プライマリ ISP のリンクがデュアル ISP セットアップで再度オンラインになったら ASA を経由する UDP のトラフィックが失敗する

内容

概要

適応型セキュリティ アプライアンス (ASA) に宛先サブネットごとに 2 つの出力インターフェイスがあり、宛先への優先ルートをルーティング テーブルからある期間削除した場合、その優先ルートをルーティング テーブルに再び追加したときに User Datagram Protocol (UDP) 接続が失敗する可能性があります。TCP 接続もこの問題の影響を受ける場合がありますが、TCP はパケット損失を検出するため、これらの接続はエンドポイントによって自動的に中断され、ルート変更後により最適なルートを使用して再構築されます。

この問題は、ルーティング プロトコルが使用され、トポロジ変更によって ASA のルーティング テーブルが変更される場合にも発生することがあります。

はじめに

要件

この問題が発生するには、ASA のルーティング テーブルを変更する必要があります。これは、2 つの ISP リンクが冗長構成されている場合や、ASA が IGP (OSPF、EIGRP、RIP) からルートを設定する場合によく見られます。

この問題は、プライマリ ISP リンクが再びオンラインになるか、前述の IGP で再コンバージェンスが起こり、ASA で使用されていた優先度の低いルートが、優先度の高い低メトリック ルートに置き換えられるときに発生します。その際、プライマリ ルートまたは優先ルートが ASA のルーティング テーブルに再度追加されると、UDP SIP 登録や GRE などの長時間接続の中断が発生することがあります。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- 任意の Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- ASA バージョン 8.2(5)、8.3(2)、8.4(1)、8.5(1) 以降

表記法

ドキュメントの表記法の詳細は、「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

ルーティング テーブル エントリが ASA のルーティング テーブルから削除され、インターフェイスから宛先に到達するルートがない場合、ファイアウォールを介して構築されたその外部宛先との接続は、ASA によって削除されます。これは、その宛先に対するルーティング エントリを持つ別のインターフェイスを使用して、接続を再構築できるようにするために発生します。

ただし、より具体的なルートがテーブルに追加されると、接続は新しい、より具体的なルートを使用するように更新されず、最適ではないインターフェイスの使用を続けます。

たとえば、ファイアウォールに、インターネットに接続した 2 つのインターフェイス、「外部」および「バックアップ」があり、これらの 2 つのルートが ASA の設定に存在するとします。

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

外部インターフェイスとバックアップインターフェイスの両方が「up」の場合、ファイアウォールを介して発信される接続は外部インターフェイスを使用します。外部インターフェイスがシャットダウンされた場合（または、ルートを追跡するSLA監視機能が追跡IPへの接続が失われた場合）宛先。

問題が発生するのは、外部インターフェイスが再度起動したとき、または追跡対象のルートが再び優先ルートになったときです。ルーティング テーブルは元のルートを優先するように更新されますが、既存の接続は ASA にその後も存在してバックアップ インターフェイスを経由します。接続は削除されず、優先メトリックを持つ外部インターフェイスで再作成されることはありません。これは、デフォルトのバックアップ ルートがまだ ASA のインターフェイス固有のルーティング テーブルにあるためです。接続は、削除されるまで優先度の低いルートを持つインターフェイスの使用を続けます。UDP の場合、これは無期限となる可能性があります。

この状況は、外部 SIP 登録や他の UDP 接続など存続期間の長い接続で、問題が発生する可能性があります。

解決方法

この特定の問題に対処するために、新しい機能が ASA に追加されました。この機能は、宛先までの優先度の高いルートがルーティング テーブルに追加された場合に接続を中断し、新しいインターフェイスで再構築します。この機能（デフォルトでは無効）を有効にするには、**timeout floating-conn コマンドにゼロ以外のタイムアウトを設定します。**このタイムアウト（HH:MM:SSで指定）は、より優先ルートがルーティングテーブルに追加された後、ASAが接続を切断するまで待機する時間を指定します。

この機能を有効にする CLI の例を示します。この CLI では、宛先への優先度の高い別のルートがある既存の接続でパケットが受信された場合に、接続が 1 分後に中断されます (そして新しい、より優先されるルートを使用して再構築されます) 。

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

この機能は、ASA プラットフォームのバージョン 8.2(5)、8.3(2)12、8.4(1) 1、および 8.5(1) (ASA ソフトウェアの以降のバージョンを含む) に追加されています。

この機能を実装していないバージョンの ASA コードを実行する場合は、clear local-host *<IP>* または clear-conn <IP> **を使用して、利用可能な良いルートを使用せず優先度の低いルートをとり続ける UDP 接続を手動で中断します。**

この新しい機能はコマンド リファレンスの「timeout」セクションに記載されています。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems