Когда ASA Перезагружен, беспроводной Сбой Соединений Мобильности и Не Восстанавливается

Содержание

Введение

Этот документ описывает проблему, где связь пути мобильности (использующий Протокол UDP и Протокол "IP" 93), который пересекает Устройство адаптивной защиты (ASA) , могла бы выключиться и продолжить прерываться, пока устройства мобильности не повторно загружены, или трафик пути мобильности остановлен и оставлен неактивный в течение короткого времени и затем перезапустил.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Устройство адаптивной защиты Cisco (ASA)
- Контроллер беспроводной локальной сети (WLC)

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям

программного обеспечения и оборудования.

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

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Проблема

В этой ситуации Контроллер беспроводной локальной сети (WLC) при 10.10.1.2 попытках связаться с WLC в 10.10.9.3, но сбои связи.

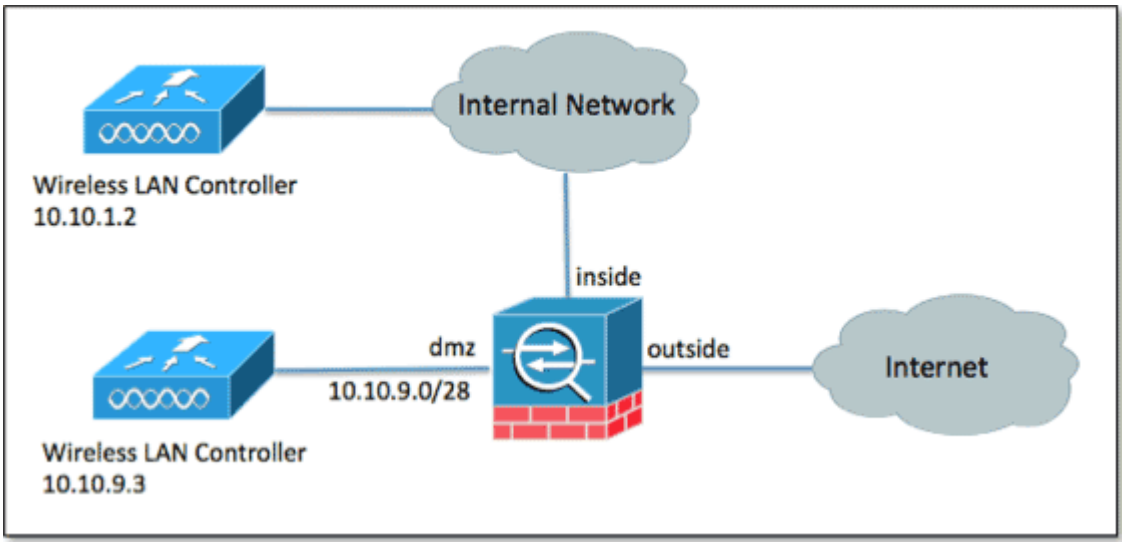
Эта проблема может быть инициирована любым из этих событий:

- ASA перезагружен.
- Таблица маршрутизации модифицируется администратором или протоколом маршрутизации.
- Интерфейс закрыт, затем принесен резервное копирование администратором.

Помимо трафика мобильности, эта проблема могла бы быть испытана для любого UDP или Протоколов "IP" не TCP.

Этой проблемой не является дефект, а последствие конфигурации ASA и топологии сети. Посмотрите ниже по причине и решению этой проблемы.

Примерная топология сети



Настройка маршрутизации ASA:

