

BGP AS-opheffing in beveiligde firewall configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[BGP AS-pakketverwerkingsstroom negeren](#)

[Configureren](#)

[Netwerkdigram](#)

[Stroom routeupdate](#)

[Overzicht van functies](#)

[Configuratiestappen op FMC](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten](#)

[Debugs](#)

[Systeembestanden](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u BGP Autonomous System (AS) kunt configureren en negeren in Cisco Secure Firewall Threat Defence.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Management Center met versie 7.7.0.
- Cisco Secure Firewall Threat Defense, versie 7.7.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Voor grote ondernemingen met geografisch verspreide locaties kan het moeilijk zijn om end-to-end bereikbaarheid te bereiken wanneer meerdere locaties hetzelfde Autonomous System (AS)-nummer gebruiken. Het huidige BGP-gedrag is om de ontvangen routingupdates te negeren als het AS-pad het eigen AS-nummer bevat, om lijnen in het netwerk te vermijden.

De 7.6 release is geïntroduceerd als ondersteuning voor SD-WAN-gerelateerde gebruikscases. Vanaf de 7.7-release is er echter ondersteuning voor as-override voor eBGP beschikbaar voor alle implementaties vanwege de basisvereisten voor routing. Hierdoor kunt u identieke sites hebben met hetzelfde AS-nummer.

Toepassingen en beheerders:

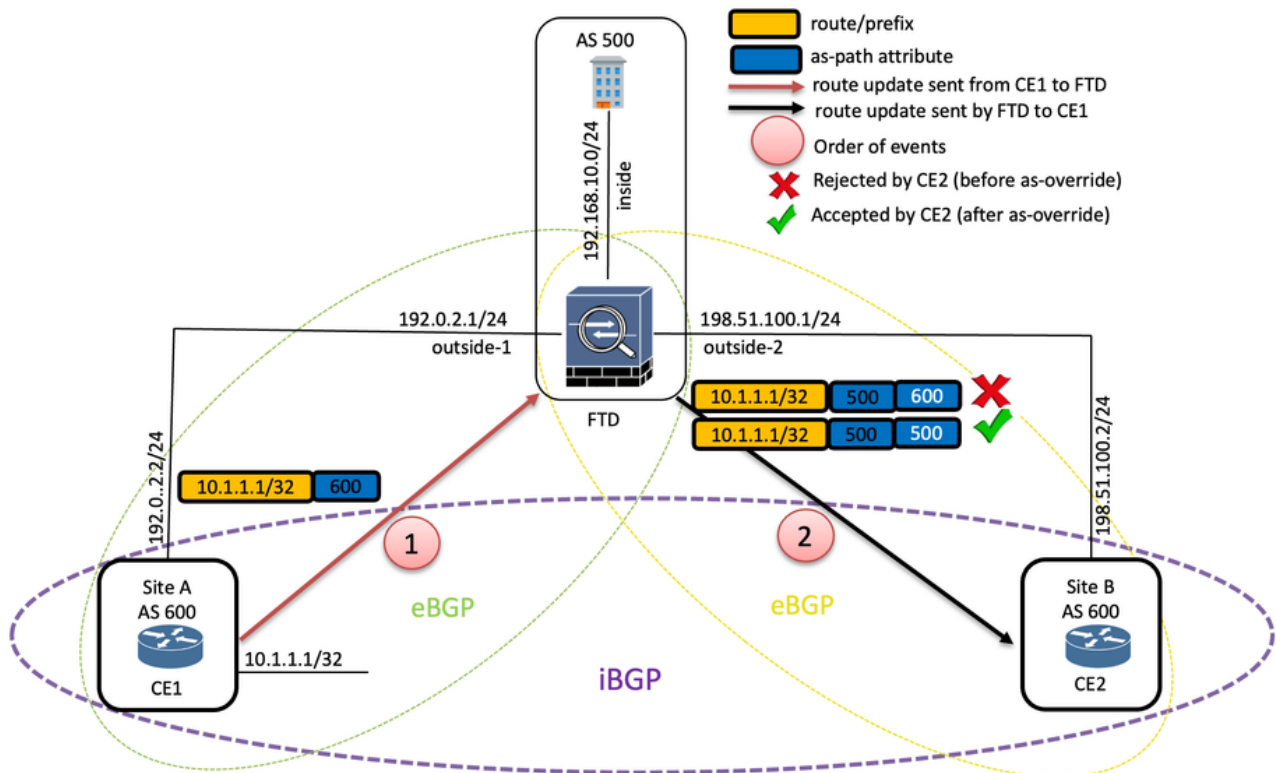
FTD	Alle FTD-platforms
VCC op 7.7.0	Ja
FMC REST API	Ja
FTD-ondersteuningsversies	alleen 7.7.0
Snelondersteuning	Sorteren 3
FDM op 7.7.0	Niet ondersteund

BGP AS-pakketverwerkingsstroom negeren

- BGP stuurt routeupdates naar haar peers/buren via UPDATE-berichten.
- De bekende, verplichte eigenschappen worden herkend door alle BGP-peers, doorgegeven aan alle peers en aanwezig in alle UPDATE-berichten.
- Het attribuut AS-path in het UPDATE-bericht bevat een geordende lijst van alle autonome systemen waardoor deze update is doorgegeven.
- Als as-override CLI is ingeschakeld, wordt elk exemplaar van de buren als nummer vervangen door het lokale AS-nummer in het as-pad.

