | Используйте это приводящее в порядок для включения Защищенного доступа по протоколу Wi-Fi. |
| | 802.1x | Используйте это приводящее в порядок для включения аутентификации 802.1x. |
| | Статический ключ WEP | Используйте это приводящее в порядок для включения шифрования Статического ключа WEP. |
| | Статический ключ WEP + 802.1x | Используйте это приводящее в порядок для включения и Статического ключа WEP и параметров 802.1x. |
| | SKIP | Используйте это приводящее в |

| | | |
|--|--|---|
| | | <p>порядок для включения протокола целостности ключей Cisco (SKIP). Функциональный на использованных моделях точки доступа 1100, 1130, и 1200, но не AP 1000. IE aironet должен быть позволен для этой функции работать. SKIP разворачивает ключи шифрования до 16 байтов.</p> |
|--|--|---|

| | |
|---------------------------|--|
| Фильтрация по MAC-адресам | <p>Выберите для фильтрации клиентов MAC-адресом. Локально настройте клиентов MAC-адресом на странице MAC Filters> New. В противном случае настройте клиентов на сервере RADIUS.</p> |
|---------------------------|--|

Механизм безопасности уровня 3 (для WLAN)

| Параметр | | Описание |
|-----------------------|-------|---|
| Безопасность уровня 3 | Нет | Никакая безопасность уровня 3 не выбрана. |
| | IPSec | <p>Используйте это приводящее в порядок для включения IPSec. Необходимо проверить доступность ПО и совместимость оборудования клиента перед реализацией IPSec.</p> <p>Примечание: У вас должен быть дополнительный Модуль VPN/Усиленной безопасности</p> |

| | | |
|---------------------|---|--|
| | | <p>(крипто-карта процессора) установленный для включения IPSec. Проверьте, что это установлено на вашем контроллере на странице Inventory.</p> |
| | <p>Passthrough VPN</p> | <p>Используйте это приводящее в порядок для включения Passthrough VPN. Примечание: Эта опция не доступна на Контроллерах серии 5500 Cisco и Cisco Контроллеры серии 2100. Однако можно реплицировать эту функциональность в Контроллер серии 5500 Cisco или Cisco Контроллер серии 2100 путем создания открытого WLAN с помощью ACL.</p> |
| <p>Веб-политика</p> | <p>Установите этот флажок для включения веб-Политики. Контроллер передает трафик DNS к и от беспроводных клиентов перед аутентификацией. Примечание: Веб-Политика не может использоваться в сочетании с опциями Pass-Through VPN или IPSec. Эти параметры отображены:</p> <ul style="list-style-type: none"> • Аутентификация? Если вы выбираете эту опцию, пользователю предлагают для имени пользователя и пароля при подключении клиента с беспроводной сетью. | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Passthrough? Если вы выбираете эту опцию, пользователь может обратиться к сети непосредственно без аутентификации имени пользователя и пароля. • Условное веб-Перенаправление? Если вы выбираете эту опцию, пользователь может быть условно перенаправлен к определенной веб-странице после того, как аутентификация 802.1X успешно завершает. Можно задать страницу перенаправления и условия, при которых перенаправление происходит на сервере RADIUS. • Веб-Перенаправление Страницы-заставки? Если вы выбираете эту опцию, пользователь перенаправлен к определенной веб-странице после того, как аутентификация 802.1X успешно завершает. После перенаправления у пользователя есть полный доступ к сети. Можно задать веб-страницу всплеска на сервере RADIUS. • На сбоее Фильтра MAC? Включает сбой фильтра MAC web-аутентификации. |
| ACL предварительной проверки подлинности | Выберите ACL, который будет использоваться для трафика между клиентом и контроллером. |
| Over-ride Global Config | Показы, если вы выбираете Authentication. Установите этот флажок для переопределения набора конфигурации глобальной аутентификации на Веб-странице для входа. |
| Веб-Подлинный тип | Показы, если вы выбираете Web Policy и Over-ride Global Config. Выберите тип Web-аутентификации: <ul style="list-style-type: none"> • Внутренний • Настроенный (Загруженный) Страница входа в систему? |

| | |
|--|---|
| | <p>Выберите страницу входа от выпадающего списка. Страница Login Failure? Выберите страницу входа, которая отображается клиенту, если отказывает Web-аутентификация. Страница Logout? Выберите страницу входа, которая отображается клиенту когда входы пользователя в систему из системы.</p> <ul style="list-style-type: none"> • Внешний (Перенаправление к внешнему серверу) Url ? Введите URL внешнего сервера. |
|--|---|

| | |
|---------------|---|
| Почтовый ввод | Показы, если вы выбираете Passthrough. При выборе этой опции вам предлагают для вашего адреса электронной почты при соединении с сетью. |
|---------------|---|

