# FirePOWER Management Center visualizza alcuni eventi di connessione TCP nella direzione sbagliata

## Sommario



## Introduzione

In questo documento vengono descritti i motivi e le misure di attenuazione per la visualizzazione da parte di FirePOWER Management Center (FMC) degli eventi di connessione TCP nella direzione inversa, dove Initiator IP è l'IP server della connessione TCP e Responder IP è l'IP client della connessione TCP.

> **Nota:** Il verificarsi di tali eventi è dovuto a più motivi. Questo documento spiega la causa più comune di questo sintomo.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Tecnologia FirePOWER
- Conoscenze base di Adaptive Security Appliance (ASA)
- Informazioni sul meccanismo di temporizzazione TCP (Transmission Control Protocol)

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA Firepower Threat Defense (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 6.0.1 e successive

- ASA Firepower Threat Defense (5512-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X,FP9300,FP4100) con software versione 6.0.1 e successive
- ASA con moduli Firepower (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X,5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) con software versioni 6.0.0 e successive
- Firepower Management Center (FMC) versione 6.0.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Sfondo

In una connessione TCP, il termine **client** si riferisce all'indirizzo IP che invia il pacchetto iniziale. FirePOWER Management Center genera un evento di connessione quando il dispositivo gestito (sensore o FTD) rileva il pacchetto TCP iniziale di una connessione.

Per i dispositivi che tengono traccia dello stato di una connessione TCP, viene definito un **timeout di inattività** per garantire che le connessioni che per errore non vengono chiuse dagli endpoint non utilizzino la memoria disponibile per lunghi periodi di tempo. Il timeout di inattività predefinito per le connessioni TCP stabilite su FirePOWER è di **tre minuti**. Una connessione TCP rimasta inattiva per tre o più minuti non viene rilevata dal sensore FirePOWER IPS.

Il pacchetto successivo dopo il timeout viene considerato come un nuovo flusso TCP e la decisione di inoltro viene presa in base alla regola che corrisponde a questo pacchetto. Quando il pacchetto proviene dal server, l'IP del server viene registrato come iniziatore di questo nuovo flusso. Quando la registrazione è abilitata per la regola, viene generato un evento di connessione in FirePOWER Management Center.

> **Nota:** In base alle policy configurate, la decisione di inoltro per il pacchetto che arriva dopo il timeout è diversa dalla decisione per il pacchetto TCP iniziale. Se l'azione predefinita configurata è "Blocca", il pacchetto viene scartato.

Un esempio di questo sintomo è dato dallo screenshot seguente:

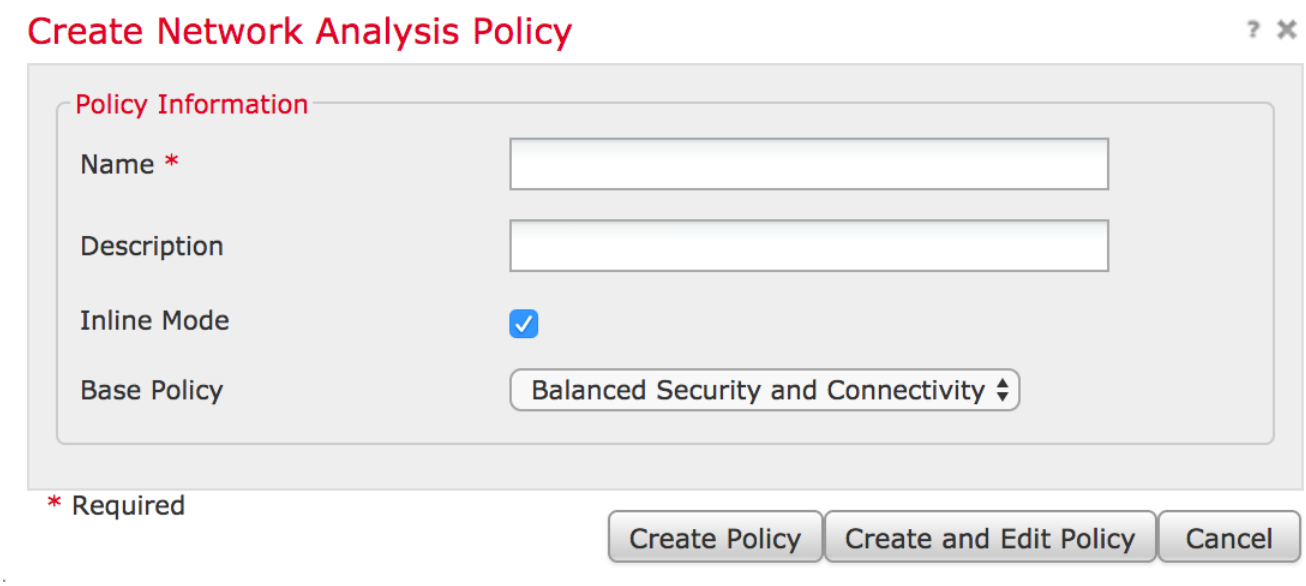
| First Packet | Last Packet | Action | Reason | Initiator IP | Initiator Country | Responder IP | Responder Country | Ingress Security Zone | Egress Security Zone | Source Port / ICMP Type | Destination Port / ICMP Code |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2017-05-12 17:48:05 | | Block | | 10.32.38.30 | | 192.168.38.30 | | | | 443 (https) / tcp | 44705 / tcp |
| 2017-05-12 17:39:13 | | Allow | | 192.168.38.30 | | 10.32.38.30 | | | | 44705 / tcp | 443 (https) / tcp |

