Risolvere i problemi relativi alle perdite di pacchetti FTD (tcp-not-syn) quando "Enhanced application and URL Detection" È abilitato sulle interfacce inline con flusso di traffico asimmetrico

Sommario

Problema

Gli accessori Firewall Threat Defense (FTD) configurati con insiemi di interfacce inline eliminano il traffico di ritorno TCP con il motivo di rilascio ASP (Accelerated Security Path) tcp-not-syn. Questo si verifica immediatamente dopo l'attivazione della funzionalità TLS Server Identity Discovery (TSID), in particolare l'opzione "Enhanced application and URL Detection" (Rilevamento avanzato applicazione e URL). Nelle versioni precedenti di Firewall Management Center (FMC), l'opzione è denominata "Early application detection and URL categorization" (Rilevamento rapido applicazioni e classificazione URL). I pacchetti TCP SYN-ACK sul percorso di ritorno vengono scartati dallo stesso dispositivo FTD che ha inoltrato la SYN originale, impedendo la creazione di sessioni TCP.

Il problema si manifesta come errori diffusi di connettività TCP e non è limitato al traffico TLS. Questi sintomi vengono osservati quando la funzione è attivata:

- I pacchetti TCP SYN-ACK sul percorso di ritorno vengono scartati con il motivo di rilascio ASP tcp-not-syn.
- Le nuove sessioni TCP non vengono visualizzate nella tabella di connessione FTD.
- I contatori di rilascio ASP alti si accumulano rapidamente, come illustrato da questo output, acquisito circa 10 minuti dopo l'attivazione della funzionalità:

