在软件上配置并捕获嵌入式数据包

目录

简介

本文档介绍Cisco IOS®软件中的嵌入式数据包捕获(EPC)功能。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS版本12.4(20)T或更高版本
- Cisco IOS XE®版本15.2(4)S - 3.7.0或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

启用时，路由器会捕获发送和接收的数据包。数据包存储在DRAM中的缓冲区中，不会持续到重新加载过程。捕获数据后，可以在路由器的摘要视图或详细视图中查看数据。

此外，数据可以导出为数据包捕获(PCAP)文件以供进一步检查。该工具是在执行模式下配置的，被视为临时助理工具。因此，该工具配置不存储在路由器配置中，并且在系统重新加载后不会保持不变。

Packet Capture Config Generator and Analyzer工具可供思科客户用于帮助配置、捕获和提取数据包捕获。

Cisco IOS配置示例

基本EPC配置

1. 定义“捕获缓冲区”，它是存储捕获数据包的临时缓冲区。
2. 定义缓冲区时，可以选择各种选项；例如大小、最大数据包大小和循环/线性：

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

3. 过滤器适用于将捕获限制为所需流量。在配置模式下定义访问控制列表(ACL)并将过滤器应用到缓冲区：

```
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. 定义一个捕获点，用于定义发生捕获的位置。
5. 捕获点还定义捕获是IPv4还是IPv6以及交换路径（进程与cef）：

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

6. 将缓冲区附加到捕获点：

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

7. 开始捕获：

```
monitor capture point start POINT
```

8. 捕获现在处于活动状态。允许收集必要数据。

9. 停止捕获：

```
monitor capture point stop POINT
```

10. 检查设备上的缓冲区：

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

注意：此输出仅显示数据包捕获的十六进制转储。为了便于阅读，有两种方法。从路由器导出缓冲区以进行进一步分析：

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

前面的方法并不总是实用，因为它需要通过T/FTP访问路由器。在这种情况下，请制作十六进制转储的副本，并使用任何在线十六进制转换器来查看文件。

11. 收集完必要的数据后，删除“捕获点”和“捕获缓冲区”：

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

其他Cisco IOS配置信息

- 在早于Cisco IOS®版本15.0(1)M的版本中，缓冲区大小限制为512K。
- 在早于Cisco IOS®版本15.0(1)M的版本中，捕获的数据包大小限制为1024字节。
- 数据包缓冲区存储在DRAM中，在重新加载过程中不会持续存在。
- 捕获配置不存储在NVRAM中，并且在重新加载过程中不会持续下去。
- 可以定义捕获点以在cef或进程交换路径中捕获。
- 捕获点可以定义为仅在接口上或全局进行捕获。
- 以PCAP格式导出捕获缓冲区时，不会保留L2信息（例如以太网封装）。
- 有关本节中使用的命令的详细信息，请参阅搜索命令的最佳实践。

基本IP流量导出配置

IP Traffic Export是导出多个并发WAN或LAN接口上接收的IP数据包的另一种方法。

1.在配置模式下定义IP流量导出配置文件。

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

2.在配置文件中配置双向流量。

```
Device(config-rite)# bidirectional
```

3.退出

4.指定导出流量的接口。

```
Device(config-if)# interface GigabitEthernet 0/1
```

5.在接口上启用IP流量导出。

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

6.退出

7.开始捕获。捕获现在处于活动状态。允许收集必要数据。

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8.停止捕获。

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9.将捕获导出到外部TFTP服务器。

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10.收集必要数据后，删除配置文件。

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

IP流量导出的缺点

与EPC方法相比，IP流量导出具有以下缺点：

- 导出捕获流量的接口必须是以太网接口。
- 不支持IPv6。
- 没有第2层信息，只有第3层及更高层。

Cisco IOS-XE配置示例

嵌入式数据包捕获功能是在Cisco IOS-XE®版本3.7 - 15.2(4)S中引入的。捕获的配置与Cisco IOS®不同，因为它添加了更多功能。

基本EPC配置

1. 定义捕获发生的位置：

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```

2. 关联过滤器。过滤器是内联指定的，或者可以引用ACL或类映射：

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

3. 开始捕获：

```
monitor capture CAP start
```

4. 捕获现在处于活动状态。允许它收集必要的数据。

5. 停止捕获：

```
monitor capture CAP stop
```

6. 在摘要视图中检查捕获：

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

7. 在详细视图中检查捕获：

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

8. 此外，以PCAP格式导出捕获以供进一步分析：

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

9. 收集完必要的数据后，删除捕获：

```
no monitor capture CAP
```

其他信息

- 捕获在物理接口、子接口和隧道接口上执行。
- 基于网络的应用识别(NBAR)过滤器(使用 **match protocol** 命令)。
- 有关本节中使用的命令的详细信息，请参阅搜索命令的最佳实践。

验证

当前没有可用于此配置的验证过程。

故障排除

对于在Cisco IOS-XE®上运行的EPC，此debug命令用于确保EPC设置正确：

```
debug epc provision
debug epc capture-point
```

相关信息

- 嵌入式数据包捕获 — Cisco IOS-XE
- 嵌入式数据包捕获 — Cisco IOS
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。