

# Configuring and Troubleshooting NetFlow for Cisco Stealthwatch

The purpose of this document is to describe configuration for NetFlow-enabled network devices for Stealthwatch to collect and analyze telemetry.

Version control.....	2
Introduction .....	3
Cisco Stealthwatch Enterprise .....	3
Cisco NetFlow Configuration examples .....	7
Troubleshooting NetFlow export in Cisco StealthWatch Enterprise .....	13

## Version control

Date	Version	Author	Detail	Reviewed By
10/10/16	1.0	Jonathan Stevenson, Hanna Jabbour	Initial Release	Jonathan Stevenson Hanna Jabbour Eric Rennie David Butler Richard Laval
10/2/18	1.1	Jonathan Stevenson, Hanna Jabbour	Updated release	

## Introduction

Cisco Flexible NetFlow; often referred to as FnF is the latest iteration of Cisco's embedded instrumentation protocol. NetFlow leverages IP information flowing across a network device to build a report of infrastructure activity such as users accessing your application, email or web services. NetFlow v9 is especially useful as compared with previous versions due to its extensibility by leveraging the use of templates. NetFlow v9 is the IETF standard mechanism for information export.

This guide is not meant as a comprehensive guide to Cisco NetFlow, TrustSec, or NBAR. The purpose of this document is to help configure Cisco IOS to leverage these protocols and technologies when used in conjunction with Cisco Stealthwatch. For a more complete guide on the Cisco technologies covered here, please refer the following links;

Cisco Systems NetFlow Services Export Version 9 RFC  
<https://www.ietf.org/rfc/rfc3954.txt>

Introduction to Cisco IOS NetFlow – A Technical Overview;  
[http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod\\_white\\_paper0900aecd80406232.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html)

Cisco TrustSec;  
<http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html>

Cisco NBAR2;  
[http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa\\_c67-697963.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/network-based-application-recognition-nbar/qa_c67-697963.html)

Configuring NSEL on Cisco ASA;  
[http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor\\_nsel.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_nsel.html)

## Cisco Stealthwatch Enterprise

Cisco Stealthwatch is a security analytics solution that leverages enterprise telemetry from the existing network or public cloud infrastructure. It provides advanced threat detection, accelerated threat response and simplified network segmentation using multi-layer machine learning and entity modeling. With a single, agentless solution, you get visibility across the extended network including endpoints, branch, data center and cloud. And it is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.

It consumes information about the traffic that is passing through the devices in the network such as routers, switches and firewalls. Stealthwatch can analyze enterprise telemetry from any source (NetFlow, IPFIX, sFlow, other Layer 7 protocols) across the extended network, to provide real-time visibility into assets that are using the network, while profiling each of these assets. It provides visibility into the east-west traffic in an enterprise network (in addition to north-south traffic) and analyzes network behavior to detect policy violations, anomalies as well as data consumption in the network. This document covers Stealthwatch configuration for NetFlow enabled network devices.

### Aggregation and correlation

The flow or telemetry represents unidirectional accounting information about the traffic that is passing through a network device and is stored at the level of the flow capable device for a period of time until timeout or until the flow ends. This flow will then be exported into Stealthwatch that will correlate flows from multiple devices and interfaces and perform stitching and de-duplication action to provide a single bidirectional flow of the traffic end-to-end.