<#root>

```
device#

show asp drop


Frame drop:
 Flow is denied by configured rule (acl-drop)                                  1
```

```
First TCP packet not SYN (tcp-not-syn)                                  34802

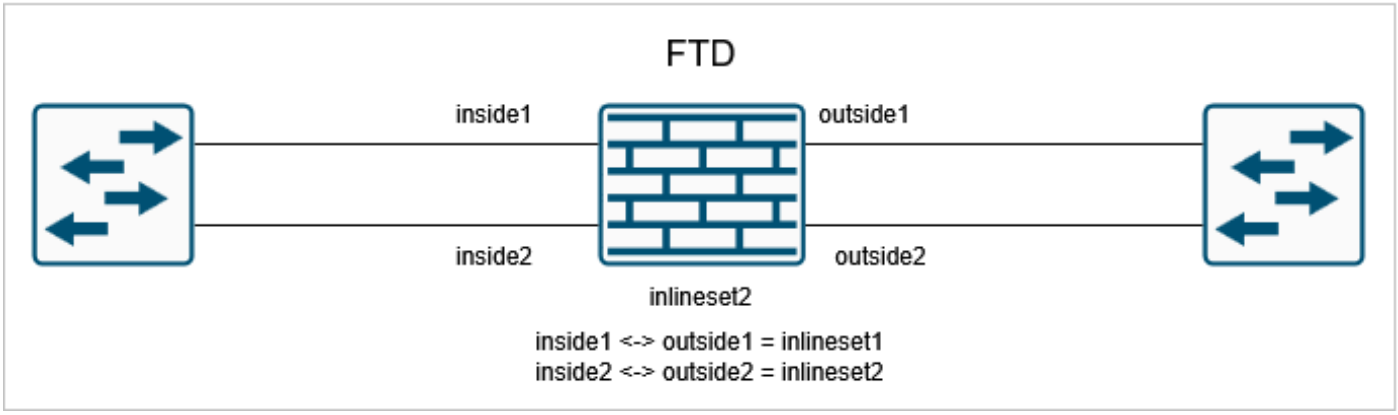
TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
Dropped pending packets in a closed socket (np-socket-closed)               3
TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               1
TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)               1
Blocked or blacklisted by the reputation preprocessor (reputation)          1

Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

Ambiente

- Piattaforma: Cisco Firepower 4115.0 Il problema può riguardare anche altre piattaforme.
- Versione software FTD: 7.6.4. Possono essere interessate anche altre versioni del software.
- Versione software FMC: 10.1.0. Possono essere interessate anche altre versioni software.
- FTD con insiemi di interfacce inline.
- FTD ha almeno due coppie di interfacce inline: inlineset1 e inlineset2 (oppure esistono due FTD diversi con un inline-set ciascuno).
- Flusso di traffico asimmetrico presente nell'ambiente: Il protocollo TCP SYN inizia tramite l'interfaccia outside1, mentre il corrispondente TCP SYN-ACK ritorna tramite l'interfaccia outside2 sullo stesso dispositivo FTD.
- La funzione TSID è abilitata su FTD.

Topologia



Risoluzione

La risoluzione consigliata per arrestare le eliminazioni tcp-not-syn e ripristinare la connettività TCP tramite le interfacce FTD in linea è disabilitare l'opzione "Rilevamento avanzato di applicazioni e URL" all'interno di TSID. In questo modo, TCP State Bypass rimane attivo sui set di interfacce inline, condizione necessaria per supportare flussi di traffico asimmetrici nell'ambiente.

Disattivare "Rilevamento avanzato applicazioni e URL" in FMC

Accedere a: Policy > Controllo accesso > [Criteri di controllo accesso] > Avanzate > Rilevamento identità server TLS. Deselezionare o disabilitare la casella di controllo "Rilevamento avanzato applicazioni e URL", quindi distribuire il criterio ai dispositivi FTD interessati.

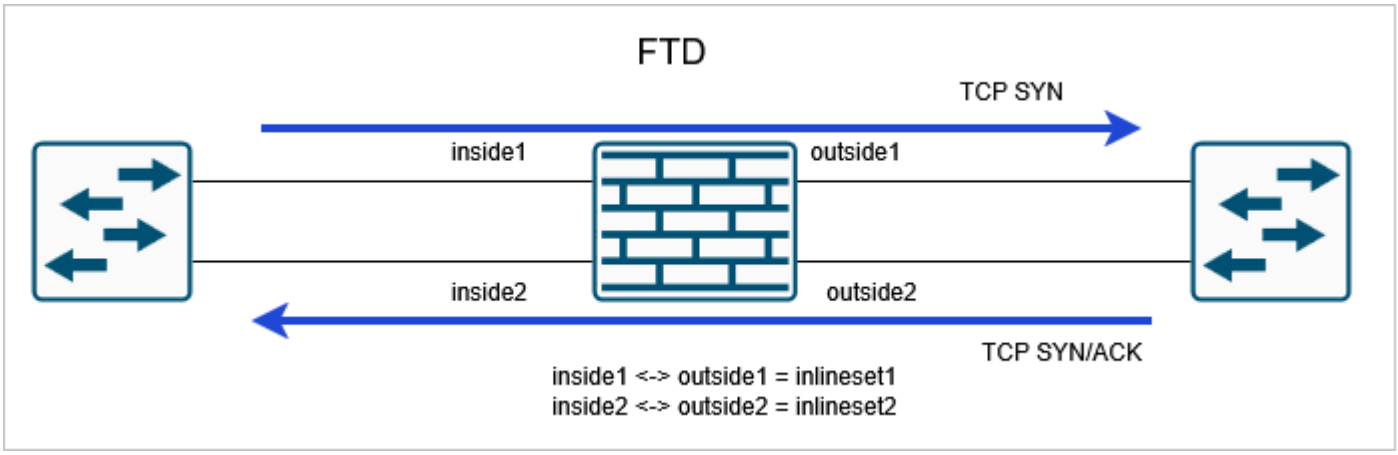
Dopo aver disattivato la funzione, le nuove sessioni vengono visualizzate nella tabella delle connessioni, a conferma che le connessioni TCP stanno completando correttamente l'handshake a tre vie.

Nota: Se TSID è disattivato, l'FTD non può più visualizzare il certificato del server nelle sessioni TLS 1.3. Le regole dell'applicazione e dell'URL associano il traffico in modo meno accurato sul traffico crittografato.

Causa

La causa principale dei cali tcp-not-syn è un'incompatibilità tra la funzionalità TLS Server Identity Discovery e TCP State Bypass sugli insiemi di interfacce inline in FTD.

