目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[問題](#)
[ネットワークトポロジー例](#)
[問題トリガー](#)
[解決策](#)
[解決策 1](#)
[解決策 2](#)
[関連情報](#)

概要

この資料は横断するモビリティ パス接続問題を記述したものです（User Datagram Protocol（UDP; ユーザ データグラム プロトコル）および IP プロトコルを使用してモビリティ デバイスがリロードされるまで 93）適応性があるセキュリティ アプライアンス モデル（ASA は）失敗し、またはモビリティ パス トラフィック少しの間停止し、残された非アクティブ次に再起動しますダウン状態になり、続けるかもしれません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Adaptive Security Appliance（ASA）
- ワイヤレス LAN コントローラ（WLC）

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

問題

この場合 10.10.1.2 のワイヤレス LAN コントローラ（WLC）は 10.10.9.3 で WLC と通信するように試みますが通信は失敗します。

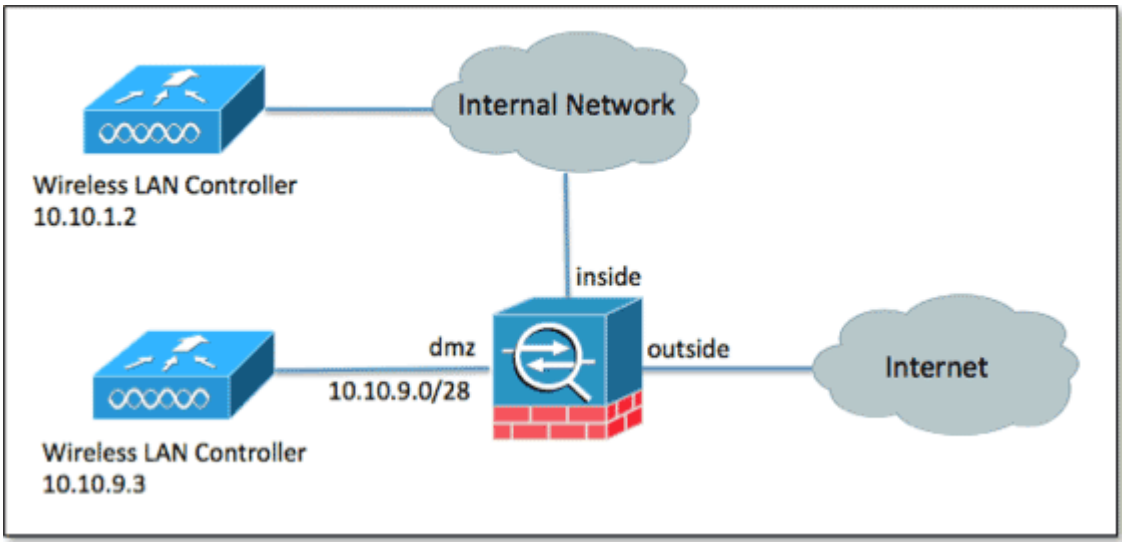
この問題はこれらのイベントの何れかによって引き起こすことができます:

- ASA はリブートされます。
- ルーティング テーブルは管理者かルーティング プロトコルによって修正されます。
- インターフェイスは管理者によってシャットダウンされましたり、そしてバックアップを持って来られます。

