Flowmon Networks

NetFlow Export Configuration

The document describes how to configure the capture and export of flow data on various devices.

Contents

NetFlow settings

It is recommended to set **active flow timeout** to 5 minutes or less (instead of the default value of 30 minutes) for faster export of flow data (useful for Flowmon ADS and Flowmon DDoS Defender).

The **minimal** flow data **required** by Flowmon Collector:
Source IP address
Destination IP address
Source port number
Destination port number
L3 protocol

Start of flow timestamp
End of flow timestamp
Number of bytes
Number of packets
Transport TCP flags

Ingress/Egress on multiple interfaces
Usually, it is sufficient to enable collecting just inbound traffic (ingress) on all the interfaces of the switch.

Cisco IOS

Setting NetFlow

```
enable
configure terminal
ip cef                                          //enables Cisco Express Forwarding
ip flow export source vlan3
ip flow-cache timeout active 5                  //active flows [minutes]
ip flow-cache timeout inactive 30               //inactive flows [seconds]
ip flow-export version 9
ip flow-export destination a.b.c.d 2055
interface FastEthernet0/0
ip flow ingress
ip flow egress
end
```

Use NetFlow **version 5** if v9 unavailable:

```
interface FastEthernet 0/0
ip route-cache flow
exit
ip flow-export destination a.b.c.d
ip flow-export source vlan3
ip flow-export version 5
ip flow-cache timeout active 5
ip flow-cache timeout inactive 30
snmp-server ifindex persist
```

Note that **older versions** (eg. Catalyst 6500) used a different command for setting cache timeout:

```
mls aging long 300
mls aging normal 32
```

In this case, also make sure to set the flow **mask**:

```
mls netflow interface
mls flow ip interface-full
```

For **CatOS** device:
set mls agingtime long 300
set mls agingtime 32

Basic Flexible NetFlow record

flow record FNF_IPv4_basic_APP
description Basic Flexible NetFlow record for IPv4
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match ipv4 protocol
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect counter bytes
collect counter packets
collect transport tcp flags

Extended Flexible NetFlow record

Flexible NetFlow (FNF) configuration on Cisco devices with NBAR2 App Name support

1. FNF record - selection of entities and how to create the records
2. Exporter - where to export the records
3. Monitor - FNF record + exporter
4. Source of data - monitor on selected interfaces

Enable Cisco Express Forwarding:

ip cef

Create flow **record**:

flow record FNF_IPv4_extended_APP
description Extended Flexible NetFlow record for IPv4 with the application name
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match ipv4 protocol
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect counter bytes
collect counter packets
collect transport tcp flags

collect ipv4 tos

collect datalink mac source address input
collect datalink mac source address output
collect datalink mac destination address input
collect datalink mac destination address output
collect datalink dot1q vlan input
collect datalink dot1q vlan output
collect interface input
collect interface output
collect routing destination as
collect routing source as
collect application name

Create flow **exporter**:

flow exporter FNF_exporter_1
description Exporter for Flexible NetFlow
destination 10.0.0.2
transport udp 2055
template data timeout 600

Turn on **monitoring** (monitor):

flow monitor FNF_IPv4_monitor_1
description Flexible NetFlow monitor 1 for IPv4
record FNF_IPv4_extended_APP
exporter FNF_exporter_1
cache timeout inactive 30
cache timeout active 300

Assign **interface** to the monitor (source of data):

interface Vlan3
ip flow monitor FNF_IPv4_monitor_1 input
ip flow monitor FNF_IPv4_monitor_1 output

IPv6

ipv6 cef
flow record FNF_IPv6_extended_APP
description Extended Flexible NetFlow record for IPv6 with the application name
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
match ipv6 protocol
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect counter bytes

collect counter packets
collect transport tcp flags
collect ipv6 dscp
collect datalink mac source address input
collect datalink mac source address output
collect datalink mac destination address input
collect datalink mac destination address output
collect datalink dot1q vlan input
collect datalink dot1q vlan output
collect interface input
collect interface output
collect routing destination as
collect routing source as
collect application name
flow monitor FNF_IPv6_monitor_1
description Flexible NetFlow monitor 1 for IPv6
record FNF_IPv6_extended_APP
exporter FNF_exporter_1
cache timeout inactive 30
cache timeout active 300
interface Vlan3
ipv6 flow monitor FNF_IPv6_monitor_1 input
ipv6 flow monitor FNF_IPv6_monitor_1 output

