Configurar o roteamento BGP com limitações de reconfiguração suave no FTD

Contents

- Problema
- Ambiente
- Resolução
  - Limitações da função
  - Abordagem alternativa (capacidade de atualização de rota)
- Causa
- Conteúdo relacionado

Problema

Quando um usuário tenta configurar a reconfiguração de software do BGP (Border Gateway Protocol) em um par BGP no FTD (Firewall Threat Defense) usando o FMC (Firewall Management Center), a configuração não pode ser concluída através da interface BGP do FMC padrão. Além disso, as tentativas de implementar essa funcionalidade usando objetos FlexConfig resultam em erros durante a entrada de texto para várias partes do comando de reconfiguração de software do vizinho BGP. O requisito específico é habilitar a entrada de reconfiguração de software em vizinhos BGP para armazenar rotas recebidas para fins de avaliação de política e solução de problemas.

Ambiente

- Hardware: Secure Firewall 3100 Outras plataformas de hardware também são afetadas.

- Software: FTD (essa limitação também se aplica ao Adaptive Security Appliance (ASA)).
- FMC versão 7.4.6. Outras versões de software também são afetadas.
- FTD versão 7.4.6. Outras versões de software também são afetadas.
- O FTD tem a configuração do protocolo de roteamento BGP.

Resolução

No momento desta escrita, a reconfiguração suave de entrada de vizinho BGP clássica (vizinho de comando BGP x.x.x.x entrada de reconfiguração suave) não é suportada em dispositivos FTD, seja através da interface de usuário BGP do FMC ou como um método FlexConfig suportado.

Limitações da função

Estes recursos de reconfiguração de software BGP não estão disponíveis:

- A configuração de BGP do FMC não fornece uma opção de configuração para a entrada de reconfiguração de software do vizinho.
- A tentativa de configurar o CLI equivalente por meio do FlexConfig falha porque não é um item de configuração de BGP gerenciado por FTD/FMC suportado.

Abordagem alternativa (capacidade de atualização de rota)

O FTD suporta o recurso de atualização de rota BGP quando negociado com pares BGP. Isso fornece o mecanismo suportado para o comportamento de reinicialização dinâmica de software após alterações de política, embora seja diferente da funcionalidade de entrada de reconfiguração de software clássica.

A abordagem recomendada inclui:

- Continue configurando vizinhos BGP, listas de prefixos, mapas de rota e filtrando pelo fluxo de trabalho de configuração BGP suportado pelo FMC.

- Confirme se os pares BGP negociam o recurso de atualização de rota:

<#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
```

- Use o comportamento de atualização de rota para reavaliação de política em vez de tentar habilitar a reconfiguração de software de entrada, por exemplo:

<#root>

```
device#

clear bgp 192.0.2.2 in
```

- Para requisitos operacionais para auditar todas as rotas recebidas e rejeitadas, verifique a partir do par BGP/lado do roteador.

Comparação

Recurso	Recurso de atualização de rota BGP	Reconfiguração de software de entrada
Compatível com FTD/ASA	Yes	No
Como funciona	O roteador envia uma mensagem de solicitação de atualização de rota BGP explícita ao vizinho, pedindo que ele anuncie novamente sua tabela de roteamento.	O roteador aloca RAM extra para salvar uma cópia bruta, não filtrada da tabela BGP do vizinho na memória local.
Requisito de configuração	Nenhum. Ativado automaticamente por padrão no FTD e no ASA.	Configuração manual necessária (`vizinho x.x.x.x soft-reconfiguration inbound`), mas o comando não é suportado em FTD/ASA.
Consumo de memória	Extremamente Baixa. Nenhuma tabela de roteamento extra é armazenada na RAM.	Muito Alta. Consome muito mais memória para os caminhos desse vizinho.
Comando de disparo	# clear bgp x x x x x in	Sem suporte no ASA/FTD.
Dependência de Vizinho	Yes. O peer BGP remoto também deve suportar e aceitar o recurso de atualização de rota.	Não. É completamente local para o firewall; o vizinho de peer não tem ideia de que esteja habilitado.
Comando: `show bgp neighbor x.x.x.x received-routes`	Sem suporte / Falha. O roteador não armazena uma cópia local. A execução desse comando retorna um erro (`% Reconfiguração de software de entrada não habilitada em x.x.x.x`).	Compatível. Exibe instantaneamente as rotas não filtradas e brutas atualmente armazenadas em cache na RAM do roteador antes da aplicação das políticas.

Causa

Essa é uma limitação de recursos em dispositivos FTD e ASA. A funcionalidade de reconfiguração de software de entrada do vizinho BGP não foi implementada na interface de configuração BGP do FMC ou como uma opção FlexConfig suportada para dispositivos FTD. Essa limitação é rastreada como um aprimoramento de software da ID de bug da Cisco CSCvy97220.

Conteúdo relacionado

- Guia de configuração do FMC BGP (10.x)
- Referência de comando FTD para vizinhos BGP e visibilidade de resumo
- ID de bug Cisco CSCvy97220 - Solicitação de aprimoramento para suporte à reconfiguração de software de entrada de vizinhos BGP
- Suporte técnico e downloads da Cisco

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.