Исключение клиента 802.1X на AireOS WLC

ID документа: 117714

Обновлено : 03 июня 2014

Внесенный Аароном Леонардом и Шанкаром Раманатаном, специалистами службы технической поддержки Cisco.

Родственные продукты

- Wireless, LAN (WLAN)

Содержание

Введение

Этот документ описывает Клиента 802.1X Экслузайона на Контроллере беспроводной локальной сети (WLC) AireOS. Исключение Клиента 802.1X является важной опцией для имения на 1X средство проверки подлинности как WLC. Это в порядке для предотвращения перегрузки инфраструктуры сервера проверки подлинности клиентами Протокола EAP, которые гиперактивны или функционируют неправильно.

Варианты использования

Варианты использования в качестве примера включают:

- Соискатель EAP может быть настроен с неправильными учетными данными. Большинство соискателей, таких как соискатели EAP, прекращает попытки аутентификации после нескольких последовательных сбоев. Однако некоторые соискатели EAP продолжают попытки повторно аутентифицироваться после сбоя,

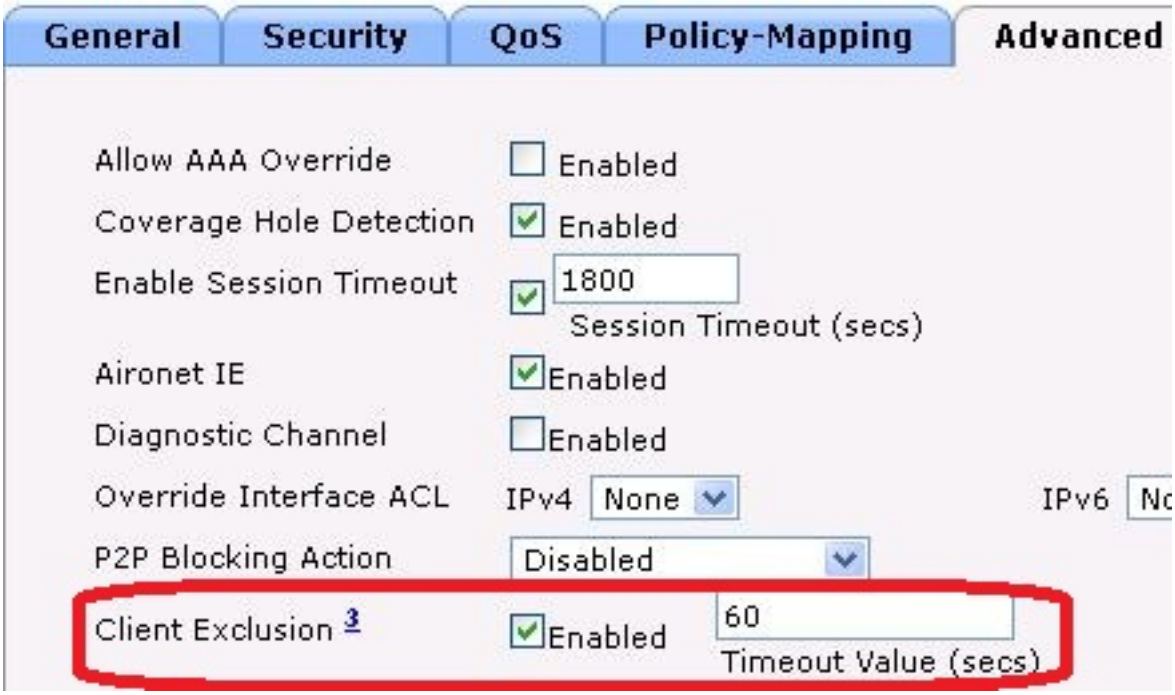
возможно много раз в секунду. Некоторые серверы RADIUS перегрузки клиентов и причина Отказ в обслуживании (DoS) для всей сети.

- После аварийного переключения крупной сети сотни или тысячи клиентов EAP могли бы одновременно попытаться аутентифицироваться. В результате серверы проверки подлинности могли бы быть перегружены и предоставить медленный ответ. Если таймаут клиентов или средства проверки подлинности перед медленным ответом обработан, то порочный круг может произойти, где попытки аутентификации продолжают вызывать таймаут, и затем пытаться обработать ответ снова.

  Примечание: Механизм контроля за соединением требуется, чтобы позволить попыткам аутентификации успешно выполняться.

Исключение 802.1X предотвращает клиентов, которые инициируют перегрузку в течение 30 секунд к нескольким минутам после сбоя, который позволяет обычным аутентификациям успешно выполняться. AireOS WLC номинально имеет исключение клиента 802.1X globablly, включил под Безопасностью> беспроводная Политика обеспечения защиты по умолчанию. Посмотрите политику, показанную здесь.

Клиентское исключение могло бы быть включено или отключено на основе на WLAN. По умолчанию это включено с таймаутом 60 секунд.



Однако из-за таймаута EAP по умолчанию и параметров настройки повторной передачи, исключение 802.1X никогда не вступает в силу.

Клиенты WLC, Не Исключенные, когда Включено Исключение 802.1X

Когда исключение 802.1X включено на WLAN, клиенты WLC не исключены. Это происходит из-за длинных таймаутов EAP по умолчанию 30 секунд, которые вызывают клиента, который плохо себя ведет, чтобы никогда поразить достаточно последовательных сбоев для инициирования исключения. Настройте более короткие таймауты EAP с увеличенными количествами повторных передач, чтобы позволить исключению 802.1X вступать в силу. Посмотрите пример таймаута здесь.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

Удостоверьтесь, что сервер RADIUS защищен от перегрузки из-за беспроводных клиентов, которые функционируют неправильно и проверяют, что эти параметры настройки в действительности:

- "Чрезмерные Ошибки проверки подлинности 802.1X" выбраны в глобальной Клиентской Политике Исключения WLC.
- Клиентское исключение включено в расширенных настройках WLAN.
- Клиентский таймаут исключения установлен в 60 - 300 секунд.

Примечание: Оценивает выше, чем 300 секунд обеспечивают лучшую защиту, но могли бы инициировать претензии пользователя.

% Warning: Некоторые соискатели требуют более длинных таймаутов, чем другие. Например, если разовые пароли используются, идентификационный период ожидания

запроса EAP мог бы потребовать 45 секунд, чтобы позволить пользователю вводить новый PIN-код. Некоторая медленная Расширяемая Гибкая Протоколом Аутентификация Authetication с помощью Защищенного протокола (EAP-FAST), соискатели могли бы потребовать более короткого таймаута 20 секунд для размещения инициализации Контроля за защищенным доступом (PAC).

Дополнительные сведения

- **Идентификатор ошибки Cisco** CSCsq16858
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 03 июня 2014
ID документа: 117714