Verifying the configuration

show flow exporter
show flow interface
show flow monitor
show flow record

show flow monitor FNF_monitor_1 statistics
show flow monitor FNF_monitor_1 cache

show ip cache flow
show ip flow interface
show ip flow export
show ip flow export template

Troubleshooting:

show cef interface name
show policy-map type mace
show policy-map type mace interface name
show flow exporter name
show flow exporter template
show flow exporter option application table
show flow record type mace name

show flow monitor type mace name
show mace metrics
show ip nbar parameter extraction

For more on troubleshooting follow the link:
https://www.cisco.com/c/en/us/td/docs/routers/access/ISRG2/AVC/api/guide/AVC_Metric_Definition_Guide/7_Troubleshooting.html

IOS version 15 reference:
https://www.cisco.com/c/en/us/td/docs/ios/netflow/configuration/guide/15_0s/nf_15_0s_book.html

IOS version 12 reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/12-4/nf-12-4-book.html

Command reference:
https://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_01.html

Catalyst 6500 reference:
https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/116434-problemsolution-product-00.html

Catalyst 5000 reference:
https://www.cisco.com/en/US/products/hw/switches/ps679/products_command_reference_chapter09186a00800d9f4d.html

Cache timeout commands comparison reference:
https://www.andrisoft.com/support/portal/kb/article/what-are-the-optimal-netflow-aging-values

Configuring SPAN

SPAN mirrors traffic from one or more source interfaces on any VLAN or from one or more VLANs to a destination interface for analysis.

Examples of setting up **source**:

//monitor bidirectional traffic from source interface fast ethernet 4/10
monitor session 1 source interface fastethernet 4/10

//differing directions within a SPAN session (parameters rx and tx)
monitor session 1 source interface fa2/3 rx //Receive
monitor session 1 source interface fa2/2 tx //Transmit

//using ranges
monitor session 1 source interface fastethernet 4/1-10

//listing several VLANs
monitor session 1 source vlan 4, 5-7

Setting up **destination**:
monitor session 1 destination interface fastethernet 4/15

//specifying the **encapsulation** type used by the destination port
monitor session 1 destination interface fastethernet 5/48 encapsulation dot1q

Encapsulation options:
isl - Use ISL
dot1q - Use 802.1Q
"replicate" is not supported
without encapsulation mode - the port default is untagged

Verifying the configuration:
show monitor

//only session 1
show monitor session 1

Removing configuration:
no monitor session 1

For more commands and options see the reference:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/span.html#wp1043935

Application Response Time (ART)

NBAR Application name provides the information regarding the L7 level information for a particular flow, e.g HTTP, FTP, SIP etc.. There is an ID exported by ART, which explains which application this flow belongs to.

Optionally, set collection of following AVC items on Cisco devices with ART support:

FlowMon "AVC **Metrics**" Extension

collect connection delay network to-client sum
collect connection delay network to-client minimum
collect connection delay network to-client maximum
collect connection delay network to-server sum
collect connection delay network to-server minimum
collect connection delay network to-server maximum
collect connection delay application sum
collect connection delay application minimum
collect connection delay application maximum

FlowMon "AVC **Histogram**" Extension

collect connection delay response to-server histogram
collect connection delay response to-server histogram late

Cisco NX-OS

Enable NetFlow:

feature netflow

Define an optional flow **exporter** by specifying the export format, protocol, destination, and other parameters:

flow exporter exporter-1
description Flow Collector
destination a.b.c.d
source Vlan3
transport udp 2055
version 9

Define a flow **monitor** based on the flow record and flow exporter:

flow monitor netflow-monitor-1
record netflow-original
exporter exporter-1

Apply the flow monitor to a source **interface**:

interface eth0/0
ip flow monitor netflow-monitor-1 input
exit

Set **timeouts**:

flow timeout active 300 (default is 1800 seconds)

Verifying the configuration:

show flow record netflow-original
show flow exporter
show flow monitor netflow-monitor-1

Optionally, create **custom record**:

flow record custom-netflow-record
description Custom Netflow Record
match ipv4 source address

match ipv4 destination address
match transport destination-port
...
collect counter bytes
collect counter packets

Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_15netflow.html

Cisco NX-OS/IOS Netflow Comparison (2012):
http://docwiki.cisco.com/wiki/Cisco_NX-OS/IOS_Netflow_Comparison

Cisco IOS XR

1. Create and configure an exporter map.
2. Create and configure a monitor map and a sampler map.
3. Apply the monitor map and sampler map to an interface.