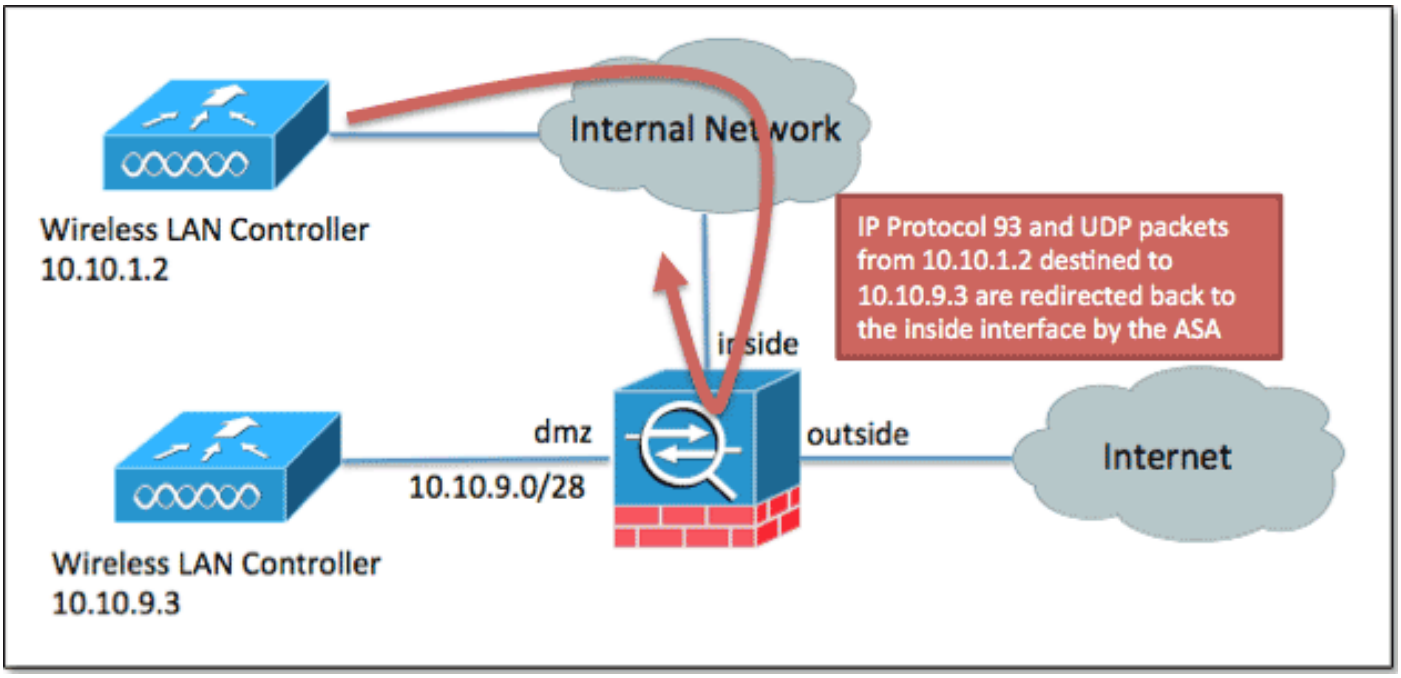
```
!
route outside 0.0.0.0 0.0.0.0 192.168.4.3 1
route inside 10.0.0.0 255.0.0.0 192.168.254.1 1
!
same-security-traffic permit intra-interface
!
```

ASA dmz конфигурация интерфейса:

```
!
interface Gigabit-Ethernet0/1.10
vlan 10
nameif dmz
security-level 75
ip address 10.10.9.1 255.255.255.240 standby 10.10.9.2
!
```

Проблемный триггер

Когда WLC в 10.10.1.2 передает трафик, предназначенный к WLC в 10.10.9.3, проблема инициирована. Эти пакеты заставляют ASA создавать соединение в своей таблице подключений, которая передает трафику мобильности неправильный интерфейс ASA (внутри).



Эта проблема вызвана интерфейсом назначения "dmz" ASA, находящегося во вниз/нерабочее состояние в то время, когда соединение было создано, который приводит к соединению, пристраиваемому другой, интерфейс неоптимального. Интерфейс dmz мог бы не работать из-за проблемы с кабелем, ethernet или проблемы согласования port-channel, или это могло бы быть административно закрыто.

Во время проблемы соединения пути мобильности могут быть замечены как создаваемый как "внутриинтерфейс" ASA, который направляет пакеты, отступают тот же внутренний интерфейс, в который они поступили:

```
ASA# show conn address 10.10.1.2
15579 in use, 133142 most used
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 32210
UDP inside 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 4338, flags -
```

```
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 157240
ASA#
```

Оконечная точка мобильности в 10.10.1.2 продолжает передавать трафик, предназначенный к 10.10.9.3, который совпадает с этими существующими соединениями. Даже если бы интерфейс dmz должен был развиться к состоянию вверх/вверх, трафик мобильности, полученный от 10.10.1.2, совпал бы с существующими соединениями в таблице (вместо того, чтобы создать новое соединение к интерфейсу dmz), который перезагружает таймаут соединений на ASA, который продлевает проблему.

Таким образом, эти события могут инициировать проблему:

1. Устройство в 10.10.1.2 передает протокол 97 или пакет UDP к 10.10.9.3.
2. ASA получает пакет на внутреннем интерфейсе, но интерфейс dmz не работает, который приводит к уточненному маршруту к сети назначения, отсутствующей в таблице маршрутизации. Так как команда **внутриинтерфейса разрешения той-же-безопасности** выполнена на ASA, она придерживается статического маршрута, настроенного для 10.0.0.0/8 сети назад через внутренний интерфейс, создает соединение в таблице подключений, и затем передает пакет обратно внутренний интерфейс к внутренней сети.
3. В некоторый момент интерфейс dmz мог бы возвратиться, и маршрут добавлен назад к таблице; однако, так как соединение для трафика протокола 97 было уже создано в шаге #2, последующие пакеты будут совпадать с соединением, и таблица маршрутизации перезаписана, и трафик не достигает сервера на dmz.

