Change in Behavior for VPN Route Advertisement in BGP Starting 7.1

Contents

Introduction

This document describes the change in behavior of VPN route injection into the BGP routing table starting with version 7.1.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower technology
- Knowledge on configuring BGP and Route advertisement

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Requirement is to advertise the VPN routes over BGP.

VPN routes are being filtered by using next-hop matching criteria.

The standard access-list is configured to match a next-hop 0.0.0.0.

Behavior Change

In version 6.6.5, VPN routes are injected into the BGP routing table with the next hop set to 0.0.0.0.

In version 7.1, VPN routes are injected into the BGP routing table with the next hop set as the network IP address of the corresponding subnet.

Configuration

BGP Configuration:

```
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 172.30.0.21 description CISCO-FTD-B
  neighbor 172.30.0.21 transport path-mtu-discovery disable
  neighbor 172.30.0.21 timers 10 40
  neighbor 172.30.0.21 fall-over bfd
  neighbor 172.30.0.21 ha-mode graceful-restart
  neighbor 172.30.0.21 activate
  neighbor 172.30.0.21 send-community
  neighbor 172.30.0.21 route-map VPN_INSIDE_IN in
  neighbor 172.30.0.21 route-map VPN_INSIDE_OUT out
  redistribute static
  redustribute connected
  no auto-summary
  no synchronization
 exit-address-family
```

Route-map configuration:

```
firepower# sh run route-map VPN_INSIDE_OUT

route-map VPN_INSIDE_PRI_OUT permit 10
 match ip next-hop NextHopZeroes

firepower# sh run access-list NextHopZeroes
access-list NextHopZeroes standard permit host 0.0.0.0
```

With this configuration, BGP advertises only those routes for which the next hop is defined as 0.0.0.0.

VPN routes installation in routing table:

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

Output of **show bgp**:

In version 6.6.5

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

It can be seen that the subnet 172.20.192.0/22 is installed in the BGP table with the next-hop IP defined as 0.0.0.0.

In version 7.1

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

It can be seen that the subnet 172.20.192.0/22 is installed in the BGP table with the next-hop IP defined as the subnet network IP : 172.20.192.0.

Impact Scenario

If the configuration includes a route-map set to match a next-hop IP of 0.0.0.0, then route filtering is affected, and VPN routes are not advertised.

Work Around

Two available work arounds:

1. Create a list of all the VPN subnets and configure them individually for advertisement over BGP. Note: This method is not scalable.
2. Configure BGP to Advertise Locally Generated Routes. Apply this configuration command:

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

By implementing one of the previously discussed solutions, FTD advertises the VPN-injected routes via BGP.