>使用在ACNS软件的tcpdump命令

Contents

Introduction

Cisco应用和内容联网软件(ACNS) 4.2.1引入**tcpdump命令**。此命令enable (event)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的您为排除故障的目的，当询问收集数据由Cisco技术支持。此工具非常类似于Linux/unix tcpdump命令。

Prerequisites

Requirements

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)

Components Used

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

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.If your network is live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

获取信息包

在ACNS的CLI当前允许管理员(必须是用户admin)从以太网获取信息包。在500系列的内容引擎，接口名字是eth0和eth1。在所有ACNS平台上，建议您在local1目录指定路径/文件名。

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。按**Ctrl-C**为了终止转储。

选项

tcpdump命令有这些选项：

- **- w*文件名***—写输出的原始的信息包获取到文件。
- **- s*计数***—捕获每个信息包第一个<count>字节。
- **- i*接口***—允许您指定一个特定接口使用获取信息包。
- **- c*计数***—限制捕获*计数*信息包。

这是示例命令：

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

此命令从以太网接口0**在**local1目录命名的**dump.pcap**文件捕获下10,000个信息包的前1500个字节，并且放置输出在内容引擎。

Note: 保证您指定选项**– s**设置信息包snaplength。DEFAULT值捕获仅64个字节和这保存仅信息包报头到捕获文件。对于排除故障重定向的信息包或高水平数据流(HTTP，认证，等等)，完全信息包的复制是需要的。

您能也运行**tcpdump**和过滤器在一个特定IP地址：

- 添加**主机10.255.1.34**到**tcpdump**线路的末端。 **Note:** 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个字节可以的坏信息包。

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，您需要从内容引擎移动文件向PC，以便可以由嗅探器译码器查看。

```
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封装隧道的信息包，使用由WCCP重定向。请参见Wireshark 网站欲知更多信息。

Note: 在许多情况下， **tcpdump**设备获取的重定向的信息包可用与ACNS CLI与在接口接收的数据有所不同。由于重定向的信息包内部实施和处理，目的地IP地址和TCP端口编号修改反射设备IP地址和端口号8999。

Related Information

- Cisco应用和内容联网软件(ACNS)软件支持
- Technical Support & Documentation - Cisco Systems