Reg : Cisco configuration for Netflow V9

Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>

Thu 12/12/2019 18:57

To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

1 attachments (6 KB)

cisco 7200 .txt;

Hi Sriram,

NetFlow v9 configuration in Cisco 7200

Flow record :

```
 flow record flow_record
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
```

Flow exporter:

```
flow exporter EXPORTER-1
description linux-server
destination 192.168.56.106
source FastEthernet0/0
output-features
ttl 15
transport udp 9995
template data timeout 120
```

Flow monitor :

```
flow monitor FLOW-MONITOR-1
exporter EXPORTER-1
record flow_record
```

Interface configuration :

```
interface FastEthernet0/0
description to_Linux_server
ip address 192.168.56.105 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
ip flow monitor FLOW-MONITOR-1 output
ip flow ingress
ip flow egress
duplex full
```

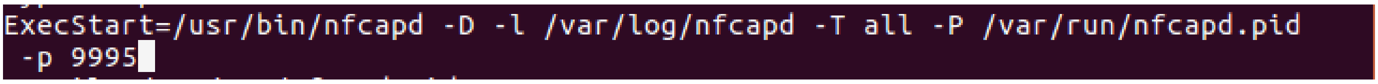
Command in global configuration :

```
ip cef
ip flow-export version 9
ip flow-cache timeout inactive 20
ip flow-cache timeout active 1
```

I have also attached the running configuration file of the Cisco router.

For the NFdump ,

Configuration in **/lib/system/system/nfdump.service**



```
ExecStart=/usr/bin/nfcapd -D -l /var/log/nfcapd -T all -P /var/run/nfcapd.pid
 -p 9995
```

Or else in CLI
sudo nfcapd -p 9995 -4 -l /var/log/nfcapd -T all -D -w

For viewing I used the commands from the nfdump cheat sheet

Thanks and Regards,
Lavanya Singaravelan