Configure BGP AS Override in Secure Firewall

Contents

Introduction

This document describes how to configure BGP Autonomous System (AS) Override in Cisco Secure Firewall Threat Defense.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center running version 7.7.0.
- Cisco Secure Firewall Threat Defense running version 7.7.0.

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

For large enterprises with geographically dispersed locations, achieving end-to-end reachability can be challenging when multiple sites use the same Autonomous System (AS) number. Current BGP behavior is to discard the routing updates received if the AS path contains the AS number of its own, to avoid loops in the network.

The 7.6 release introduced as-override support specifically for SD-WAN-related use cases. However, starting with the 7.7 release, as-override support for eBGP is available for all deployments due to its core routing requirement. This enable you to have identical sites with same AS number.

Applications and Managers:

FTD	All FTD Platforms
FMC on 7.7.0	Yes
FMC REST API	Yes
FTD Support Versions	7.7.0 only
Snort Support	Snort 3
FDM on 7.7.0	Not supported

BGP AS Override Packet Processing Flow

- BGP sends route updates to its peers/neighbors via UPDATE messages.
- Well-known, mandatory attributes are recognized by all BGP peers, passed to all peers, and present in all UPDATE messages.
- AS-path attribute in the UPDATE message contains an ordered list of all the autonomous systems through which this update has passed.
- When as-override CLI is enabled, each occurrence of the neighbors AS number is replaced by the local AS number in the as-path.

Configure

Network Diagram
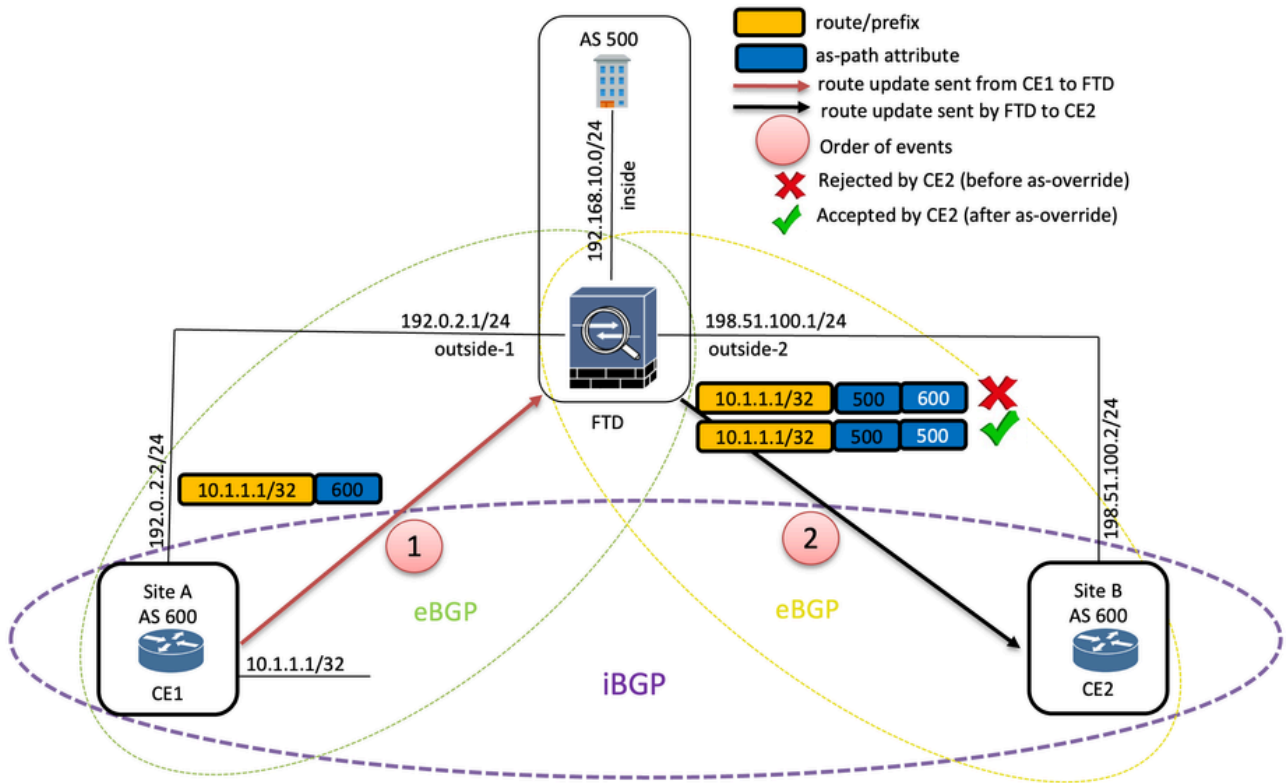
Topology

Route Update Flow

- Site A and Site B are two identical sites containing device/peers with the same AS number.
- In this case, 10.1.1.1/32 is the prefix/route update which is being advertised from CE1 of site A to CE2 of site B via FTD.
- Before enabling **as-override**, the FTD forwards the route updates as it is to CE2 of site B. But, CE2 upon receiving it, discards the route update as it sees its own AS number in the as-path(600).
- After enabling **as-override**, the FTD forwards the route update to CE2 by replacing the AS number of CE1 in the as-path to its own/local AS number (500). Now CE2 accepts the route update.