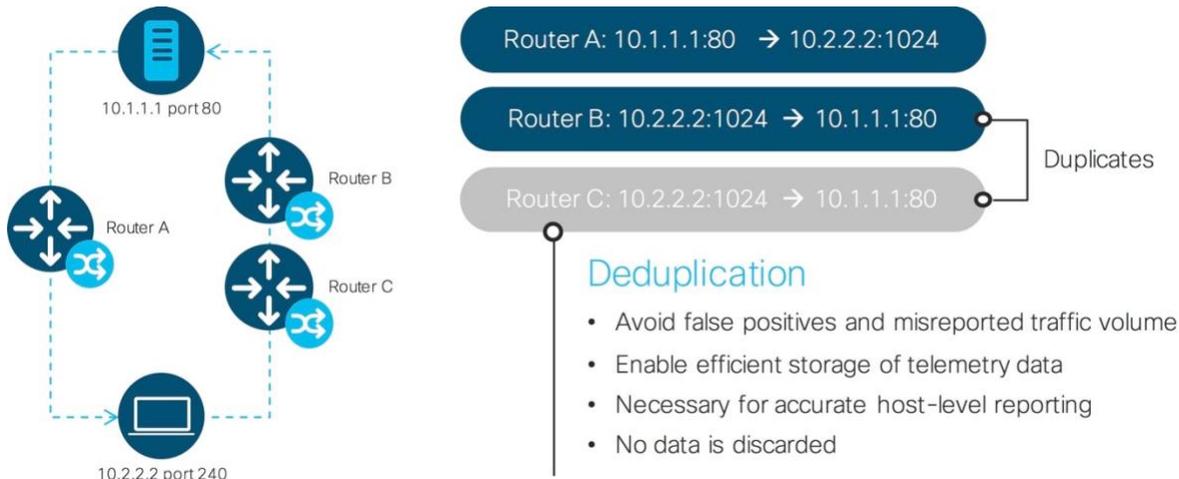


Figure 1: Scaling and Optimization: Deduplication

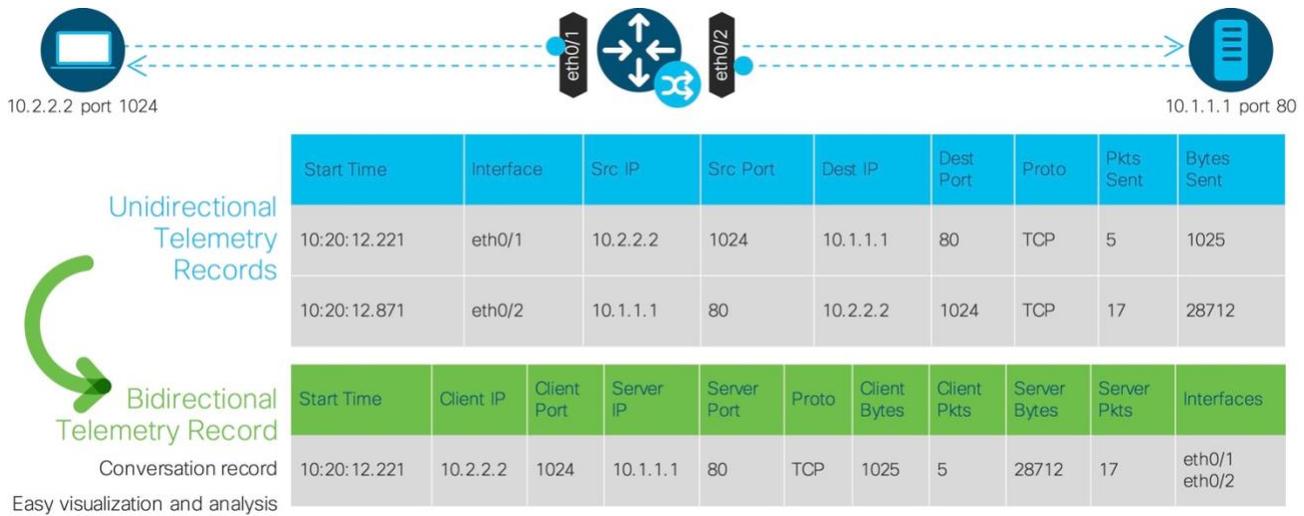


Figure 2: Scaling and Optimization: Restitching

### Anomaly and threat detection

Stealthwatch Enterprise applies advanced security analytics in the form of **entity modeling**. The telemetry from the existing network is collected and optimized. Multiple heuristics, also known as Security Events are applied to be able to detect anomalous network behavior, and these are then associated with specific hosts. This results in high level alarm categories, so that security teams can prioritize risks and trouble-shoot issues easily.

Stealthwatch Enterprise also integrates with a cloud based multi-stage machine learning analytics engine, that correlates threat behaviors seen in the local environment with those seen globally. It employs a funnel of analytical techniques to detect advanced threats.

Figure 3: Detect anomalies and threats



For more information about the Stealthwatch components and architecture, please refer to the [Stealthwatch Enterprise Data Sheet](#).

### Cisco IOS Flexible NetFlow Configuration

As mentioned earlier, Stealthwatch can collect NetFlow telemetry from network devices to analyze it for anomaly and threat detection, and provide end-to-end visibility across the extended network. The network device needs to be configured for Stealthwatch to collect NetFlow.

Netflow configuration on a Cisco device consists of four steps:

- Define a Flow Record
- Configure a Flow Exporter
- Configure a Flow Monitor
- Apply the Flow Monitor on an interface

### Define a Flow Record

The Flow Record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. If you would like to build a custom Flow Record outside of the predefined netflow-original, you would specify a series of match and collect commands that tell the device what fields to include in the outgoing NetFlow PDU.

The match fields are the key fields. They are used to determine the uniqueness of the flow. The collect fields are just extra info that we include to provide more detail to the Stealthwatch Flow Collector for reporting and analysis.

You shouldn't need to modify the match fields a lot. The seven match entries shown below should always be included in your config. The collect fields however can vary quite a bit depending on how much info you want to send to the collector.

The configuration listed below is recommended for Stealthwatch installations.

The fields marked as "required" below, are necessary for Stealthwatch to accept and build a flow record.

```
flow record STEALTHWATCH1
match ipv4 protocol (required; key field)
match ipv4 source address (required; key field)
match ipv4 destination address (required; key field)
```

```
match transport source-port      (required; key field)
match transport destination-port (required; key field)
match interface input            (required; key field)
match ipv4 tos                   (required; key field)
collect interface output         (required; key field)
collect counter bytes            (required; key field)
collect counter packets          (required; key field)
collect timestamp sys-uptime first (required; for calculating duration)
collect timestamp sys-uptime last (required; for calculating duration)
collect routing next-hop address ipv4 (optional; used for closest interface determination)
collect ipv4 dscp                (optional; used for closest interface determination)
collect ipv4 ttl minimum         (optional; used for closest interface determination)
collect ipv4 ttl maximum         (optional; used for closest interface determination)
collect transport tcp flags      (optional; used for closest interface determination)
collect routing destination as    (optional; used for closest interface determination)
```

## Define a Flow Exporter

Once the Flow Record has been created you would tie it to a Flow Exporter.

Flow Exporter configuration defines the physical or virtual Flow Collector IP Address to which NetFlow data is sent. It also defines the source interface from which the Flow Exporter device will send NetFlow data, this can be a physical or logical address; it is also worth considering using a Loopback interface to source NetFlow data from as a Loopback typically will remain up even when other interfaces fail therefore enabling continuous transport (where routing permits) This is also where the transport protocol (TCP or UDP) and destination port is defined; the destination port is specific to the NetFlow Collector and in this case refers to the port used by the Stealthwatch Flow Collector.