Configureren

Netwerkdigram



Topologie

Stroom routeupdate

- Site A en Site B zijn twee identieke sites die apparaten/peers bevatten met hetzelfde AS-nummer.
- In dit geval is 10.1.1.1/32 de prefix/route update die wordt geadverteerd van CE1 van site A naar CE2 van site B via FTD.
- Alvorens as-override in te schakelen, stuurt de FTD de routeupdates door zoals het is naar CE2 van site B. Maar, CE2 bij ontvangst, verwijpt de routeupdate aangezien het zijn eigen AS-nummer in de as-path(600) ziet.
- Na het inschakelen van as-override, stuurt de FTD de routeupdate naar CE2 door het AS-nummer van CE1 in het as-pad te vervangen naar het eigen/lokale AS-nummer (500). Nu aanvaardt CE2 de routeupdate.

Overzicht van functies

- Nieuw aanvinkvakje in FMC om AS Override in te schakelen.
- De nieuwe CLI-opdrachtbuur <buuradres-ip-adres> wordt als overbrugging in BGP geïntroduceerd als deel van deze functie.



Opmerking: De functie BGP AS Override kan alleen worden geconfigureerd via het Secure Firewall Management Center (FMC).

Configuratiestappen op FMC

Stap 1: Navigeer naar Apparaten > Apparaatbeheer en bewerk het bedreigingsbeschermingsapparaat.

Stap 2: Selecteer routing.

Stap 3: (Voor een virtueel-router-bewust apparaat) Klik onder Algemene instellingen op BGP.

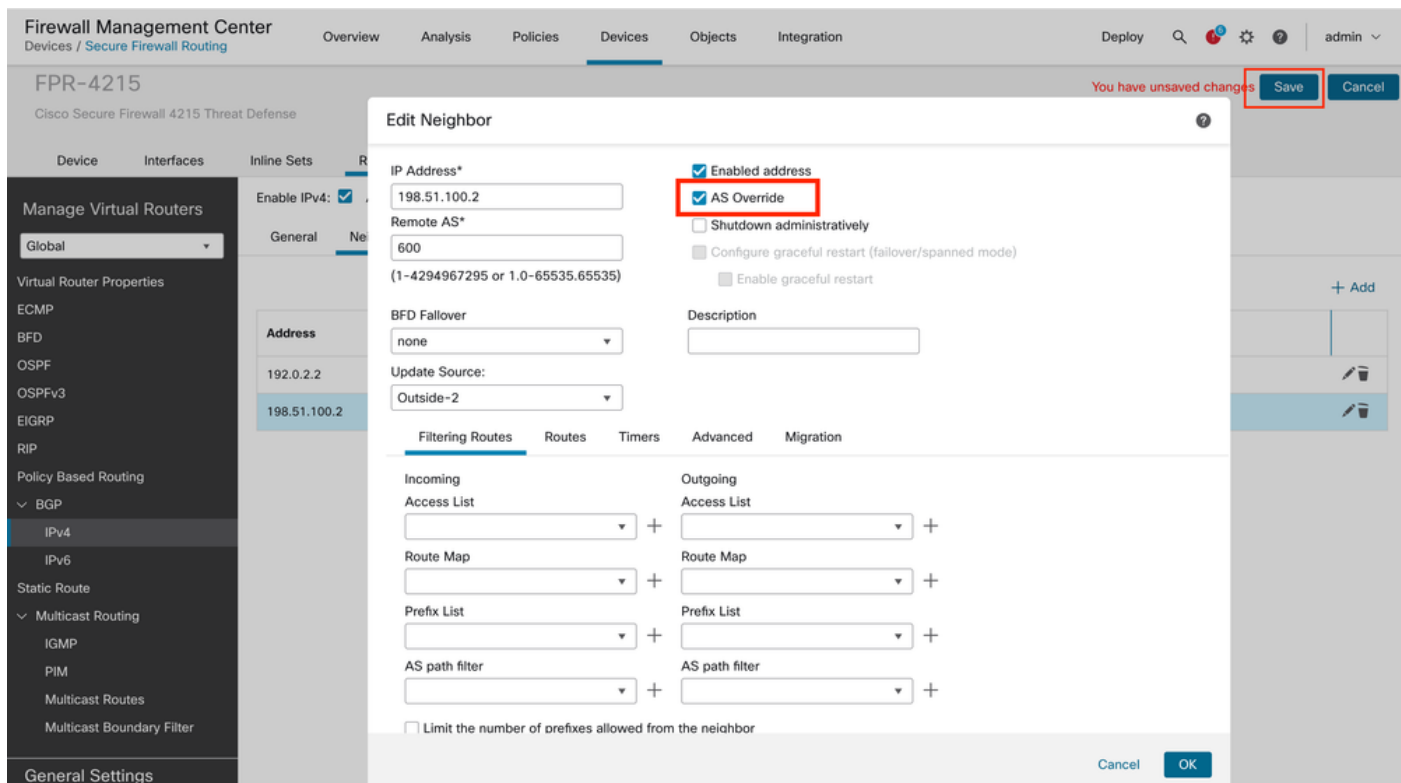
Stap 4: Schakel het aanvinkvakje BGP inschakelen in om het BGP-routeringsproces in te schakelen.



