How to config Netflow monitor

DOCUMENT VERSION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR/EDITOR
0.9	10/01/2024	1 st . version	Jacky.zou, Spencer.hung
			Nickle.Wu, Double.lin

Contents

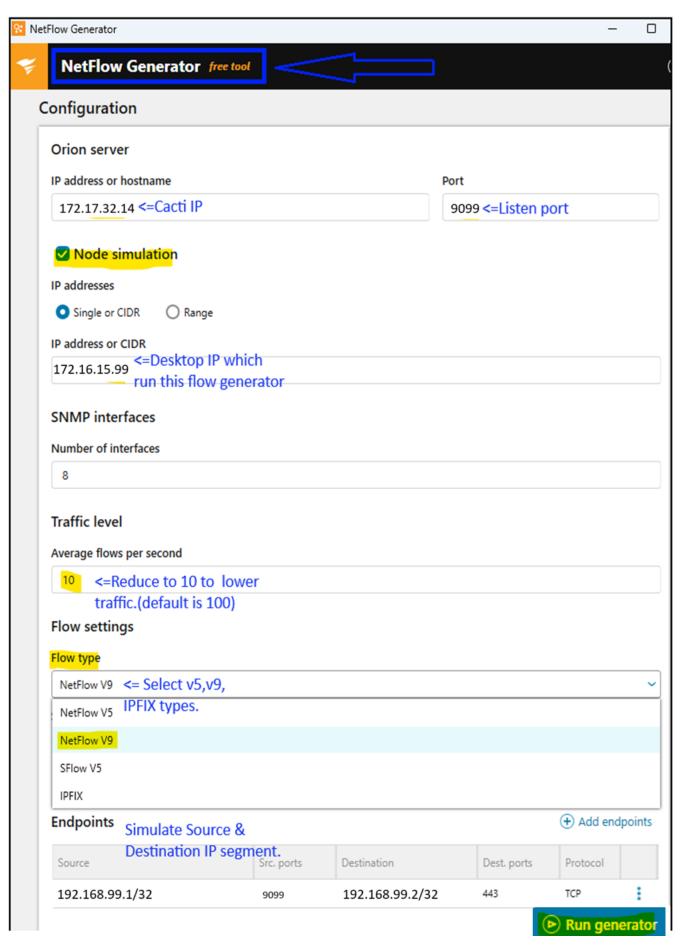
1	Config	ure flowview monitor	2
		Configure flowview generator simulator	
		Configure listeners	
		Configure filters	
	1.4	Statistical Report	6
	1.5	Check DB size & Row numbers	6
	1.6	Sample flow export configuration on Cisco SW & Fortigate	6

1 Configure flowview monitor

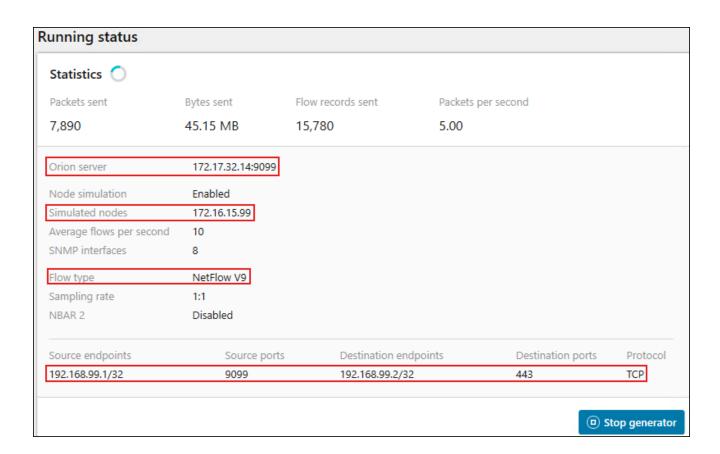
Steps: Configure Netflow Generator (simulator) Listener => Configure filter => view flow status

1.1 Configure flowview generator simulator

Download and Configure NetFlow Generator to create test flow source traffic on UDP port 9099, version 9



Start generating flow v9 traffics...



1.2 Configure listeners

Configure folwview generator to create test flow traffic on UDP port 9099 (v9)





