BGP AS-Außerkraftsetzung in sicherer Firewall konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie BGP Autonomous System (AS) Override in Cisco Secure Firewall Threat Defense konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- BGP (Border Gateway Protocol)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco Secure Firewall Management Center mit Version 7.7.0
- Cisco Secure Firewall Threat Defense mit Version 7.7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Für große Unternehmen mit geografisch verteilten Standorten kann es schwierig sein, eine End-to-End-Erreichbarkeit zu erreichen, wenn mehrere Standorte die gleiche AS-Nummer (Autonomous System) verwenden. Aktuelles BGP-Verhalten besteht darin, die empfangenen Routing-Updates zu verwerfen, wenn der AS-Pfad die eigene AS-Nummer enthält, um Schleifen im Netzwerk zu vermeiden.

Version 7.6 bietet Unterstützung für AS-override, speziell für SD-WAN-bezogene Anwendungsfälle. Ab Version 7.7 ist eBGP aufgrund seiner Core-Routing-Anforderungen jedoch für alle Bereitstellungen als überschreibende Unterstützung verfügbar. Dadurch können Sie identische Standorte mit derselben AS-Nummer haben.

Anwendungen und Manager:

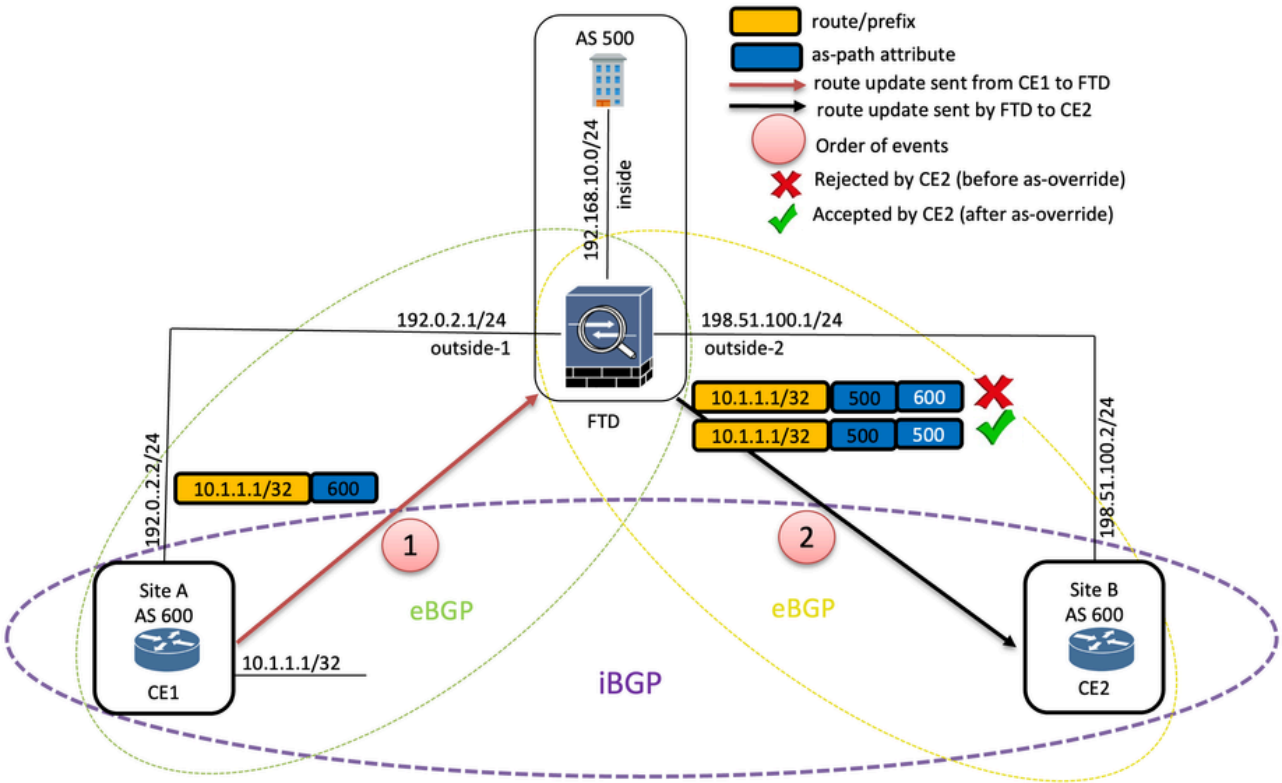
FTD	Alle FTD-Plattformen
FMC auf 7.7.0 FMC REST-API	Ja Ja
FTD-Supportversionen	Nur 7.7.0
Snort-Unterstützung	Snort 3
FDM auf 7.7.0	Nicht unterstützt

