DNS/PTR Lookup Packet Visibility Issues in FTD 7.4 Packet Captures

Issue

When blocked by security intelligence, Firewall Threat Defense (FTD) packet capture does not display
DNS queries to the malicious domains that are being blocked by the FTD security intelligence. Connection events or

Environment

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (applicable to a
- Software Version: 7.4.2 / 7.4.2.4 (applicable to all systems using security intelligence)
- Perimeter Firepower device monitoring DNS traffic between Infoblox DNS server and CIRA Cloud
- Security Intelligence configured to block DNS crypto mining threats
- Lab topology involving FPR2110 and FPR2100 devices for reproduction
- DNS query targeting domain: static.vdc.vn
- Threat classification: DNS crypto mining threat
- Packet capture and connection events analyzed on Firepower device
- Infoblox DNS server as internal DNS infrastructure

Resolution

1. Analyze connection events on the FTD to confirm that DNS queries from the DNS server to the external domain a

```
Connection Event
```

Example:

Domain: static.vdc.vn
Action: Blocked (DNS crypto mining threat)

2. Initiate a packet capture on the FTD targeting DNS traffic between the relevant IP addresses. In a Wireshark analy

```
FTD# capture CAP interface  match udp host SRCIP host DESTIP eq 53
```

```
(no output for the expected packets)
```

- According to Cisco documentation, Security Intelligence filtering is an early phase of access control. If a pack can be dropped before further inspection and before being processed by other policies (including access control, packet capture, DNS inspection).
- Security Intelligence filtering occurs before resource-intensive inspection.
- Packets blocked by Security Intelligence are sometimes not be captured by standard packet capture mechanisms on the device.
- Prefilter rules evaluated before Security Intelligence can also affect visibility.

3. Utilize the **system support url-si-debug** command in the FTD CLISH to trace PTR lookups between source and destination IPs to understand how and

```
> system support url-si-debug


SRCIP 37046 -&gt; DSTIP 53 17 AS=0 ID=39 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 49094 -&gt; DSTIP 53 17 AS=0 ID=42 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 48508 -&gt; DSTIP 53 17 AS=0 ID=12 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
```

4. Use the source ports as a reference to correlate with packet captures and logs from **system support trace**. This is t next example, the related packets show as PTR (reverse DNS) lookups instead of normal DNS queries. This is why t **which show** on an event even if the same connection shows as Blocked by security intelligence.

```
8847 2026-01-29 20:41:15.940854Z SRCIP DSTIP DNS 98 Standard query 0x20ef PTR 23.172.189.113.in-
addr.arpa OPT
9582 2026-01-29 20:41:18.348889Z SRCIP DSTIP DNS 98 Standard query 0x8b58 PTR 23.172.189.113.in-
addr.arpa OPT
10190 2026-01-29 20:41:21.556901Z SRCIP DSTIP DNS 98 Standard query 0x636a PTR
23.172.189.113.in-addr.arpa OPT
11362 2026-01-29 20:41:24.652950Z SRCIP DSTIP DNS 99 Standard query 0xf6f5 PTR
135.238.166.113.in-addr.arpa OPT
13670 2026-01-29 20:41:27.964885Z SRCIP DSTIP DNS 98 Standard query 0xfb40 PTR
23.172.189.113.in-addr.arpa OPT
```

5. Review the reply packets to these PTR lookups from the destination and the malicious domain can be seen. This t

```
981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn Standard query response
0xc5c3 PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT
```

Coordinate with
the customer team to investigate if any reverse DNS queries or unexpected traffic patterns are observed for given IPs
Not-
Block list or permit via prefilter as appropriate. This can allow subsequent inspection and visibility in packet capture

- Add IPs to Security Intelligence Do-Not-Block list if further analysis is required.
- Permitting in prefilter allows traffic to bypass Security Intelligence block.

Cause

The root cause is that the PTR (reverse DNS) Lookup passes through the FTD initially by access rule as it is still per
as associated with DNS crypto mining threat), the packet is dropped. As a result, the malicious domain is only found

Related Content

- Cisco Secure Firewall Management Center Device Configuration Guide, 7.4: About Security Intelligence
- Cisco Technical Support & Downloads
- Cisco bug ID CSCwt16755 -
  DOC: PTR lookups pass FTD by AC policy, but response is blocked by Security Intelligence