To define a Flow Exporter, follow these steps:

```
flow exporter Stealthwatch_Exporter
description Stealthwatch Export to Flow Collector
destination [Collector_IP_Address]
source [Physical Interface | Logical Interface]
transport udp 2055
```

## Define a Flow Monitor

A Flow Monitor ties all of the construct together, referencing the Flow Exporter and the Flow Record. To define a Flow Monitor, follow these steps:

```
flow monitor Stealthwatch_Monitor
description Stealthwatch Flow Monitor
exporter Stealthwatch_Exporter
cache timeout active 60
record STEALTHWATCH1
```

Note the cache timeout line above, this is the recommended setting for Stealthwatch. The default setting on Cisco devices is 30 minutes which is too long for anomaly reporting.

The Flow Monitor configuration ties the previously configured Flow Exporter and Flow Record together, the naming convention can be whatever you chose providing you refer to the correct name; using context sensitive help in IOS will help as it will always show any previously configured parameters.

See below for an example of how context sensitive help reminds you of configured Flow Records and Flow Exporters as well as system default Records which are available.

```
BR_ASW1(config)#flow monitor STEALTHWATCH_MONITOR
BR_ASW1(config-flow-monitor)#record ?
```

```
STEALTHWATCH_RECORD User defined
wireless Templates for Wireless Traffic
BR ASW1(config-flow-monitor)#exporter ?
STEALTHWATCH_EXPORTER Stealthwatch Export to Flow Collector
```

## Apply the Flow Monitor to interfaces

Finally, you need to apply all of the above NetFlow configuration to each interface on which you require flow analysis with the following:

```
interface [Interface_ID]
ip flow monitor Stealthwatch_Monitor input
```

## Cisco NetFlow Configuration examples

Below are examples of Netflow configurations. Commands for configuring NetFlow record fields may differ, depending on platform.

```
flow record Stealthwatch_FlowRecord
description Flow Record for Export to Stealthwatch (optional)

match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match ipv4 tos
match transport source-port
match transport destination-port
match interface input
match flow direction
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 ttl minimum
collect ipv4 ttl maximum
collect transport tcp flags
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

### TrustSec Specific Match Fields

```
match flow cts source group-tag
match flow cts destination group-tag
```

### NBAR2 Specific collection (where protocol pack is active on router)

```
collect application name
collect application http url
collect application http host
```

### AVC Specific fields

```
collect connection initiator
collect connection new-connections
collect connection sum-duration
collect connection delay response to-server sum
```

```
collect connection delay response to-server min
collect connection delay response to-server max
collect connection server counter responses
collect connection delay response to-server histogram late
collect connection delay network to-server sum
collect connection delay network to-client sum
collect connection client counter packets retransmitted
collect connection delay network client-to-server sum
collect connection delay application sum
collect connection delay application min
collect connection delay application max
collect connection delay response client-to-server sum
collect connection transaction duration sum
collect connection transaction counter complete
collect connection server counter packets long
collect connection client counter packets long
collect connection client counter bytes retransmitted
collect connection server counter bytes network long
collect connection client counter bytes network long
collect connection delay network client-to-server num-samples
collect connection delay network to-server num-samples
collect connection delay network to-client num-samples
```

## Debug Commands

The following commands are available when checking the operation of NetFlow on a Cisco router or switch;

```
show flow exporter - Flow Exporter information
show flow interface - Flow interface information
show flow internal - Show the flow fields
show flow monitor - Flow Monitor information
show flow record - Show Flow Record configuration
show flow ssid - SSID Interface Information
```

## Configuring IOS NetFlow on Catalyst 3k Switch (3650 tested)

The structure of creating a NetFlow configuration on Catalyst 3k is very much the same as above with routing platforms, the Match fields are identical. There are some subtle differences with the Collect fields, the following fields are supported in Stealthwatch deployments.

```
flow record Stealthwatch_FlowRecord
description Flow Record for Export to Stealthwatch (optional)

match ipv4 source address
match ipv4 destination address
match ipv4 protocol
match ipv4 tos
match ipv4 ttl
match transport source-port
match transport destination-port
match interface input
match flow direction
match datalink mac source address input
match datalink mac destination address output
match datalink vlan input
collect transport tcp flags
collect interface input
```

```
collect interface output
collect counter bytes' long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

#### TrustSec specific Match fields;

```
match flow cts source group-tag
match flow cts destination group-tag
```

Configuring the Flow Exporter and Flow Monitor details are identical to the commands for routing platforms.

It is worth noting that should you ever need to edit a Flow Record on a platform, you will need to temporarily remove the reference to it in the Flow Monitor configuration with the 'no' keyword.

### Configuring IOS NetFlow on Catalyst 6k Switch (6880X - SUP-2T)

```
flow record STEALTHWATCH_RECORD
description Flow Record for Export to Stealthwatch
match datalink vlan input
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 routing next-hop address ipv4
collect transport tcp flags
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp sys-uptime first
collect timestamp sys-uptime last
```

Configuring the Flow Exporter, Flow Monitor and applying to an interface is identical to the commands shown previously.