BGP AS setzt Paketverarbeitungsablauf außer Kraft

- BGP sendet Routen-Updates über UPDATE an seine Peers/Nachbarn.
- Bekannte, obligatorische Attribute werden von allen BGP-Peers erkannt, an alle Peers übergeben und in allen UPDATE-Meldungen angezeigt.
- Das AS-path-Attribut in der UPDATE-Nachricht enthält eine geordnete Liste aller autonomen Systeme, über die diese Aktualisierung durchgeführt wurde.
- Wenn AS-override-CLI aktiviert ist, wird jedes Vorkommen der AS-Nummer des Nachbarn durch die lokale AS-Nummer im AS-Pfad ersetzt.

Konfigurieren

Netzwerkdiagramm



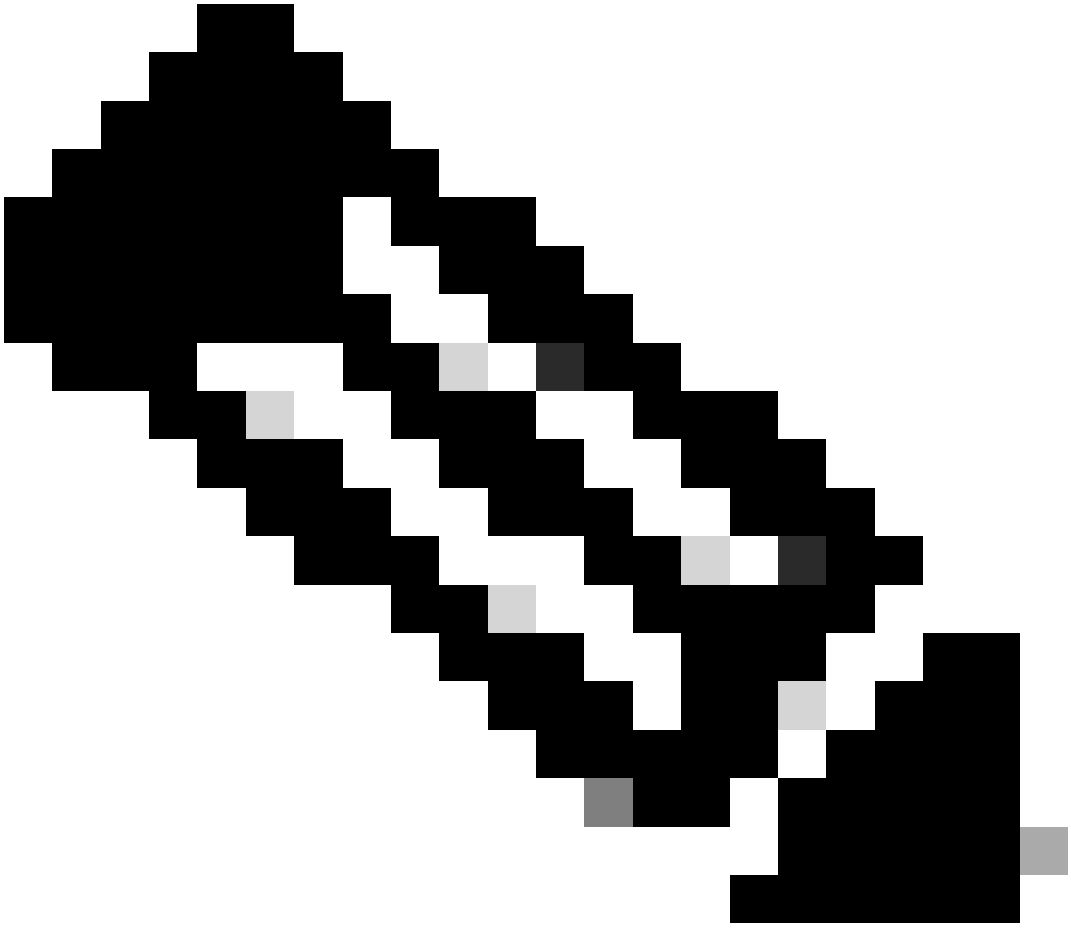
Topologie

Fluss der Routenaktualisierung

- Standort A und B sind zwei identische Standorte, die Geräte/Peers mit derselben AS-Nummer enthalten.
- In diesem Fall ist 10.1.1.1/32 das Präfix/Routen-Update, das von CE1 von Standort A an CE2 von Standort B über FTD angekündigt wird.
- Vor dem Aktivieren von as-override leitet die FTD die Routen-Updates wie bisher an CE2 des Standorts B weiter. CE2 verwirft jedoch beim Empfang die Routen-Updates, da sie ihre eigene AS-Nummer im as-path(600) sieht.
- Nach der Aktivierung von as-override leitet die FTD die Routen-Aktualisierung an CE2 weiter, indem sie die AS-Nummer von CE1 im as-path durch ihre eigene/lokale AS-Nummer (500) ersetzt. CE2 akzeptiert jetzt die Routen-Aktualisierung.

Funktionsüberblick

- Neues Kontrollkästchen in FMC zum Aktivieren von AS Override.
- Der neue CLI-Befehl neighbor <neighbor-ip-address> als Überschrift wird als Teil dieser Funktion in BGP eingeführt.



Anmerkung: Die Funktion "BGP AS Override" (AS-Außerkraftsetzung) kann nur über das Secure Firewall Management Center (FMC) konfiguriert werden.

