

BGP-routing configureren met beperkingen voor zachte herconfiguratie op FTD

Inhoud

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Beperkingen van functies](#)

[Alternatieve benadering \(mogelijkheid voor het vernieuwen van de route\)](#)

[Oorzaak](#)

[Gerelateerde inhoud](#)

- [uitgifte](#)
 - [milieu](#)
 - [resolutie](#)
 - [Beperkingen van functies](#)
 - [Alternatieve benadering \(mogelijkheid voor het vernieuwen van de route\)](#)
 - [Oorzaak](#)
 - [Gerelateerde inhoud](#)
-

uitgifte

Wanneer een gebruiker via Firewall Management Center (FMC) probeert de soft-reconfiguratie van het Border Gateway Protocol (BGP) te configureren op een BGP-peer in Firewall Threat Defense (FTD), kan de configuratie niet worden voltooid via de standaard FMC BGP-interface. Bovendien resulteren pogingen om deze functionaliteit te implementeren met FlexConfig-objecten in fouten tijdens het invoeren van tekst voor verschillende delen van de opdracht voor soft-reconfiguratie bij de burens van BGP. De specifieke vereiste is om inkomende soft-reconfiguratie op BGP-burens in staat te stellen ontvangen routes op te slaan voor beleidsevaluatie en probleemoplossing.

milieu

- Hardware: Secure Firewall 3100. Ook andere hardwareplatforms worden getroffen.

- Software: FTD (deze beperking geldt ook voor Adaptive Security Appliance (ASA)).
- FMC versie 7.4.6. Ook andere softwareversies worden getroffen.
- FTD versie 7.4.6. Ook andere softwareversies worden getroffen.
- FTD heeft een BGP routing protocol configuratie.

resolutie

Op het moment van dit schrijven wordt de klassieke BGP neighbor inbound soft-reconfiguration (BGP command neighbor x.x.x.x soft-reconfiguration inbound) niet ondersteund op FTD-apparaten, noch via de FMC BGP-gebruikersinterface, noch als een ondersteunde FlexConfig-methode.

Beperkingen van functies

Deze soft-reconfiguratiemogelijkheden van BGP zijn niet beschikbaar:

- De FMC BGP-configuratie biedt geen configuratieoptie voor de inkomende soft-reconfiguratie van de burens.
- Het configureren van de equivalente CLI via FlexConfig mislukt omdat het geen door FTD/FMC beheerd BGP-configuratiedoeldeel is.

Alternatieve benadering (mogelijkheid voor het vernieuwen van de route)

FTD ondersteunt wel de mogelijkheid om de BGP-route te vernieuwen wanneer er wordt onderhandeld met BGP-collega's. Dit biedt het ondersteunde mechanisme voor dynamisch soft reset-gedrag na beleidswijzigingen, hoewel het verschilt van de klassieke inkomende functionaliteit voor soft-reconfiguration.

De aanbevolen aanpak omvat:

- Ga door met het configureren van BGP-burens, prefixlijsten, routekaarten en filtering via de

ondersteunde BGP-configuratieworkflow van FMC.

- Bevestig dat BGP-peers onderhandelen over de mogelijkheid om de route te vernieuwen:

<#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

- Gebruik gedrag voor het vernieuwen van de route voor beleidsevaluatie in plaats van te proberen inkomende soft-reconfiguratie in te schakelen, bijvoorbeeld:

<#root>

device#

clear bgp 192.0.2.2 in

- Voor operationele vereisten om alle ontvangen en afgewezen routes te controleren, controleert u vanaf de BGP-peer-/routerzijde.

vergelijking

Feature	Vernieuwingsmogelijkheid voor BGP-route	Inkomende zachte herconfiguratie
Ondersteund op FTD/ASA	Ja	Nee
Hoe het werkt	De router stuurt een expliciet BGP Route Refresh request bericht naar de buurman, met het verzoek om zijn routingstabel opnieuw te adverteren.	De router wijst extra RAM toe om een rauwe, ongefilterde kopie van de BGP-tabel van de burens in het lokale geheugen op te slaan.
Configuratievereiste	None. Standaard automatisch ingeschakeld op FTD en ASA.	Handmatige configuratie vereist (aangrenzende x.x.x.x soft-reconfiguration inbound), maar de opdracht wordt niet ondersteund op FTD/ASA.
geheugenverbruik	Extreem laag. Er worden geen extra routingstabellen opgeslagen in RAM.	Zeer hoog. Verbruikt veel meer geheugen voor de paden van die buurman.
Trigger, opdracht	# BGP wissen x.x.x.x in	Niet ondersteund op ASA/FTD.
afhankelijkheid van buurlanden	Ja. De externe BGP-peer moet ook de mogelijkheid voor het vernieuwen van de route ondersteunen en accepteren.	Nee. Het is volledig lokaal aan de firewall; de peer-buurman heeft geen idee dat het is ingeschakeld.
Opdracht: bgp buurman x.x.x.x ontvangen routes weergeven	Niet ondersteund / mislukt. De router slaat geen lokale kopie op. Als u deze opdracht uitvoert, wordt een fout geretourneerd (% Inbound soft reconfiguration niet ingeschakeld op x.x.x.x).	Ondersteund. Geeft direct de onbewerkte, ongefilterde routes weer die momenteel in het RAM-geheugen van de router zijn opgeslagen voordat

		het beleid werd toegepast.
--	--	----------------------------

Oorzaak

Dit is een functiebeperking op FTD- en ASA-apparaten. De inkomende soft-reconfiguratiefunctie van de BGP van de burens is niet geïmplementeerd in de FMC BGP-configuratieinterface of als een ondersteunde FlexConfig-optie voor FTD-apparaten. Deze beperking wordt bijgehouden als een softwareverbetering Cisco bug ID [CSCvy97220](#).

Gerelateerde inhoud

- [FMC BGP-configuratiehandleiding \(10.x\)](#)
- [FTD-opdrachtreferentie voor BGP-buurman en overzicht van zichtbaarheid](#)
- [Cisco bug ID CSCvy97220 - Verbeteringsverzoek voor BGP Neighbor Inbound Soft-Reconfiguration-ondersteuning](#)
- [Cisco Technical Support en downloads](#)

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.