# Soluzione

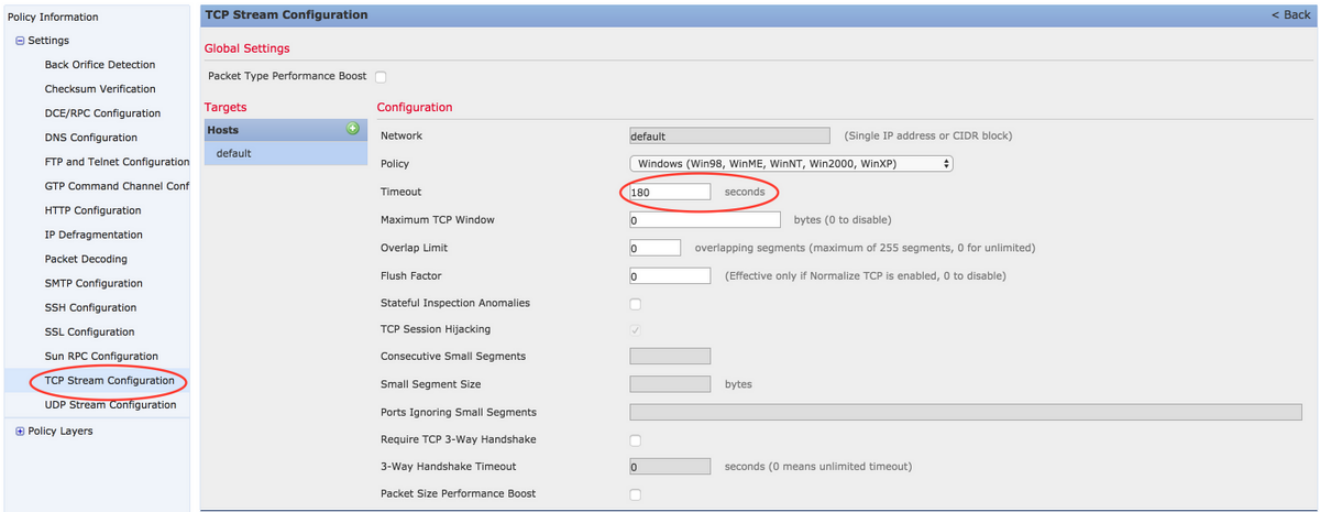
Per risolvere questo problema, aumentare il **timeout** delle connessioni TCP. Per modificare il timeout,

1. Selezionare **Policy > Controllo accesso > Intrusione**.
2. Passare all'angolo superiore destro e selezionare **Criteri di accesso alla rete**.


3. Selezionare **Crea criterio**, scegliere un nome e fare clic su **Crea e modifica criterio**. Non modificare i **criteri di base.**

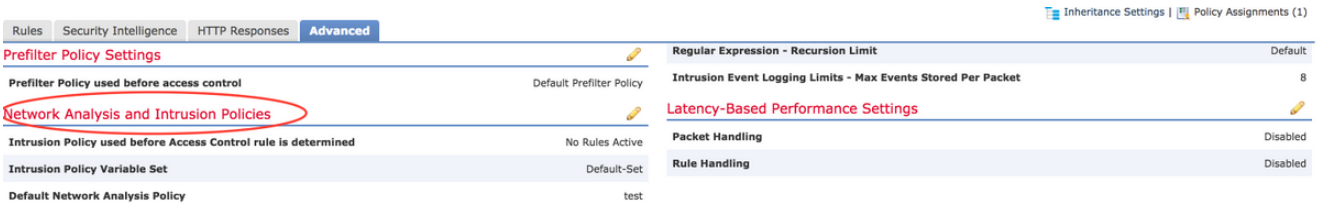



4. Espandere l'opzione **Settings** (Impostazioni) e scegliere **TCP Stream Configuration** (Configurazione flusso TCP).
5. Passare alla sezione di configurazione e modificare il valore di **Timeout** come desiderato.




6. Passare a **Policy > Controllo accesso > Controllo accesso**.
7. Selezionare l'opzione **Edit** (Modifica) per modificare il criterio applicato al dispositivo gestito pertinente o creare un nuovo criterio.


8. Selezionare la scheda **Avanzate** nel criterio di accesso.
9. Individuare la sezione **Analisi di rete e criteri intrusione** e fare clic sull'icona **Modifica**.




10. Dal menu a discesa di **Criterio di analisi della rete predefinito**, scegliere il criterio creato nel passaggio 2.
11. Fare clic su **OK** e **salvare** le modifiche.
12. Fare clic sull'opzione **Deploy** per distribuire i criteri ai dispositivi gestiti pertinenti.

**Attenzione:** L'aumento del timeout dovrebbe causare un maggiore utilizzo della memoria, FirePOWER deve tenere traccia dei flussi che non vengono chiusi dagli endpoint per un periodo di tempo più lungo. L'effettivo aumento nell'utilizzo della memoria è diverso per ogni singola rete in quanto dipende dalla durata dell'inattività delle connessioni TCP da parte delle applicazioni di rete.

## Conclusioni

I benchmark di ogni rete per il timeout di inattività delle connessioni TCP sono diversi. Dipende completamente dalle applicazioni in uso. È necessario stabilire un valore ottimale osservando per quanto tempo le applicazioni di rete mantengono inattive le connessioni TCP. Per i problemi relativi al modulo di servizio FirePOWER su un'appliance ASA Cisco, quando non è possibile dedurre un valore ottimale, il timeout può essere regolato aumentandolo a intervalli fino al valore di timeout dell'appliance ASA.

## Informazioni correlate

- Guida rapida di Cisco Firepower Threat Defense per l'appliance ASA
- Documentazione e supporto tecnico – Cisco Systems
- Guida rapida di ASA Firepower