启用TSID时，FMC将思科智能许可流量报告为toos.cisco.com

目录

问题

Firepower管理中心(FMC)和Firepower威胁防御(FTD)将思科智能许可HTTPS流量报告为`toos.cisco.com`，而不是`tools.cisco.com`。
这会导致思科设备许可流量（ASA、路由器、交换机）被基于URL的策略或安全情报策略阻止，可能导致许可证过期。

流量本身是合法的，并且发往思科许可基础设施。

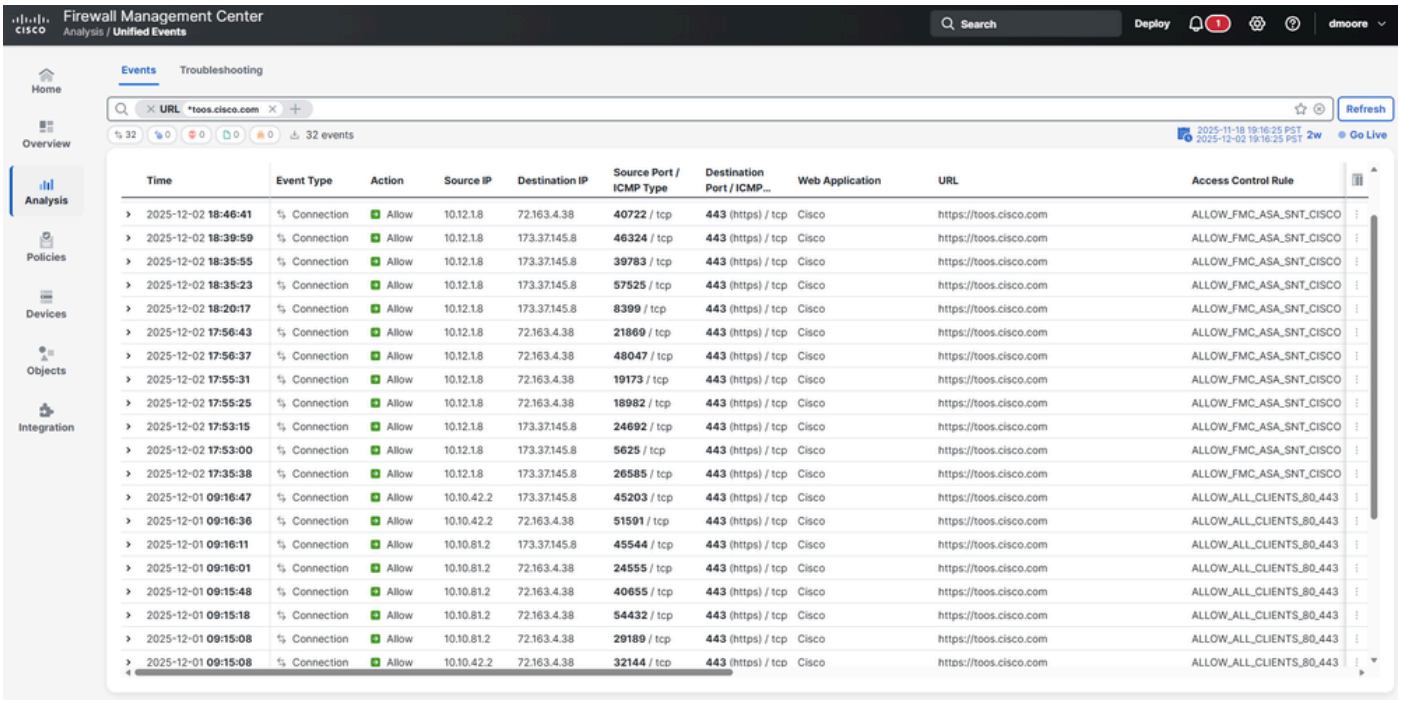
环境

- 产品系列：思科安全防火墙
- 流量类型:思科智能许可(HTTPS/TCP 443)
- 已启用TLS服务器标识(TSID)功能

分辨率

症状

- FMC连接事件或FTD系统支持跟踪显示：



- 智能许可命令(例如，`license smart renew auth`)失败。
- URL过滤/安全情报策略阻止`toos.cisco.com`。
- 数据包捕获确认流量已发送到思科许可IP(如`tools1.cisco.com`)。
- 禁用TSID会导致FMC报告`tools.cisco.com`。

