FMC informa del tráfico de Cisco Smart Licensing como toos.cisco.com cuando TSID está habilitado

Contenido

Problema

Firepower Management Center (FMC) y Firepower Threat Defense (FTD) informan del tráfico HTTPS de Cisco Smart Licensing como `tools.cisco.com` en lugar de `tools.cisco.com`.
Esto hace que el tráfico de licencias de dispositivos de Cisco (ASA, routers, switches) se bloquee por políticas de inteligencia de seguridad o basadas en URL, lo que puede provocar el vencimiento de la licencia.

El tráfico en sí es legítimo y está destinado a la infraestructura de licencias de Cisco.

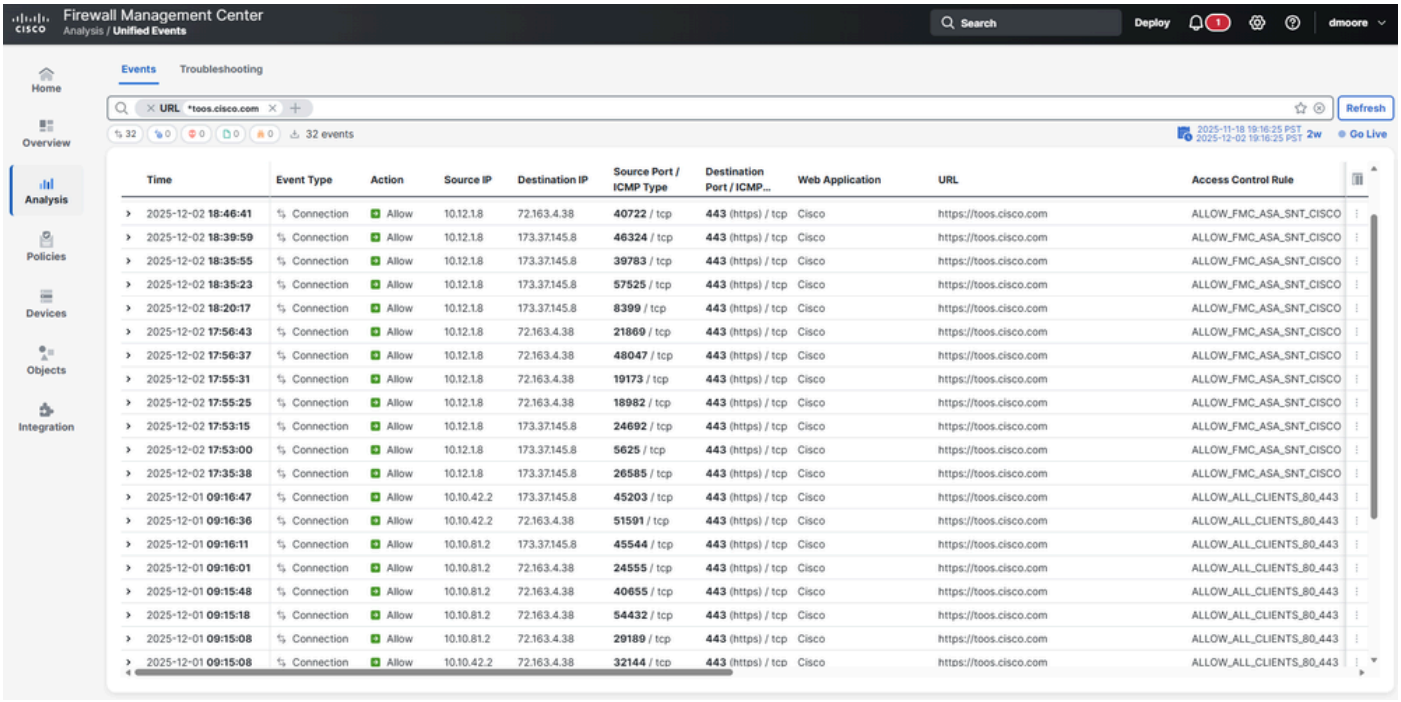
Entorno

- Familia de productos: Firewall seguro de Cisco
- Tipo de tráfico: Cisco Smart Licensing (HTTPS/TCP 443)
- Función TLS Server Identity (TSID) activada

Resolución

Síntomas

- Los eventos de conexión FMC o el seguimiento de compatibilidad del sistema FTD muestran:



- Los comandos de Smart Licensing (por ejemplo, `license smart renew auth`) fallan.
- Filtrado de URL / Políticas de inteligencia de seguridad que bloquean `toos.cisco.com`.
- La captura de paquetes confirma que el tráfico se envía a las IP de licencias de Cisco (como `tools1.cisco.com`).
- La desactivación de TSID hace que FMC informe a `tools.cisco.com`.

