ASA をリブートすると、無線モビリティ接続が失敗し、復旧しない

目次

概要

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）経由のモビリティ パスの接続（User Datagram Protocol（UDP）および IP プロトコル 93 を使用）がダウン状態になり、モビリティ デバイスがリロードされるまで接続失敗が続くという問題、またはモビリティ パスのトラフィックが停止されて短時間非アクティブになってから再起動されるという問題について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- 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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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

この問題が発生した場合、10.10.1.2 に位置するワイヤレス LAN コントローラ（WLC）が 10.10.9.3 に位置する WLC と通信しようとすると失敗します。

この問題は、次のいずれかによって引き起こされると考えられます。

- ASA が再起動された。
- 管理者またはルーティング プロトコルによってルーティング テーブルが変更された。
- 管理者によってインターフェイスがシャットダウンされてから再起動された。

この問題は、モビリティ トラフィックだけでなく、任意の UDP または非 TCP IP プロトコルでも発生する場合があります。

この問題はバグではなく、ネットワーク トポロジと ASA 設定が原因で発生します。 この問題の原因と解決策については、以下を参照してください。

ネットワーク トポロジの例

ASA ルーティングの設定は次のとおりです。

```
!
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 インターフェイスの設定は次のとおりです。

```
!
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
!
```

問題のトリガー

この問題は、10.10.1.2 に位置する WLC が 10.10.9.3 に位置する WLC を宛先とするトラフィックを送信したときに発生します。 これらのパケットによって ASA が接続テーブル内に作成する接続は、モビリティ トラフィックを誤った（内部）ASA インターフェイスに送信するためです。

この問題は、接続が作成される時点で ASA の宛先インターフェイス「DMZ」がダウン/ダウン状態になっているため、最適ではない別のインターフェイスからの接続が作成されたことによって発生します。 DMZ インターフェイスがダウン状態になる理由としては、ケーブルの問題、イーサネットまたはポート チャネル ネゴシエーションの問題、または管理目的でシャットダウンされていることが考えられます。

この問題が発生した場合に作成されるモビリティ パス接続は、パケットが到着した内部インターフェイスに再びパケットをルーティングする、ASA の「内部インターフェイス」とみなせます。

```
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#
```

作成されたこれらの接続は、10.10.1.2 に位置するモビリティ エンドポイントが引き続き送信する 10.10.9.3 宛てのトラフィックと一致します。 DMZ インターフェイスがアップ/アップ状態に移行したとしても、（DMZ インターフェイスとの新しい接続は作成されずに）10.10.1.2 から送信されるモビリティ トラフィックはテーブル内の既存の接続と一致するため、ASA 上の接続タイムアウトがリセットされます。これによって、問題が長引くことになります。

要約すると、この問題は次のイベントによって発生します。

1. 10.10.1.2 に位置するデバイスがプロトコル 97 または UDP パケットを 10.10.9.3 に送信します。
2. ASA はこのパケットを内部インターフェイスで受信しますが、DMZ インターフェイスがダウンしているため、ルーティング テーブルには宛先ネットワークへの具体的なルートがありません。 ASA 上では same-security permit intra-interface コマンドが有効にされていることから、ASA は内部インターフェイスに戻る 10.0.0.0/8 ネットワーク用のスタティック ルートに従って接続テーブル内に接続を作成し、その内部インターフェイスから内部ネットワークに向けてパケットを送信します。
3. ある時点で DMZ インターフェイスがアップ状態になると、そのルートがテーブルに再び追加されます。 しかし、ステップ 2 でプロトコル 97 トラフィックの接続がすでに作成されているため、以降のパケットもその接続と一致します。そのためルーティング テーブルが上書きされ、トラフィックは DMZ 上のサーバに到達しません。

解決策

解決策 1

この問題の 1 つの解決策として考えられるのは、ASA から same-security permit intra-interface コマンドを削除することです。 こうすることにより、元のパケットを受信したインターフェイスから、その同じインターフェイスに戻る U ターン接続が作成されなくなるため、インターフェイスがアップ状態になった時点で適切な接続が作成されるようになります。 ただし、ASA のルーティング テーブルによっては、この解決策が有効でない場合もあります（ルーティング テ

ーブルに基づく対象の宛先以外の別のインターフェイスにトラフィックがルーティングされる場合）。また、ASA 上の他の接続に **same-security permit intra-interface** コマンドが必要な場合もあります。

解決策 2

以下の特定のインスタンスでは、**timeout floating-conn** 機能を有効にすることによって、問題を軽減することができました。 この機能（デフォルトでは無効）により、DMZ インターフェイスがアップ状態になると、ASA の新しいインターフェイスからエンドポイントへの優先ルートがルーティング テーブルに追加され、その 1 分後に ASA は問題の接続を切断します。 そして次のパケットが ASA に到着すると同時に、より優先されるインターフェイス（10.10.9.3 ホスト用の内部インターフェイスではなく DMZ インターフェイス）を使用した接続が作成し直されます。

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

問題が軽減されると、適切な接続が ASA 接続テーブルに作成されて、接続が自動的に復元されます。

```
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 リファレンス - timeout floating-conn コマンド
- テクニカル サポートとドキュメント – Cisco Systems