# 灵活NetFlow过滤用性能监控程序

## 目录



## 简介

本文描述如何过滤某些IP以便不由Netflow记录。

贡献用Vishal Kothari， Cisco TAC工程师。

## 先决条件

### 要求

Cisco建议您有灵活NetFlow知识。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 3650交换机
- 综合服务路由器(ISR) 4351路由器

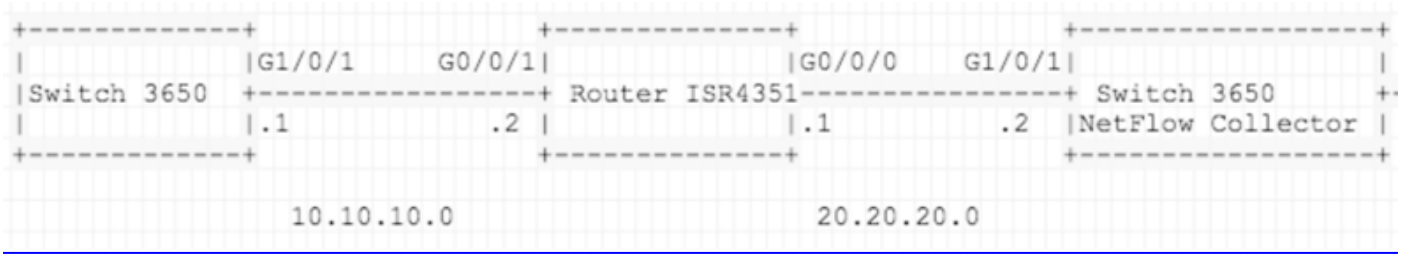
> **Note**:为了达到此必需的过滤在Netflow下，您将需要安装AppxK9许可证。对于测试，您能利用正确对使用(RTU) AppxK9许可证。

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。如果您的网络实际，请保证您了解所有命令的潜在影响。

## 配置

在此部分，要求您过滤不需要由Netflow记录，更加进一步意味着IP的列表的，路由器不应该派出关于被定义的IP源的在ACL的详细资料和目的地。如何能通过灵活NetFlow达到此，您将发现这里。

## 网络图




## 配置

准备您要过滤，当发送它到NetFlow收集器时所有那些网络的列表。在本例中，请拒绝/过滤器Telnet数据流被发送到收集器并且允许其他数据流。

ISR4351配置：

```
IP access-list extended acl-filter

deny   tcp host 10.10.10.1 host 10.10.10.2 eq telnet

deny   tcp host 10.10.10.2 eq telnet host 10.10.10.1

permit ip any any



flow record type performance-monitor NET-FLOW

match ipv4 tos

match ipv4 protocol

match ipv4 source address

match ipv4 destination address

match transport source-port

match transport destination-port

match interface output

match flow direction

match flow sampler

match application name

collect routing source as

collect routing destination as

collect routing next-hop address ipv4

collect ipv4 source mask
```

```
collect ipv4 destination mask
collect transport tcp flags
collect interface input
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
!
flow exporter NET-FLOW
description NET-FLOW
destination 20.20.20.2
source Loopback28
transport udp 2055
!
!
flow monitor type performance-monitor NET-FLOW
record NET-FLOW
exporter NET-FLOW

class-map match-any class-filter
match access-group name acl-filter
!
policy-map type performance-monitor policy-filter
class class-filter
  flow monitor NET-FLOW



interface Loopback28
ip address 10.11.11.28 255.255.255.255


interface GigabitEthernet0/0/1
```

```
 ip address 10.10.10.2 255.255.255.0

negotiation auto

service-policy type performance-monitor input policy-filter
```

# 验证

使用本部分可确认配置能否正常运行。

如何确认网络是否过滤了，当您传送他们到NetFlow收集器？

为了证明，您能采取嵌入式信息包获取(EPC)在ISR4351 Gi0/0/0 (指向往NetFlow收集器)的接口。配置如下：

```
ip access-list extended CAP-FILTER

permit ip host 10.11.11.28 host 20.20.20.2

permit ip host 20.20.20.2 host 10.11.11.28




monitor capture CAP access-list CAP-FILTER buffer size 10 interface GigabitEthernet 0/0/0 both

monitor capture CAP start
```

```
++  TEST I

3650: -
```

```
telnet 10.10.10.2

Trying 10.10.10.2 ... Open
```

信息包为Telnet数据流不是获取的在EPC下，是的原因数据流被拒绝在访问控制表(ACL) (ACL过滤器)下，并且其余一切允许。

```
show monitor capture CAP buffer brief

------------------------------------------------------------

#   size   timestamp     source             destination   protocol

------------------------------------------------------------
```

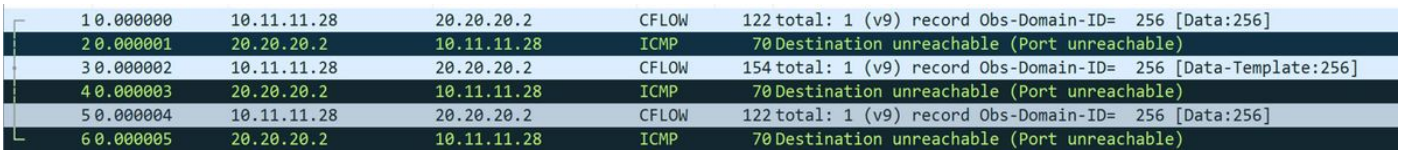
现在测试02，请生成ping数据流为了发现是否得到配比在EPC下：

```
++ TEST II

3650: -
```

```
ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

!!!!!
```

ISR4351 ：

```
++ TEST II

3650: -

ping 10.10.10.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:

!!!!!
```



| | | | | | |
|---|---|---|---|---|---|
| 1 | 0.000000 | 10.11.11.28 | 20.20.20.2 | CFLOW | 122 total: 1 (v9) record Obs-Domain-ID= 256 [Data:256] |
| 2 | 0.000001 | 20.20.20.2 | 10.11.11.28 | ICMP | 70 Destination unreachable (Port unreachable) |
| 3 | 0.000002 | 10.11.11.28 | 20.20.20.2 | CFLOW | 154 total: 1 (v9) record Obs-Domain-ID= 256 [Data-Template:256] |
| 4 | 0.000003 | 20.20.20.2 | 10.11.11.28 | ICMP | 70 Destination unreachable (Port unreachable) |
| 5 | 0.000004 | 10.11.11.28 | 20.20.20.2 | CFLOW | 122 total: 1 (v9) record Obs-Domain-ID= 256 [Data:256] |
| 6 | 0.000005 | 20.20.20.2 | 10.11.11.28 | ICMP | 70 Destination unreachable (Port unreachable) |

## 故障排除

目前没有针对此配置的故障排除信息。