Reg : IPFIX Configuration on Cisco Router

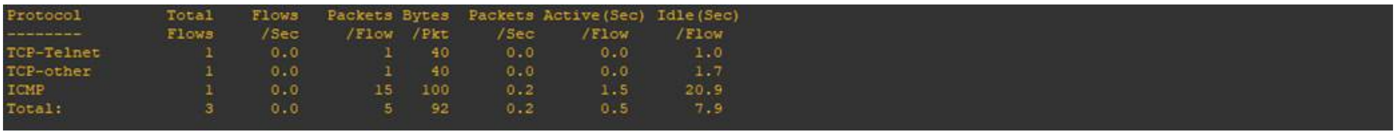
Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>
Fri 13/12/2019 13:43
To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

1 attachments (6 KB)
Cisco running_config_IPFIX.txt;

Hi Sriram,

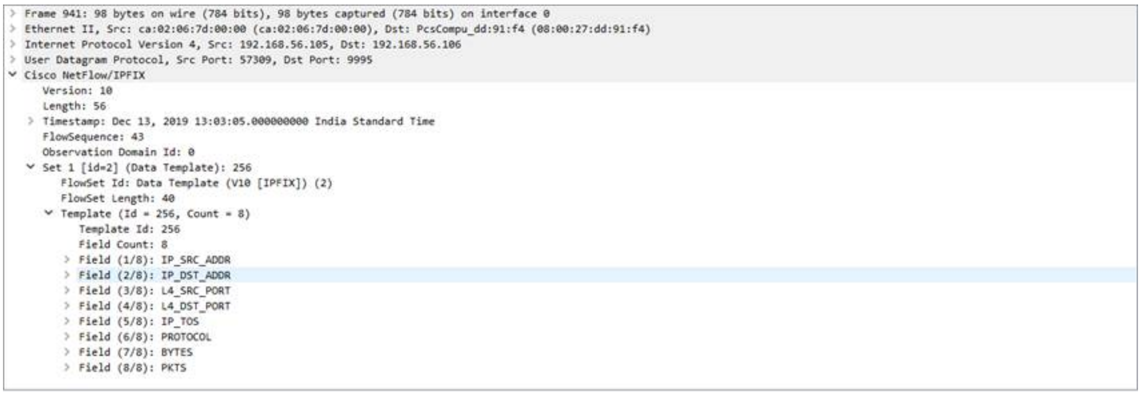
I have configured IPFIX in place of Netflow V9 in the Cisco router based on the discussion we had yesterday

For the IPFIX cache details:



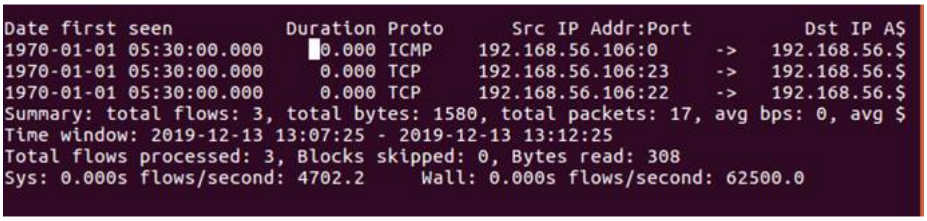
```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           1      0.0         1    40      0.0       0.0       1.0
TCP-other            1      0.0         1    40      0.0       0.0       1.7
ICMP                 1      0.0        15   100      0.2       1.5      20.9
Total:               3      0.0         5    92      0.2       0.5       7.9
```