Configuring an **Exporter** Map:

```
configure
flow exporter-map fem
destination a.b.c.d
source vlan3
transport udp 2055
version v9
options sampler-table 300
commit
exit
exit
show flow exporter-map fem
```

Configuring a **Sampler** Map:

```
configure
sampler-map fsm
random 1 out-of 1
commit
exit
exit
show sampler-map fsm
```

Configuring a **Monitor** Map:

```
configure
flow monitor-map fmm
```

```
record ipv4
cache timeout inactive 300
exporter fem
commit
exit
exit
show flow monitor-map fmm
```

Applying a Monitor Map and a Sampler Map to an **Interface**:

```
configure
interface gigabitEthernet 0/0/0/0
flow ipv4 monitor fmm sampler fsm ingress
commit
```

Reference:
https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-2/netflow/configuration/guide/b_netflow_cg42crs/b_netflow_cg42asr_chapter_00.html

Juniper

Juniper has a wide support of flow export called jFlow. It's available on MX router series as well as J-Series and SRX. There is a different support for different versions of the operating system, platforms and cards. There is also a known issue with sampling rate detection on Flowmon side. We have it implemented based on IPFIX RFC which is not followed by Juniper. As a workaround you can configure a static sampling rate per listening port. Please note that in jFlow duration of flow works differently than in traditional NetFlow as it is always counted since start of connection and does not get reseted with flow export.

jFlow v5 on MX320

This configuration example shows jFlow v5 using sampling 1:500 with active timeout of 60s and inactive timeout of 15s. We recommend to use active timeout 300s and inactive timeout 30s. Replace x.x.x.x by Collector address and y.y.y.y by router address. You can also replace destination port, 9999 in this case.

```
sampling {
  input {
     rate 500;
     run-length 0;
  }
  family inet {
     output {
        flow-inactive-timeout 15;
        flow-active-timeout 60;
        file filename cflow;
        flow-server [x.x.x.x] {
           port 9999;
           source-address [y.y.y.y];
```

```
        version 5;
    }
```

jFlow v9 on MX960

Following configuration comes from MX960 using Junos 15.1F6. Sampling rate set to 1:300 packets and configuration is as follows, just IPs of Collector and router needs to be added.

You need to set the option to let the router know where to send data and which format.

```
set forwarding-options sampling input rate 300
set forwarding-options sampling family inet output flow-server a.b.c.d autonomous-system-type peer
set forwarding-options sampling family inet output flow-server a.b.c.d no-local-dump
set forwarding-options sampling family inet output flow-server a.b.c.d source-address b.c.d.e
set forwarding-options sampling family inet output flow-server a.b.c.d version9 template ipv4
```

Configure Flow monitoring templates and timeouts

```
set services flow-monitoring version9 template ipv4 flow-active-timeout 60
set services flow-monitoring version9 template ipv4 flow-inactive-timeout 60
set services flow-monitoring version9 template ipv4 template-refresh-rate seconds 300
set services flow-monitoring version9 template ipv4 option-refresh-rate seconds 300
set services flow-monitoring version9 template ipv4 ipv4-template
set services flow-monitoring version9 template ipv6 flow-active-timeout 60
set services flow-monitoring version9 template ipv6 flow-inactive-timeout 60
set services flow-monitoring version9 template ipv6 template-refresh-rate seconds 300
set services flow-monitoring version9 template ipv6 option-refresh-rate seconds 300
set services flow-monitoring version9 template ipv6 ipv6-template
set services flow-monitoring version9 template mpls flow-active-timeout 60
set services flow-monitoring version9 template mpls flow-inactive-timeout 60
set services flow-monitoring version9 template mpls template-refresh-rate seconds 300
set services flow-monitoring version9 template mpls option-refresh-rate seconds 300
set services flow-monitoring version9 template mpls mpls-ipv4-template label-position 1
set services flow-monitoring version9 template mpls mpls-ipv4-template label-position 2
set services flow-monitoring version9 template mpls mpls-ipv4-template label-position 3
```

