在Firepower设备上使用数据包捕获过程

目录

简介

本文档介绍如何使用tcpdump命令捕获Firepower设备的网络接口看到的数据包。

先决条件

要求

Cisco建议您了解Cisco Firepower设备和虚拟设备型号。

使用的组件

本文档不限于特定的软件和硬件版本。 它使用Berkeley数据包过滤器(BPF)语法。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

 警告：如果在生产系统上运行tcpdump命令，可能会影响网络性能。

捕获数据包的步骤

登录到Firepower设备的CLI。

在版本6.1及更高版本中，输入capture-traffic。例如，

<#root>

```
> capture-traffic


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

在6.0.x.x及更低版本中，输入system support capture-traffic。例如，

<#root>

```
> system support capture-traffic


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

进行选择后，系统将提示您输入选项：

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

为了从数据包中捕获足够的数据，必须使用-s选项来正确设置长度。可将带宽设置为与接口集配置的已配置最大传输单位(MTU)值（默认为1518）匹配的值。

警告：捕获到屏幕的流量时，可能会降低系统和网络的性能。Cisco建议您将 — w <filename>选项与tcpdump命令配合使用。它将数据包捕获到文件中。如果运行不带-w选项的命令，请按Ctrl-C组合键退出。

-w <filename>选项示例：

<#root>

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

注意：指定数据包捕获(pcap)文件名时，请勿使用任何路径元素。必须仅指定要在设备中创建的pcap文件名。

如果希望捕获有限数量的数据包，您可以使用-c <packets>标志指定要捕获的数据包数量。例如，要准确捕获5000个数据包：

<#root>

```
-w capture.pcap -s 1518 -c 5000
```

此外，可以在命令末尾添加BPF过滤器以限制捕获的数据包。例如，为了将数据包捕获限制为源或目标IP地址为192.0.2.1的5000个数据包，可以使用以下选项：

<#root>

-w capture.pcap -s 1518 -c 5000 host 192.0.2.1

捕获标记了虚拟LAN(VLAN)的流量时，必须使用BPF语法指定VLAN。否则，pcap不包含任何VLAN标记的数据包。例如，此示例将捕获限制为从192.0.2.1标记VLAN的流量：

<#root>

-w capture.pcap -s 1518 -c 5000 vlan and host 192.0.2.1

如果您不确定流量是否标记为VLAN，可以使用此语法捕获来自192.0.2.1的流量，该流量标记为VLAN或未标记VLAN:

<#root>

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

注：在上一个示例中，需要使用括号，以便“or”不仅适用于“vlan”。然后，需要单引号以防止外壳可能对圆括号的任何误解。

指定VLAN标记会捕获与您的BPF其余部分匹配的所有VLAN流量。但是，如果要捕获特定VLAN标记，可以指定要捕获的VLAN标记，如下所示：

<#root>

-w capture.pcap -s 1518 -c 5000 vlan 1 and host 192.0.2.1

指定所需选项并按Enter后，tcpdump开始捕获流量。

提示：如果未使用 — c选项，请按Ctrl-C组合键停止捕获。

一旦停止捕获，您将收到确认。例如：

<#root>

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

要将pcap文件从FirePOWER设备复制到接受入站SSH连接的另一个系统，请使用以下命令：

<#root>

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

按Enter后，系统将提示您输入远程系统的密码。文件可以在网络上复制。

注意：在本示例中，主机名是指目标远程主机的名称或IP地址，用户名指定远程主机上的用户的名称，destination_directory指定远程主机上的目标路径，pcap_file指定用于传输的本地pcap文件。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。