Configurar e capturar pacotes incorporados no software

Contents

Introduction

Este documento descreve o recurso EPC (Embedded Packet Capture) no software Cisco IOS®.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS versão 12.4(20)T ou posterior
- Cisco IOS XE® versão 15.2(4)S - 3.7.0 ou posterior

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.

Informações de Apoio

Quando ativado, o roteador captura os pacotes enviados e recebidos. Os pacotes são armazenados em um buffer na DRAM e não persistem por meio de um recarregamento. Uma vez capturados, os dados podem ser examinados em uma exibição resumida ou detalhada no roteador.

Além disso, os dados podem ser exportados como um arquivo de captura de pacotes (PCAP) para permitir um exame mais aprofundado. A ferramenta é configurada no modo exec e é considerada uma ferramenta de assistência temporária. Como resultado, a configuração da ferramenta não é armazenada na configuração do roteador e não permanece no lugar após um recarregamento do sistema.

A ferramenta Packet Capture Config Generator and Analyzer está disponível para que os clientes da Cisco ajudem na configuração, captura e extração de capturas de pacotes.

Exemplo de configuração do Cisco IOS

Configuração básica do EPC

1. Defina um 'buffer de captura', que é um buffer temporário onde os pacotes capturados são armazenados.
2. Há várias opções que podem ser selecionadas quando o buffer é definido; como tamanho, tamanho máximo de pacote e circular/linear:

```
monitor capture buffer BUF size 2048 max-size 1518 linear
```

3. Um filtro é aplicável para limitar a captura ao tráfego desejado. Defina uma Access Control List (ACL) no modo de configuração e aplique o filtro ao buffer:

```
ip access-list extended BUF-FILTER
permit ip host 192.168.1.1 host 172.16.1.1
permit ip host 172.16.1.1 host 192.168.1.1

monitor capture buffer BUF filter access-list BUF-FILTER
```

4. Defina um ponto de captura que defina o local onde a captura ocorre.
5. O ponto de captura também define se a captura ocorre para IPv4 ou IPv6 e em que caminho de switching (processo versus cef):

```
monitor capture point ip cef POINT fastEthernet 0 both
```

6. Anexe o buffer ao ponto de captura:

```
monitor capture point associate POINT BUF
```

7. Inicie a captura:

```
monitor capture point start POINT
```

8. A captura está ativa agora. Permitir a coleta dos dados necessários.

9. Pare a captura:

```
monitor capture point stop POINT
```

10. Examine o buffer na unidade:

```
show monitor capture buffer BUF dump
```

Note: Esta saída mostra apenas o dump hexadecimal das capturas de pacotes. Para vê-los legíveis, há duas maneiras.Exporte o buffer do roteador para análise adicional:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```

O método anterior nem sempre é prático, pois exigia acesso T/FTP ao roteador. Nessas situações, faça uma cópia do hex dump e use qualquer conversor hex-pcap on-line para visualizar os arquivos.

11. Depois que os dados necessários tiverem sido coletados, exclua o 'ponto de captura' e o 'buffer de captura':

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

Informações adicionais sobre a configuração do Cisco IOS

- Em versões anteriores ao Cisco IOS® Release 15.0(1)M, o tamanho do buffer era limitado a 512K.
- Em versões anteriores ao Cisco IOS® Release 15.0(1)M, o tamanho do pacote capturado era limitado a 1024 bytes.
- O buffer de pacote é armazenado na DRAM e não persiste por meio de recarregamentos.
- A configuração de captura não é armazenada na NVRAM e não persiste por meio de recarregamentos.
- O ponto de captura pode ser definido para capturar no cef ou caminhos de switching de processo.
- O ponto de captura pode ser definido para capturar somente em uma interface ou globalmente.
- Quando o buffer de captura é exportado no formato PCAP, as informações de L2 (como o encapsulamento Ethernet) não são preservadas.
- Consulte Práticas recomendadas para comandos de pesquisa para obter mais informações sobre os comandos usados nesta seção.

Configuração básica de exportação de tráfego IP

A exportação de tráfego IP é um método diferente de exportar pacotes IP recebidos em várias interfaces WAN ou LAN simultâneas.

1. No modo de configuração, defina um perfil de exportação de tráfego IP.

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2. Configure o tráfego bidirecional no perfil.

```
Device(config-rite)# bidirectional
```
3. Saída

4. Especifique a interface para o tráfego exportado.

```
Device(config-if)# interface GigabitEthernet 0/1
```
5. Ative a exportação de tráfego IP na interface.

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```
6. Saída

7. Inicie a captura. A captura está ativa agora. Permitir a coleta dos dados necessários.

```
Device# traffic-export interface GigabitEthernet 0/1 start
```
8. Pare a captura.

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```
9. Exporte a captura para um servidor TFTP externo.

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```
10. Quando os dados necessários tiverem sido coletados, delete o perfil.

```
Device(config)# no ip traffic-export profile mypcap
```

Desvantagens de exportação de tráfego IP

A exportação de tráfego IP tem estas desvantagens em comparação com o método EPC:

- A interface onde o tráfego capturado é exportado deve ser uma interface ethernet.
- Sem suporte para IPv6.
- Nenhuma informação da camada 2, somente a camada 3 e superior.

Exemplo de configuração do Cisco IOS-XE

O recurso Embedded Packet Capture foi introduzido no Cisco IOS-XE® Release 3.7 - 15.2(4)S. A configuração da captura é diferente do Cisco IOS® porque adiciona mais recursos.

Configuração básica do EPC

1. Defina o local onde a captura ocorre:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```
2. Associe um filtro. O filtro é especificado em linha ou uma ACL ou um mapa de classe pode ser referenciado:

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

3. Inicie a captura:

```
monitor capture CAP start
```

4. A captura está ativa agora. Permita que ele colete os dados necessários.

5. Pare a captura:

```
monitor capture CAP stop
```

6. Examine a captura em uma exibição resumida:

```
show monitor capture CAP buffer brief
```

7. Examine a captura em uma exibição detalhada:

```
show monitor capture CAP buffer detailed
```

8. Além disso, exporte a captura no formato PCAP para análise adicional:

```
monitor capture CAP export tftp://10.0.0.1/CAP.pcap
```

9. Quando os dados necessários tiverem sido coletados, remova a captura:

```
no monitor capture CAP
```

Additional Information

- A captura é realizada em interfaces físicas, subinterfaces e interfaces de túnel.
- Filtros baseados em Network Based Application Recognition (NBAR) (que usam o comando **match protocol** no mapa de classes) não são suportados no momento.
- Consulte Práticas recomendadas para comandos de pesquisa para obter mais informações sobre os comandos usados nesta seção.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Para o EPC executado no Cisco IOS-XE®, este comando debug é usado para garantir que o EPC seja configurado corretamente:

```
debug epc provision
```

```
debug epc capture-point
```

Informações Relacionadas

- Captura de pacotes incorporada - Cisco IOS-XE
- Captura de pacotes incorporada - Cisco IOS
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.