

TSIDが有効な場合、FMCはCisco Smart Licensingトラフィックをtools.cisco.comとして報告します

内容

お問い合わせ内容

Firepower Management Center(FMC)およびFirepower Threat Defense(FTD)では、Cisco Smart Licensing HTTPSトラフィックが、tools.cisco.comではなくtoos.cisco.comとして報告されます。これにより、シスコデバイスライセンスのトラフィック (ASA、ルータ、スイッチ) がURLベースまたはセキュリティインテリジェンスポリシーによってブロックされ、ライセンスの期限切れが発生する可能性があります。

トラフィック自体は正規のものであり、シスコのライセンスインフラストラクチャ宛てです。

環境

- 製品ファミリ: Cisco Secure Firewall
- トラフィックタイプ: Cisco Smart Licensing (HTTPS/TCP 443)
- TLSサーバーID (TSID)機能が有効になりました

解決策

症状

- FMC接続イベントまたはFTDシステムサポートのトレースは次のように表示されます。

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	21809 / 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

- スマートライセンスコマンド(`license smart renew auth`など)が失敗します。
- `toos.cisco.com`をブロックするURLフィルタリング/セキュリティインテリジェンスポリシー
- パケットキャプチャにより、トラフィックがシスコのライセンスIP(`tools1.cisco.com`など)に送信されていることを確認します。
- TSIDを無効にすると、FMCによって`tools.cisco.com`が報告されます。

トラブルシューティング/調査手順

スマートライセンストラフィックの確認

Ciscoデバイス (例 : ASA) で、次の手順を実行します。

```
license smart renew auth
```

シスコデバイスでのトラフィックのキャプチャ (ASAの例)

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

キャプチャをエクスポートし、宛先IPがシスコライセンスホストに解決されることを確認します。

tools1.cisco.com

FTDでのトラフィックのキャプチャまたはトレース

パケットキャプチャ(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
```

システムサポートトレース

```
system support trace
```

次のようなログエントリを探します。

[url toos.cisco.com](https://tools.cisco.com)

FMCでのTSID設定の確認

- アクセスコントロールポリシーに移動
- 該当するルールの編集
- 詳細設定の確認
- TLSサーバーID検出(TSID)が有効になっていることを確認します

TSIDへの影響の検証 (オプションのテスト)

- ルールのTSIDを無効にする
- ポリシーの展開
- ライセンスの再実行

注 : TSIDが無効になっている場合、予期される動作 : FMCはtools.cisco.comを報告します

サーバ証明書の検査 (オプション)

パケットキャプチャまたはブラウザツールで、次の点を確認します。

- SANリストの最初のエントリーはtoos.cisco.comです

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 08:05:48.162839	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)	03b0 0f 74 6f 6f 6c 73 2e 63 69 73 63 6f 2e 63 6f 6d	tools.cisco.com
Extension Id: 2.5.29.17 (id-ce-subjectAltName)	03c0 82 10 74 6f 6f 6c 73 31 2e 63 69 73 63 6f 2e 63	tools1.cisco.com
GeneralNames: 7 items	03d0 6f 6d 82 10 74 6f 6f 6c 73 32 2e 63 69 73 63 6f	tools2.cisco.com
GeneralName: dNSName (2)	03e0 2e 63 6f 6d 82 10 74 6f 6f 6c 73 33 2e 63 69 73	tools3.cisco.com
dNSName: toos.cisco.com	03f0 63 6f 2e 63 6f 6d 82 14 74 6f 6f 6c 73 31 2d 73	tools1-s2.cisco.com
dNSName: dNSName (2)	0400 73 32 2e 63 69 73 63 6f 2e 63 6f 6d 82 14 74 6f	tools2-ss1.cisco.com
dNSName: tools1.cisco.com	0410 6f 6c 73 32 2d 73 73 31 2e 63 69 73 63 6f 2e 63	tools3.cisco.com
dNSName: tools2.cisco.com	0420 6f 6d 30 1d 06 03 55 1d 0e 04 16 04 14 04 31 2f	tools4.cisco.com
dNSName: tools3.cisco.com	0430 6a ec 1e 3e ae 89 c8 99 62 6e 6a ae 73 34 fa 76	tools5.cisco.com
dNSName: tools1-ss2.cisco.com	0440 e2 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06	tools6.cisco.com
dNSName: tools2-ss1.cisco.com	0450 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02	tools7.cisco.com
dNSName: tools3-ss1.cisco.com	0460 30 82 01 80 06 0a 2b 06 01 04 01 d6 79 02 04 02	tools8.cisco.com
dNSName: tools4-ss1.cisco.com	0470 04 82 01 70 04 82 01 6c 01 6a 00 77 00 d7 6d 7d	tools9.cisco.com
dNSName: tools5-ss1.cisco.com	0480 10 d1 a7 f5 77 c2 c7 e9 5f d7 00 bf f9 82 c9 33	tools10.cisco.com
dNSName: tools6-ss1.cisco.com	0490 5a 65 e1 d0 b3 01 73 17 c0 c8 c5 69 77 00 00 01	tools11.cisco.com
dNSName: tools7-ss1.cisco.com	04a0 99 51 49 fb a5 00 00 04 03 00 48 30 46 02 21 00	tools12.cisco.com
dNSName: tools8-ss1.cisco.com	04b0 0e 9a cb d6 61 9e 56 68 ef 11 e2 1d 09 41 b4 14	tools13.cisco.com
dNSName: tools9-ss1.cisco.com	04c0 bb 5e 90 34 7b ad 8e 83 cd 76 d3 6b 30 40 61 c2	tools14.cisco.com
dNSName: tools10-ss1.cisco.com	04d0 02 21 00 c3 d6 d1 3b 23 f5 69 d7 a3 7e 8c e2 29	tools15.cisco.com

解決策/推奨処置

不具合はありません。行動は意図的なものです。次のオプションのいずれかを指定します。

- 1.- URLフィルタリング/セキュリティインテリジェンスポリシーでtoos.cisco.comを許可
- 2.- URLカテゴリまたはより広範なドメインパターンでCisco Smart Licensingトラフィックを許可します。

原因

TLS ClientHelloにSNIが含まれていない場合のTSIDの動作の設計

TSIDが有効でSNIが見つからない場合、FMCは証明書属性を次の順序で使用してサーバIDを決定します。

1. – 共通名(CN)
- 2.- First Subject Alternative Name(SAN)
3. – 組織単位(OU)

Cisco Smart Licensingサーバの証明書には、最初のSANエントリとしてtoos.cisco.comが含まれています。

その結果、次の場合でも、FMCはtoos.cisco.comを報告します。

- DNS解決が正しい
- 宛先IPはシスコライセンスインフラストラクチャに属します
- トラフィックの整合性は影響を受けない

これは、URLレポーティングとポリシー適用にのみ影響します。

関連コンテンツ

- [TLSサーバIDの検出](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。