Gedragsverandering voor VPN-routeadvertenties in BGP vanaf 7.1

Inhoud

Inleiding

Dit document beschrijft de wijziging in gedrag van VPN-routeinjectie in de BGP-routeringstabel, te beginnen met versie 7.1.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER-technologie
- Kennis over het configureren van BGP- en routeradvertenties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De voorwaarde is dat de VPN-routes via BGP worden geadverteerd.

VPN-routes worden gefilterd met behulp van next-hop matching criteria.

De standaard toegangslijst is ingesteld op een volgende hop 0.0.0.0.

Gedragsverandering

In versie 6.6.5 worden VPN-routes in de BGP-routeringstabel ingespoten, waarbij de volgende hop op 0.0.0.0 wordt ingesteld.

In versie 7.1 worden VPN-routes in de BGP-routeringstabel ingespoten, waarbij de volgende hop wordt ingesteld als IP-netwerkadres van het corresponderende subsysteem.

Configuratie

BGP-configuratie:

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.

Routekaartconfiguratie:

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

Met deze configuratie, adverteert BGP slechts die routes waarvoor de volgende hop als 0.0.0.0 wordt gedefinieerd.

VPN-routerinstallatie in routertabel:

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

Output van **show bgp**:

In versie 6.6.5

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

Het is duidelijk dat het subnetnummer 172.20.192.0/22 is geïnstalleerd in de BGP-tabel met de volgende hop-IP gedefinieerd als 0.0.0.0.

In versie 7.1

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

Het is duidelijk dat het subnetnummer 172.20.192.0/22 in de BGP-tabel is geïnstalleerd met de volgende hop-IP die is gedefinieerd als het subnetnetwerk IP: 172.20.192.0.

Effectscenario

Als de configuratie een route-kaart omvat die is ingesteld om een volgende-hop IP van 0.0.0 aan te passen, heeft dit gevolgen voor routefiltering en worden VPN-routes niet geadverteerd.

Rond werken

Twee beschikbare werk rondom:

- Maak een lijst van alle VPN-subnetten en configureer ze individueel voor advertenties via BGP. Opmerking: deze methode is niet schaalbaar.
- Configureer BGP om lokaal gegenereerde routers te adverteren. Pas deze configuratieopdracht toe:

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

Door een van de eerder besproken oplossingen te implementeren, adverteert FTD de VPN-geïnjecteerde routes via BGP.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.