# TSIDが有効な場合、FMCはCisco Smart Licensingトラフィックをtoos.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。

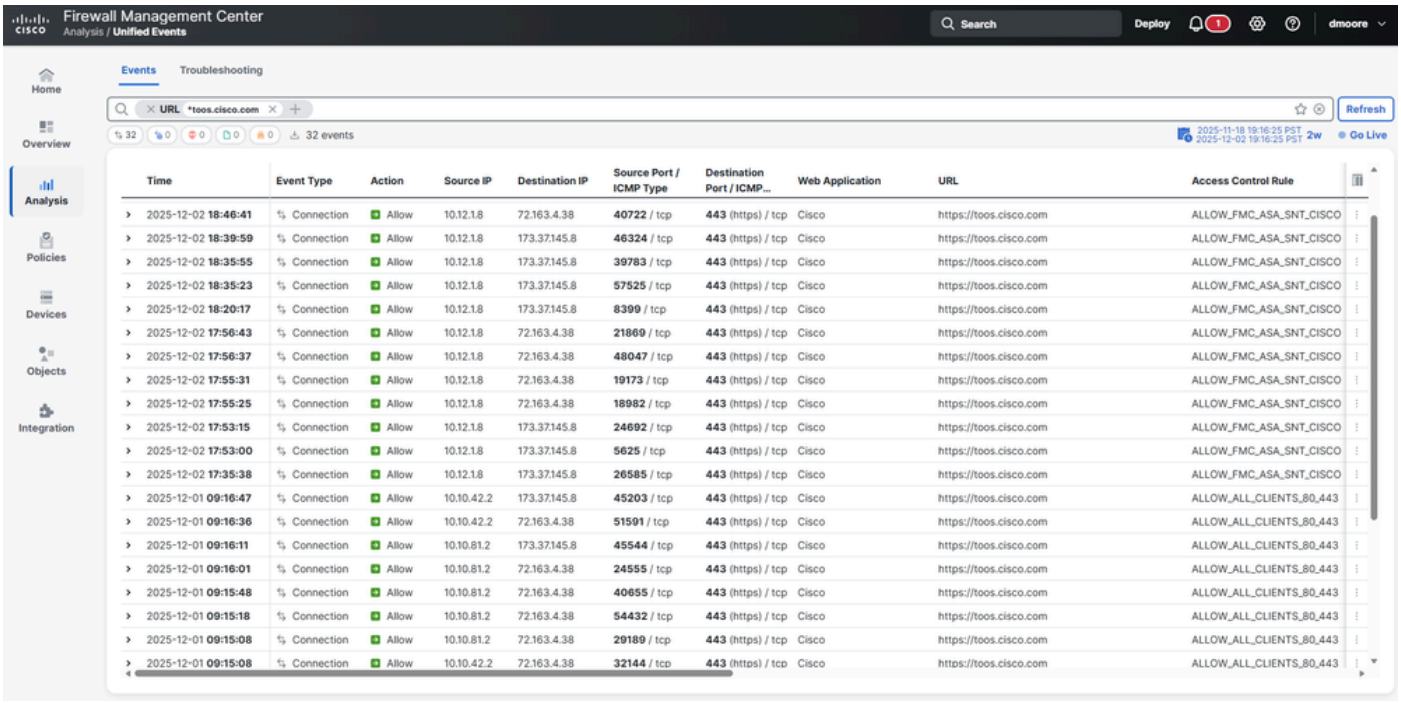
## 環境

- 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。




- 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
```

## 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）

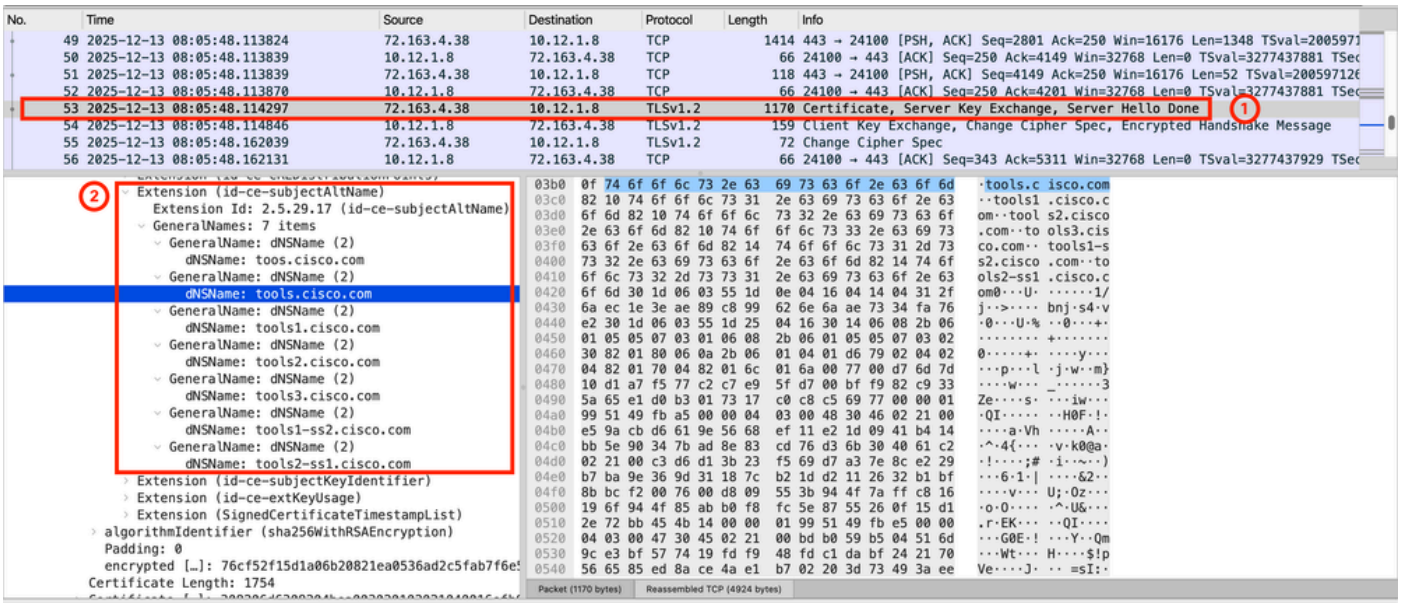
- ルールのTSIDを無効にする
- ポリシーの展開
- ライセンスの再実行

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は`toos.cisco.com`です



## 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。