To apply it to all interfaces you can configure it on firewall, ideally as a first rule to sample all the traffic

```
user1@router1.re0> show configuration firewall family inet filter peer1_inbound
interface-specific;
term sample {
        then {
                sample;
                next term;
        }
}
```

References to other Juniper platforms

https://kb.juniper.net/InfoCenter/index?page=content&id=KB12512

https://www.juniper.net/us/en/local/pdf/app-notes/3500204-en.pdf

Huawei

Huawei devices support NetStream.
NetStream V5 ~ NetFlow v5
NetStream v9 ~ NetFlow v9

Sampling
In case of using sampling make sure to set it on the collector as well. Sampling information is not included in templates.

Routers & Switches

ip netstream export source 10.1.2.1
ip netstream export host 10.1.2.2 3000
ip netstream export version 9
ip netstream export index-switch 32
interface gigabitethernet 1/0/0
ip netstream sampler fix-packets 1 inbound
ip netstream sampler fix-packets 1 outbound
ip netstream inbound
ip netstream outbound

Set the active **aging** time to 20 minutes and the inactive aging time to 100 seconds, and enable FIN- and RST-based aging:

ip netstream timeout active 20
ip netstream timeout inactive 100
ip netstream tcp-flag enable

Verifying the configuration:

display ip netstream statistic
display ip netstream all
display ip netstream global

Optionally, create custom flexible **record**
Note that it must be done before running ip netstream command

ip netstream record myrecord
match ip source-address
match ip destination-address
match ip source-port
match ip destination-port
collect counter bytes
collect counter packets

collect interface input
collect interface output

For **Huawei S Series** where **NetStream** is **not supported** and we have to use **sFlow**. The lowest sample rate is 256 and the smallest polling interval is 20 sec (depending on the size of the switch):

interface GigabitEthernet0/0/1
sflow counter-sampling collector 1
sflow counter-sampling interval 20
sflow flow-sampling collector 1
sflow flow-sampling rate 256

interface GigabitEthernet0/0/48
sflow counter-sampling collector 1
sflow counter-sampling interval 20
sflow flow-sampling collector 1
sflow flow-sampling rate 256

sflow collector 1 ip 192.168.34.210
sflow agent ip 192.168.34.197

Firewalls

USG firewalls support only inbound.
NE firewalls support both.

ip netstream export host 192.168.2.2 3000
ip netstream export source 192.168.2.1
interface vlanif 100
ip netstream export version 9
ip netstream inbound
ip netstream sampler fix-packets 20 inbound

display ip netstream cache

Reference:
http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000019448&partNo=10022

NetStream (Integrated) Technology Whitepaper:
http://enterprise.huawei.com/ilink/enenterprise/download/HW_201022 (2012)
http://enterprise.huawei.com/ilink/enenterprise/download/HW_353223 (2014)

Gigamon

Enable **SSH**
Settings > Global Settings > SSH

Enable **Packet slicing**
With this configuration in place, Gigamon appliance provided us the IPv6 header so all **key information** to generate **flow data** were present while we can reduce by using it **utilization** on link connected to monitoring device. Or the other option would be to combine it with aggregation and then we could handle traffic from multiple lines with one interface.

gsop alias Gigaslicing slicing protocol ipv6 offset 4 port-list gsg1

Configure **map** to get slicing to required ports:

```
map alias Pacslic1
  type regular byRule
  roles replace admin to owner_roles
  comment "packet slicing"
  use gsop Gigaslicing
  rule add pass ipver 6
  to 1/1/x15
  from 1/1/x1
```