### Configuring NetFlow on Cisco Nexus 7k (SUP-1)

Netflow on the Nexus platform is somewhat different, firstly you need to enable the feature and set some timeout parameters with the following;

```
feature netflow
flow timeout active 60
flow timeout inactive 15
```

So, as we did with the previous sections we configure a Flow Record, a Flow Exporter and Flow Monitor as follows;

```
flow record Stealthwatch_FlowRecord
description Flow Record for Export to Stealthwatch (optional)

match ipv4 source address
match ipv4 destination address
match ip protocol
match ip tos
```

```
match transport source-port
match transport destination-port
```

(Notice the match protocol and tos statements are not IPv4 specific)

```
collect routing next-hop address ipv4
collect transport tcp flags
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last

flow exporter Stealthwatch_Exporter
description Stealthwatch Export to Flow Collector
version 9
destination [Collector_IP_Address]
source [Physical_Interface | Logical_Interface]
transport udp 2055
```

(note that the NetFlow version must be specified under the Exporter configuration)

```
flow monitor Stealthwatch_Monitor
description Stealthwatch Flow Monitor
exporter Stealthwatch_Exporter
record Stealthwatch_Record

interface eth3/1
 ip flow monitor STEALTHWATCH_MONITOR input
(Interface commands can optionally include a Sampler configuration)
```

## Configuring NSEL on Cisco ASA

Cisco's implementation of NetFlow on the ASA Firewall line of products differs than the configuration of NetFlow using NX-OS, XR IOS, and IOS. The use of ACL's and existing policy maps is required. Rather than NetFlow, the ASA series uses Network Secure Event Logging (NSEL)

### Global Configuration

```
flow-export destination inside [Flow Collector IP] 2055
flow-export delay flow-create 30
flow-export template timeout-rate 5
```

### Disable SysLog Messages (Optional)

```
logging flow-export syslog disable
```

### Create ACL for traffic to capture and apply it to a class map

```
access-list [NameofACL] extended permit ip any any
class-map [NameofClassMap]
match access-list [NameofACL]
```

Policy Map definition - you can use the global policy or an already existing policy rather than creating a new one

```
policy-map [PolicyMapName]
class [NameofClass]
flow-export event-type all destination [Flow Collector IP]
service-policy [PolicyMapName] global
```

### NetFlow Debug Commands

```
show flow-export counters - Displays runtime counters for NetFlow including statistics and errors
clear flow-export counters - Clears all runtime counters to zero
```

## Netflow with Encrypted Traffic Analytics (ETA) on Catalyst 9k example

When configuring ETA to work with Stealthwatch you will configure both a Flexible NetFlow Monitor (and enable ETA enhanced NetFlow export (for the ETA specific fields). The below configuration was validated with IOS v16.6.2

```
flow record ETA-C9K-RECORD
description Flow Record for ETA with Stealthwatch
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
collect timestamp absolute first
collect timestamp absolute last
!

flow exporter STEALTHWATCH-EXPORTER
description Send NetFlow to Stealthwatch.
destination <dest ip address>
source <source ip address/interface>
transport udp 2055
!

flow monitor ETA-FLOWMONITOR
description NetFlow Monitor for use with ETA
exporter STEALTHWATCH-EXPORTER
cache timeout active 60
record ETA-C9K-RECORD
!
interface GigabitEthernet1/0/1
description Uplink Interface
no switchport
ip flow monitor ETA-FLOWMONITOR input
ip flow monitor ETA-FLOWMONITOR output
!

et-analytics
ip flow-export destination <dest ip address> 2055
!

interface gigabitEthernet 1/0/2
description access layer interface
switchport
switchport access vlan 5
et-analytics enable
```

## Netflow with ETA on ASR/ISR/CSR

When configuring ETA to work with Stealthwatch you will configure both a Flexible NetFlow Monitor and enable ETA enhanced NetFlow export (for the ETA specific fields). The below configuration was validated with IOS v16.6.2

```
flow record ETA-ISR-RECORD
description Flow Record for ETA with Stealthwatch
```

```
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 routing source as
collect routing destination as
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 id
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination mask
collect transport tcp flags
collect interface output
collect flow sampler
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
collect application http url
collect application http host
```

```
!
!
```

```
flow exporter STEALTHWATCH-EXPORTER
description Send NetFlow to Stealthwatch.
destination <dest ip address>
source <source ip address/interface>
transport udp 2055
!
```

```
flow monitor ETA-FLOWMONITOR
description NetFlow Monitor for use with ETA
exporter STEALTHWATCH-EXPORTER
cache timeout active 60
record ETA-ISR-RECORD
!
```

```
interface GigabitEthernet1/0/1
description LAN facing Interface
no switchport
ip flow monitor ETA-FLOWMONITOR input
ip flow monitor ETA-FLOWMONITOR output
et-analytics enable
```

## Troubleshooting NetFlow export in Cisco StealthWatch Enterprise

This section introduces troubleshooting strategies when encountering problems with a Cisco Stealthwatch deployment. Cisco Stealthwatch system uses NetFlow exported from Cisco routers, switches, and ASA devices to provide traffic and security information for the customer about their network. NetFlow from these devices is exported either to a Stealthwatch Flow Collector, or to the Stealthwatch UDP Director which in turn forwards the NetFlow to the Flow Collector. The Flow Collector receives and analyses the NetFlow pdu's in the NetFlow export packets and saves consolidated flow data. It also sends consolidated data sets to the Stealthwatch Management Console (SMC). One SMC can manage many Flow Collectors. The customer uses a Web Interface or a Java based desktop client to communicate with the SMC to see the system data.