Механизм безопасности уровня 3 (для гостевой LAN)

| Параметр | | Описание |
|--|--------------------|---|
| Безопасность уровня 3 | Нет | Никакая безопасность уровня 3 не выбрана. |
| | Web-аутентификация | При выборе этой опции вам предлагают для имени пользователя и пароля при подключении клиента с сетью. |
| | Веб-Passthrough | При выборе этой опции можно обратиться к сети непосредственно без аутентификации имени пользователя и пароля. |
| ACL предварительной проверки подлинности | | Выберите ACL, который будет использоваться для трафика между клиентом и контроллером. |

| | |
|-------------------------|---|
| Over-ride Global Config | Установите этот флажок для переопределения набора конфигурации глобальной аутентификации на Веб-странице для входа. |
| Веб-Подлинный тип | <p>Показы, если вы выбираете Over-ride Global Config. Выберите тип Web-аутентификации:</p> <ul style="list-style-type: none">• Внутренний• Настроенный (Загруженный) Страница входа в систему? Выберите страницу входа от выпадающего списка. Страница Login Failure? Выберите страницу входа, которая отображается клиенту, если отказывает Web-аутентификация. Страница Logout? Выберите страницу входа, которая отображается клиенту когда входы пользователя в систему из системы. |

| | |
|---------------|---|
| | <ul style="list-style-type: none"> • Внешний (Перенаправление к внешнему серверу) Url ? Введите URL внешнего сервера. |
| Почтовый ввод | Показы, если вы выбираете Web Passthrough. При выборе этой опции вам предлагают для вашего адреса электронной почты при соединении с сетью. |

Примечание: В выпуске ПО контроллера 4.1.185.0 или позже, SKIP поддерживается для использования только со статическим ключом WEP. Это не поддерживается для использования с динамическим WEP. Поэтому беспроводной клиент, который настроен для использования SKIP с динамическим WEP, неспособен связаться к беспроводной локальной сети, которая настроена для SKIP. Cisco рекомендует использовать любой динамический WEP без SKIP (который менее безопасен), или WPA/WPA2 с TKIP, или AES (которые более безопасны).

[Матрица совместимости безопасности контроллеров беспроводной LAN 2-го и 3-го уровней](#)

При настройке безопасности на Беспроводной локальной сети и Уровень 2 и методы безопасности уровня 3 могут использоваться совместно. Однако не все методы безопасности уровня 2 могут использоваться со всеми методами безопасности уровня 3. Эта таблица показывает матрицу совместимости для Уровня 2 и методов безопасности уровня 3, поддерживаемых на Контроллере беспроводной локальной сети.

| Механизм безопасности уровня 2 | Механизм безопасности уровня 3 | Совместимость |
|--------------------------------|--------------------------------|---------------|
| Нет | Нет | Допустимый |
| WPA+WPA2 | Нет | Допустимый |
| WPA+WPA2 | Web-аутентификация | Недопустимый |
| WPA-PSK/WPA2-PSK | Web-аутентификация | Допустимый |
| WPA+WPA2 | Веб-Passthrough | Недопустим |

| | | |
|-------------------------------|---------------------------------------|--------------|
| | | ый |
| WPA-PSK/WPA2-PSK | Веб-Passthrough | Допустимый |
| WPA+WPA2 | Условное веб-перенаправление | Допустимый |
| WPA+WPA2 | Веб-перенаправление страницы-заставки | Допустимый |
| WPA+WPA2 | VPN-PassThrough | Допустимый |
| 802.1x | Нет | Допустимый |
| 802.1x | Web-аутентификация | Недопустимый |
| 802.1x | Веб-Passthrough | Недопустимый |
| 802.1x | Условное веб-перенаправление | Допустимый |
| 802.1x | Веб-перенаправление страницы-заставки | Допустимый |
| 802.1x | VPN-PassThrough | Допустимый |
| Статический ключ WEP | Нет | Допустимый |
| Статический ключ WEP | Web-аутентификация | Допустимый |
| Статический ключ WEP | Веб-Passthrough | Допустимый |
| Статический ключ WEP | Условное веб-перенаправление | Недопустимый |
| Статический ключ WEP | Веб-перенаправление страницы-заставки | Недопустимый |
| Статический ключ WEP | VPN-PassThrough | Допустимый |
| Статический ключ WEP + 802.1x | Нет | Допустимый |
| Статический ключ WEP + 802.1x | Web-аутентификация | Недопустимый |
| Статический ключ WEP + 802.1x | Веб-Passthrough | Недопустимый |
| Статический ключ WEP + 802.1x | Условное веб-перенаправление | Недопустимый |
| Статический ключ WEP + 802.1x | Веб-перенаправление страницы-заставки | Недопустимый |
| Статический ключ | VPN-PassThrough | Недопустимый |

| | | |
|--------------|---------------------------------------|--------------|
| WEP + 802.1x | | ый |
| SKIP | Нет | Допустимый |
| SKIP | Web-аутентификация | Допустимый |
| SKIP | Веб-Passthrough | Допустимый |
| SKIP | Условное веб-перенаправление | Недопустимый |
| SKIP | Веб-перенаправление страницы-заставки | Недопустимый |
| SKIP | VPN-PassThrough | Допустимый |

[Дополнительные сведения](#)

- [Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа](#)
- [Регистрация облегченных точек доступа у контроллере беспроводных LAN \(WLC\)](#)
- [Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0.116.0](#)
- [Часто задаваемые вопросы по контроллеру беспроводной LAN \(WLC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)