

FTDでのソフト再設定の制限によるBGPルーティングの設定

内容

[問題](#)

[環境](#)

[解決方法](#)

[機能制限](#)

[別のアプローチ \(ルートリフレッシュ機能 \)](#)

[原因](#)

[関連コンテンツ](#)

- [問題](#)
 - [環境](#)
 - [解決方法](#)
 - [機能制限](#)
 - [別のアプローチ \(ルートリフレッシュ機能 \)](#)
 - [原因](#)
 - [関連コンテンツ](#)
-

問題

ユーザがFirewall Management Center(FMC)を使用して、Firewall Threat Defense(FTD)のBGPピアでBorder Gateway Protocol(BGP)ソフト再設定を設定しようとした場合、標準のFMC BGPインターフェイスでは設定を完了できません。さらに、FlexConfigオブジェクトを使用してこの機能を実装しようとする、BGP neighbor soft-reconfigurationコマンドのさまざまな部分でテキストを入力する際にエラーが発生します。具体的な要件は、ポリシー評価とトラブルシューティングの目的で、受信したルートを保存するために、BGPネイバーでsoft-reconfiguration inboundを有効にすることです。

環境

- ハードウェア：ファイアウォール3100を保護します。他のハードウェアプラットフォームも影響を受けます。

- ソフトウェア：FTD(この制限は適応型セキュリティアプライアンス(ASA)にも適用されます)。
- FMCバージョン7.4.6他のソフトウェアバージョンも該当します。
- FTDバージョン7.4.6。他のソフトウェアバージョンも該当します。
- FTDにはBGPルーティングプロトコルの設定があります。

解決方法

このドキュメントの執筆時点では、従来のBGPネイバー着信ソフト再設定 (BGPコマンド neighbor x.x.x.x soft-reconfiguration inbound) は、FMC BGPユーザインターフェイスを介して、またはサポートされているFlexConfig方式としてFTDデバイスではサポートされていません。

機能制限

次のBGPソフト再設定機能は使用できません。

- FMCのBGP設定には、neighbor soft-reconfiguration inboundの設定オプションがありません。
- FlexConfigを使用して同等のCLIを設定しようとしても、サポートされているFTD/FMC管理のBGP設定項目ではないため、失敗します。

別のアプローチ (ルートリフレッシュ機能)

FTDは、BGPピアとのネゴシエート時にBGPルートリフレッシュ機能をサポートします。これは、従来のsoft-reconfiguration inbound機能とは異なりますが、ポリシー変更後の動的ソフトリセット動作をサポートするメカニズムを提供します。

推奨されるアプローチは次のとおりです。

- 引き続き、BGPネイバー、プレフィックスリスト、ルートマップの設定を行い、FMCでサポートされるBGP設定ワークフローを使用してフィルタリングを行います。

- BGPピアがルートリフレッシュ機能をネゴシエートすることを確認します。

```
<#root>
```

```
device#
```

```
show bgp neighbors 192.0.2.2
```

```
BGP neighbor is 192.0.2.2, context single_vf, remote AS 65535, internal link
  BGP version 4, remote router ID 192.0.2.2
  BGP state = Established, up for 00:17:39
  Last read 00:00:31, last write 00:00:31, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
```

Route refresh: advertised and received(new)

```
<----- BGP Route Refresh capability is enabled on both peers
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	3
Keepalives:	17	20

Route Refresh: 1 0

```
<----- The neighbor sent 1 BGP Route Refresh message
Total:                      20                      24
```

- ポリシーの再評価には、着信のソフト再設定を試行する代わりに、ルートリフレッシュ動作を使用します。次に例を示します。

```
<#root>
```

```
device#
```

```
clear bgp 192.0.2.2 in
```

- すべての受信および拒否されたルートを監査する運用要件については、BGPピア/ルータ側から確認します。

比較

機能	BGPルートリフレッシュ機能	着信側ソフト再設定
FTD/ASAでサポート	Yes	No
動作の仕組み	ルータは、明示的なBGPルートリフレッシュ要求メッセージをネイバーに送信し、ルーティングテーブルの再アドバタイズを要求します。	ルータは余分なRAMを割り当て、ネイバーのBGPテーブルのフィルタリングされていない生のコピーをローカルメモリに保存します。
設定要件	ありません。FTDおよびASAでは、デフォルトで自動的に有効になります。	手動設定が必要(<code>neighbor x.x.x.x soft-reconfiguration inbound</code>)ですが、このコマンドはFTD/ASAではサポートされていません。
メモリ消費	非常に低い余分なルーティングテーブルはRAMに保存されません。	非常に高い。そのネイバーのパスに対して、より多くのメモリを消費します。
Triggerコマンド	<code># clear bgp x.x.x.x in</code>	ASA/FTDではサポートされません。
ネイバーの依存関係	はい。あります。リモートBGPピアもルートリフレッシュ機能をサポートし、受け入れる必要があります。	No.これはファイアウォールに対して完全にローカルです。ピアネイバーはこの機能が有効であることを認識していません。
コマンド : <code>show bgp neighbor x.x.x.x received-routes</code>	サポート対象外/障害ルータはローカルコピーを保存しません。このコマンドを実行すると、エラー(<code>% Inbound soft reconfiguration not enabled on x.x.x.x</code>)が返されます。	サポート対象.ポリシーが適用される前に、現在ルータのRAMにキャッシュされている、フィルタリングされていない未加工のルートを即座に表示します。

原因

これは、FTDおよびASAデバイスの機能制限です。BGPネイバーの着信ソフト再設定機能は、FMCのBGP設定インターフェイスや、FTDデバイスでサポートされるFlexConfigオプションとしては実装されていません。この制限は、ソフトウェア拡張Cisco Bug ID [CSCvy97220](#)として追跡されています。

関連コンテンツ

- [FMC BGPコンフィギュレーションガイド\(10.x\)](#)
- [BGPネイバーおよびサマリーの可視性のためのFTDコマンドリファレンス](#)
- [Cisco Bug ID CSCvy97220 - BGPネイバー着信ソフト再設定サポートの拡張要求](#)
- [シスコのテクニカルサポートとダウンロード](#)

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。