### Prerequisite Requirements

Readers of this document should be knowledgeable on these topics:

- Cisco device NetFlow export configuration for versions v5, v9, and Flexible NetFlow.
- Cisco ASA NetFlow export.

This troubleshooting covered in this document is based on version 6.2 and higher of Stealthwatch on any platform.

### Terminology;

- **Stealthwatch:** The Cisco StealthWatch system is minimally comprised of a Flow Collector and a Stealthwatch Management Console.
- **SMC:** Stealthwatch Management Console
- **SMC client:** Java based thick client that runs on the Customers desktop and communicates with the SMC server. The primary user is 'admin'.
- **Administrative Web Interface:** Each Stealthwatch device has a web UI used mainly for server administration and other tasks. The primary user is 'admin'.
- **CLI:** Stealthwatch devices can support SSH access to the Debian cli if it is enabled. Primary user is 'sysadmin'.
- **Exporter:** Any device that can export NetFlow.
- **UDP Director:** A packet forwarding appliance used to create multiple streams of NetFlow or combine streams of NetFlow on different ports to a single port.

## Summary of possible NetFlow export issues

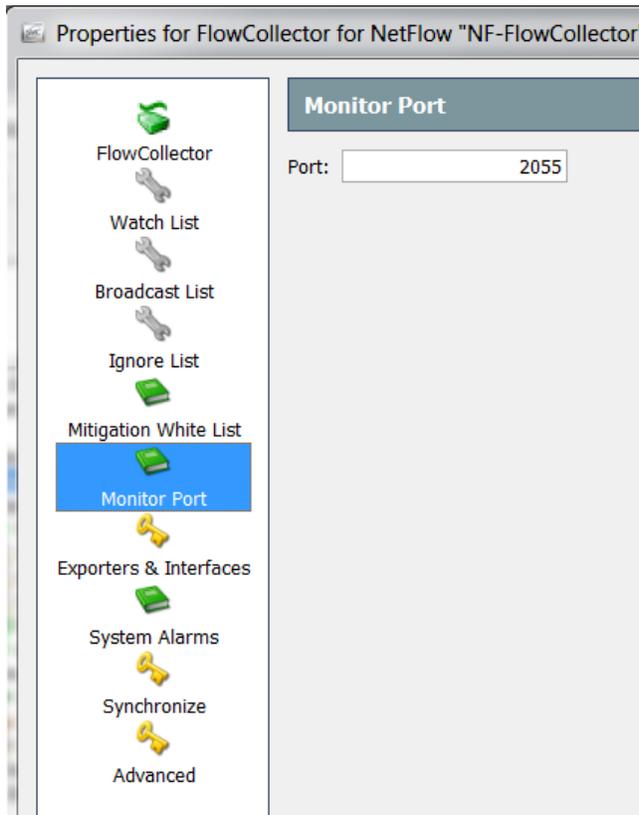
Problems with setting up NetFlow in a network for use by Stealthwatch usually fall into one of these three categories:

- 1) Configuration of the exporter to send NetFlow to the flow collector via the customer's network.
- 2) Transport of the exported UDP NetFlow packets via the network to the Flow Collector. The customer is the expert of their own network topology and packet transport, but Stealthwatch has useful tools to help the customer determine if NetFlow packets are reaching the Flow Collector. The Stealthwatch team can work with the customer if needed to use these tools. They are discussed below briefly.
- 3) NetFlow is reaching the Flow Collector but there are problems with the data interpretation, presentation, or recording of data. This is a Stealthwatch problem with a few exceptions caused by exporter configuration such as insufficient templates in V9 or FNF, incomplete NetFlow configuration of the exporter's interfaces, or limitations of NetFlow for certain hardware and exporter OS configurations and configurations.

## Exporter configuration for Stealthwatch

- The Flow Collector listens on port 2055, this Export Port is defined in the Flow Exporter config on a NetFlow capable Cisco device. Sometimes a customer may already have NetFlow enabled on a different port for previous products or may have different export ports

configured for each exporter. The Flow Collector can only listen on one port so the export port should be configured to match the listening port the Flow Collector is using. This listening port is configured for the Flow Collector within the SMC client here:

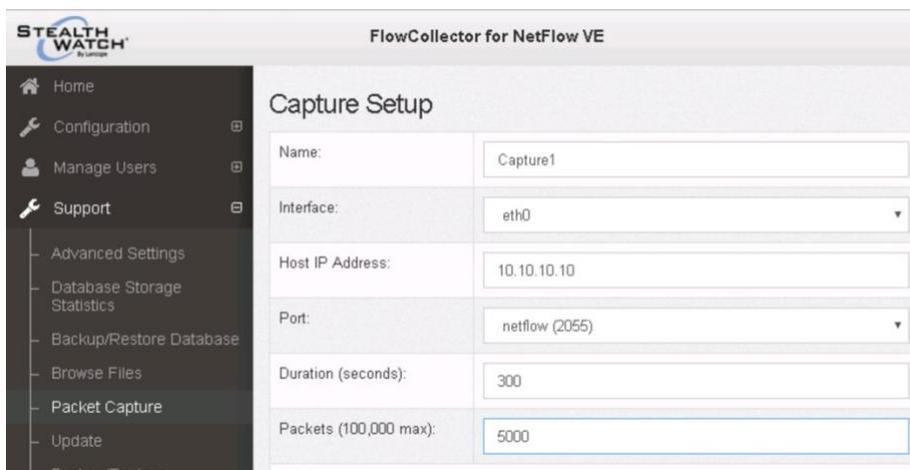


- The Flow Collector receives NetFlow traffic on the configured management interface IP. This IP should be used as the destination IP for the NetFlow export unless:
  - The Customer is using a UDP Director to steer traffic. Use its management IP then.
  - The Customer needs to receive the traffic in a subnet outside the management IP subnet. Each Flow Collector has at least one additional network interface and the Customer should have this additional network interface configured with an IP Address and connected to the network if they want to receive traffic in another subnet rather than routing it to the management interface IP.

