FMC Reports Cisco Smart Licensing Traffic as toos.cisco.com When TSID Is Enabled

Contents

Issue

Firepower Management Center (FMC) and Firepower Threat Defense (FTD) report Cisco Smart Licensing HTTPS traffic as `toos.cisco.com` instead of `tools.cisco.com`.
This causes Cisco device licensing traffic (ASA, routers, switches) to be blocked by URL-based or Security Intelligence policies, potentially resulting in license expiration.

The traffic itself is legitimate and destined to Cisco licensing infrastructure.

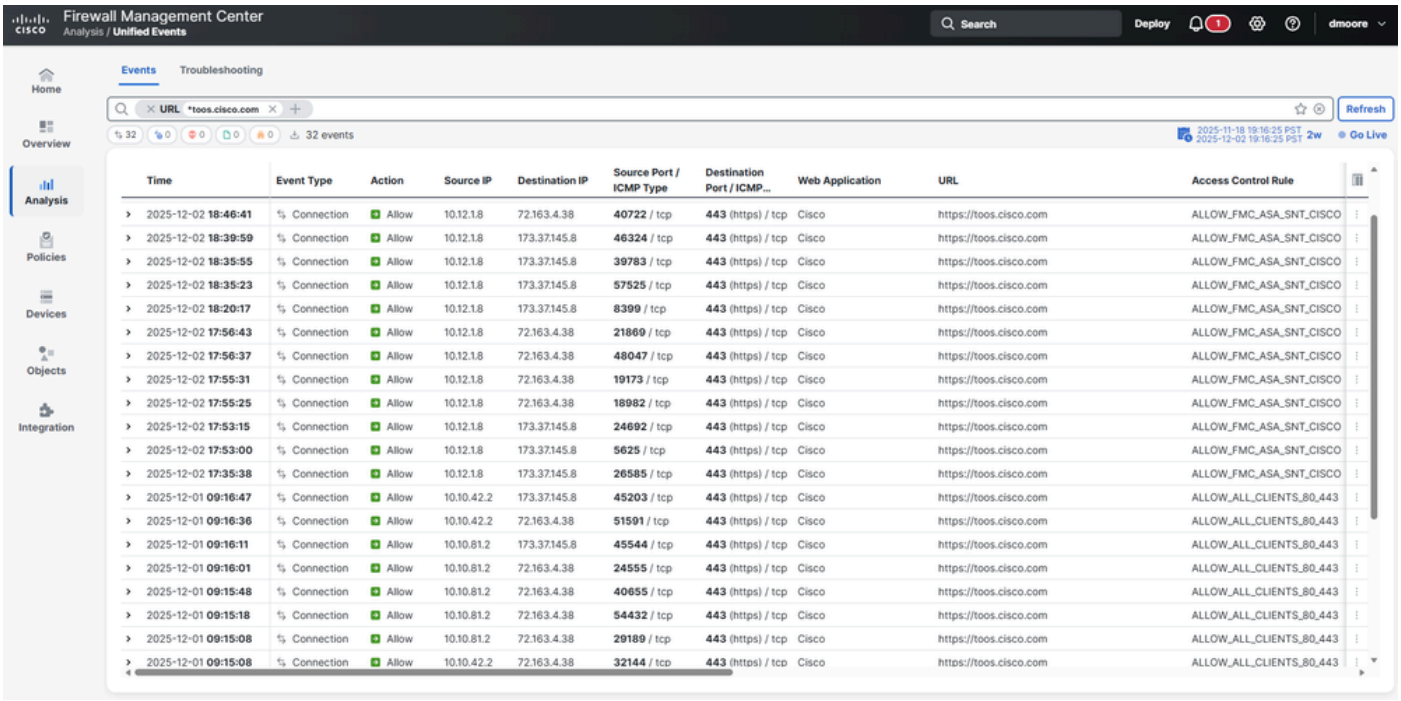
Environment

- **Product Family**: Cisco Secure Firewall
- **Traffic Type**: Cisco Smart Licensing (HTTPS / TCP 443)
- TLS Server Identity (TSID) feature enabled

Resolution

Symptoms

- FMC connection events or FTD system support trace show:



- Smart Licensing commands (for example, `license smart renew auth`) fail.
- URL filtering / Security Intelligence policies blocking `toos.cisco.com`.
- Packet capture confirms traffic is sent to Cisco licensing IPs (like `tools1.cisco.com`).
- Disabling TSID causes FMC to report `tools.cisco.com`.

