Alteração no comportamento do anúncio de rota de VPN no BGP a partir do 7.1

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Mudança de comportamento](#)

[Configuração](#)

[Cenário de impacto](#)

[Solução alternativa](#)

Introdução

Este documento descreve a mudança no comportamento da injeção de rota VPN na tabela de roteamento BGP começando com a versão 7.1.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower
- Conhecimento sobre a configuração do anúncio de BGP e de Rota

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O requisito é anunciar as rotas VPN sobre BGP.

As rotas VPN estão sendo filtradas usando critérios de correspondência do próximo salto.

A lista de acesso padrão é configurada para corresponder a um próximo salto 0.0.0.0.

Mudança de comportamento

Na versão 6.6.5, as rotas VPN são injetadas na tabela de roteamento BGP com o próximo salto definido como 0.0.0.0.

Na versão 7.1, as rotas VPN são injetadas na tabela de roteamento BGP com o próximo salto definido como o endereço IP de rede da sub-rede correspondente.

Configuração

Configuração do BGP:

```
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 172.30.0.21 description CISCO-FTD-B
    neighbor 172.30.0.21 transport path-mtu-discovery disable
    neighbor 172.30.0.21 timers 10 40
    neighbor 172.30.0.21 fall-over bfd
    neighbor 172.30.0.21 ha-mode graceful-restart
    neighbor 172.30.0.21 activate
    neighbor 172.30.0.21 send-community
    neighbor 172.30.0.21 route-map VPN_INSIDE_IN in
    neighbor 172.30.0.21 route-map VPN_INSIDE_OUT out
  redistribute static
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
```

Configuração do mapa de rotas:

```
firepower# sh run route-map VPN_INSIDE_OUT
```

```
route-map VPN_INSIDE_PRI_OUT permit 10
  match ip next-hop NextHopZeroes
```

```
firepower# sh run access-list NextHopZeroes
access-list NextHopZeroes standard permit host 0.0.0.0
```

Com essa configuração, o BGP anuncia somente as rotas para as quais o próximo salto é definido como 0.0.0.0.

A VPN roteia a instalação na tabela de roteamento:

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

Saída de show bgp:

Na versão 6.6.5

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

Pode ser visto que a sub-rede 172.20.192.0/22 está instalada na tabela BGP com o IP do próximo salto definido como 0.0.0.0.

Na versão 7.1

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

Pode ser visto que a sub-rede 172.20.192.0/22 está instalada na tabela BGP com o IP do próximo salto definido como o IP da rede de sub-rede : 172.20.192.0.

Cenário de impacto

Se a configuração incluir um mapa de rota definido para corresponder a um IP do próximo salto de 0.0.0.0, a filtragem de rota será afetada e as rotas VPN não serão anunciadas.

Solução alternativa

Duas soluções alternativas disponíveis:

1. Crie uma lista de todas as sub-redes VPN e configure-as individualmente para anúncio sobre BGP. Note: Este método não é escalável.

2. Configure o BGP para anunciar rotas geradas localmente. Aplique este comando de configuração:

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

Implementando uma das soluções discutidas anteriormente, o FTD anuncia as rotas injetadas por VPN via BGP.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.