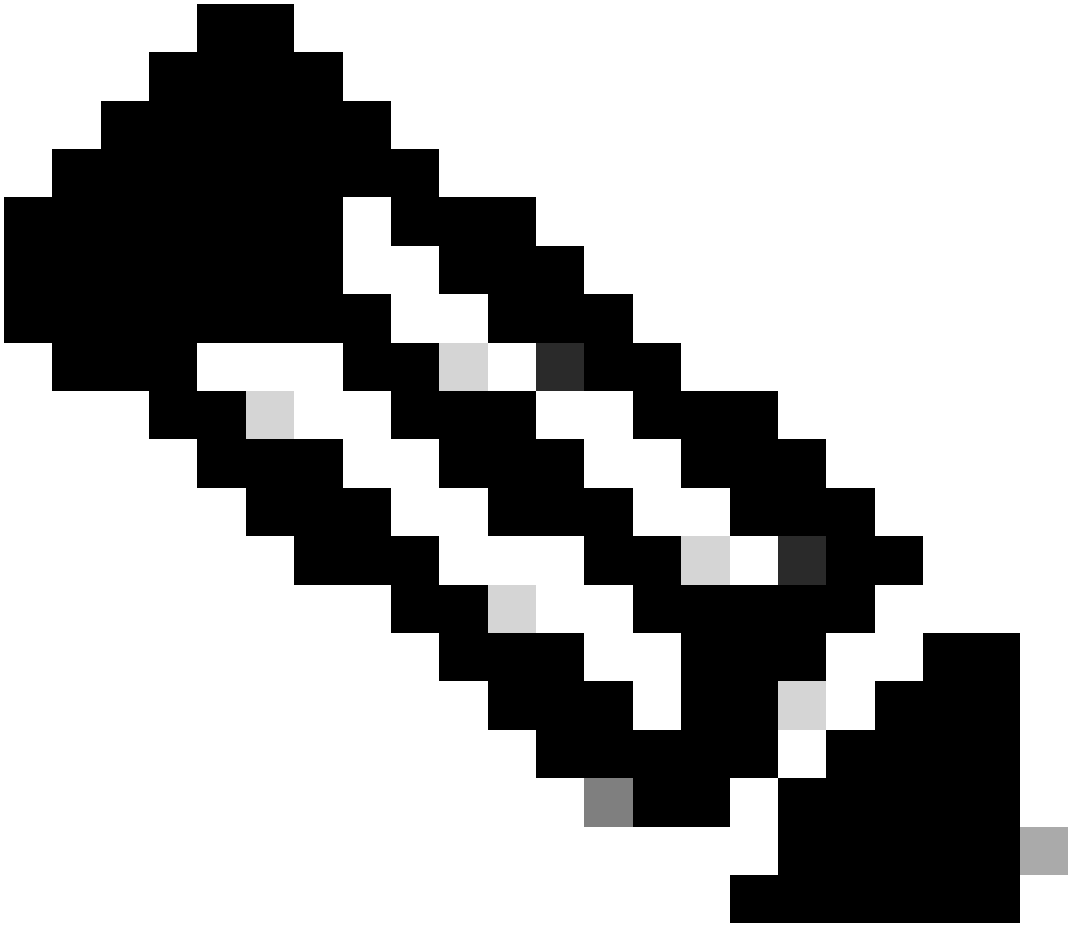
Konfigurationsschritte auf FMC

Schritt 1: Navigieren Sie zu Devices > Device Management (Geräte > Geräteverwaltung), und bearbeiten Sie das Gerät zur Bedrohungsabwehr.

Phase 2: Wählen Sie Routing aus.