Troubleshooting / Investigation Steps

Confirm Smart Licensing Traffic

On the Cisco device (example: ASA):

```
license smart renew auth
```

Capture Traffic on the Cisco Device (ASA Example)

```
capture LIC interface outside trace detail match tcp host <ASA_IP> any eq 443
```

```
show capture LIC
```

Export the capture and confirm destination IP resolves to Cisco licensing hosts:

```
tools1.cisco.com
```

Capture or Trace Traffic on FTD

Packet Capture (FTD CLI)

```
capture capin interface <inside> match tcp host <DEVICE_IP> any eq 443
capture capout interface <outside> match tcp host <DEVICE_IP> any eq 443
```

System Support Trace

```
system support trace
```

Look for log entries similar to:

```
url toos.cisco.com
```

Verify TSID Configuration in FMC

- Navigate to Access Control Policy
- Edit the applicable rule
- Check Advanced Settings
- Confirm TLS Server Identity Discovery (TSID) is enabled

Validate TSID Impact (Optional Test)

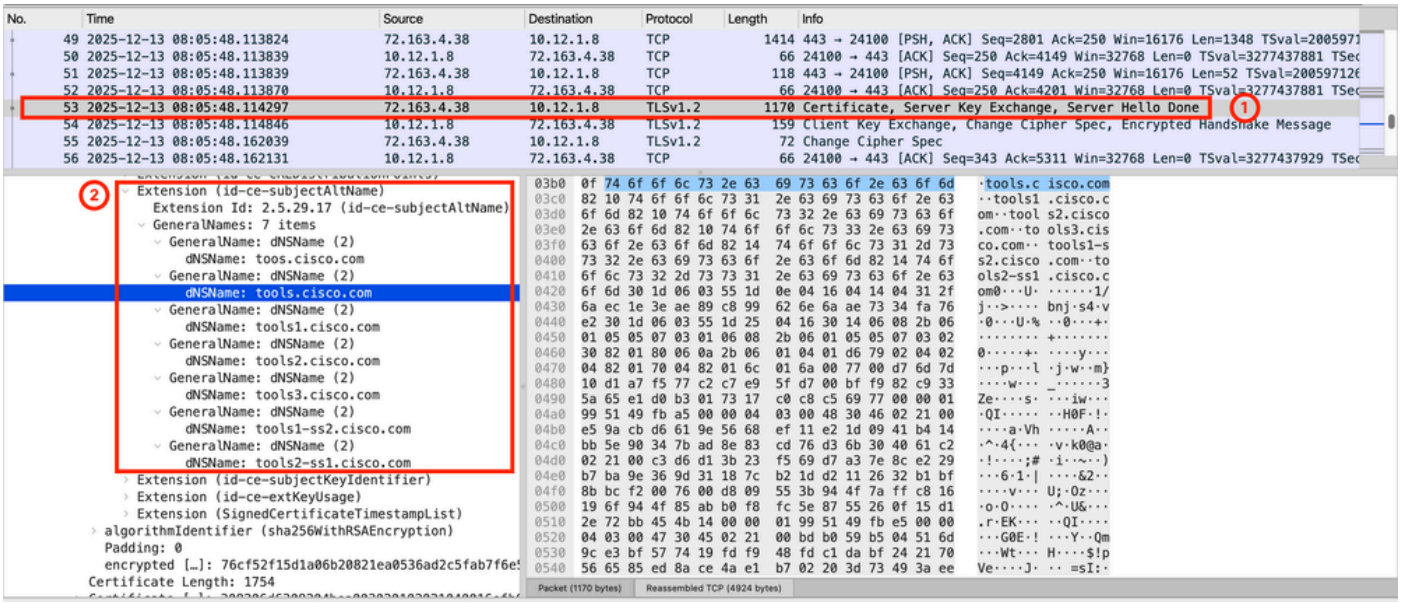
- Disable TSID on the rule
- Deploy policy
- Re-run licensing attempt

Note - Expected behavior: FMC reports `tools.cisco.com` when TSID is disabled

Inspect Server Certificate (Optional)

From packet capture or browser tools, confirm:

- SAN list includes `toos.cisco.com` as the first entry



Resolution / Recommended Handling

No defect. Behavior is by design. Advise one of these options:

1.- Allow `toos.cisco.com` in URL filtering / Security Intelligence policies

2.- Permit Cisco Smart Licensing traffic by: URL category or Broader domain pattern

Cause

By-design TSID behavior when TLS ClientHello does not contain SNI.

When TSID is enabled and SNI is missing, FMC determines the server identity using certificate attributes in this order:

1.- Common Name (CN)

2.- First Subject Alternative Name (SAN)

3.- Organizational Unit (OU)

Cisco Smart Licensing server certificates contain `toos.cisco.com` as the first SAN entry.
As a result, FMC reports `toos.cisco.com` even though:

- DNS resolution is correct
- The destination IP belongs to Cisco licensing infrastructure
- Traffic integrity is not affected

This impacts URL reporting and policy enforcement only.

Related Content

- TLS Server Identity Discovery