>使用在ACNS软件的tcpdump命令

目录

简介

Cisco应用和内容联网软件(ACNS) 4.2.1介绍**tcpdump命令**。此命令使您为故障排除的目的搜集在内容引擎、内容路由器或者内容分配管理器的嗅探器跟踪，当询问收集数据由思科技术支持。此工具非常类似于Linux/unix tcpdump命令。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- FTP
- ACNS
- ACNS命令行界面(CLI)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ACNS 4.2.1软件及以上版本
- 运行ACNS 4.2.X及以上版本的所有平台

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

捕获数据包

在ACNS的CLI当前允许管理员(必须是用户admin)获取从以太网的数据包。在Content Engine 500系列，接口名称是eth0和eth1。在所有ACNS平台上，推荐您指定一个路径/文件名在local1目录。

如果发出**tcpdump命令**在CLI，您能执行一平直的信息包报头转储到屏幕。**ctrl-c**普雷斯为了终止转储。

选项

tcpdump命令有这些选项：

- **- w*文件名***—写原始数据包捕获输出到文件。
- **- s*计数***—捕获每数据包第一个<count>字节。
- **- i*接口***—允许您指定一个特定接口使用捕获数据包。
- **- c*数量限制***计数数据包的捕获。

这是示例命令：

tcpdump - w /local1/dump.pcap - i eth0 - s 1500 - c10000

此命令**在**local1目录命名的**dump.pcap**文件捕获下10,000数据包的前1500个字节从接口Ethernet 0的，并且放置输出在内容引擎。

注意： 保证您指定选项**– s**设置数据包snaplength。默认值只捕获64个字节，并且这保存仅信息包报头到捕获文件。对于排除故障重定向的数据包或高水平流量(HTTP，验证，等等)，完整数据包的复制是需要的。

您在特定IP地址能也运行**tcpdump**和过滤：

- 添加**主机10.255.1.34**到**tcpdump**线路的末端。 **注意：** 用IP地址替换**10.255.1.34**客户端使用。
- 并且，请使用1600作为大小为了捉住大于1500个字节可以的坏数据包。

示例如下：

```
tcpdump -w /local/mydump -s 1600 -c10000 host 10.255.2.34
```

FTP

在TCP转储收集了后，您需要移动从内容引擎的文件向PC，以便可以由嗅探器编码器查看。

```
ftp <ip address of the CE>
 !--- Log in with the admin username and password. cd local1 bin hash get <name of the file> !--
- Using the previous example, it is dump.pcap.

     bye
```

Ethereal

Ethereal是读的TCP转储推荐的软件应用，由于其功能和他们的使用的范围与内容联网，包括能力解码被封装到GRE隧道的数据包，使用由WCCP重定向。参考Wireshark 网站欲知更多信息。

注意： 在大多数情况下，与ACNS CLI的tcpdump设备联机捕获的重定向的数据包与在接口接收的数据有所不同。由于重定向的数据包、目的IP地址和TCP端口号内部实施和处理修改反射设备IP地址和端口号8999。

相关信息

- Cisco应用和内容联网软件(ACNS)软件支持
- 技术支持和文档 - Cisco Systems