The data template sent out by the IPFIX protocol



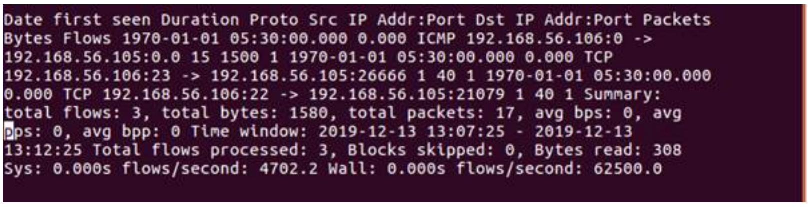
```
> Frame 941: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: ca:02:06:7d:00:00 (ca:02:06:7d:00:00), Dst: PcsCompu_dd:91:f4 (08:00:27:dd:91:f4)
> Internet Protocol Version 4, Src: 192.168.56.105, Dst: 192.168.56.106
> User Datagram Protocol, Src Port: 57309, Dst Port: 9995
v Cisco NetFlow/IPFIX
     Version: 10
     Length: 56
   > Timestamp: Dec 13, 2019 13:03:05.000000000 India Standard Time
     FlowSequence: 43
     Observation Domain Id: 0
   v Set 1 [id=2] (Data Template): 256
        FlowSet Id: Data Template (V10 [IPFIX]) (2)
        FlowSet Length: 40
      v Template (Id = 256, Count = 8)
           Template Id: 256
           Field Count: 8
         > Field (1/8): IP_SRC_ADDR
         > Field (2/8): IP_DST_ADDR
         > Field (3/8): L4_SRC_PORT
         > Field (4/8): L4_DST_PORT
         > Field (5/8): IP_TOS
         > Field (6/8): PROTOCOL
         > Field (7/8): BYTES
         > Field (8/8): PKTS
```

The output obtained in nfcpad file



```
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP A$
1970-01-01 05:30:00.000     0.000 ICMP    192.168.56.106:0      ->    192.168.56.$
1970-01-01 05:30:00.000     0.000 TCP     192.168.56.106:23     ->    192.168.56.$
1970-01-01 05:30:00.000     0.000 TCP     192.168.56.106:22     ->    192.168.56.$
Summary: total flows: 3, total bytes: 1580, total packets: 17, avg bps: 0, avg $
Time window: 2019-12-13 13:07:25 - 2019-12-13 13:12:25
Total flows processed: 3, Blocks skipped: 0, Bytes read: 308
Sys: 0.000s flows/second: 4702.2     Wall: 0.000s flows/second: 62500.0
```

I changed the alignment to justification :



```
Date first seen Duration Proto Src IP Addr:Port Dst IP Addr:Port Packets
Bytes Flows 1970-01-01 05:30:00.000 0.000 ICMP 192.168.56.106:0 ->
192.168.56.105:0.0 15 1500 1 1970-01-01 05:30:00.000 0.000 TCP
192.168.56.106:23 -> 192.168.56.105:26666 1 40 1 1970-01-01 05:30:00.000
0.000 TCP 192.168.56.106:22 -> 192.168.56.105:21079 1 40 1 Summary:
total flows: 3, total bytes: 1580, total packets: 17, avg bps: 0, avg
bps: 0, avg bpp: 0 Time window: 2019-12-13 13:07:25 - 2019-12-13
13:12:25 Total flows processed: 3, Blocks skipped: 0, Bytes read: 308
Sys: 0.000s flows/second: 4702.2 Wall: 0.000s flows/second: 62500.0
```

The configuration used for IPFIX in Cisco Router 7200 series:

Flow record:
flow record flow_record
match ipv4 tos
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
destination 192.168.56.106
source FastEthernet0/0

```
output-features
ttl 15
transport udp 9995
export-protocol ipfix
template data timeout 120
```

Flow monitor:

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

Specific interface configuration:

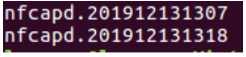
```
interface FastEthernet0/0
description to_Linux_server
ip address 192.168.56.105 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
ip flow monitor FLOW-MONITOR-1 output
ip flow ingress
ip flow egress
duplex full
```

Command in global configuration :

```
ip cef
ip flow-cache timeout inactive 20
ip flow-cache timeout active 1
```

I have attached the running configuration file with this mail

The file generated by nfcapd will be with this name nfcapd.<yyyymmddhhmm>



```
nfcapd.201912131307
nfcapd.201912131318
```

Thanks and Regards,
Lavanya Singaravelan