Содержание

Введение

Этот документ предоставляет пример конфигурации для проверки подлинности для администратора HTTP на версии 1.01 Точки доступа (AP).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 2.6.4 Access Control Server (ACS) и позже

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 в документах см. Cisco Technical Tips Conventions.

Общие сведения

Нет никакой опции для настройки TACACS + или учет RADIUS или авторизация для выполнения команд для Сеансов exec в GUI. Эти опции могут быть настроены в CLI, но *не* рекомендуются. Если вы настраиваете эти опции, они могут сильно сорвать AP и ACS с учетом, или запросы авторизации (каждый элемент каждой страницы должен считаться или авторизоваться для).

Конфигурация AcS

Настройка интерфейса

Выполните эти шаги для настройки интерфейса:

1. В TACACS + (Cisco IOS), выберите Групповой блок для первого неопределенного нового сервисного поля.
2. В поле Service введите **Aironet**.
3. В Поле протокола введите **Shell**.
4. В Пунктах меню Advanced Configuration Option выберите **Advanced TACACS + Функции> Показ окно для каждого выбранного сервиса**.
5. **Нажмите кнопку Submit (Отправить).**

Пользовательская конфигурация

Выполните эти шаги для настройки пользователя:

1. В Advanced TACACS + Параметры настройки, выберите **Shell (exec)**.
2. Выберите Уровень привилегий.
3. В поле войдите **15**.
4. **Нажмите кнопку Submit (Отправить).**

Конфигурация группы

Выполните эти шаги для настройки группы:

1. Выберите **TACACS +**.
2. Выберите **Aironet Shell> Настраиваемые атрибуты**.
3. В поле Custom Attributes войдите **aironet:admin-capability=write+ident+firmware+admin+snmp**.
4. **Нажмите кнопку Submit (Отправить).**
5. Перезапуск.

Конфигурация сети

Выполните эти шаги для настройки сети:

1. Создайте NAS для AP с помощью TACACS + как протокол.
2. Ключ является общим секретным ключом от AP.
3. **Нажмите кнопку Submit (Отправить).**
4. Перезапуск.

Примечание: При использовании символического сервера с одноразовым паролем необходимо настроить маркер, кэширующийся во избежание того, чтобы быть непрерывно предложенным для паролей уровня 15 и уровня 1. Выполните эти шаги для настройки маркерного кэширования:

1. Введите конфигурацию группы для группы, которой принадлежат ваши пользователи с правами администратора.
2. Выберите **Token Card Settings**.
3. Выберите **Duration**.
4. Выберите продолжительность, которая балансирует ваши потребности в безопасности и удобстве.

Если ваш типичный сеанс admin длится пять минут или меньше, то значение продолжительности пяти минут является лучшим. Если ваш сеанс выполняется дольше, чем пять минут, вам предлагают снова для вашего пароля в пятиминутных интервалах. Обратите внимание на то, что Параметр сеанс не работает, не считая, включил. Кроме того, обратите внимание, что маркерное кэширование в действительности для *всех* пользователей в группе, и для *всех* сеансов группы со всеми устройствами (не только Сеансы exec к AP).

Конфигурация точки доступа для VxWorks

Пользовательская конфигурация

Выполните следующие действия:

1. Выберите **Setup> Security> User Information> Add New User**.
2. Add a New User с полными административными возможностями (все проверенные параметры настройки возможности).
3. Нажмите **Back**. Вы возвращены к странице Security Setup.
4. Нажмите **User Manager**. Страница настройки Менеджера пользователей появляется.
5. Включите **менеджеру пользователей**.
6. **Нажмите кнопку OK.**

Конфигурация сервера

Выполните следующие действия:

1. Выберите **Setup> Security> Authentication Server**.
2. Введите TACACS + IP-адрес сервера.
3. Выберите тип Сервера tacacs.
4. В поле введите **порт 49**.
5. В поле введите **общий секретный ключ**.

6. Выберите коробку **Проверки подлинности пользователя**.

Конфигурация точки доступа для IOS

Выполните эти шаги для настройки AP для IOS:

1. Выберите **Security> Server Manager**.
2. Выберите настроенный TACACS + Сервер или настройте новый.
3. **Щелкните "Применить".**
4. Выберите TACACS +, IP сервера в Admin Authentication (TACACS +) выпадает.
5. **Щелкните "Применить".**
6. Выберите **Security> Admin Access**.
7. Создайте локального пользователя с доступом для чтения-записи (если вы поэтому уже не сделали).
8. **Щелкните "Применить".**
9. Выберите Authentication Server Only или Authentication Server (если не найденный в Локальном списке).
10. **Щелкните "Применить".**

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка Продукта серии Aironet 1200
- Terminal Access Controller Access Control System (TACACS) (TACACS +) поддержка технологии
- Поддержка продуктов сервера безопасного контроля доступа Cisco для Windows
- Поддержка продуктов сервера управления безопасного доступа Cisco для Unix
- Техническая поддержка - Cisco Systems