モビリティ トラフィックのほかに、この問題はあらゆる UDP または非 TCP IP プロトコルのためにベテランであるかもしれません。

この問題はない不具合 ネットワーク トポロジおよび ASA 設定の結果でありではない。 この問題に原因およびソリューションについては次を参照して下さい。

ネットワークトポロジー例



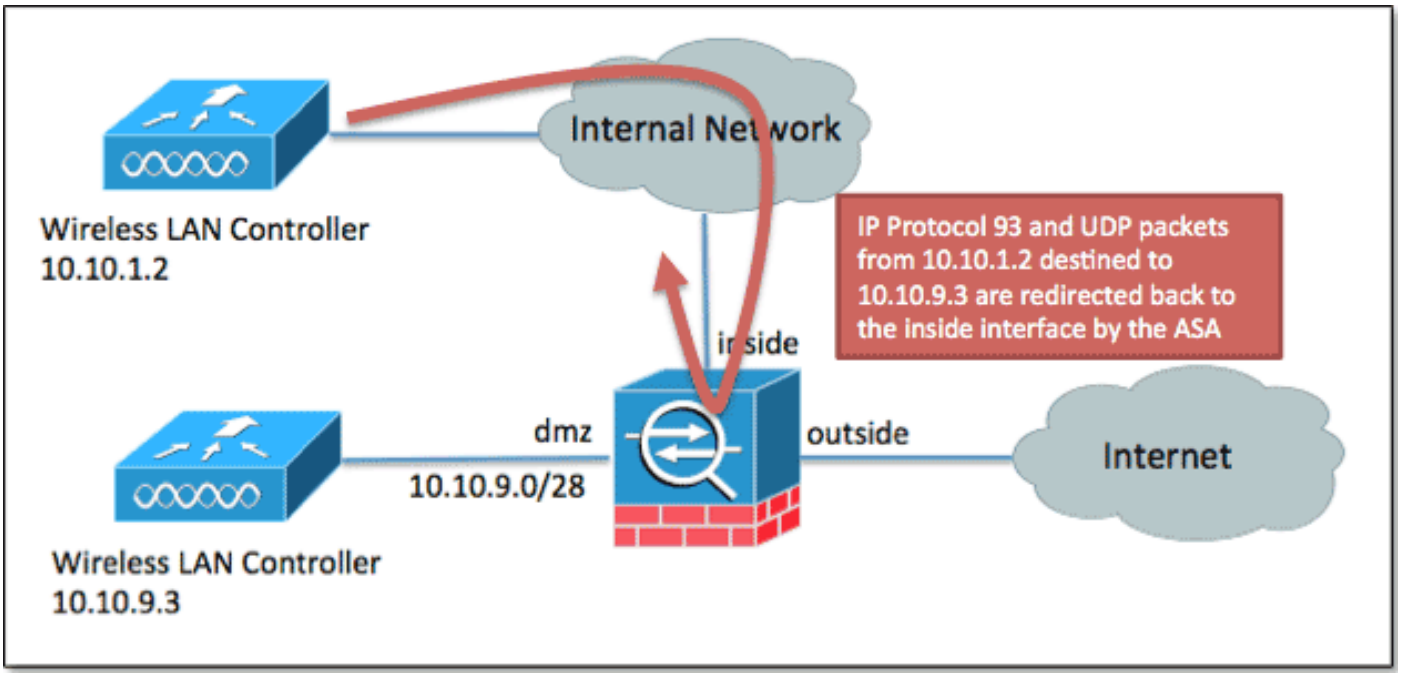
ASA ルーティングコンフィギュレーション:

ASA dmz インターフェイスコンフィギュレーション:

問題トリガー

問題は 10.10.1.2 の WLC が WLC に 10.10.9.3 で送信されるトラフィックを送信 するとき引き起こされます。 これらのパケットにより ASA はモビリティ トラフィックを間違った ASA インタ

ーフェイス 送信 する 接続テーブルで接続を構築します（ 中 ）。



この問題は down/down 状態である ASA のデスティネーションインターフェイス「dmz」によって構築される接続という結果に別、非最適 な インターフェイス終る接続が構築された時引き起こされています。 dmz インターフェイスはケーブル問題、イーサネットまたは port-channel ネゴシエーション問題が原因での下にあるかもしれませんかまたは管理上のシャットダウン状態になるかもしれません。

問題の時に、モビリティ パス接続はルーティングしている ASA の「内部インターフェイス」として作成されて、パケットが同じ内部インターフェイス着いたキャンセルするように見られる場合があります:

```
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#
```

これらの現在の接続と一致する 10.10.1.2 のモビリティ エンドポイントは送信される 10.10.9.3 にトラフィックを送信 し続けます。 dmz インターフェイスが up/upステートへ進歩することでも 10.10.1.2 から送信されたモビリティ トラフィックは問題を延長する、ASA の接続のタイムアウトをリセットする表の現在の接続を一致する（ dmz インターフェイスへの新しい接続を構築するかわりに ）。

要約すると、これらのイベントは問題を引き起こすことができます:

1. 10.10.1.2 のデバイスは 10.10.9.3 にプロトコル 97 か UDP パケットを送信 します。
2. ASA は内部インターフェイスのパケットを受信しますが、ルーティング テーブルに抜けている宛先ネットワークにより多くの特定のルートという結果に終る dmz インターフェイスはダウンしています。 **同じセキュリティ割り当て内部インターフェイス** コマンドが ASA で有効に なるので、内部インターフェイスを通して 10.0.0.0/8 ネットワークのために設定されるスタティック ルートに続き、接続テーブルで接続を構築し、次にパケットを内部インターフェイス キャンセルします内部ネットワークの方の送信 します。
3. ある時点で dmz インターフェイスは戻って来るかもしれないし、ルートは表に戻って追加されます; ただし、プロトコル 97 トラフィックのための接続がステップ #2 で既に構築され

