How to Enable Netflow export on Cisco SW & Fortigate

By Spencer.Hung 10/1/2024

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
!
!
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
!
!
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
```