O FMC relata o tráfego do Cisco Smart Licensing como toos.cisco.com quando o TSID está habilitado

Contents

Problema

O Firepower Management Center (FMC) e o Firepower Threat Defense (FTD) relatam o tráfego HTTPS do Cisco Smart Licensing como `toos.cisco.com` em vez de `tools.cisco.com`.
Isso faz com que o tráfego de licenciamento de dispositivos da Cisco (ASA, roteadores, switches) seja bloqueado por políticas baseadas em URL ou de inteligência de segurança, resultando potencialmente na expiração da licença.

O tráfego em si é legítimo e destinado à infraestrutura de licenciamento da Cisco.

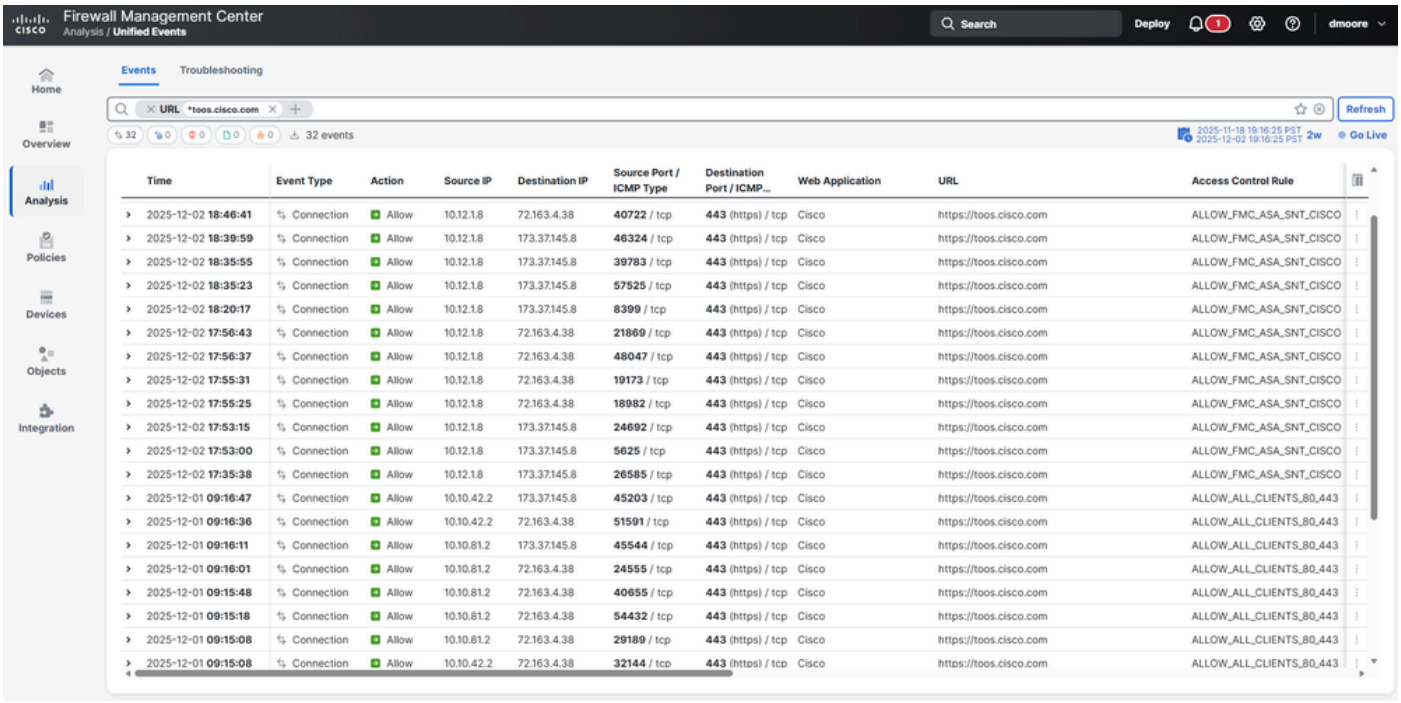
Ambiente

- Linha de produtos: Firewall seguro da Cisco
- Tipo de tráfego: Cisco Smart Licensing (HTTPS/TCP 443)
- Recurso TSID (Identidade do servidor TLS) habilitado

Resolução

Sintomas

- Os eventos de conexão do FMC ou o rastreamento de suporte do sistema FTD mostram:



- Os comandos do Smart Licensing (por exemplo, `license smart renew auth`) falham.
- Filtragem de URL/políticas de inteligência de segurança bloqueando `toos.cisco.com`.
- A captura de pacotes confirma que o tráfego é enviado para os IPs de licenciamento da Cisco (como `tools1.cisco.com`).
- Desabilitar o TSID faz com que o FMC relate `tools.cisco.com`.

