# How To Configure Switches And Routers To Send NetFlow Data To Nagios Network Analyzer 2026

## Purpose

This document describes how to configure switches and routers to send NetFlow data to a Nagios Network Analyzer 2026 instance.

## Considerations

All the following examples will be sending UDP traffic on a specific, uncommon port. This means that any firewall devices between your sending devices and Nagios Network Analyzer will need to allow this traffic. Each individual NetFlow source will need to be sending the data on a different port, so you will need to be aware of which ports are currently being used for existing NetFlow sources when adding new sources. This document provides examples for several devices, other models and manufacturers commands and directions may vary.

## Configuring A Cisco 2600 Series Router

You will need to enable NetFlow on each individual interface that you want to collect statistics on. In the following example, the interface that is being configured is `Ethernet0/0`. The Nagios Network Analyzer server is at `192.168.5.191` and NetFlow information will be sent on port `9912`.

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9912`.

Please execute the following commands from the exec command prompt:

```
enable
configure terminal
interface Ethernet0/0
ip route-cache flow
exit
ip flow-export 192.168.5.191 9912 version 5
exit
clear ip flow stats
```

Now all traffic flowing through interface `Ethernet0/0` will be analyzed by the Cisco device and will be sent to the Nagios Network Analyzer for further processing. Be sure to save the config once you have determined the proper functionality of exporting the NetFlow data.

## Configuring A Cisco ASA Series Firewall

These settings will allow terminal based configuration of most Cisco ASA devices. In this particular example, the flows are being exported to the collector at `192.168.5.191` on port `9911`. Specifies a one-minute schedule of sending data to the collector. It also allows for multiple smaller flows to be included in a single transmission. The NetFlow syslogging functionality is also disabled, although this is entirely optional. An access-list is created to allow NetFlow traffic to be collected on all interfaces. A new classmap is also created for NetFlow exporting, that matches the access-list. The global-policy policy-map is entered and maps the netflow-export-class to the global-policy. Finally setting all NSEL types to be exported to the collector server.

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9911`.

```
enable
configure terminal
flow-export destination inside 192.168.5.191 9911
flow-export template timeout-rate 1
flow-export delay flow-create 60
logging flow-export-syslogs disable
access-list netflow-export extended permit any any
class-map netflow-export-class
match access-list netflow-export
policy-map global-policy
class netflow-export-class
flow-export event-type all destination 192.168.5.191
exit
```

Now all NetFlow data is configured to be sent to the Network Analyzer collector for further analysis.

## Configuring A Cisco 4500 Series With WS-X45-SUP8-E Supervisor Engine

These settings are for a Cisco 4500 Series With WS-X45-SUP8-E Supervisor Engine. In this particular example, the flows are being exported to the collector at `192.168.5.191` on port `9913`. This example only sends the flow information for the interface called `GigabitEthernet 1/3/1`.

```
flow exporter e1
!
destination 192.168.5.191
transport udp 9913
!
flow record r1
match ipv4 source address
match ipv4 destination address
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor m1
record r1
exporter e1
cache timeout active 60
cache timeout inactive 30
cache entries 1000
!
interface GigabitEthernet 1/3/1
ip flow monitor m1 layer2-switched input
!
```

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9913`.

Now all NetFlow data is configured to be sent to the Network Analyzer collector for further analysis.

## Configuring A Cisco 3850

These settings are for a Cisco 3850. In this particular example, the flows are being exported to the collector at `192.168.5.191` on port `9914`. This example only sends the flow information for the interface `vlan 1`.

```
flow record Netflow1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match flow direction
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
!
flow exporter Netflow-to-Nagios
destination 192.168.5.191
transport udp 9914
flow monitor Netflow1
exporter Netflow-to-Nagios
cache timeout active 60
record Netflow1
vlan configuration 1
ip flow monitor Netflow1 input
```

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9914`.

Now all NetFlow data is configured to be sent to the Network Analyzer collector for further analysis.

## FortiGate v5.2 And FortiGate v5.4 Devices

These settings are for FortiGate v5.2 and FortiGate v5.4 devices. In this particular example, the flows are being exported to the collector at `192.168.5.191` on port `9915.` You will need to change `<interface name>` to suit your environment.

Configuring the NetFlow collector IP:

```
config system netflow
set collector-ip 192.168.5.191
set collector-port 9915
end
```

Enabling NetFlow on the Interface:

```
config system interface
edit <interface name>
set netflow-sampler both
end
```

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9915`.

Now all NetFlow data is configured to be sent to the Network Analyzer collector for further analysis.

## Fortinet VDOM Environments

These settings are for Fortinet VDOM Environments. In this particular example, the flows are being exported to the collector at 192.168.5.191 on port 9916. Refer to the comments in these commands to see what specific options need defining.

### Configuring The Global Config:

```
con global
con sys netflow
set collector-ip 192.168.5.191
set collector-port 9916
set source-ip <source-ip>
end
end
```

### Configure The VDOM:

```
con vdom
edit root ----> root is an example, change to the required VDOM name
con sys interface
edit wan1 ----> change the interface to the one to be used
set netflow-sampler both
end
```

**Note:** You will want to replace your Nagios Network Analyzer IP address for `192.168.5.191` and the specific port you want to use for `9916`.

Now all NetFlow data is configured to be sent to the Network Analyzer collector for further analysis.

## More Information

To learn how to set up your source on the Network Analyzer side of things, you can review this document:

Understanding Sources and Source Groups in Network Analyzer

## Finishing Up

This completes the documentation on configuring switches and routers to send NetFlow data to a Nagios Network Analyzer instance. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum  Visit Nagios Knowledge Base  Visit Nagios Library