故障排除/调查步骤

确认智能许可流量

在Cisco设备上(例如：ASA):

```
license smart renew auth
```

捕获思科设备上的流量（ASA示例）

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

导出捕获并确认目标IP解析到思科许可主机：

```
tools1.cisco.com
```

在FTD上捕获或跟踪流量

数据包捕获(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
```

系统支持跟踪

```
system support trace
```

查找类似于以下内容的日志条目：

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

验证FMC中的TSID配置

- 导航到“访问控制策略”
- 编辑适用的规则
- 检查高级设置
- 确认已启用TLS服务器身份发现(TSID)

验证TSID影响（可选测试）

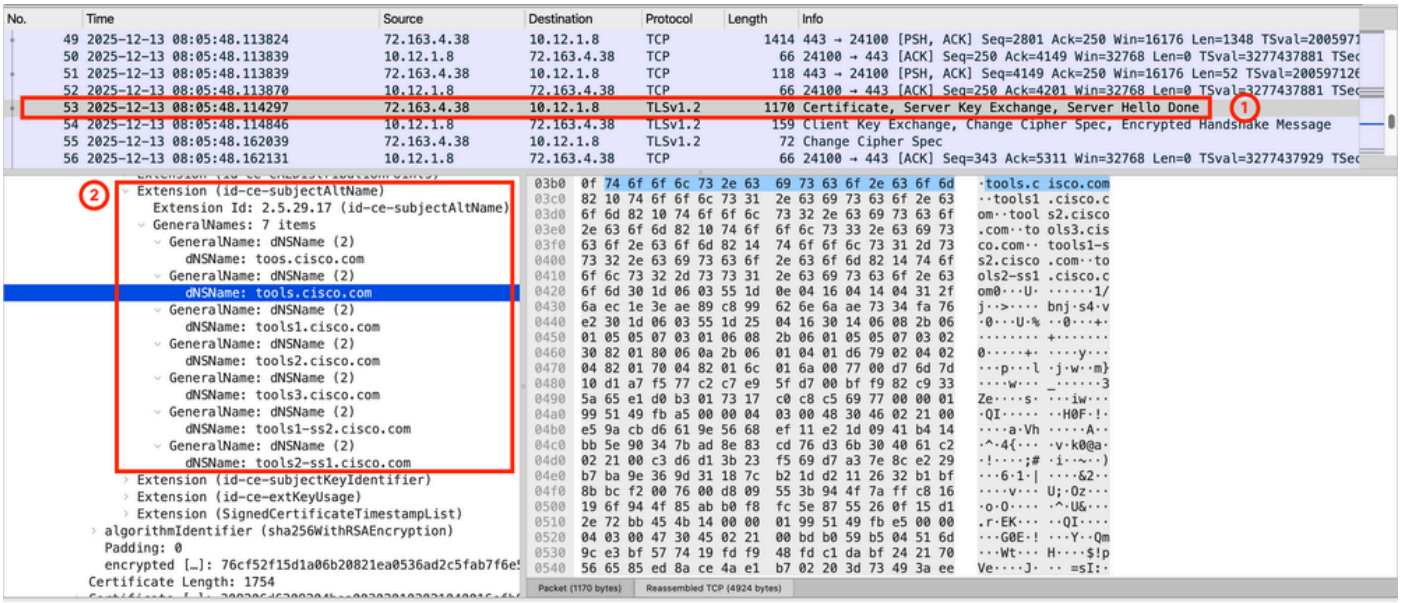
- 在规则上禁用TSID
- 部署策略
- 重新运行许可尝试

注意 — 预期行为：禁用TSID时，FMC报告`tools.cisco.com`

检查服务器证书（可选）

从数据包捕获或浏览器工具中确认：

- SAN列表将`toos.cisco.com`作为第一个条目



解决方案/推荐处理

没有缺陷。行为是由设计决定的。建议以下选项之一：

1. — 在URL过滤/安全情报策略中允许`toos.cisco.com`

2. — 通过以下方式允许思科智能许可流量：URL类别或更广泛的域模式

原因

当TLS ClientHello不包含SNI时的按设计TSID行为。

启用TSID且缺少SNI时，FMC使用证书属性按以下顺序确定服务器身份：

1. — 公用名称(CN)

2. — 第一个主题备用名称(SAN)

3.组织单位

思科智能许可服务器证书包含`tоos.cisco.com`作为第一个SAN条目。
因此，FMC报告`tоos.cisco.com`，即使：

- DNS解析正确
- 目标IP属于思科许可基础设施
- 流量完整性不受影响

这只会影响URL报告和策略实施。

相关内容

- TLS服务器身份发现

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。