FMC segnala il traffico di Cisco Smart Licensing come toos.cisco.com quando TSID è abilitato

Sommario

Problema

Firepower Management Center (FMC) e Firepower Threat Defense (FTD) segnalano il traffico HTTPS di Cisco Smart Licensing come `tos.cisco.com` anziché `tools.cisco.com`.
In questo modo, il traffico delle licenze dei dispositivi Cisco (ASA, router, switch) viene bloccato da policy basate su URL o Security Intelligence, con la possibilità di una scadenza della licenza.

Il traffico è in sé legittimo e destinato all'infrastruttura di licenze Cisco.

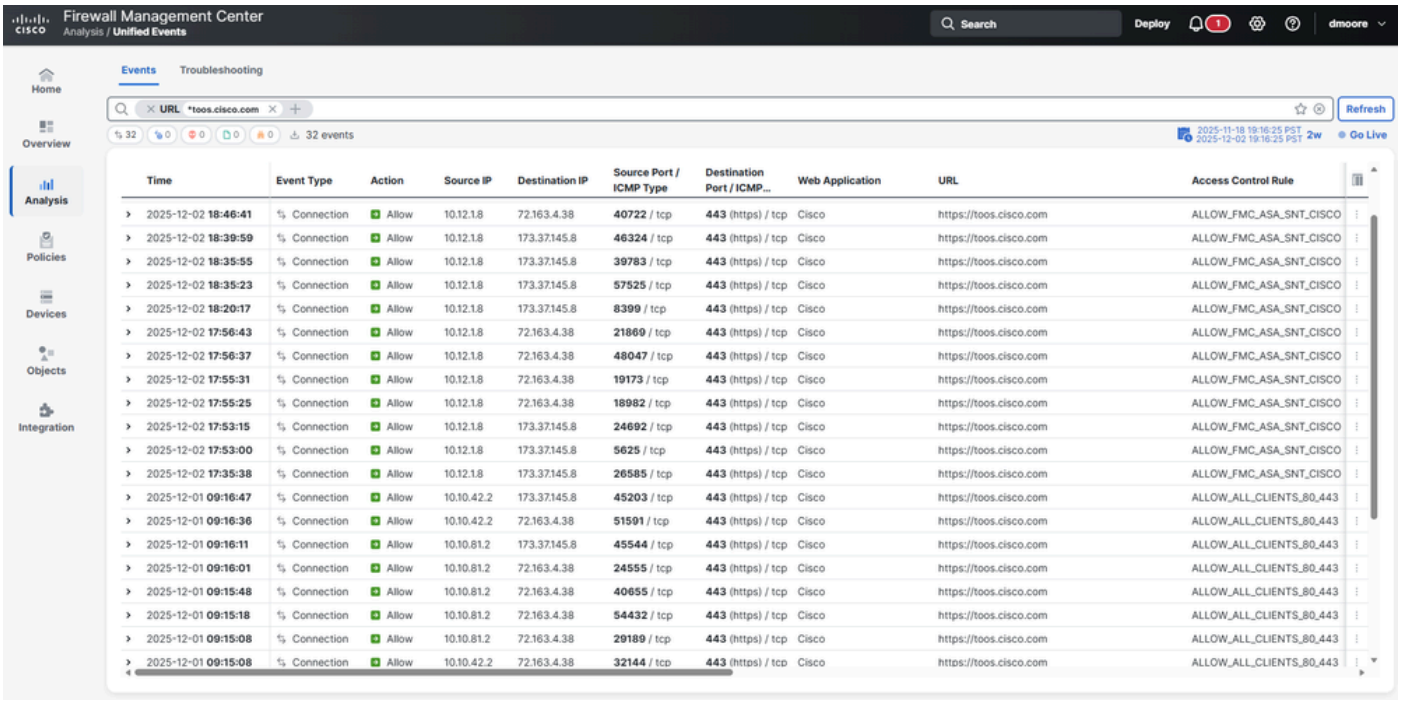
Ambiente

- Famiglia di prodotti: Cisco Secure Firewall
- Tipo di traffico: Cisco Smart Licensing (HTTPS / TCP 443)
- Caratteristica Identità server TLS (TSID) abilitata

Risoluzione

Sintomi

- Gli eventi di connessione FMC o la traccia di supporto del sistema FTD mostrano:



- I comandi di Smart Licensing (ad esempio, `license smart renew auth`) hanno esito negativo.
- Filtro URL / Policy di Security Intelligence che bloccano `tos.cisco.com`.
- L'acquisizione dei pacchetti conferma l'invio del traffico agli IP di licenza Cisco (come `tools1.cisco.com`).
- La disattivazione di TSID determina la segnalazione da parte di FMC di `tools.cisco.com`.

