

BGP Starting 7.1에서 VPN 경로 알림의 동작 변경

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[동작 변경](#)

[설정](#)

[영향 시나리오](#)

[해결 방법](#)

소개

이 문서에서는 버전 7.1부터 시작되는 BGP 라우팅 테이블로의 VPN 경로 삽입의 동작 변경에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- firepower 기술에 대한 지식
- BGP 및 경로 광고 구성에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FTD(Firepower 위협 방어)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

BGP를 통해 VPN 경로를 광고해야 합니다.

VPN 경로는 next-hop matching 기준을 사용하여 필터링됩니다.

표준 액세스 목록은 next-hop 0.0.0.0과 일치하도록 구성됩니다.

동작 변경

버전 6.6.5에서는 VPN 경로가 다음 홉이 0.0.0.0으로 설정된 BGP 라우팅 테이블에 삽입됩니다.

버전 7.1에서는 VPN 경로가 해당 서브넷의 네트워크 IP 주소로 설정된 다음 홉과 함께 BGP 라우팅 테이블에 삽입됩니다.

설정

BGP 구성:

```
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.
```

경로 맵 컨피그레이션:

```
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
```

이 컨피그레이션에서 BGP는 다음 홉이 0.0.0.0으로 정의된 경로만 광고합니다.

VPN은 라우팅 테이블에서 설치를 라우팅합니다.

```
firepower# sh route | inc 172.20.192
```

```
V 172.20.192.0 255.255.252.0 connected by VPN (advertised), VPN-OUTSIDE
```

show bgp의 출력:

버전 6.6.5

show bgp :

```
*> 172.20.192.0/22 0.0.0.0 0 32768 ?
```

서브넷 172.20.192.0/22은 next-hop IP가 0.0.0.0으로 정의된 BGP 테이블에 설치되어 있음을 확인할 수 있습니다.

버전 7.1

show bgp :

```
*> 172.20.192.0/22 172.20.192.0 0 32768 ?
```

서브넷 172.20.192.0/22이 서브넷 네트워크 IP: 172.20.192.0으로 정의된 next-hop IP와 함께 BGP 테이블에 설치되어 있음을 확인할 수 있습니다.

영향 시나리오

컨피그레이션에 next-hop IP 0.0.0.0과 일치하도록 설정된 route-map이 포함된 경우 경로 필터링이 영향을 받으며 VPN 경로는 광고되지 않습니다.

해결 방법

두 가지 해결 방법:

- 모든 VPN 서브넷의 목록을 생성하고 BGP를 통한 알림을 위해 개별적으로 구성합니다. 참고: 이 방법은 확장 가능하지 않습니다.
- 로컬에서 생성된 경로를 광고하도록 BGP를 구성합니다. 다음 컨피그레이션 명령을 적용합니다.

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

앞서 설명한 솔루션 중 하나를 구현하여 FTD는 BGP를 통해 VPN 주입 경로를 광고합니다.

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.