NetFlow et d'autres fonctionnalités ne sont pas prises en charge en raison d'une vérification partielle du moteur de liaison si un FTD transparent fonctionne comme une paire en ligne

Contenu

Introduction

Ce document décrit et aide à comprendre pourquoi NetFlow et d'autres fonctionnalités ne fonctionneront pas dans un pare-feu FTD (Firepower Threat Defense) en mode transparent avec une paire en ligne, et comment contourner ce problème.

Contribué par Christian G. Hernandez R., ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base de Cisco Firepower Management Center (FMC).
- Configuration de base de Cisco FTD.
- Configuration flexconfig de Cisco FMC.

Components Used

L'information fournie dans ce document est basée sur les versions logicielles et matérielles suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème : NetFlow et d'autres fonctionnalités ne sont pas prises en charge en raison d'une vérification partielle du moteur de liaison si un FTD transparent fonctionne comme une paire en ligne.

Une fois NetFlow configuré et déployé sur le système via Flex Config, NetFlow ne génère pas de flux vers le collecteur (destination d'exportation de flux) configuré.

```
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
```

Selon le tableau ci-dessous, ce comportement est confirmé comme attendu sur le FTD en raison de vérifications limitées du moteur Lina pour certaines fonctionnalités lorsque le système est configuré en mode de paire en ligne. Voir les détails ci-dessous :

Mode d'interface FTD	Mode de déploiement FTD	Description	Le trafic peut être abandonné
Routé	Routé	Contrôles complets du moteur LINA et du moteur Snort	Oui
Commuté	Transparence	Contrôles complets du moteur LINA et du moteur Snort	Oui
Paire en ligne	**Routé ou transparent**	**Contrôles partiels du moteur LINA et du moteur Snort complet**	**Oui**
Paire en ligne avec bouton	Routé ou transparent	Contrôles partiels du moteur LINA et du moteur Snort complet	Non
Passif	Routé ou	Contrôles partiels du moteur	Non

	transparent	LINA et du moteur Snort complet	
Passif (ERSPAN)	Routé	Contrôles partiels du moteur LINA et du moteur Snort complet	Non

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

NetFlow est une fonctionnalité qui a été confirmée comme non prise en charge lorsque le FTD fonctionne en mode de paire inline.

> **Note**: Les fonctionnalités spécifiques non prises en charge par le FTD, lorsqu'il fonctionne en mode de paire en ligne, sont inconnues pour le moment, pour cette raison, la demande d'amélioration a été ouverte pour demander à l'équipe d'ingénierie de Cisco Firepower d'aider à confirmer les fonctionnalités non prises en charge connues dans ce mode : CSCvo5596 DOC : Section relative à la limitation FMC indiquant quelles fonctionnalités sont prises en charge/non prises en charge lorsque FTD est en ligne.

Solution de contournement

Si votre configuration est telle que spécifiée dans ce document et nécessite NetFlow, la seule solution connue est de laisser le FTD en mode transparent et de configurer des interfaces BVI (Bridge Virtual Interface) à la place. Cette solution de contournement est basée sur l'ENH ouverte pour inclure la fonctionnalité NetFlow pour les déploiements en mode paire inline :

CSCvo55574 ENH : FTD n'a pas pu collecter les données netflow lors de leur configuration en mode de paire en ligne.

Bogues associés

CSCvo55574 ENH : FTD n'a pas pu collecter les données netflow lors de leur configuration en mode de paire en ligne.

CSCvo55585 DOC : Section de limitation FMC pour la prise en charge de netflow lorsqu'elle est configurée en mode de paire inline.

CSCvo55596 DOC : Section relative à la limitation FMC indiquant quelles fonctionnalités sont prises en charge/non prises en charge lorsque FTD est en ligne.