たので、後続パケットは接続を一致する、ルーティング テーブルは上書きされ、トラフィックは dmz のサーバに達しません。

解決策

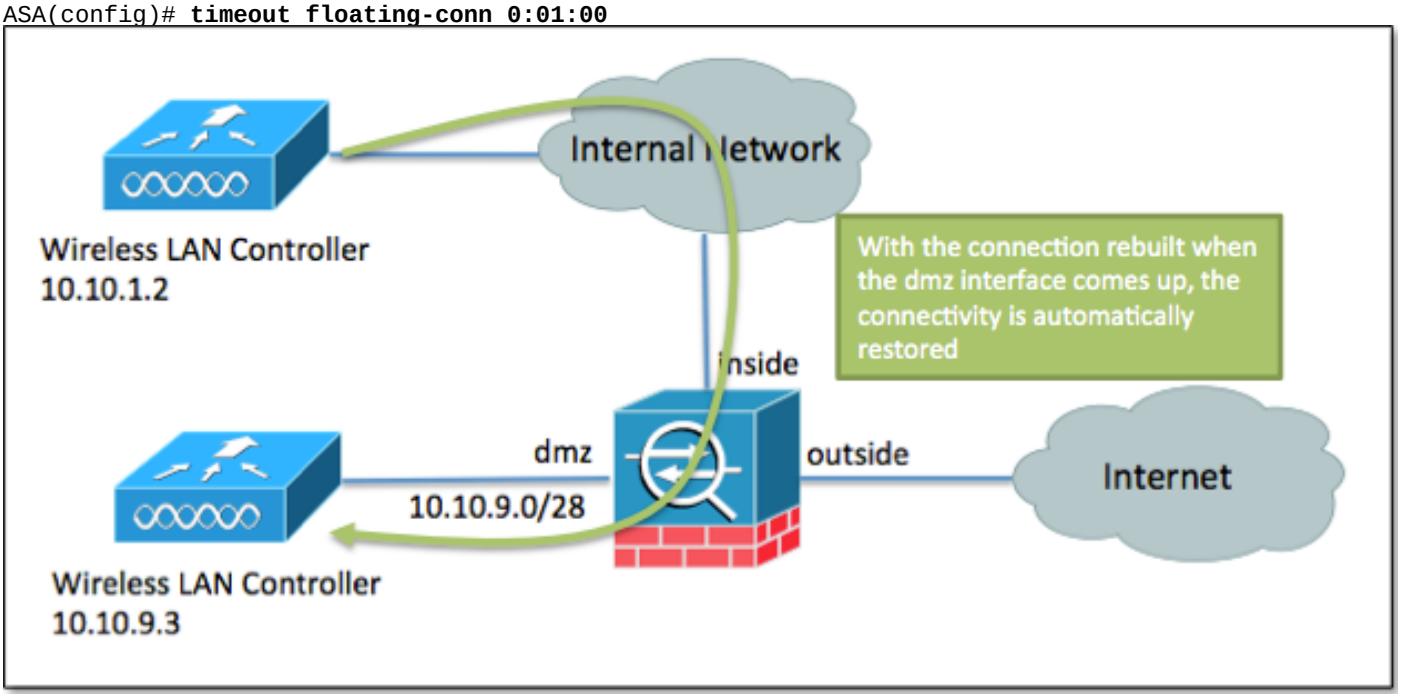
解決策 1

この問題のための 1 つの可能 な 解決策は ASA から同じ**セキュリティ割り当て内部インターフェイス** コマンドを削除することです。 このソリューションは U ターン接続がキャンセルするインターフェイスがアップする時正しい接続が構築されるようにする、オリジナルパケットが受信された構築されることを同じインターフェイス防ぎます。 ただし、ASA のルーティング テーブルによって、このソリューションは (トラフィックはルーティング テーブルに基づいて意図されたデスティネーション以外別のインターフェイスにルーティングされるかもしれました) はたらき、同じ**セキュリティ割り当て内部インターフェイス** コマンドは ASA の他の接続に必要であるかもしれません。

解決策 2

この特定の例に関しては、問題は**タイムアウト浮かべ conn** 機能を有効に することによって正常に軽減されました。 デフォルトで有効に ならないこの機能により ASA はこれらの接続を中断 しました エンドポイントの 1 へのより多くの優先ルートがルーティング テーブルに dmz インターフェイスがアップするとき発生する ASA の新しいインターフェイス追加された 1 分後。 接続はそれからすぐに次 の パケットがより優先 する インターフェイス (10.10.9.3 ホストのための内部の代りの dmz、) を使用して ASA で、着くとき再製されます。

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



問題が軽減されるとき、正しい接続は ASA 接続テーブルで構築され、接続は自動的に復元する:

```
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#
```

関連情報

- ASA 9.1 コマンドレファレンス-タイムアウト浮かべ conn コマンド
- テクニカルサポートとドキュメント - Cisco Systems