

FTD의 소프트 재구성 제한으로 BGP 라우팅 구성

목차

[문제](#)

[환경](#)

[해결](#)

[기능 제한 사항](#)

[대체 접근 방식\(경로 갱신 기능\)](#)

[원인](#)

[관련 콘텐츠](#)

- [문제](#)
 - [환경](#)
 - [해결](#)
 - [기능 제한 사항](#)
 - [대체 접근 방식\(경로 갱신 기능\)](#)
 - [원인](#)
 - [관련 콘텐츠](#)
-

문제

사용자가 FMC(Firewall Management Center)를 사용하여 FTD(Firewall Threat Defense)의 BGP 피어에서 BGP(Border Gateway Protocol) 소프트 리컨피그레이션을 구성하려고 하면 표준 FMC BGP 인터페이스를 통해 컨피그레이션을 완료할 수 없습니다. 또한 FlexConfig 개체를 사용하여 이 기능을 구현하려고 하면 BGP neighbor soft-reconfiguration 명령의 다양한 부분에 대한 텍스트 입력 중에 오류가 발생합니다. 특정 요구 사항은 정책 평가 및 문제 해결을 위해 수신된 경로를 저장하기 위해 BGP 인접 디바이스에서 소프트 리컨피그레이션 인바운드를 활성화하는 것입니다.

환경

- 하드웨어: 보안 방화벽 3100. 다른 하드웨어 플랫폼도 영향을 받습니다.
- 소프트웨어: FTD(이 제한은 ASA(Adaptive Security Appliance)에도 적용됩니다.)
- FMC 버전 7.4.6. 기타 소프트웨어 버전도 영향을 받습니다.

- FTD 버전 7.4.6. 기타 소프트웨어 버전도 영향을 받습니다.
- FTD에는 BGP 라우팅 프로토콜 컨피그레이션이 있습니다.

해결

이 쓰기 시점에 FTD 디바이스에서는 FMC BGP 사용자 인터페이스를 통해 또는 지원되는 FlexConfig 메서드로 클래식 BGP 네이버 인바운드 소프트웨어 리컨피그레이션(BGP 명령 네이버 x.x.x.x 소프트웨어 리컨피그레이션 인바운드)이 지원되지 않습니다.

기능 제한 사항

다음과 같은 BGP 소프트웨어 재구성 기능을 사용할 수 없습니다.

- FMC BGP 컨피그레이션에서는 네이버 소프트웨어 리컨피그레이션 인바운드에 대한 컨피그레이션 옵션을 제공하지 않습니다.
- 지원되는 FTD/FMC 관리 BGP 컨피그레이션 항목이 아니므로 FlexConfig를 통해 해당 CLI를 구성하려는 시도가 실패합니다.

대체 접근 방식(경로 갱신 기능)

FTD는 BGP 피어와 협상할 때 BGP 경로 새로 고침 기능을 지원합니다. 이는 기존의 소프트웨어 리컨피그레이션 인바운드 기능과는 다르지만, 정책 변경 후 동적 소프트웨어 리셋 동작에 대해 지원되는 메커니즘을 제공합니다.

권장되는 접근 방식은 다음과 같습니다.

- FMC에서 지원하는 BGP 컨피그레이션 워크플로를 통해 BGP 인접 디바이스, 접두사 목록, 경로 맵 및 필터링을 계속 구성합니다.
- BGP 피어가 경로 새로 고침 기능을 협상하는지 확인합니다.

<#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

- 인바운드 소프트웨어 리컨피그레이션을 활성화하는 대신 정책 재평가에 Route Refresh 동작을 사용합니다. 예:

<#root>

device#

clear bgp 192.0.2.2 in

- 수신 및 거부된 모든 경로를 감사하기 위한 운영 요구 사항을 보려면 BGP 피어/라우터 측에서 확인하십시오.

비교

기능	BGP 경로 새로 고침 기능	인바운드 소프트웨어 재구성
FTD/ASA에서 지원	예	아니요
운영 방식	라우터는 라우터에 라우팅 테이블을 다시 광고하도록 요청하는 명시적 BGP 경로 새로 고침 요청 메시지를 인접 디바이스에 전송합니다.	라우터는 추가 RAM을 할당하여 인접 디바이스 BGP 테이블의 필터링되지 않은 원시 복사본을 로컬 메모리에 저장합니다.
구성 요구 사항	None. FTD 및 ASA에서 기본적으로 자동으로 활성화됩니다.	수동 컨피그레이션이 필요하지만 (인접 디바이스 x.x.x.x 소프트웨어 리컨피그레이션 인바운드), 이 명령은 FTD/ASA에서 지원되지 않습니다.
메모리 소비	매우 낮습니다. RAM에는 추가 라우팅 테이블이 저장되지 않습니다.	매우 높음. 해당 네이버의 경로에 더 많은 메모리를 사용합니다.
트리거 명령	# clear bgp x.x.x in	ASA/FTD에서는 지원되지 않습니다.
네이버 종속성	예. 원격 BGP 피어도 Route Refresh 기능을 지원 및 수락해야 합니다.	아니요. 방화벽에 완전히 로컬입니다. 피어 네이버는 피어 네이버가 활성화된 것을 알지 못합니다.
명령을 사용합니다: show bgp neighbor x.x.x.x received- routes	지원되지 않음/실패. 라우터가 로컬 복사본을 저장하지 않습니다. 이 명령을 실행하면 오류(% Inbound 소프트웨어 리컨피그레이션이 x.x.x.x에서 활성화되지 않음)가 반환됩니다.	지원. 정책이 적용되기 전에 라우터의 RAM에 현재 캐시되어 있는 필터링되지 않은 원시 경로를 즉시 표시합니다.

원인

이는 FTD 및 ASA 디바이스의 기능 제한입니다. BGP 네이버 인바운드 소프트웨어 재구성 기능은 FMC BGP 컨피그레이션 인터페이스에서 또는 FTD 디바이스에 대해 지원되는 FlexConfig 옵션으로 구현되지 않았습니다. 이 제한은 소프트웨어 개선 사항인 Cisco 버그 ID CSCvy97220 [으로 추적됩니다.](#)

관련 콘텐츠

- [FMC BGP 컨피그레이션 가이드\(10.x\)](#)
- [BGP 인접 디바이스 및 요약 가시성을 위한 FTD 명령 참조](#)
- [Cisco 버그 ID CSCvy97220 - BGP 인접 디바이스 인바운드 소프트 리컨피그레이션 지원을 위한 개선 요청](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.