BGP 7.1からのVPNルートアドバタイズメントの動作の変更

内容

はじめに

このドキュメントでは、バージョン7.1以降のBGPルーティングテーブルへのVPNルートインジェクションの動作の変更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あることが推奨されます。

- FirePOWER の知識
- BGPの設定とルートアドバタイズメントに関する知識

使用するコンポーネント

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

- Cisco Secure Firewall Management Center(FMC)
- Cisco Firepower Threat Defense(FTD)

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

要件は、BGP経由でVPNルートをアドバタイズすることです。

VPNルートは、ネクストホップ一致基準を使用してフィルタリングされます。

標準アクセスリストは、ネクストホップ0.0.0.0に一致するように設定されています。

動作の変更

バージョン6.6.5では、VPNルートはネクストホップが0.0.0.0に設定された状態でBGPルーティングテーブルに挿入されます。

バージョン7.1では、VPNルートは、対応するサブネットのネットワークIPアドレスとして設定されたネクストホップを使用してBGPルーティングテーブルに挿入されます。

コンフィギュレーション

BGP 設定：

router bgp 12345 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 172.30.0.21 remote-as 12346 neighbor 172.

ルートマップ設定：

firepower# sh run route-map VPN_INSIDE_OUT route-map VPN_INSIDE_PRI_OUT permit 10 match ip next-hop NextHopZeroes firepower# sh run acc

この設定では、BGPはネクストホップが0.0.0.0として定義されているルートだけをアドバタイズします。

ルーティングテーブルのVPNルートのインストール：

firepower# sh route | inc 172.20.192
V 172.20.192.0 255.255.252.0 connected by VPN (advertised), VPN-OUTSIDE

show bgpの出力：

バージョン6.6.5では

show bgp :
*> 172.20.192.0/22 0.0.0.0 0 32768 ?

サブネット172.20.192.0/22が、ネクストホップIPが0.0.0.0として定義されたBGPテーブルにインストールされていることがわかります。

バージョン7.1では、

show bgp :
*> 172.20.192.0/22 172.20.192.0 0 32768 ?

サブネット172.20.192.0/22がBGPテーブルにインストールされており、ネクストホップIPがサブネットネットワークIP(172.20.192.0)として定義されていることが確認できます。

影響シナリオ

設定に、0.0.0.0のネクストホップIPに一致するように設定されたルートマップが含まれている場合、ルートフィルタリングが影響を受け、VPNルートはアドバタイズされません。

回避策

次の2つの回避策を使用できます。

- すべてのVPNサブネットのリストを作成し、BGP経由のアドバタイズメント用に個々に設定します。注：この方法はスケーラブルではありません。
- ローカルで生成されたルートをアドバタイズするようにBGPを設定します。次の設定コマンドを適用します。

route-map <route-map-name> permit 10
match route-type local

前述のソリューションの1つを実装することで、FTDはVPN挿入ルートをBGP経由でアドバタイズします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。