Troubleshoot FTD Blocking Private IP URLs Due to SI Parsing Issue

Contents

Issue

FTD devices started blocking production internal traffic when the URL host contains a private IP address after receiving Security Intelligence URL/network feed updates from Talos.

The affected traffic includes URLs such as http://10.54.1.7:8200/v1/sys/health and http://172.31.14.7:9100. The traffic is being categorized as "Private IP Addresses as Host" and blocked by Talos-related Security Intelligence policies with verdicts including "URL Block", "blacklist", and "si, force_block". This behavior impacts internal service communications and business operations.

When examining the FTD system support traces, this blocking behavior was observed:

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Firewall: allow rule, 'Access_Rule', allow
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Generating an EOF event with rule_id = 26845
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 SI: URL security intelligence list id 104862
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict: blacklist
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 Verdict Reason: si, force_block
```

Environment

- Cisco FTD Version 7.6.4 (FMC Managed)
- Security Intelligence feeds enabled with URL Malicious categories
- Internal production services using private IP addresses in URLs
- Issue occurred after Security Intelligence URL/network feed updates from Talos

Understanding System Support Trace Logs :

```
172.17.255.3 63554 -> 172.31.14.7 9100 6 AS=0 ID=11 GR=1-1 InsightUrlListEventHandler: num_list_matched
```

- In system support trace logs, category value is printed.
- Category Value : [1048627]
- Mapping of Category Value and corresponding SI feed file is available in FTD at location:

Location in FTD: /ngfw/var/sf/siurl_download/url.rules

Location in Tshoot file: /file-contents/var/sf/siurl_download/url.rules

<#root>

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$
```

cat url.rules

```
# security intelligence manifest file
si,5915d129-0d33-4e9c-969a-eab3cde32156.lf,1048589,white,any
si,ac0ef862-1cff-11ef-a575-4cf8bc134a1f.lf,1074790408,block,any
si,005056bf-1643-0ed3-0000-030068648887.lf,1048646,block,any
si,127dc4a2-1ea3-4423-a02d-1f02069828ac.lf,1048590,block,any
si,c87fe5d4-5868-11ef-8843-a8b3afb1bf74.lf,1048645,block,any
si,7c51a74a-d984-11ef-8637-e77eccc0d672.lf,1048649,block,any
si,1b117672-7453-478c-be31-b72e89ca4bfc.lf,1048616,block,any
si,2b15cb6f-a3fc-4e0e-a342-ccc5e5806394.lf,1048619,block,any
si,30f9e69c-d64c-479c-821d-0e4edab852ab.lf,1048620,block,any
si,5f8148f1-e5e4-427a-aa3b-ee1c2745f481.lf,1048623,block,any
si,8af156ca-8020-4608-9278-01b8745811b7.lf,1048626,block,any
si,d3899830-d481-4773-b4e2-7daa7acf8f75.lf,1048633,block,any
si,03709ed4-faab-47af-bade-4435f8da11f5.lf,1048615,block,any
si,bde824fd-36dd-4a7c-9cc1-80e40ac7db66.lf,1048632,block,any
si,a27c6aae-8e52-4174-a81a-47c59fecf1c3.lf,1048629,block,any
si,6ba968f4-7a25-4793-a2c8-7cc77f1f1256.lf,1048625,block,any
si,02213098-6d94-4680-8ce8-2d081638d087.lf,1048613,block,any
si,5a0b6d6b-e2c3-436f-b4a1-48248b333b57.lf,1048622,block,any
si,3e2af68e-5fc8-4b1c-b5bc-b4e7cab5c9eb.lf,1048621,block,any
si,2ccda18e-ddff-4f5c-af9a-f0098521b525.lf,1048618,block,any
si,60f4e2ab-d96c-44a0-bd38-830252b67077.lf,1048624,block,any
si,23f2a124-8278-4c03-8c9d-d28fe08b8fc9.lf,1048617,block,any
si,937cf5e8-76d1-4ba2-a83c-475dc80c6976.lf,1048628,block,any
si,032ba433-c295-11e4-a919-d4ae5275d599.lf,1048614,block,any
si,d7d996a6-6b92-4a56-8f10-e8506e434dd6.lf,1048634,block,any
si,abdc925f-4f85-4504-90a7-c891979af648.lf,1048630,block,any
```

si,8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf,1048627,block,any >>>>>>matching category ID

```
si,b1df3aa8-2841-4c88-8e64-bfaacec71300.lf,1048631,block,any
si,ac0f6900-1cff-11ef-a575-4cf8bc134a1f.lf,1074790407,monitor,any
ac,5846a44a-3d2a-11f0-a12d-7a89a4a10ab3.lf,1048650
```

```
kkhapeka@tex-7db6f6c675-8kcnb:.../siurl_download$ pwd
```

How to interpret the prior line(s):

- Content in the file with name "8c3e31be-ca41-43c8-87cb-82a35b0f5213.lf" has been assigned category ID: 1048627
- To check what the actual category is, open the file using vi and any editor tool, and the name of the category is on top.

<#root>

```
kkhapeka@KKHAPEKA-M-F6H2 Downloads %
```

```
cat -n  8c3e31be-ca41-43c8-87cb-82a35b0f5213| more
```

```
     1  #Cisco DNS and URL intelligence feed: URL Malicious >>>>>name of the category
     2  fadoz.metrs.workers.dev/sell/2641c1ef
     3  oauth-opensea.com
     4  account8133944-complaince.com
```

- Using the logical path corresponding security Intelligence feed files can be traced, and one of the important aspect of collecting evidence is to manually download the Security Intelligence feed files from FTD to a local machine.
- Security Intelligence feeds are updated at regular intervals and during the feed update, no change logs exists on FMC and FTD indicating what the changes made.
- By downloading the Security Intelligence feed, you can take a snapshot of the feed at that moment, and it can be provided to the BU/TALOS later.

Resolution

The resolution involves updating the Security Intelligence feeds and implementing a temporary workaround while awaiting a permanent software fix.

Step 1: Update Security Intelligence Feeds

Update the Security Intelligence feeds to obtain the corrected feed content from Talos:

Navigate to **Policies > Security Intelligence** in the FMC and manually trigger a feed update, or wait for the automatic update cycle to complete.

Step 2: Implement Temporary Workaround (if the issue persists)

If the issue continues after the feed update, add the affected URLs or domains to the "Do not block" list as a temporary workaround:

Navigate to **Policies > Security Intelligence** and add the private IP URLs to the "Do not block" list under the URL tab.

Step 3: Re-enable URL Malicious Category

After confirming the feed update resolves the issue, re-add the "URL Malicious" category to the Security Intelligence configuration:

Navigate to **Policies > Security Intelligence** and re-enable the "URL Malicious" category under the Block List.

Step 4: Remove Workaround Entries

Remove the affected URL/domains from the "Do not block" list once the permanent fix is confirmed and working.

Step 5: Validation

Verify that private IP URL destinations are no longer being blocked by Security Intelligence by testing the previously affected URLs and monitoring the connection events in FMC.

Cause

The issue was caused by a parsing problem in the Security Intelligence feeds content that impacted FTD

behavior. In the Security intelligence feed, there were URLs with length longer than 2047 characters.

When an entry exceeds the supported length, part of this issue can be because it was incorrectly loaded as a separate malicious entry, potentially blocking unrelated traffic. This behavior is tracked under Cisco bug ID: CSCww11335. The issue was resolved through corrective changes made by the Talos team to the feed content, with a permanent software fix planned for a later release to add guard rails preventing future occurrences.

Related Content

- Cisco bug ID: CSCww11335
- Cisco Technical Support & Downloads