per impostazione predefinita, per il traffico che passa attraverso le interfacce inline su FTD, è abilitato il bypass dello stato TCP. TCP State Bypass è progettato per consentire il traffico asimmetrico, in cui i percorsi di inoltro e di ritorno di una connessione TCP possono attraversare diverse interfacce o persino diversi dispositivi, di passare senza che l'FTD richieda una rigida tracciatura dello stato TCP. Questo è un comportamento necessario negli ambienti in cui è presente asimmetria di routing:

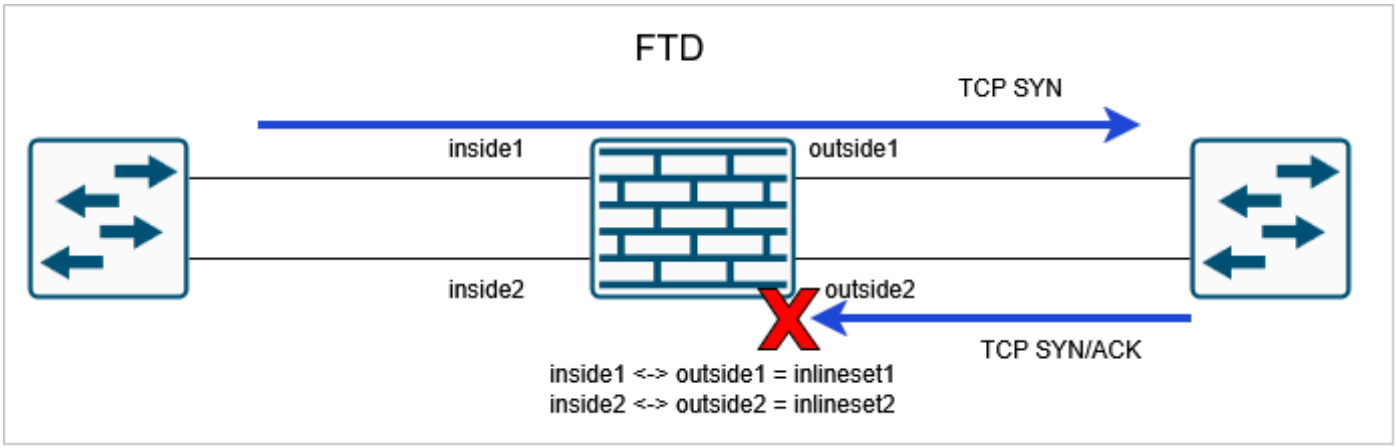


Flusso TCP asimmetrico attraverso set inline FTD quando TSID è disabilitato.

Tuttavia, quando una di queste funzioni è abilitata, il sistema FTD ignora il Bypass dello stato TCP e inizia a eseguire controlli completi sullo stato TCP sul traffico dell'interfaccia in linea:

- L'opzione "Rilevamento URL e applicazione migliorato" in Rilevamento identità server TLS.
- Qualsiasi criterio di decrittografia TLS/SSL attivo.

Una volta applicati i controlli dello stato TCP, l'FTD tiene traccia dell'intera sequenza di handshake TCP. Negli ambienti con routing asimmetrico - dove, ad esempio, il pacchetto TCP SYN esce tramite l'interfaccia external1 ma il corrispondente TCP SYN-ACK restituisce i dati tramite l'interfaccia esterna sullo stesso dispositivo - l'FTD non riconosce il SYN-ACK come appartenente a una sessione TCP nota e tracciata. Poiché il SYN-ACK arriva su un'interfaccia diversa da quella prevista e non è stato visto alcun SYN corrispondente su quell'interfaccia, il FTD lo classifica come un pacchetto non SYN per una connessione sconosciuta e lo scarta con il motivo di rilascio ASP tcp-not-syn.



Flusso TCP asimmetrico attraverso set inline FTD quando TSID è abilitato.

Contenuto correlato

- Cisco Bug ID CSCwp84746 — Documentazione: Incompatibilità di TLS Server Identity Discovery con TCP State Bypass su interfacce inline-set
- Cisco ID bug CSCwx42897 — DOC: TLS Server Identity Discovery esegue l'override del bypass dello stato TCP sulle interfacce inline-set, causando l'eliminazione del traffico TCP (tcp-not-syn)
- Cisco Bug ID CSCwx42901 — Quando si abilita "Early Application Detection and URL categorization" (TSID), viene aggiunto un avviso in cui si avvisa che disabilita TCP State Bypass sulle interfacce inline-set
- Documentazione di Cisco — Linee guida per il bypass dello stato TCP (include la restrizione TLS Server Identity Discovery)
- Caso di studio: traffico asimmetrico attraverso set inline
- Nota tecnica Cisco - Come generare FTD e FMC per risolvere i problemi dei bundle
- Supporto tecnico Cisco e download

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).