Create a **record:**

```
apps netflow record alias Netflow_v9
  description "Test of Netflow export"
  netflow-version netflow-v9
  collect add counter bytes long
  collect add ipv4 fragmentation offset
  collect add ipv4 protocol
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add transport source-port
  collect add transport destination-port
  collect add transport tcp flags ack enable cwr enable ece enable fin enable psh enable rst enable syn enable urg
enable
  collect add timestamp sys-uptime first
  collect add timestamp sys-uptime last
  collect add counter packets long
  collect add datalink mac source
  collect add datalink mac destination
  collect add datalink vlan
  collect add interface output physical width 4
  collect add ipv4 tos
  collect add ipv4 version
  collect add ipv4 fragmentation id
  match add ipv4 protocol
  match add ipv4 source address
  match add ipv4 destination address
```

match add transport source-port
match add transport destination-port

Associate record with **monitor** and define **timeouts:**

apps netflow monitor alias Netflow
description "test of netflow"
cache timeout active 300
cache timeout inactive 30
cache timeout event transaction-end
record add Netflow_v9

Define **exporter**:

apps netflow exporter alias export1
destination ip4addr 192.168.47.80
dscp 0
netflow-version netflow
transport udp 3002
template-refresh-interval 600
ttl 64

Configure **network map** to create a connection between the network and port tunnel (port tunnel can work as a destination for flow):

map alias Netflow
type regular byRule
roles replace admin to owner_roles
comment "to flowmon"
use gsop netflow
rule add pass ipver 4
to 1/1/x8
from 1/1/x1

nProbe

```
nprobe -G -q 10.50.9.60:6002 -n 10.50.9.115:3002 -i eth3 -t 300 -d 30 -l 30 -b 1
--biflows-export-policy 0 -e 50 -V 10 --vlanid-as-iface-idx outer --tunnel
--account-l2 -L 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 -S 1:1 -T "%IPV4_SRC_ADDR
%IPV4_DST_ADDR %IPV4_NEXT_HOP %INPUT_SNMP %OUTPUT_SNMP %IN_PKTS %IN_BYTES %L4_SRC_PORT
%L4_DST_PORT %TCP_FLAGS %PROTOCOL %SRC_TOS %IPV4_SRC_MASK %IPV4_DST_MASK %IN_SRC_MAC
%OUT_DST_MAC %SRC_VLAN %DST_VLAN %IPV6_SRC_ADDR %IPV6_DST_ADDR %IPV6_SRC_MASK
%IPV6_DST_MASK %ICMP_TYPE %SRC_AS %DST_AS %FRAME_LENGTH %FLOW_START_MILLISECONDS
%FLOW_END_MILLISECONDS %PACKETS_OBSERVED"
```

Reference:

https://github.com/ntop/nProbe/raw/master/doc/nProbe-UsersGuide.pdf

VMware NSX

1. Login to vCenter
2. Choose a switch, select Manage > Netflow
3. Setup IP address of collector and switch
   set port to 3000
   set active timeout to 300
   set inactive to 30
4. Enable NetFlow monitoring on dvPortGroup corresponding to the Logical Switch
5. Enable NetFlow export and save changes
6. Enable NetFlow on the dvUplink
7. Finally, enable NetFlow export on NSX
   Home > NSX Edges > Flow Monitoring > IPFIX > Edit

Visit support portal for more detailed configuration
https://support.flowmon.com/download.php?did=1701

Extreme Networks

Extreme Networks S-Series, K-Series and N-Series support NetFlow. ExtremeSwitching 8000-Series, Ethernet Routing Switch (ERS) 4900 and ERS 5900 support sFlow and IPFIX.

The following sample configuration is capturing data for Netflow on ge.2.110, and it is sending it to the Netflow collector at 10.20.30.40 on UDP port 2055:

 # netflow
set netflow export-interval 1
set netflow export-destination 10.20.30.40 2055
set netflow export-version 9
set netflow port ge.2.110 enable both
set netflow template refresh-rate 600 timeout 1
set netflow cache enable
!
end

and it is also necessary to include the "primary" and "management" values on your default interface:

interface vlan.0.192
 ip address 192.168.0.1 255.255.254.0 primary management
 no shutdown
 exit

Reference:
https://gtacknowledge.extremenetworks.com/articles/How_To/Sample-Netflow-Config
https://www.extremenetworks.com/products/extremeswitching/