### Troubleshooting NetFlow Transport

- The Flow Collector can be used to confirm NetFlow is being received at the Flow Collector interface and is properly configured to export on the correct port:
  1. The Administrative Web Interface of the Flow Collector has a front end GUI for tcpdump to see if NetFlow from an exporter is being received. Captures can be downloaded and analyzed with Wireshark or equivalent packet viewer to check the pdu's for missing required or optional fields. If the NetFlow is V9 based the capture needs to be big enough to capture template export.

Shown below is a capture setup for exporter IP 10.10.10.10 sending NetFlow on port 2055. If the capture is not incrementing packet then the NetFlow is not arriving or is not on the expected port.



### Troubleshooting NetFlow configuration using Stealthwatch

- The SMC has two documents that can report the NetFlow export status of exporters and the configuration of the exporter. As exporters are configured the NetFlow Collection Status document is useful to check which exporters are currently seen by the Flow Collector:

Summary							
Interface Count	Current NetFlow Traffic (bps)	Average NetFlow Traffic (bps)	Maximum NetFlow Traffic (bps)	Average Flow Rate (fps)	Total Flows		
NF-FlowCollector: 126	445.24k	345.14k	472.3k	434	413.85k		
Details - 9 records							
Exporter	Exporter Type	Average ...	Longest Duration Export ...	Average NetFlow Traffic...	Interface Count	Highest Current Utilization...	Highest Current Utilization ...
lchqgw01 (10.201.0.1)	Exporter	181	72	65.24k	8	10%	3%
10.202.3.112	FlowSensor	138	1.8k	189.68k	1	11%	0%
PrimaryASA (10.240.200.1)	Cisco ASA	107		66.45k		0%	0%
edge router (209.182.184.1)	Exporter	7	61	23.03k	3	1%	5%
10.203.9.100	FlowSensor VE	1		416	114	0%	0%
10.201.0.84	Exporter					0%	0%
citrix-netscaler.lancope.local (10.202.1.102)	Exporter					0%	0%
Catsk-ISE-Lab (10.203.0.3)	Exporter					0%	0%
10.202.3.114	FlowSensor VE			328		0%	0%

- The Flow Collector usually only needs ingress export from all interfaces on the exporter to create interface traffic data for inbound and outbound traffic. For devices that use logical interfaces enabling both may cause the Flow Collector to double report traffic stats in non-interface documents. We usually ask the Customer to choose which data set is most important.
- For each exporter the interface status document shows which interface is reporting traffic using NetFlow. Any interface that is missing inbound or outbound traffic is not configured properly. Any interface not showing here is not sending NetFlow. In the example below 16 interfaces are NetFlow configured. Notice that all are reporting inbound and outbound traffic.

Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic (...)	Maximum Utilization	Maximum Traffic (...)
Ichgwgw01 (10.201.0.1)	VI1	Inbound	1G	10.87%	108.74M	10.9%	108.96M
Ichgwgw01 (10.201.0.1)	VI240	Outbound	10M	4.13%	413.43k	5.35%	535.14k
Ichgwgw01 (10.201.0.1)	VI240	Inbound	10M	3.58%	358.25k	48.48%	4.85M
Ichgwgw01 (10.201.0.1)	VI203	Inbound	1G	1.19%	11.92M	1.25%	12.46M
Ichgwgw01 (10.201.0.1)	VI202	Outbound	1G	1.09%	10.89M	1.09%	10.89M
Ichgwgw01 (10.201.0.1)	VI202	Inbound	1G	0.6%	6.02M	0.72%	7.17M
Ichgwgw01 (10.201.0.1)	VI1	Outbound	1G	0.4%	4M	0.82%	8.17M
Ichgwgw01 (10.201.0.1)	ifIndex-0	Outbound	1G	0.29%	2.94M	0.31%	3.08M
Ichgwgw01 (10.201.0.1)	VI203	Outbound	1G	0.27%	2.69M	0.27%	2.69M
Ichgwgw01 (10.201.0.1)	VI232	Outbound	1G	0.14%	1.42M	0.14%	1.42M
Ichgwgw01 (10.201.0.1)	VI210	Outbound	1G	0.08%	829.14k	0.11%	1.06M
Ichgwgw01 (10.201.0.1)	VI232	Inbound	1G	0.05%	457.91k	0.06%	554.58k
Ichgwgw01 (10.201.0.1)	VI210	Inbound	1G	<0.01%	56.75k	0.01%	100.87k