Schritt 3: (Für ein virtuelles Router-fähiges Gerät) Klicken Sie unter Allgemeine Einstellungen auf BGP.

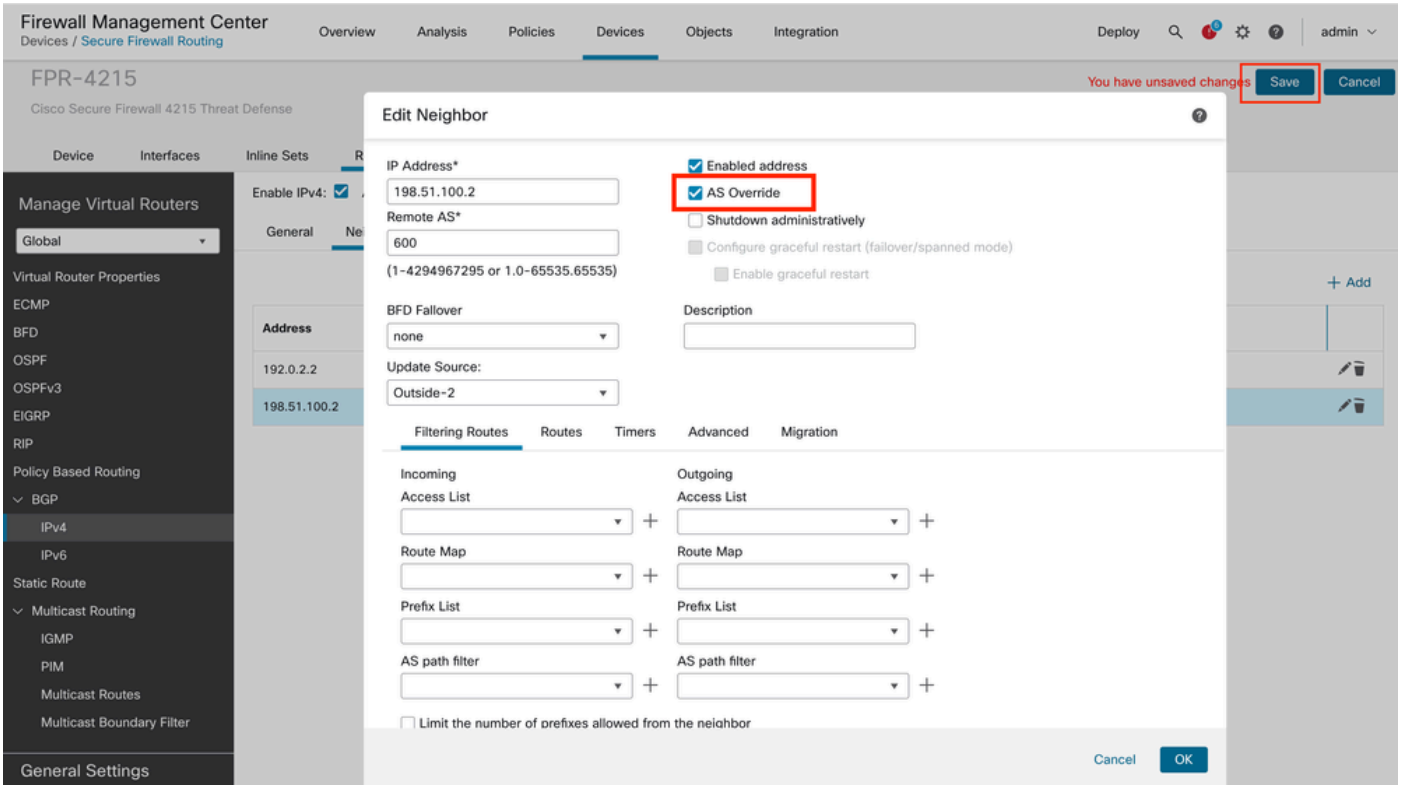
Schritt 4: Aktivieren Sie das Kontrollkästchen Enable BGP (BGP aktivieren), um den BGP-Routing-Prozess zu aktivieren.