Etapas de solução de problemas/investigação

Confirmar tráfego de Smart Licensing

No dispositivo Cisco (exemplo: ASA):

```
license smart renew auth
```

Capturar o tráfego no dispositivo Cisco (exemplo do ASA)

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

Exportar a captura e confirmar IP de destino resolve para hosts de licenciamento da Cisco:

```
tools1.cisco.com
```

Capturar ou Rastrear Tráfego no FTD

Captura de pacotes (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
```

Rastreamento de suporte do sistema

```
system support trace
```

Procure entradas de log semelhantes a:

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

Verificar a configuração do TSID no FMC

- Navegue até Access Control Policy (Política de controle de acesso)

- Editar a regra aplicável
- Verificar configurações avançadas
- Confirmar se a TSID (Descoberta de Identidade de Servidor TLS) está habilitada

Validar o impacto do TSID (teste opcional)

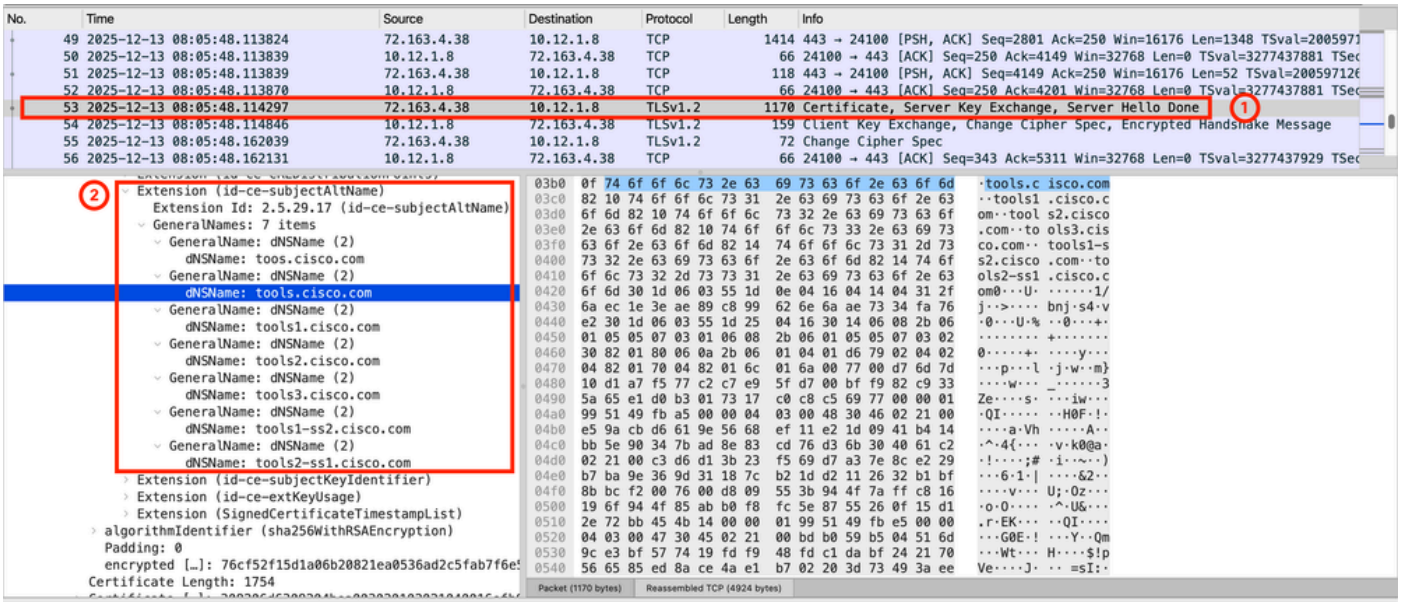
- Desativar TSID na regra
- Implantar política
- Nova tentativa de licenciamento

Observação - comportamento esperado: O FMC informa `tools.cisco.com` quando o TSID está desabilitado

Inspecionar certificado do servidor (opcional)

Nas ferramentas de captura de pacotes ou do navegador, confirme:

- A lista de SAN inclui `toos.cisco.com` como a primeira entrada



Resolução / Manuseio recomendado

Sem defeito. O comportamento é por design. Aconselhe uma destas opções:

1.- Permitir `toos.cisco.com` em políticas de filtragem de URL / Inteligência de segurança

2.- Permita o tráfego do Cisco Smart Licensing: Categoria de URL ou padrão de domínio mais amplo

Causa

Comportamento TSID subestimado quando o TLS ClientHello não contém SNI.

Quando o TSID está habilitado e a SNI está ausente, o FMC determina a identidade do servidor usando atributos de certificado nesta ordem:

1.- Denominação comum (NC)

2.- Nome Alternativo da Entidade (SAN)

3.- Unidade Organizacional (UO)

Os certificados de servidor do Cisco Smart Licensing contêm `toos.cisco.com` como a primeira entrada de SAN.
Como resultado, o FMC informa o `toos.cisco.com` mesmo que:

- A resolução DNS está correta
- O IP de destino pertence à infraestrutura de licenciamento da Cisco
- A integridade do tráfego não é afetada

Isso afeta apenas a emissão de relatórios de URL e a aplicação de políticas.

Conteúdo relacionado

- Descoberta de identidade do servidor TLS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.