

NetFlow e altre funzionalità non sono supportati a causa della verifica parziale del motore di linea se un FTD trasparente funziona come coppia inline

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema: NetFlow e altre funzioni non sono supportati a causa della verifica parziale del motore di linea se un FTD trasparente funziona come coppia inline.](#)

[Soluzione alternativa](#)

[Bug correlati](#)

Introduzione

Questo documento descrive e spiega perché NetFlow e altre funzionalità non funzionano in Firepower Threat Defense (FTD) in modalità trasparente con coppia inline e come risolvere il problema.

Contributo di Christian G. Hernandez R., Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di base di Cisco Firepower Management Center (FMC).
- Configurazione di base Cisco FTD.
- Configurazione della configurazione flessibile di Cisco FMC.

Componenti usati

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

- Cisco FMC v6.3.0
- Cisco FTD v6.3.0

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.

Problema: NetFlow e altre funzioni non sono supportati a causa della verifica parziale del motore di linea se un FTD trasparente funziona come coppia inline.

Una volta che NetFlow è stato configurato e distribuito sul sistema tramite Flex Config, NetFlow non genera flussi al collector (destinazione di esportazione del flusso) configurato.

flow-export destination Management 10.1.2.3 2055

```
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect rsh
  inspect sqlnet
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class-default
  flow-export event-type flow-create destination 10.1.2.3
  flow-export event-type flow-denied destination 10.1.2.3
  flow-export event-type flow-teardown destination 10.1.2.3
  flow-export event-type flow-update destination 10.1.2.3
!
```

service-policy global_policy global

Come indicato nella tabella seguente, questo comportamento è confermato nel FTD a causa dei limitati controlli del motore Lina per alcune funzionalità quando il sistema è impostato in modalità coppia inline. Vedere i dettagli seguenti:

Modalità interfaccia FTD	Modalità di distribuzione FTD	Descrizione	Il traffico può essere interrotto
Stesura	Stesura	Controlli completi dei motori LINA e Snort	Sì
Commutato	Trasparente	Controlli completi dei motori LINA e Snort	Sì
Coppia inline	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	Sì
Coppia inline con tap	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	No
Passivo	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	No

Passivo
(ERSPAN)

Stesura

Controlli parziali del motore LINA
e completi del motore Snort No

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html>

NetFlow è una funzionalità di cui è stato confermato che non è supportata quando il FTD funziona in modalità inline-pair.

Nota: Le funzionalità specifiche non supportate dal FTD, quando funziona in modalità coppia inline, sono sconosciute al momento. Per questo motivo, è stata aperta la richiesta di miglioramento per chiedere al team di progettazione di Cisco Firepower di confermare le funzionalità note non supportate in questa modalità: [CSCvo5596](#) DOC: Sezione di limitazione FMC in cui sono indicate le funzionalità supportate/non supportate quando FTD è impostato in linea.

Soluzione alternativa

Se la configurazione è quella specificata in questo documento e richiede NetFlow, l'unica soluzione nota è lasciare l'FTD in modalità trasparente e configurare invece le interfacce BVI (Bridge Virtual Interface). Questa soluzione si basa sull'interfaccia ENH aperta per includere la funzionalità NetFlow per le distribuzioni in modalità inline-pair:

[CSCvo5574](#) ENH: FTD non è in grado di raccogliere i dati netflow durante la configurazione in modalità coppia inline.

Bug correlati

[CSCvo5574](#) ENH: FTD non è in grado di raccogliere i dati netflow durante la configurazione in modalità coppia inline.

[CSCvo5585](#) DOC.: Sezione di limitazione FMC per il supporto netflow quando configurato in modalità inline-pair.

[CSCvo5596](#) DOC.: Sezione di limitazione FMC in cui sono indicate le funzionalità supportate/non supportate quando FTD è impostato in linea.