Anmerkung: Informationen zur Konfiguration des BGP-Routings finden Sie im Cisco Secure Firewall Management Center Device Configuration Guide, 7.7

BGP-IPv4-Nachbar

- Aktivieren Sie AS Override für 198.51.100.2 Neighbor.
- Klicken Sie auf Speichern und Bereitstellen.



AS-Außerkraftsetzung aktivieren

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

FTD-Ende:

<#root>

FTD# show running-config router bgp all

router bgp 500

```
 bgp log-neighbor-changes
 address-family ipv4 unicast
```

(Same applicable for IPv6 as well)

```
   neighbor 192.0.2.2 remote-as 600
   neighbor 192.0.2.2 update-source Outside-1
   neighbor 192.0.2.2 activate
   neighbor 198.51.100.2 remote-as 600
   neighbor 198.51.100.2 update-source Outside-2
   neighbor 198.51.100.2 activate
```

neighbor 198.51.100.2 as-override

```
   no auto-summary
   no synchronization
 exit-address-family
```

FTD# show bgp ipv4 unicast neighbors 198.51.100.2

```
BGP neighbor is 198.51.100.2,  vrf single_vf,  remote AS 600, external link
 BGP version 4, remote router ID 198.51.100.2
 BGP state = Established, up for 01:13:02
 Last read 00:00:07, last write 00:00:54, 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)
   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

.


.
For address family: IPv4 Unicast
 Session: 198.51.100.2
 BGP table version 4, neighbor version 4/0
 Output queue size : 0
 Index 5
 5 update-group member
```

Overrides the neighbor AS with my AS before sending updates

```
.
.


Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

FTD# show bgp ipv4 unicast neighbors 198.51.100.2 advertised-routes

```
BGP table version is 4, local router ID is 198.51.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*> 10.1.1.1/32     192.0.2.2           0               0  600 i
Total number of prefixes 1
```

Ende der Empfangsgeräte:

<#root>

```
As-path for 10.1.1.1/32 prefix/route has been modified from 600 to 500 by FTD (where as-override is enab

Cisco_C1127#show bgp ipv4 unicast


BGP table version is 10, local router ID is 198.51.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   10.1.1.1/32      198.51.100.1                           0

500 500

 i


Cisco_C1127#show bgp ipv4 unicast 10.1.1.1


BGP routing table entry for 10.1.1.1/32, version 10
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1

