

Verhaltensänderung bei VPN-Routenankündigung in BGP ab 7.1

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Verhaltensänderung](#)

[Konfiguration](#)

[Auswirkungsszenario](#)

[Herumarbeiten](#)

Einleitung

In diesem Dokument wird die Änderung des Verhaltens bei der VPN-Routen-Injection in der BGP-Routing-Tabelle beschrieben, die mit Version 7.1 beginnt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse zur Konfiguration von BGP und Routenankündigung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die VPN-Routen müssen über das BGP angekündigt werden.

VPN-Routen werden mithilfe von Next-Hop-Zuordnungskriterien gefiltert.

Die Standard-Zugriffsliste ist so konfiguriert, dass sie mit einem Next-Hop 0.0.0.0 übereinstimmt.

Verhaltensänderung

In Version 6.6.5 werden VPN-Routen in die BGP-Routing-Tabelle eingefügt, wobei der nächste Hop auf 0.0.0.0 festgelegt ist.

In Version 7.1 werden VPN-Routen in die BGP-Routing-Tabelle eingefügt, wobei der nächste Hop als Netzwerk-IP-Adresse des entsprechenden Subnetzes festgelegt wird.

Konfiguration

BGP-Konfiguration:

```
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.
```

Routing-Map-Konfiguration:

```
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
```

Bei dieser Konfiguration kündigt das BGP nur die Routen an, für die der nächste Hop als 0.0.0.0 definiert ist.

Installation von VPN-Routen in Routing-Tabelle:

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

Ausgabe von **show bgp**:

In Version 6.6.5

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

Es ist ersichtlich, dass das Subnetz 172.20.192.0/22 in der BGP-Tabelle installiert ist, wobei die Next-Hop-IP als 0.0.0.0 definiert ist.

In Version 7.1

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

Es ist ersichtlich, dass das Subnetz 172.20.192.0/22 in der BGP-Tabelle installiert ist, wobei die Next-Hop-IP als Subnetz-IP definiert ist: 172.20.192.0.

Auswirkungsszenario

Wenn die Konfiguration eine Routing-Map enthält, die mit einer Next-Hop-IP 0.0.0.0 übereinstimmt, ist dies mit einer Routenfilterung verbunden, und VPN-Routen werden nicht angekündigt.

Herumarbeiten

Zwei mögliche Problemumgehungen:

- Erstellen Sie eine Liste aller VPN-Subnetze, und konfigurieren Sie sie einzeln für die Ankündigung über das BGP. Hinweis: Diese Methode ist nicht skalierbar.
- Konfigurieren Sie das BGP so, dass lokal generierte Routen angekündigt werden. Diesen Konfigurationsbefehl anwenden:

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

Durch die Implementierung einer der zuvor angesprochenen Lösungen kündigt FTD die VPN-Routen über das BGP an.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.