Cisco IOS和IOS-XE配置示例的嵌入式数据包捕获

目录

简介

本文在Cisco IOS软件方面描述嵌入式数据包捕获(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或以上
- Cisco IOS XE版本15.2(4)S - 3.7.0或以上

本文档中的信息从在实验室环境的设备创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

当启用，接收的路由器捕获发送的数据包和。数据包在DRAM的一缓冲区内存储并且通过重新加载不因而是不变的。一旦数据捕获，在一摘要或详细信息可以被检查在路由器。另外，数据可以导出作为数据包捕获(PCAP)文件允许进一步考试。工具在EXEC模式配置和认为一个临时协助工具。结果，工具配置没有在路由器配置内存储，并且到位不会在系统重新加载以后保持。

数据包捕获设置生成器和分析器工具是可用为了Cisco用户能帮助在数据包捕获的配置、捕获和提取。

Cisco IOS配置示例

基本EPC配置

1. 定义‘捕获缓冲区’，是一临时缓冲区获取数据包存储内。有可以选择的多种选项，当缓冲区定义时;例如大小， maxium数据包大小和圆/线性：

   ```
   monitor capture buffer BUF size 2048 max-size 1518 linear
   ```
2. 过滤器可能也应用对所需流量限制捕获。定义在配置模式内的访问控制表(ACL)并且适用于过滤器缓冲区：

   ```
   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 192.168.1.1monitor capture buffer BUF filter access-list
   BUF-FILTER
   ```
3. 定义‘捕获点’，定义了位置捕获发生。捕获点也定义了捕获是否为IPv4或IPv6发生，并且在哪条交换路径(进程与CEF) ：

   ```
   monitor capture point ip cef POINT fastEthernet 0 both
   ```
4. 附加缓冲区到捕获点：

   ```
   monitor capture point associate POINT BUF
   ```
5. 开始捕获：

   ```
   monitor capture point start POINT
   ```
6. 捕获当前是活跃的。允许必要数据的集。

7. 终止捕获：

   ```
   monitor capture point stop POINT
   ```
8. 检查在单元的缓冲区：

   `show monitor capture buffer BUF dump`**注意**：此输出只显示信息包获取的HEX转储。为了看到他们在人类易读那里是两种方式。导出从路由器的缓冲区进一步分析的：

   `monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap`**提示**：提出增强请求CSCuw77601为了添加MAIL对选项的a在出口下，因此您能给缓冲区发电子邮件diretly给电子邮件ID。然而上一个方法总是不是实用的，要求对路由器的T/FTP访问。在这些情况下，您能采取HEX转储的复制和使用所有联机HEX pcap转换器为了查看文件。
9. 一旦必要数据收集了，请删除‘捕获点’，并且‘请捕获缓冲区’： `no monitor capture point ip cef POINT fastEthernet 0 both`
   `no monitor capture buffer BUF`

注意：

- 在版本中早于Cisco IOS版本15.0(1)M，缓冲区大小对512K被限制了。
- 在版本中早于Cisco IOS版本15.0(1)M，获取数据包大小对1024个字节被限制了。
- 数据包缓冲在DRAM存储，并且不会通过重新加载仍然存在。

- 捕获配置在NVRAM没有存储，并且不会通过重新加载仍然存在。
- 捕获点可以定义在CEF或进程交换路径捕获。
- 捕获点仅可以定义捕获在接口或全局。
- 当捕获缓冲区在PCAP格式时导出， L2信息(例如以太网封装)没有保留。
- SeeBest为搜索命令为了得到关于用于此部分的命令的更多信息实践。

Cisco IOS XE配置示例

嵌入式数据包捕获功能在Cisco IOS XE版本3.7介绍- 15.2(4)S。因为添加更多功能，捕获的配置跟Cisco IOS不同。

基本EPC配置

1. 定义捕获将发生的位置：

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

2. 关联过滤器。过滤器可能指定线型，或者ACL或类映射可以被参考：

```
monitor capture CAP match ipv4 protocol tcp any any
```

3. 开始捕获：

```
monitor capture CAP start
```

4. 捕获当前是活跃的。允许它收集必要数据。

5. 终止捕获：

```
monitor capture CAP stop
```

6. 检查在一张概略的视图的捕获：

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

7. 检查在详细信息的捕获：

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

8. 另外，请导出在PCAP格式的捕获进一步分析的：

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

9. 一旦必要数据收集了，请删除捕获：

```
no monitor capture CAP
```

注意：

- 捕获在物理接口、sub-interface和隧道接口可以执行。
- 基于网络的应用程序识别(NBAR)根据过滤器，该使用**match protocol命令**在类映射下，当前不支持。
- 请参阅最佳实践关于搜索命令为了得到关于用于此部分的命令的更多信息。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

对于在Cisco IOS XE运行的EPC，此debug命令可以用于保证EPC适当地设置：

```
no monitor capture CAP
```

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