ESA数据包捕获步骤

目录

简介

本文描述如何执行思科电子邮件安全工具的(ESA)数据包捕获。

先决条件

要求

思科建议您有思科ESA的知识。

使用的组件

运行AsyncOS所有版本的本文档中的信息根据思科ESA。

背景信息

当您与与问题时的IronPort用户支持联系，您也许询问提供见解到ESA的出站和入站网络活动。设备提供能力拦截和显示TCP ， IP和在网络传送或接收设备附加的其他数据包。您也许要运行数据包捕获为了调试网络设置和为了验证到达或留下设备的网络流量。

Note:本文参考没有维护也IronPort不支持的软件。信息被提供作为礼貌为您的便利。对于进一

步协助，请联系软件供应商。

请注意CLI命令以前使用的**tcpdump**用新的**packetcapture** in命令AsyncOS版本7.0和以上替换。此命令提供功能类似于**tcpdump命令**，并且也是可用的为在GUI的使用。

如果运行AsyncOS版本6.x或以下，在**AsyncOS**本文的**版本6.x和以下**部分的**数据包捕获**参考关于如何的说明使用**tcpdump命令**。并且，在**数据包捕获过滤器**部分描述的过滤器选项为新的**packetcapture**命令是有效。

AsyncOS版本7.x和以上的数据包捕获

此部分描述在AsyncOS版本7.x和以上的数据包捕获进程。

开始或终止数据包捕获

为了开始有GUI的一数据包捕获，请导航对支持和Help菜单，选择**数据包捕获**和然后单击**启动捕获**。为了终止数据包捕获进程，请点击**终止捕获**。

Note:在GUI开始的捕获保留在会话之间。

为了开始有CLI的一数据包捕获，请输入**packetcapture > start命令**。为了终止数据包捕获进程，请输入**packetcapture > stop命令**，并且ESA终止数据包捕获，当会话结束时。

数据包捕获功能

这是您能使用为了操作数据包捕获有用的信息的列表：

- ESA保存获取数据包活动到文件并且存储文件本地。您能配置最大数据包捕获文件大小，数据包捕获运行，并且在哪个的时间长度网络接口捕获运行。您能也使用过滤器为了对从一个特定客户端或服务器IP地址的流量通过一个特定端口或流量限制数据包捕获。
- 导航**支持和**从GUI的**帮助>数据包捕获**为了查看在硬盘驱动器存储数据包捕获文件的完整列表。当数据包捕获运作时，数据包捕获页显示捕获的状况进展中与当前统计信息，例如文件大小和时间流逝了。
- 点击**file按钮的下载**为了下载数据包捕获文件。您在电子邮件能转发它到IronPort用户支持为了调试和排除所有问题故障。
- 为了删除数据包捕获文件，选择一个或更多文件和点击**删除选择的文件**。
- 为了编辑与GUI的数据包捕获设置，选择从支持的**数据包捕获**和Help菜单和单击**编辑设置**。
- 为了编辑与CLI的数据包捕获设置，请输入**packetcapture > setup命令**。

Note:GUI只显示在GUI开始的数据包捕获，不是开始与CLI的那些。同样地， CLI只显示在CLI开始一当前数据包捕获的状况。仅一个捕获能每次运行。

提示：关于数据包捕获选项和过滤器设置的更多信息，参考本文的**数据包捕获过滤器**部分。为了访问从GUI的AsyncOS在线帮助，导航**帮助和支持>Online帮助>索引> P >数据包捕获**。

AsyncOS版本6.x和以下的数据包捕获

此部分描述在AsyncOS版本6.x和以下的数据包捕获进程。

开始或终止数据包捕获

您能使用**tcpdump命令**为了获取在网络传送或接收ESA附加的TCP/IP和其他数据包。

完成这些步骤为了开始或终止数据包捕获：

1. 进入**诊断>网络> tcpdump命令**到ESA的CLI。下面是示例输出：

```
example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
[]> network

Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> tcpdump

- START - Start packet capture
- STOP - Stop packet capture
- STATUS - Status capture
- FILTER - Set packet capture filter
- INTERFACE - Set packet capture interface
- CLEAR - Remove previous packet captures
[]>
```

2. 设置接口(数据1、数据2或者管理)和过滤器。

   Note:过滤器使用格式和unix tcpdump命令一样。
3. 选择**开始**为了开始捕获和**停下来**为了结束它。

   Note:当捕获进展中时，请勿退出tcpdump菜单。 您必须使用秒钟CLI窗口为了运行所有其他命令。一旦捕获进程完成，您必须使用思科安全复制(SCP)或文件传输协议(FTP)从您的本地桌面为了下载文件从名为Diagnostic的目录(参考**数据包捕获过滤**部分关于详细信息)。文件使用

数据包捕获(PCAP)格式，并且可以查看与一个程序例如Ethereal或Wireshark。

数据包捕获过滤器

诊断> NET CLI命令用途标准的tcpdump过滤器语法。此部分关于tcpdump捕获过滤器提供信息并且提供一些示例。

这些是使用的标准的过滤器：

- **ip -**所有IP协议流量的过滤器
- **tcp -**所有TCP协议流量的过滤器
- **IP主机**-一个特定IP地址来源或目的地的过滤器

这是过滤器的一些示例在使用中：

- **IP主机10.1.1.1** -此过滤器捕获包括10.1.1.1作为来源或目的地的所有流量。
- **IP主机10.1.1.1或IP主机10.1.1.2** -此过滤器捕获包含10.1.1.1或10.1.1.2作为来源或目的地的流量。

对于获取文件的检索，请导航对**var >日志>诊断**或者**数据>客栈>诊断**为了到达诊断目录。

Note:当使用时此命令，造成您的ESA磁盘空间填满，并且能也导致性能下降。思科建议您在思科IronPort客户支持工程师的帮助下只使用此命令。