

O NetFlow e outros recursos não são suportados devido à verificação parcial do Mecanismo de Lina se um FTD transparente funciona como par em linha

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema: O NetFlow e outros recursos não são suportados devido à verificação parcial do Mecanismo de Lina se um FTD transparente funciona como par em linha.](#)

[Solução](#)

[Erros relacionados](#)

Introduction

Este documento descreve e ajuda a entender por que o NetFlow e outros recursos não funcionarão em um Firepower Threat Defense (FTD) no modo Transparente com par em linha e como contornar isso.

Contribuído por Christian G. Hernandez R., Engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração básica do Cisco Firepower Management Center (FMC).
- Configuração básica do Cisco FTD.
- Configuração do Cisco FMC flexconfig.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema: O NetFlow e outros recursos não são suportados devido à verificação parcial do Mecanismo de Lina se um FTD transparente funciona como par em linha.

Depois que o NetFlow é configurado e implantado no sistema por meio do Flex Config, o NetFlow não gera fluxos para o coletor (destino de exportação de fluxo) configurado.

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

De acordo com a tabela abaixo, esse comportamento é esperado no FTD devido a verificações limitadas do Lina Engine para determinados recursos quando o sistema é definido no modo de par em linha. Veja os detalhes abaixo:

modo de interface FTD	modo de Implantação FTD	Descrição	O tráfego pode ser descartado
Roteado	Roteado	Verificações completas do mecanismo LINA e do mecanismo Snort	Yes
Comutado	Transparente	Verificações completas do mecanismo LINA e do mecanismo Snort	Yes
Par em linha	Roteado ou Transparente	Verificações parciais do mecanismo LINA e do mecanismo Snort completo	Yes
Par em linha com torneira	Roteado ou Transparente	Verificações parciais do mecanismo LINA e do	No

Passivo	Roteado ou Transparente	mecanismo Snort completo Verificações parciais do mecanismo LINA e do mecanismo Snort completo	No
Passivo (ERSPAN)	Roteado	Verificações parciais do mecanismo LINA e do mecanismo Snort completo	No

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

O NetFlow é um recurso que foi confirmado como não suportado quando o FTD funciona no modo de par em linha.

Note: Os recursos específicos não suportados pelo FTD, quando ele funciona no modo de par em linha, são desconhecidos no momento. Por isso, a solicitação de aprimoramento foi aberta para solicitar à equipe de engenharia do Cisco Firepower ajuda a confirmar os recursos não suportados conhecidos neste modo: [CSCvo5596](#) DOC: Seção de limitação do FMC indicando quais recursos são suportados/não suportados quando o FTD está em linha definida.

Solução

Se sua configuração for especificada neste documento e exigir o NetFlow, a única solução conhecida é deixar o FTD no modo Transparente e configurar as interfaces BVI (Bridge Virtual Interface). Essa solução alternativa é baseada no ENH aberto para incluir a funcionalidade do recurso NetFlow para implantações de modo de par em linha:

[CSCvo5574](#) ENH: O FTD não consegue coletar dados do netflow enquanto está configurado no modo de par em linha.

Erros relacionados

[CSCvo5574](#) ENH: O FTD não consegue coletar dados do netflow enquanto está configurado no modo de par em linha.

[CSCvo55585](#) DOC: Seção de limitação de FMC para suporte a netflow quando configurado no modo de par em linha.

[CSCvo5596](#) DOC: Seção de limitação do FMC indicando quais recursos são suportados/não suportados quando o FTD está em linha definida.