在思科Firepower设备的数据包捕获步骤

目录

简介

本文描述如何使用**tcpdump命令**为了获取由您的Firepower设备网络接口看到的数据包。它使用伯克利数据包过滤器(BPF)语法。

先决条件

要求

思科建议您有思科Firepower设备和虚拟设备型号的知识。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

> 警告：如果运行**tcpdump**在生产系统，能影响网络性能。

获取数据包的步骤

登陆对您的Firepower设备CLI。

在版本6.1和以上，请输入捕获**流量**。例如，

```
> capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```

在版本6.0.x.x和以下，回车**系统支持捕获流量**。例如，

```
> system support capture-traffic
```

```
Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```
在您做一选择后，将提示对于选项：

```
> system support capture-traffic

Please choose domain to capture traffic from:
0 - eth0
1 - Default Inline Set (Interfaces s2p1, s2p2)
```
为了获取从数据包的足够的数据，使用- s选项为了正确地设置snaplength是必要的。应该设置snaplength为匹配接口集合配置已配置的最大传输单元(MTU)值，默认到1518的值。

> 警告：因为捕获对屏幕的流量能降低系统和网络性能， Cisco建议您使用- w <filename>选项用tcpdump。它获取数据包到文件。如果运行命令，不用- w选项，按**Ctrl-C键**组合为了退出。

- w <filename>选项示例：

```
-w capture.pcap -s 1518
```

> **警告：**请勿使用任何路径元素，当您指定数据包捕获(pcap)时文件名。您必须指定在设备将创建的仅pcap文件名。

如果获取数据包有限数量是理想的，您能使用- c <packets>标志为了指定数据包数量捕获。例如，为了正确地获取5000数据包：

```
-w capture.pcap -s 1518 -c 5000
```
另外， BPF过滤器可以被添加在命令结束时为了限制哪些数据包捕获。例如，为了限制数据包捕获到有192.0.2.1来源或目的IP地址的5000数据包，您可能使用这些选项：

```
-w capture.pcap -s 1518 -c 5000 host 192.0.2.1
```
当您捕获是被标记的虚拟LAN (VLAN)的流量时，您必须指定与BPF语法的VLAN。否则， pcap不包含其中任一个VLAN标记信息包。例如，此示例对是从192.0.2.1标记的VLAN的流量限制捕获：

```
-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1
```
如果是不确定的，如果是VLAN被标记的流量，此语法可能用于为了捕获是并且不是被标记的VLAN从192.0.2.1的流量：

```
-w capture.pcap -s 1518 -c 5000 'host 192.0.2.1 or (vlan and host 192.0.2.1)'
```

> **注意**：在前一个示例中，括号是需要的，以便''不仅适用于'VLAN'。单引号由shell然后必要为了防止括号的所有可能的误解。

VLAN标记的规格捕获匹配其余您的BPF的所有VLAN流量。然而，如果要捕获特定VLAN标记，VLAN标记您希望抓住类似如此的您能指定：

```
-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1
```
在您指定希望的选项并且按回车后， tcpdump开始捕获流量。

> **提示**：如果-使用c选项，按**Ctrl-C键**组合为了终止捕获。

一旦终止捕获，您将接收确认。例如：

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -w capture.pcap -s 1518 -c 5000 host 192.0.2.1
Cleaning up.
Done.
```

复制Pcap文件

为了复制从FirePOWER设备的一个pcap文件到接受入站SSH连接的另一个系统，请使用此命令：

```
> system file secure-copy hostname username destination_directory pcap_file
```

在您按回车后，将提示对于对远程系统的密码。文件在间网络将复制。

> **注意**：在本例中，**主机名**是指目标远程主机的名称或IP地址，**用户名**指定用户的名称远程主机的， **destination_directory**指定远程主机的目的地路径，并且**pcap_file**指定转移的本地pcap文件。