  500 500


    198.51.100.1 from 198.51.100.1 (198.51.100.1)
    Origin IGP, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0x0
    Updated on Apr 6 2025 17:02:24 UTC
```

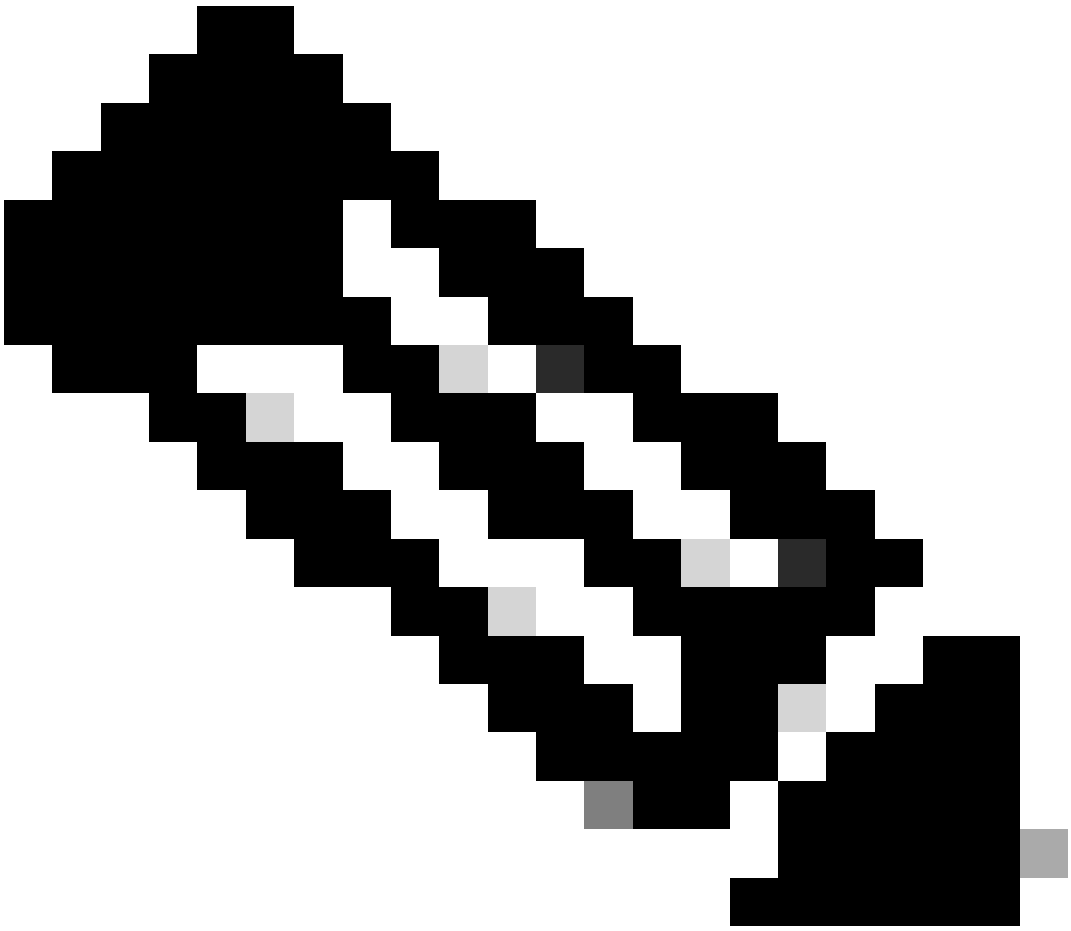
Fehlerbehebung

Befehle

- show run router bgp all muss AS-override CLI in FTD aktiviert haben.
- show bgp <ipv4/ipv6> unicast neighbors auf FTD muss diesen Text angeben, der angibt, dass as-override aktiviert ist -> Überschreibt den Nachbar-AS mit meinem AS, bevor Updates gesendet werden.
- show bgp <ipv4/ipv6> unicast auf der Empfängerseite muss über die geänderten Pfadinformationen verfügen.

Fehlerbehebung

```
debug ip bgp updates
debug ip bgp ipv6 unicast updates
debug ip bgp all updates
```



Anmerkung: Vor und nach der Aktivierung von as-override werden keine Änderungen an den Debugs vorgenommen.

Systemdateien

Diese Protokolldatei enthält Informationen zur Bereitstellung von AS-override-Funktion von FMC.

/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log

<#root>

```
router bgp 500
address-family ipv4 unicast
```

neighbor 198.51.100.2 as-override

```
exit-address-family
```

Zugehörige Informationen

Technischer Support und Downloads von Cisco

Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.7

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.