

问题描述

【MVS】Cisco FlexNetFlow详细配置举例

解决方法

Cisco的Flexible NetFlow (FlexNetFlow) 是NetFlow的一个增强版, 它提供了更高的灵活性和定制选项。FlexNetFlow允许用户定义自己的流记录、流集合和流导出器。以下是一个使用Cisco IOS的Flexible NetFlow的详细配置示例:

1. **定义流记录**:

流记录定义了要捕获哪些数据字段。

```
``cisco
flow record MY_FLOW_RECORD
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
``
```

在这个例子中, `MY_FLOW_RECORD`是我们定义的流记录名称, 它将匹配IPv4源和目的地址、源和目的端口, 并收集流量字节数、数据包数以及第一个和最后一个数据包的系统运行时间。

2. **定义流导出器**:

流导出器定义了将流记录发送到哪里以及如何发送。

```
``cisco
flow exporter MY_FLOW_EXPORTER
destination [收集器IP地址]
source [出口接口]
transport udp [端口号]
``
```

将`[收集器IP地址]`替换为你的NetFlow收集器的IP地址, 将`[出口接口]`替换为用于发送NetFlow数据的接口, 将`[端口号]`替换为你的NetFlow收集器监听的端口号。

3. **定义流监视器**:

流监视器将流记录和流导出器关联起来, 并应用于接口。

```
``cisco
flow monitor MY_FLOW_MONITOR
record MY_FLOW_RECORD
exporter MY_FLOW_EXPORTER
cache timeout active 60
cache timeout inactive 15
``
```

`MY_FLOW_MONITOR`是我们定义的流监视器名称, 它使用我们之前定义的流记录`MY_FLOW_RECORD`和流导出器`MY_FLOW_EXPORTER`。`cache timeout active`和`cache timeout inactive`定义了流缓存的超时设置。

4. **将流监视器应用到接口**:

```
``cisco
interface [接口名称]
ip flow monitor MY_FLOW_MONITOR input
ip flow monitor MY_FLOW_MONITOR output
``
```

将`[接口名称]`替换为你想要收集NetFlow数据的接口, 比如`GigabitEthernet0/0`。这将流监视器应用于接口的输入和输出方向。

5. **验证配置**:

使用下面的命令来验证你的Flexible NetFlow配置。

```
``cisco
show flow record
show flow exporter
show flow monitor
show flow interface
show ip cache flow
``
```

这些 `show` 命令将帮助你查看流记录、流导出器、流监视器的配置，以及正在监视的接口和IP流缓存中的统计信息。

请注意，这只是一个基本的Flexible NetFlow配置示例。根据你的Cisco设备型号和IOS版本，可能需要进行调整或添加其他配置选项。在配置之前，请确保查阅官方文档以了解所有可用选项和最佳做法。