Решение

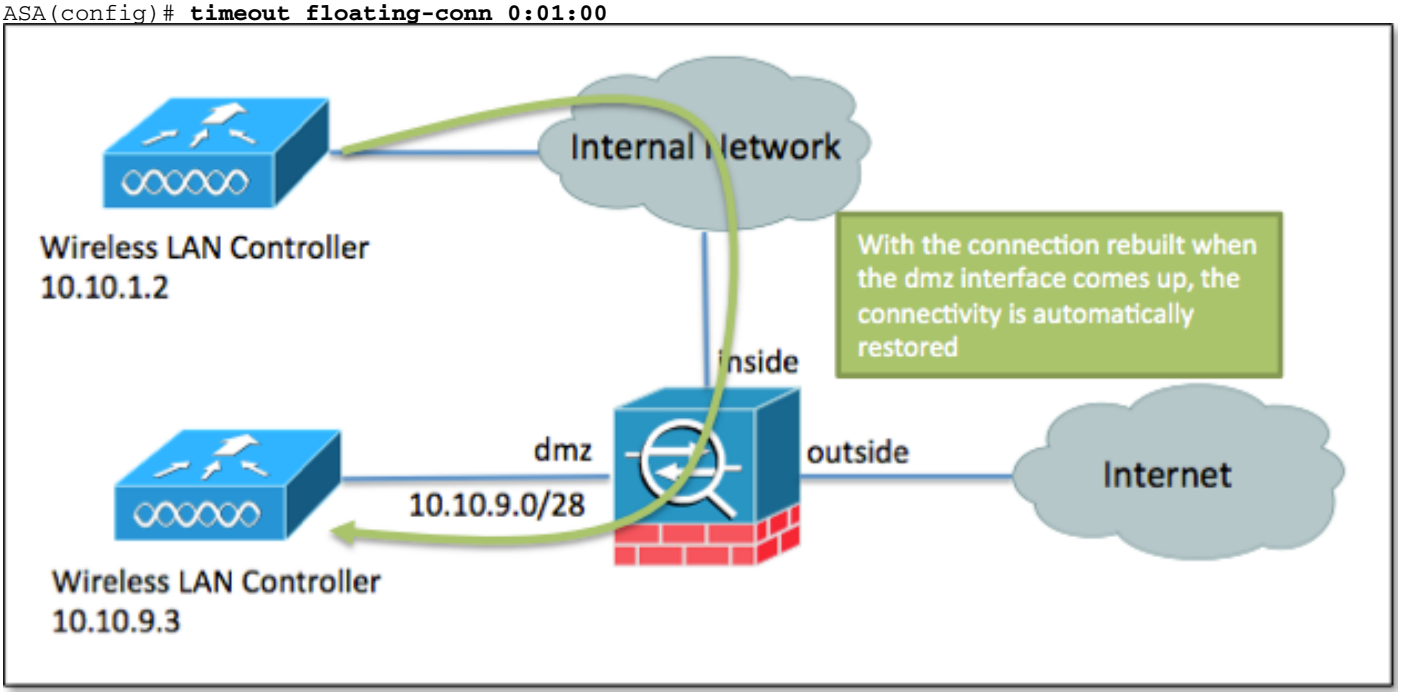
Решение 1

Одно возможное решение для этой проблемы должно удалить команду **внутриинтерфейса разрешения той-же-безопасности** из ASA. Это решение препятствует тому, чтобы соединение разворота было пристроено назад тот же интерфейс, на котором был получен оригинальный пакет, который позволяет корректному соединению быть созданным, когда подходит интерфейс. Однако в зависимости от таблицы маршрутизации ASA, это решение не могло бы работать (трафик мог бы маршрутизироваться к другому интерфейсу кроме целевого места назначения на основе таблицы маршрутизации), и **разрешение той-же-безопасности, внутриинтерфейсная** команда могла бы быть необходимой для других соединений на ASA.

Решение 2

Для этого определенного экземпляра проблема была успешно смягчена путем активации опции **плавания таймаута - ведет**. Эта опция, которая не активирована по умолчанию, заставила ASA разъединять эти соединения спустя одну минуту после этого, больше предпочитаемого маршрута к одной из оконечных точек добавлено к таблице маршрутизации новый интерфейс ASA, который происходит, когда подходит интерфейс dmz. Когда следующий пакет поступает в ASA, с помощью более предпочтительного интерфейса (dmz, вместо внутренней части для этих 10.10.9.3 хостов), соединения тогда сразу восстановлены.

```
ASA(config)# timeout floating-conn 0:01:00
```



Когда проблема смягчена, корректные соединения созданы в таблице подключений ASA, и подключение автоматически восстановлено:

```
ASA# show conn address 10.10.1.2
15329 in use, 133142 most used
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 3175742510
UDP dmz 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 40651338, flags -
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 1593457240
ASA#
```

Дополнительные сведения

- Справочник по командам ASA 9.1 - команда timeout floating-conn
- Cisco Systems – техническая поддержка и документация