

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:

Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP...	Web Application	URL	Access Control Rule
2025-12-02 18:46:41	Connection	Allow	10.12.1.8	72.163.4.38	40722 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:39:59	Connection	Allow	10.12.1.8	173.37.145.8	46324 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:35:55	Connection	Allow	10.12.1.8	173.37.145.8	39783 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:35:23	Connection	Allow	10.12.1.8	173.37.145.8	57525 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 18:20:17	Connection	Allow	10.12.1.8	173.37.145.8	8399 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:56:43	Connection	Allow	10.12.1.8	72.163.4.38	21869 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:56:37	Connection	Allow	10.12.1.8	72.163.4.38	48047 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:55:31	Connection	Allow	10.12.1.8	72.163.4.38	19173 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:55:25	Connection	Allow	10.12.1.8	72.163.4.38	18982 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:53:15	Connection	Allow	10.12.1.8	173.37.145.8	24692 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:53:00	Connection	Allow	10.12.1.8	173.37.145.8	5625 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-02 17:35:38	Connection	Allow	10.12.1.8	173.37.145.8	26585 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_FMC_ASA_SNT_CISCO
2025-12-01 09:16:47	Connection	Allow	10.10.42.2	173.37.145.8	45203 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:36	Connection	Allow	10.10.42.2	72.163.4.38	51591 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:11	Connection	Allow	10.10.81.2	173.37.145.8	45544 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:16:01	Connection	Allow	10.10.81.2	72.163.4.38	24555 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:48	Connection	Allow	10.10.81.2	72.163.4.38	40655 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:18	Connection	Allow	10.10.81.2	72.163.4.38	54432 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:08	Connection	Allow	10.10.81.2	72.163.4.38	29189 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443
2025-12-01 09:15:08	Connection	Allow	10.10.42.2	72.163.4.38	32144 / tcp	443 (https) / tcp	Cisco	https://toos.cisco.com	ALLOW_ALL_CLIENTS_80_443

- 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

No.	Time	Source	Destination	Protocol	Length	Info
49	2025-12-13 08:05:48.113824	72.163.4.38	10.12.1.8	TCP	1414	443 → 24100 [PSH, ACK] Seq=2801 Ack=250 Win=16176 Len=1348 TSval=2005971
50	2025-12-13 08:05:48.113839	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=250 Ack=4149 Win=32768 Len=0 TSval=3277437881 TSec
51	2025-12-13 08:05:48.113839	72.163.4.38	10.12.1.8	TCP	118	443 → 24100 [PSH, ACK] Seq=4149 Ack=250 Win=16176 Len=52 TSval=200597126
52	2025-12-13 08:05:48.113870	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=250 Ack=4201 Win=32768 Len=0 TSval=3277437881 TSec
53	2025-12-13 08:05:48.114297	72.163.4.38	10.12.1.8	TLSv1.2	1170	Certificate, Server Key Exchange, Server Hello Done
54	2025-12-13 08:05:48.114846	10.12.1.8	72.163.4.38	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
55	2025-12-13 08:05:48.162039	72.163.4.38	10.12.1.8	TLSv1.2	72	Change Cipher Spec
56	2025-12-13 08:05:48.162131	10.12.1.8	72.163.4.38	TCP	66	24100 → 443 [ACK] Seq=343 Ack=5311 Win=32768 Len=0 TSval=3277437929 TSec

```

Extension (id-ce=subjectAltName)
  Extension Id: 2.5.29.17 (id-ce=subjectAltName)
  GeneralNames: 7 items
    GeneralName: dNSName (2)
      dNSName: toos.cisco.com
      GeneralName: dNSName (2)
        dNSName: tools.cisco.com
        GeneralName: dNSName (2)
          dNSName: tools1.cisco.com
          GeneralName: dNSName (2)
            dNSName: tools2.cisco.com
            GeneralName: dNSName (2)
              dNSName: tools3.cisco.com
              GeneralName: dNSName (2)
                dNSName: tools1-ss2.cisco.com
                GeneralName: dNSName (2)
                  dNSName: tools2-ss1.cisco.com
    Extension (id-ce=subjectKeyIdentifier)
    Extension (id-ce=extKeyUsage)
    Extension (SignedCertificateTimestampList)
  algorithmIdentifier (sha256WithRSAEncryption)
  Padding: 0
  encrypted [...]: 76cf52f15d1a06b20821ea0536ad2c5fab7f6e
  Certificate Length: 1754
  
```

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](#)