

Configuración del Ruteo BGP con Limitaciones de reconfiguración de software en FTD

Contenido

[Problema](#)

[Entorno](#)

[Resolución](#)

[Limitaciones de la función](#)

[Enfoque alternativo \(capacidad de actualización de rutas\)](#)

[Causa](#)

[Contenido relacionado](#)

- [Problema](#)
 - [Entorno](#)
 - [Resolución](#)
 - [Limitaciones de la función](#)
 - [Enfoque alternativo \(capacidad de actualización de rutas\)](#)
 - [Causa](#)
 - [Contenido relacionado](#)
-

Problema

Cuando un usuario intenta configurar la reconfiguración de software del protocolo de gateway fronterizo (BGP) en un par BGP en Firewall Threat Defence (FTD) mediante Firewall Management Center (FMC), la configuración no se puede completar a través de la interfaz BGP de FMC estándar. Además, los intentos de implementar esta funcionalidad mediante objetos FlexConfig producen errores durante la entrada de texto para varias partes del comando de reconfiguración de software BGP neighbor. El requisito específico es habilitar la reconfiguración de software entrante en los vecinos BGP para almacenar las rutas recibidas para fines de evaluación de políticas y resolución de problemas.

Entorno

- Hardware Firewall seguro 3100. Otras plataformas de hardware también se ven afectadas.

- Software: FTD (esta limitación también se aplica al dispositivo de seguridad adaptable (ASA)).
- FMC versión 7.4.6. Otras versiones de software también se ven afectadas.
- FTD versión 7.4.6. Otras versiones de software también se ven afectadas.
- FTD tiene configuración de protocolo de ruteo BGP.

Resolución

En el momento de escribir esto, la reconfiguración suave entrante de vecino BGP clásico (comando BGP neighbor x x x x x soft-reconfiguration inbound) no se soporta en los dispositivos FTD, ya sea a través de la interfaz de usuario FMC BGP o como un método FlexConfig soportado.

Limitaciones de la función

Estas capacidades de reconfiguración de software BGP no están disponibles:

- La configuración BGP de FMC no proporciona una opción de configuración para la reconfiguración de software de vecino entrante.
- Error al intentar configurar la CLI equivalente a través de FlexConfig porque no es un elemento de configuración BGP administrado por FTD/FMC compatible.

Enfoque alternativo (capacidad de actualización de rutas)

FTD no soporta la capacidad BGP Route Refresh cuando se negocia con peers BGP. Esto proporciona el mecanismo soportado para el comportamiento de reinicio de software dinámico después de los cambios de política, aunque difiere de la funcionalidad entrante de reconfiguración de software clásica.

El enfoque recomendado incluye:

- Continúe configurando los vecinos BGP, las listas de prefijos, los mapas de ruta y el filtrado a través del flujo de trabajo de configuración BGP soportado por FMC.
- Confirme que los peers BGP negocian la capacidad de actualización de rutas:

```
<#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
```

- Utilice el comportamiento Route Refresh para la reevaluación de políticas en lugar de intentar habilitar la reconfiguración de software entrante, p. ej.:

```
<#root>
```

```
device#
```

```
clear bgp 192.0.2.2 in
```

- Para conocer los requisitos operativos para auditar todas las rutas recibidas y rechazadas, verifique desde el lado del router/peer BGP.

Comparación

Función	Capacidad de actualización de ruta BGP	Reconfiguración de software entrante
Compatible con FTD/ASA	Yes	No
Cómo funciona	El router envía un mensaje de solicitud de actualización de ruta BGP explícito al vecino, pidiéndole que vuelva a anunciar su tabla de ruteo.	El router asigna memoria RAM adicional para guardar una copia sin procesar y sin filtrar de la tabla BGP del vecino en la memoria local.
Requisito de configuración	Ninguno. Se activa automáticamente de forma predeterminada en FTD y ASA.	Se requiere configuración manual (neighbor x x x x x soft-reconfiguration inbound), pero el comando no se soporta en FTD/ASA.
Consumo de memoria	Extremadamente baja. No hay tablas de ruteo adicionales almacenadas en la RAM.	Muy alto. Consume mucha más memoria para los trayectos de ese vecino.
Comando Trigger	# clear bgp x x x x in	No compatible con ASA/FTD.
Dependencia del vecino	Yes. El par BGP remoto también debe admitir y aceptar la capacidad de actualización de rutas.	No. Es completamente local al firewall; el vecino de peer no tiene idea de que está habilitado.
Comando: show bgp neighbor x.x.x.x received-routes	No compatible / Fallos. El router no almacena una copia local. La ejecución de este comando devuelve un error (% Inbound soft reconfiguration not enabled on x.x.x.x).	Admitido. Muestra al instante las rutas sin filtrar sin procesar almacenadas actualmente en la memoria caché del router antes de que se aplicaran las políticas.

Causa

Se trata de una limitación de las funciones de los dispositivos FTD y ASA. La funcionalidad de reconfiguración de software entrante del vecino BGP no se ha implementado en la interfaz de configuración BGP de FMC ni como una opción FlexConfig admitida para dispositivos FTD. Esta limitación se rastrea como una mejora de software con el ID de bug de Cisco [CSCvy97220](#).

Contenido relacionado

- [Guía de configuración de BGP FMC \(10.x\)](#)
- [Referencia de Comandos de FTD para el Vecino BGP y la Visibilidad de Resumen](#)
- [ID de bug de Cisco CSCvy97220 - Solicitud de mejora para el soporte de reconfiguración de software entrante del vecino BGP](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).