Pasos de Troubleshooting/Investigación

Confirmar tráfico de licencias inteligentes

En el dispositivo Cisco (ejemplo: ASA):

```
license smart renew auth
```

Capturar tráfico en el dispositivo de Cisco (ejemplo de ASA)

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

Exporte la captura y confirme las resoluciones IP de destino a los hosts de licencias de Cisco:

```
tools1.cisco.com
```

Captura o seguimiento del tráfico en FTD

Captura de paquetes (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
```

Seguimiento de compatibilidad del sistema

```
system support trace
```

Busque entradas de registro similares a:

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

Verificar la configuración de TSID en FMC

- Vaya a Política de control de acceso

- Editar la regla aplicable
- Comprobar configuración avanzada
- Confirmar que TLS Server Identity Discovery (TSID) está habilitado

Validar el impacto de TSID (prueba opcional)

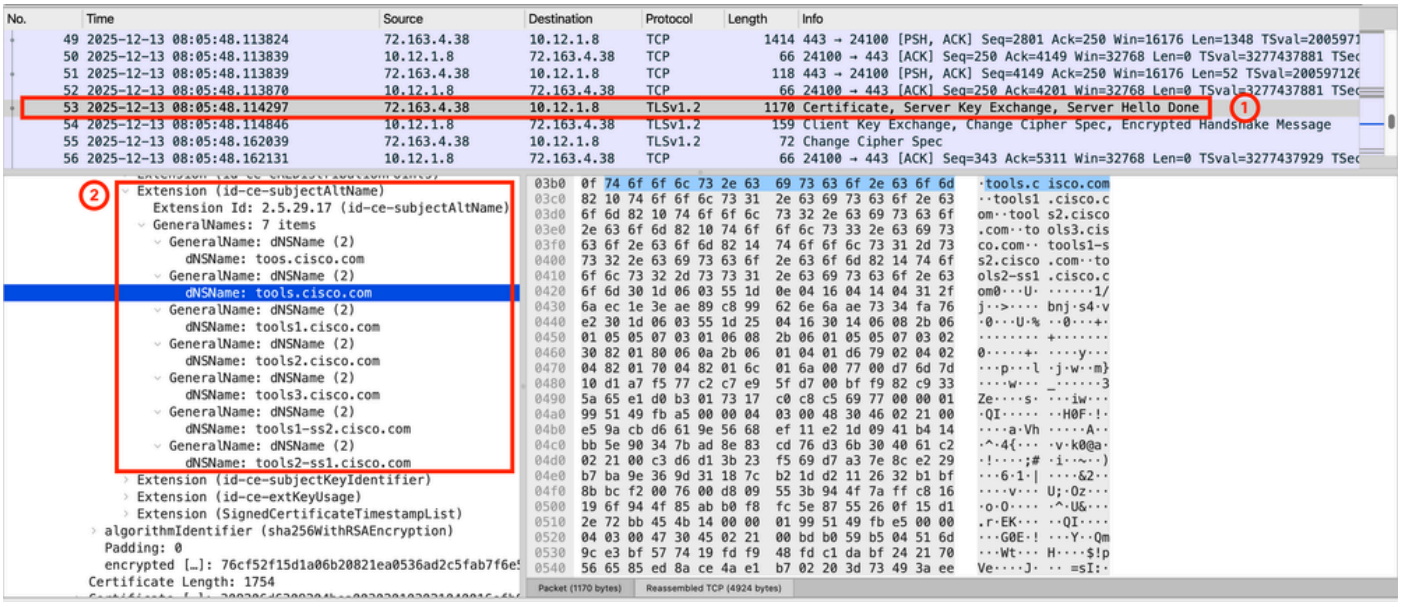
- Deshabilitar TSID en la regla
- Implementar la política
- Volver a ejecutar intento de licencia

Nota: comportamiento esperado: FMC informa de `tools.cisco.com` cuando TSID está desactivado

Inspeccionar certificado de servidor (opcional)

Confirme lo siguiente en las herramientas de captura de paquetes o del navegador:

- La lista de SAN incluye `tools.cisco.com` como la primera entrada



Resolución / Manejo recomendado

Ningún defecto. El comportamiento es por diseño. Aconseje una de estas opciones:

1.- Permitir a `toos.cisco.com` en filtrado de URL / políticas de inteligencia de seguridad

2.- Permitir el tráfico de Cisco Smart Licensing mediante: Categoría de URL o patrón de dominio más amplio

Causa

Comportamiento TSID del diseño secundario cuando TLS ClientHello no contiene SNI.

Cuando TSID está habilitado y falta SNI, FMC determina la identidad del servidor mediante los atributos de certificado en este orden:

1.- Denominación común (NC)

2.- Nombre alternativo del primer sujeto (SAN)

3.- Unidad Organizativa (UO)

Los certificados de servidor de Cisco Smart Licensing contienen `toos.cisco.com` como la primera entrada de SAN.
Como resultado, FMC informa a `toos.cisco.com` aunque:

- La resolución de DNS es correcta
- La IP de destino pertenece a la infraestructura de licencias de Cisco
- La integridad del tráfico no se ve afectada

Esto afecta únicamente a los informes de URL y a la aplicación de políticas.

Contenido relacionado

- Detección de identidad del servidor TLS

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).