- If packet capture from the Flow Collector confirms receipt of NetFlow from an exporter but the exporter is not listed in the NetFlow collection status document, an exporter of type unknown will show and an insufficient template configuration may be the cause.
- The Flow Collector supports NetFlow versions 5, 9, flexible NetFlow and IPFIX. Please refer to the Netflow configuration matrix and the Netflow configuration document for recommended NetFlow configurations for the Flow Collector. NetFlow V9 and FNF need to export these fields: <https://communities.cisco.com/docs/DOC-77020> & [https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco\\_NetFlow\\_Configuration.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf)

```

NF_F_LAST_SWITCHED(21)
NF_F_FIRST_SWITCHED(22)
NF_F_IN_BYTES(1)
NF_F_IN_PKTS(2)
NF_F_SRC_ADDR_IPV4(8)
NF_F_DST_ADDR_IPV4(12)
NF_F_PROTOCOL(4)
NF_F_L4_SRC_PORT(7)
NF_F_L4_DST_PORT(11)
Add these also for best operations:
NF_F_SRC_INTF_ID(10)
NF_F_DST_INTF_ID(14)
NF_F_TCP_FLAGS(6)

```

## Troubleshooting suspected insufficient template problems

The Flow Collector engine creates .log files in the /lancope/var/sw/data/ directory when insufficient templates are detected. The log file is created using the naming convention:

<exporter\_ip>\_<source\_id>\_<template\_id>.log.

Once per hour a templates file (templates.bin) is written out for properly configured exporters and a check is made to see if an insufficient template log file exists for that exporter template, and if so, it is removed. Once the template issues are resolved with the exporter and the templates from the exporter are accepted, the log files created for that exporter will be cleaned out of the system.

The Flow Collector web interface or a SSH session to the Flow Collector can be used to download and view these plain text files. If the Flow Collector web interface is used use the Support > Browse Files menu option to navigate to /sw/data:

The screenshot shows the 'FlowCollector for NetFlow VE' web interface. On the left is a navigation menu with options: Home, Configuration, Manage Users, Support, Advanced Settings, Database Storage Statistics, Backup/Restore Database, Browse Files (highlighted), and Packet Capture. The main content area is titled 'Browse Files (/sw/data)' and shows the current directory as '/sw/data'. Below this is a 'Parent Directory' section and a table of files:

	Name	Size	Last Modified
📁	db	-	Mar 6, 2018 9:59:02 AM UTC
📁	trends	-	Sep 19, 2017 4:00:00 AM UTC
📄	SWversion.log	138	Mar 6, 2018 9:46:59 AM UTC
📄	atm_status.txt	0	Mar 6, 2018 9:47:12 AM UTC
📄	templates.bin	13.39k	Oct 10, 2017 9:40:56 PM UTC

Below is an example of what the .log file is named and what the error messages look like when exporter 10.202.5.61, engine source ID (0), template ID 310 is sent to the Flow Collector, when only src and dest IP fields are specified in the template:

```
cat /lancope/var/sw/data/010.202.005.061_0_310.log
```

```
flow_src_addr: NF_F_SRC_ADDR_IPV6(27) specified  
flow_dst_addr: NF_F_DST_ADDR_IPV6(28) specified
```

If this template is for Stealthwatch flow creation, a flow end time field needs to be added. Please add one of the following fields:

```
NF_F_LAST_SWITCHED(21)  
NF_F_FLOW_END_SECONDS(151)  
NF_F_FLOW_END_MILLISECONDS(153)  
NF_F_FLOW_END_MICROSECONDS(155)  
NF_F_FLOW_END_NANOSECONDS(157)  
NF_F_FLOW_END_DELTA_MICROSECONDS(159)
```

If this template is for Stealthwatch flow creation, a flow start time field needs to be added. Please add one of the following fields:

```
NF_F_FIRST_SWITCHED(22)
  NF_F_FLOW_START_SECONDS(150)
  NF_F_FLOW_START_MILLISECONDS(152)
  NF_F_FLOW_START_MICROSECONDS(154)
  NF_F_FLOW_START_NANOSECONDS(156)
  NF_F_FLOW_START_DELTA_MICROSECONDS(158)
```

If this template is for Stealthwatch flow creation, a flow bytes field needs to be added. Please add the following field:

```
NF_F_IN_BYTES(1)
```

If this template is for Stealthwatch flow creation, a flow packets field needs to be added. Please add the following field:

```
NF_F_IN_PKTS(2)
```

If this template is for Stealthwatch flow creation, a flow protocol field needs to be added. Please add the following field:

```
NF_F_PROTOCOL(4)
```

If this template is for Stealthwatch flow creation, a flow source port field needs to be added. Please add one of the following fields:

```
NF_F_L4_SRC_PORT(7)
  NF_F_TRANSPORT_TCP_SRC_PORT(182)
  NF_F_TRANSPORT_UDP_SRC_PORT(180)
```

If this template is for Stealthwatch flow creation, a flow destination port field needs to be added. Please add one of the following fields:

```
NF_F_L4_DST_PORT(11)
  NF_F_TRANSPORT_TCP_DST_PORT(183)
  NF_F_TRANSPORT_UDP_DST_PORT(181)
```

If this template is for Stealthwatch flow creation, a flow source interface field needs to be added. Please add the following field:

```
NF_F_SRC_INTF_ID(10)
```

If this template is for Stealthwatch flow creation, a flow destination interface field needs to be added. Please add the following field:

```
NF_F_DST_INTF_ID(14)
```

If this template is for Firewall event handling, a firewall event field needs to be added. Please add one of the following fields:

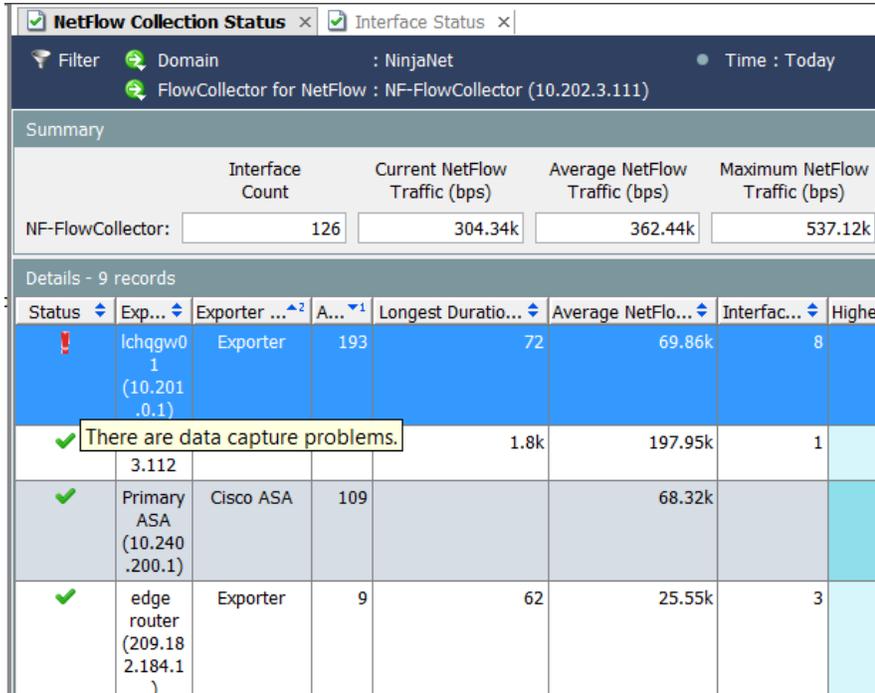
```
NF_F_ASA_FW_EVENT(40005)
  NF_F_FW_EVENT(233)
```

If this template is for Medianet event handling, please add one of the following fields:

```
NF_F_MEDIANET_TRANSPORT_ROUND_TRIP_TIME(37016)
  NF_F_MEDIANET_TRANSPORT_RTP_JITTER_MEAN(37023)
  NF_F_MEDIANET_TRANSPORT_PACKETS_LOST(37019)
```

### Troubleshooting other exporter issues with Stealthwatch

The Flow Collector does error checking on the NetFlow data to ensure the data values are within reason. Parameters like time, datagram sizes, etc. are checked and if any fail this check a status flag is raised indicating data capture problems. Stealthwatch discards the NetFlow pdu's which fail these tests. A common error would be an exported datagram with a time marked in the future. This would indicate time is not properly set on the exporter or the system time of the Flow Collector is not NTP sync'd. A NetFlow Collection Status document below shows such an error.



The screenshot shows the 'NetFlow Collection Status' window. At the top, it displays 'Domain : NinjaNet' and 'FlowCollector for NetFlow : NF-FlowCollector (10.202.3.111)'. Below this is a 'Summary' section with a table:

	Interface Count	Current NetFlow Traffic (bps)	Average NetFlow Traffic (bps)	Maximum NetFlow Traffic (bps)
NF-FlowCollector:	126	304.34k	362.44k	537.12k

Below the summary is a 'Details - 9 records' table:

Status	Exp...	Exporter ...	A...	Longest Duratio...	Average NetFlo...	Interfac...	High...
!	lchqgw01 (10.201.0.1)	Exporter	193	72	69.86k	8	
✓	There are data capture problems.			1.8k	197.95k	1	
✓	Primary ASA (10.240.200.1)	Cisco ASA	109		68.32k		
✓	edge router (209.182.184.1)	Exporter	9	62	25.55k	3	

Hovering over the status field will indicate the exporter problem. The Customer can double click the status cell and get additional details. Messages types, descriptions, and recommend actions that are displayed by the additional details are listed below:

Status Message	Description	Recommended Action
Exporter sent an invalid template	The minimum set of required fields were not defined in the template.	Make sure the NetFlow V9 template defines all the fields required by the StealthWatch FlowCollector for NetFlow.
Exporter sent invalid template data	The minimum set of required fields were not sent.	Make sure the exporter sends all the fields required by the template.
Inactive	Nothing received from the exporter in the past 5 minutes.	Ensure exporter is on-line.
Protocol 0 and Destination Address 0.0.0.0	The protocol is 0 and the destination IP address is 0 in a NetFlow record.	Check exporter; recycle exporter; contact exporter vendor with data information.
Unrealistic PDU Time	The timestamps in the NetFlow datagrams have greater than 120 seconds variance than the clock in the StealthWatch FlowCollector for NetFlow.	Verify exporter clock; verify the StealthWatch FlowCollector for NetFlow clock; verify that NTP is working properly in the network.
Unrealistic Packet/Octet Counts	The average packet size is greater than the architectural IPv4 MTU limit.	Check exporter; recycle exporter; contact exporter vendor with data information.
Unrealistic Start And End Flow Times	The end time in a NetFlow record is earlier than the start time.	Check exporter; recycle exporter; contact exporter vendor with data information.

### Summary

Customer interaction for exporter NetFlow configuration is usually limited to a few exporters in the early stages of a POC or after Stealthwatch purchase when they configure most exporters in their environment. We also see a small amount of exporter configuration activity from Customers as they add additional new sites or replace equipment through the lifecycle of the account. For any issues, please contact Stealthwatch Support for help.

### Resource

NetFlow Support Matrix (January 2018) - <https://communities.cisco.com/docs/DOC-77020>  
 Encrypted Traffic Analytics (ETA) - <https://www.cisco.com/go/eta>