systemctl status flow-capture

```
flow-capture.service - Flow Capture Service for Cacti
Loaded: loaded (/etc/systemd/system/flow-capture.service; enabled; preset: disabled)
Active: active (running) since Mon 2024-09-30 17:10:10 CST; 24min ago
Main PID: 2499 (php)
Tasks: 2 (limit: 153762)
Memory: 40.5M
CPU: 13.356s
CGroup: /system.slice/flow-capture.service
-2499 /usr/bin/php -q /usr/share/cacti/plugins/flowview/service/flow-capture --systemd
-2501 /usr/bin/php -q /usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1

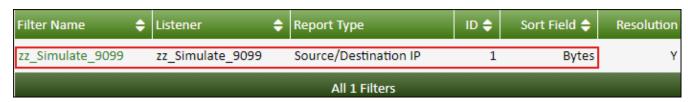
sep 30 17:10:10 twtpsvhq014.tpvaoc.com systemd[1]: Started Flow Capture Service for Cacti.
sep 30 17:10:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Starting Flow Collection
sep 30 17:10:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Launching cacti-flow-capture as '/usr/share/cacti/plugins/flowview/flow_collector.php --listener-id=1
sep 30 17:10:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:20:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
sep 30 17:30:11 twtpsvhq014.tpvaoc.com php[2499]: NOTE: Checking for new or gone listeners
```

1.3 Configure filters

Create filters map to listeners, "Stream Address" IP & Max. Row "Top 15" must be assigned to increase stability.

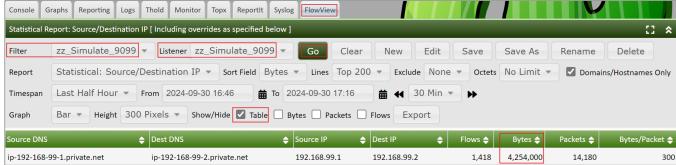


Result



1.4 Statistical Report





1.5 Check DB size & Row numbers

#Show flowview DB table size & row number

mysql -uroot -e "SELECT t.table_name AS \`Table\`, ROUND(((t.data_length + t.index_length) / 1024 / 1024), 2) AS \`Size (MB)\`, t.table_rows AS \`Rows\` FROM information_schema.tables t WHERE t.table_schema = 'flowview' ORDER BY (t.data_length + t.index_length) DESC;"

ONDER DT (t.data_longtit > t.index_longtit) DE00;		
Table	Size (MB)	Rows
plugin_flowview_irr_inetnum	6468.88	6076708
plugin flowview irr route	1099.82	4165912
plugin flowview raw 202421511	675.35	2458674
plugin flowview raw 202421510	669.52	2433973
plugin_flowview_raw_202421500	669.21	2435004
plugin flowview raw 202421509	666.79	2422586
plugin flowview raw 202421508	666.03	2419226
plugin flowview raw 202421507	662.62	2404484
plugin flowview raw 202421505	661.58	2400437
plugin flowview raw 202421504	661.52	2400879
plugin flowview raw 202421506	661.32	2399050
plugin flowview raw 202421501	660.09	2398581
plugin flowview raw 202421502	657.93	2389060
plugin flowview raw 202421503	655.13	2378987
plugin flowview raw 202421423	515.02	1878653
plugin flowview irr domain	485.66	1183215
plugin_flowview_irr_role	68.68	146182

1.6 Sample flow export configuration on Cisco SW & Fortigate

Cisco Switch:

```
flow record TPV-Flow-Record
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface input
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface output
ļ
flow record TPV-Flow-Record-OUT
match ipv4 destination address
match ipv4 source address
match transport source-port
match transport destination-port
match ipv4 protocol
match interface output
match ipv4 tos
match flow direction
collect counter bytes long
collect counter packets long
collect transport tcp flags
collect timestamp absolute first
collect timestamp absolute last
collect interface input
!
flow exporter FNFexp
destination 172.17.32.16
source Vlan99
transport udp 2055
!
flow exporter test
destination 172.17.32.14
source Vlan99
transport udp 2055
```

```
flow monitor FlowMonitor1
exporter FNFexp
exporter test
record TPV-Flow-Record
flow monitor FlowMonitorOUT
exporter FNFexp
exporter test
record TPV-Flow-Record-OUT
ļ
sampler sampler1
description sample at 50%
mode random 1 out-of 2
interface GigabitEthernet1/1/2
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active
interface GigabitEthernet2/1/2
switchport trunk allowed vlan 99
switchport mode trunk
ip flow monitor FlowMonitor1 sampler sampler1 input
ip flow monitor FlowMonitorOUT sampler sampler1 output
channel-group 2 mode active
```

Fortigate Firewall:

FG3H1E5819903613 (global) # show system netflow config system netflow set collector-ip 172.17.32.14 set collector-port 9005 set source-ip 172.17.32.100 set active-flow-timeout 60 set inactive-flow-timeout 10 end

FG3H1E5819903613 (global) # show system interface "port3" config system interface

```
edit "port3"
     set vdom "root"
     set ip 172.17.32.100 255.255.255.0
     set allowaccess ping https snmp
     set type physical
     set netflow-sampler both
    set sflow-sampler enable
    set sample-rate 50
     set explicit-web-proxy enable
     set description "LAN"
     set alias "lan"
     set device-identification enable
    set role lan
     set snmp-index 5
  next
end
```