Software Advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature

Dear Cisco Customer,

Cisco engineering has identified the following software issue. Please review this Software Advisory to determine if the issue applies to your environment.

Affected Software and Replacement Solution for CSCvq34340		
Software Type	**Software Affected**	**Software Solution**
Firepower Threat Defense (FTD)	**Versions:** 6.4.0.x 6.5.0.x	**Versions:** 6.4.0.7+ turns off egress optimization 6.5.0.2+ turns off egress optimization 6.6.0+ fixes the issue

Reason for Advisory
CSCvq34340: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature

CSCvs32023: Turn off egress-optimization processing

Affected Platforms
FTD devices running Version 6.4.0.x or 6.5.0.x

Symptom
FTD devices might experience a traffic outage caused by a 9344 block size depletion triggered by the egress optimization feature first introduced in Version 6.4.0.

Conditions
For a device to be impacted by this bug, each of the following conditions MUST be true:

1. Egress optimization is enabled. To determine this, use the following command from the unified FTD CLI:

```
> show asp inspect-dp egress-optimization
Current running state: Enabled
```
<-- Will show Enabled or Disabled

2. Non-zero ASP drops with the 'snort-blist-full' reason are present in `show asp drop` output from the unified FTD CLI:

```
> show asp drop

Frame drop:
.....
  Per-flow block limit reached on flows fast-forwarded by
Snort (snort-blist-full)                          343605
.....
```

3. There is evidence of 9344 block depletion or a very low number of blocks in the LOW or CNT column. A value less than approximately 20% of the MAX value can be considered very low in this case. Run the following command from the unified FTD CLI:

```
> show blocks

  SIZE    MAX    LOW    CNT
     0   2700   2700   2700
     4    100    100    100
    80   1000    997   1000
   256   4660     62   4655
  1550   6254   6249   6252
  2048    100    100    100
  2560    164    164    164
  4096    100    100    100
  8192    100    100    100
  9344  60000      0      0
 16384    100    100    100
```

4. Regardless of firewall mode (routed or transparent), egress optimization takes effect only on traffic passing through the following:

   - Inline sets (regular or tap)
   - Interface in passive mode

Workaround — Upgrade to Version 6.6.0
We recommend you upgrade to Version 6.6.0. This will fix the issue.

If egress optimization was enabled but turned off, the Version 6.6.0 upgrade turns it back on. (We turned off egress optimization in some Version 6.4.0.x and 6.5.0.x patches. See the next workaround.)

If egress optimization was manually disabled, we recommend you reenable it after you upgrade. Enter the following command from the unified FTD CLI:

```
> asp inspect-dp egress-optimization
```

Workaround — Patch to Version 6.4.0.7+ or 6.5.0.2+
If you cannot upgrade to Version 6.6.0, we recommend you patch to Version 6.4.0.7+ or 6.5.0.2+.

Patching turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.

Workaround — Manually disable egress optimization
If you can neither patch nor upgrade, disable egress optimization:

1. Enter the following command from the unified FTD CLI:

   ```
   > no asp inspect-dp egress-optimization
   ```

2. If you are already experiencing traffic interruption and the above symptoms, the connections should also be cleared on the firewall to eliminate stale connections that also may exist as a result of this issue. Clear connections using the following command:

   ```
   > clear conn
   ```

   Note: This will tear down current connections on the firewall, and the connections must be reestablished. If the goal is to proactively avoid the issue, this step is not necessary and can be skipped to avoid traffic impact.