Feature Overview

- New checkbox in FMC to enable **AS Override**.
- New CLI command **neighbor <neighbor-ip-address> as-override**is introduced in BGP as part of this feature.

Note: The BGP AS Override feature is available for configuration via the Secure Firewall Management Center (FMC) only.

Configuration Steps on FMC

Step 1: Navigate to **Devices** > **Device Management**, and edit the **threat defense** device.

Step 2: Select **Routing**.

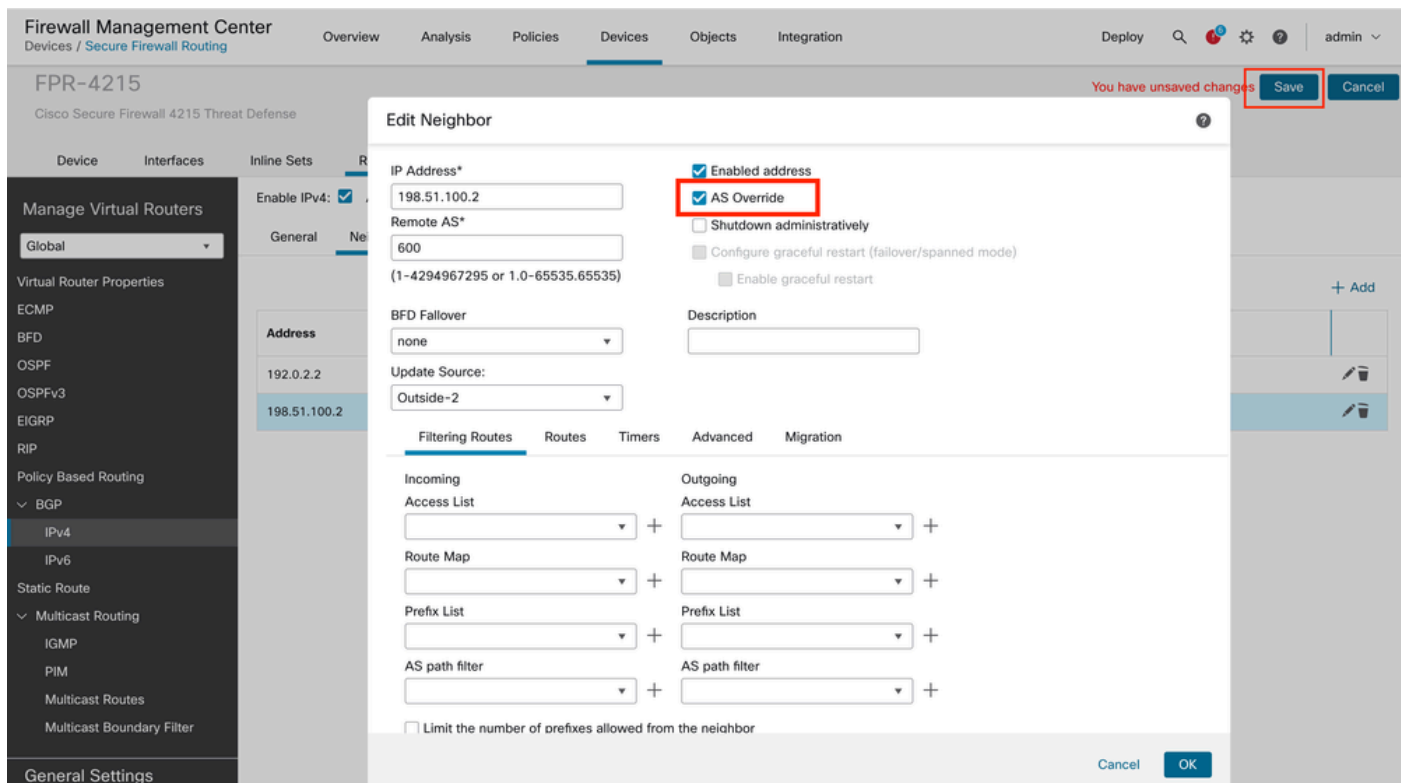Step 3: (For a virtual-router-aware device) Under **General Settings**, click **BGP**.

Step 4: Check the **Enable BGP** check box to enable the BGP routing process.

Note: To configure BGP routing, you can refer to [Cisco Secure Firewall Management Center Device Configuration Guide, 7.7](#)

BGP IPv4 Neighbor

- Enable **AS Override** for 198.51.100.2 neighbor.
- Click **save** and **deploy**.

Enable AS Override

Verify

Use this section to confirm that your configuration works properly.

FTD End:

<#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
```

Receivers End:

<#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
```

Troubleshoot

Commands

- **show run router bgp all** must have AS-override CLI enabled in FTD.

- **show bgp <ipv4/ipv6> unicast neighbors** on FTD must specify this text indicating that as-override is enabled -> Overrides the neighbor AS with my AS before sending updates.

- **show bgp <ipv4/ipv6>** unicast on the receiver end must have the changed path information.

Debugs

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

Note: There are no changes in the debugs before and after enablement of as-override.

System Files

This log file contains information related to deployment of as-override feautue from 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
```

Related Information

[Cisco Technical Support & Downloads](#)

[Cisco Secure Firewall Management Center Device Configuration Guide, 7.7](#)