Procedura di risoluzione dei problemi/indagine

Conferma traffico di Smart Licensing

Sul dispositivo Cisco (esempio: ASA)

```
license smart renew auth
```

Acquisire il traffico sul dispositivo Cisco (esempio ASA)

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

Esportare le risoluzioni IP di acquisizione e conferma sugli host di licenza Cisco:

```
tools1.cisco.com
```

Acquisisci o traccia traffico su FTD

Packet Capture (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
```

Traccia supporto di sistema

```
system support trace
```

Cerca voci di registro simili a:

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

Verifica configurazione TSID in FMC

- Passa a Criteri di controllo di accesso
- Modifica la regola applicabile
- Controlla impostazioni avanzate

- Conferma l'abilitazione di TLS Server Identity Discovery (TSID)

Convalida impatto TSID (test facoltativo)

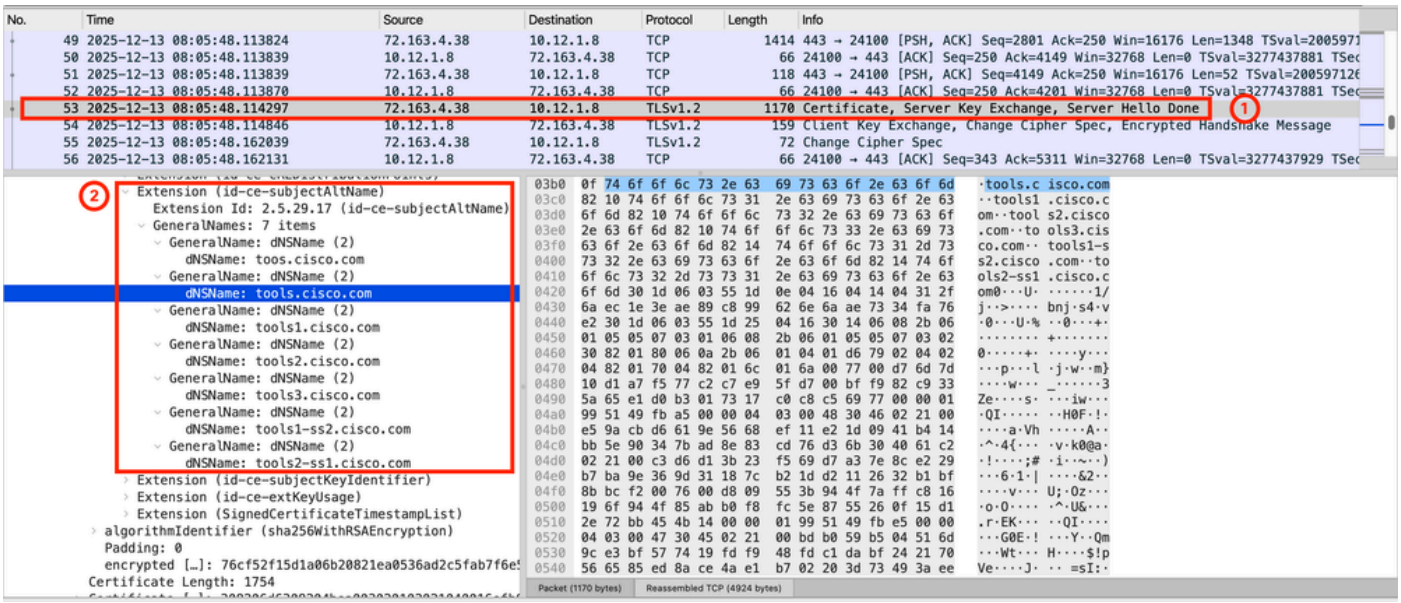
- Disabilita TSID nella regola
- Distribuisci criteri
- Riesegui tentativo di gestione licenze

Nota - Comportamento previsto: FMC segnala `tools.cisco.com` quando TSID è disabilitato

Controlla certificato server (facoltativo)

Dagli strumenti di acquisizione pacchetti o del browser, confermare:

- L'elenco delle SAN include `tos.cisco.com` come prima voce



Risoluzione / Manipolazione consigliata

Nessun difetto. Il comportamento è di progettazione. Consigliare una delle seguenti opzioni:

1.- Consenti a `tos.cisco.com` di applicare il filtro URL/le policy di Security Intelligence

2.- Autorizzare il traffico di Cisco Smart Licensing nei seguenti modi: Categoria URL o modello di dominio più ampio

Causa

Comportamento TSID non progettato quando TLS ClientHello non contiene SNI.

Quando TSID è attivato e SNI è mancante, FMC determina l'identità del server utilizzando gli attributi del certificato nell'ordine seguente:

1.- Denominazione comune (NC)

2.- Nome alternativo del primo soggetto (SAN)

3.- Unità organizzativa

I certificati del server Cisco Smart Licensing contengono `tos.cisco.com` come prima voce SAN. Di conseguenza, FMC riporta `tos.cisco.com` anche se:

- Risoluzione DNS corretta
- L'IP di destinazione appartiene all'infrastruttura delle licenze Cisco
- L'integrità del traffico non è compromessa

Questo influisce solo sulla segnalazione degli URL e sull'applicazione delle policy.

Contenuto correlato

- Individuazione identità server TLS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).