

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:

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 17:55:21	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 17:53:00	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

- 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](https://tools.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

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.c
GeneralNames: 7 items	03d0 6f 6d 82 10 74 6f 6f 6c 73 32 2e 63 69 73 63 6f	om..tool s2.cisco
GeneralName: dNSName (2)	03e0 2e 63 6f 6d 82 10 74 6f 6f 6c 73 33 2e 63 69 73	.com..to ols3.cis
dNSName: toos.cisco.com	03f0 63 6f 2e 63 6f 6d 82 14 74 6f 6f 6c 73 31 2d 73	co.com.. tools1-s
GeneralName: dNSName (2)	0400 73 32 2e 63 69 73 63 6f 2e 63 6f 6d 82 14 74 6f	s2.cisco .com..to
dNSName: tools.cisco.com	0410 6f 6c 73 32 2d 73 73 31 2e 63 69 73 63 6f 2e 63	ols2-ss1 .cisco.c
GeneralName: dNSName (2)	0420 6f 6d 30 1d 06 03 55 1d 0e 04 16 04 14 04 31 2f	om0...U... ..1/
GeneralName: dNSName (2)	0430 6a ec 1e 3e ae 89 c8 99 62 6e 6a ae 73 34 fa 76	j...>... bnj-s4-v
GeneralName: dNSName (2)	0440 e2 30 1d 06 03 55 1d 25 04 16 30 14 06 08 2b 06	.0...U-% .0...+
GeneralName: dNSName (2)	0450 01 05 05 07 03 01 06 08 2b 06 01 05 05 07 03 02+.....
GeneralName: dNSName (2)	0460 30 82 01 80 06 0a 2b 06 01 04 01 d6 79 02 04 02	0.....+.....y...
GeneralName: dNSName (2)	0470 04 82 01 70 04 82 01 6c 01 6a 00 77 00 d7 6d 7d	...p...l j.w.m}
GeneralName: dNSName (2)	0480 10 d1 a7 f5 77 c2 c7 e9 5f d7 00 bf f9 82 c9 33	...w... ..3
GeneralName: dNSName (2)	0490 5a 65 e1 d0 b3 01 73 17 c0 c8 c5 69 77 00 00 01	Ze...s...iw...0
GeneralName: dNSName (2)	04a0 99 51 49 fb a5 00 00 04 03 00 48 30 46 02 21 00	..QI... ..H0F..
GeneralName: dNSName (2)	04b0 e5 9a cb d6 61 9e 56 68 ef 11 e2 1d 09 41 b4 14	...a.Vh... ..A
GeneralName: dNSName (2)	04c0 bb 5e 90 34 7b ad 8e 83 cd 76 d3 6b 30 40 61 c2	^4{... v.k0@a
GeneralName: dNSName (2)	04d0 02 21 00 c3 d6 d1 3b 23 f5 69 d7 a3 7e 8c e2 29	!...;# i... ..)
GeneralName: dNSName (2)	04e0 b7 ba 9e 36 9d 31 18 7c b2 1d d2 11 26 32 b1 bf	..6-1 i... ..62..
Extension (id-ce-subjectKeyIdentifier)	04f0 8b bc f2 00 76 00 d8 09 55 3b 94 4f 7a ff c8 16	..U;..Oz... ..
Extension (id-ce-extKeyUsage)	0500 19 6f 94 4f 85 ab b0 f8 fc 5e 87 55 26 0f 15 d1	..o0... ..U;... ..
Extension (SignedCertificateTimestampList)	0510 2e 72 bb 45 4b 14 00 00 01 99 51 49 fb e5 00 00	..rEK... ..QI... ..
algorithmIdentifier (sha256WithRSAEncryption)	0520 04 03 00 47 30 45 02 21 00 bd b0 59 b5 04 51 6d	...G0E!... ..Y..Qm
padding: 0	0530 9c e3 bf 57 74 19 fd f9 48 fd c1 da bf 24 21 70	...Wt... ..H... ..\$p
encrypted [...]: 76cf52f15d1a06b20821ea0536ad2c5fab7f6e	0540 56 65 85 ed 8a ce 4a e1 b7 02 20 3d 73 49 3a ee	Ve... ..J... ..=sI:..

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.