Opmerking: Voor het configureren van BGP-routing kunt u verwijzen naar de [configuratiehandleiding voor het apparaat van Cisco Secure Firewall Management Center, 7.7](#)

BGP IPv4-buur

- AS negeren inschakelen voor 198.51.10.2-buur.
- Klik op Opslaan en implementeren.



AS negeren inschakelen

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Einde FTD:

<#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

Einde ontvangers:

<#root>

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

```
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
```

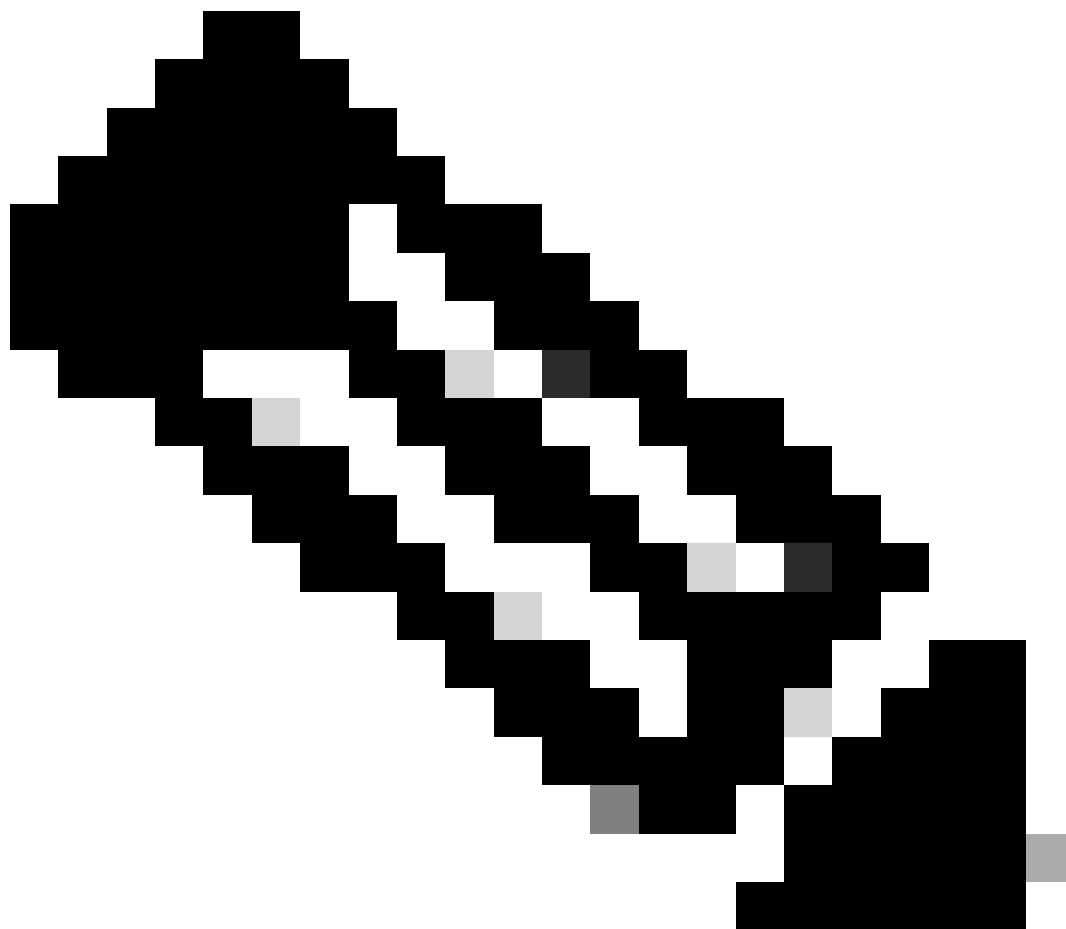
Problemen oplossen

Opdrachten

- toon looppas router bgp allen moet hebben AS-override CLI die in FTD wordt toegelaten.
- toon bgp <ipv4/ipv6> unicast-buren op FTD moeten deze tekst aangeven dat as-override is ingeschakeld -> Overschrijft de buur AS met mijn AS voordat updates worden verzonden.
- toon bgp <ipv4/ipv6> unicast op het ontvangeruiteinde moet de gewijzigde padinformatie hebben.

Debugs

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



Opmerking: Er zijn geen veranderingen in de debugs voor en na het inschakelen van as-override.

Systeembestanden

Dit logbestand bevat informatie over de inzet van de functie 'as-override' van het VCC.

/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
```

Gerelateerde informatie

[Cisco Technical Support en downloads](#)

[Handleiding voor configuratie van apparaat in Cisco Secure Firewall Management Center, 7.7](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.