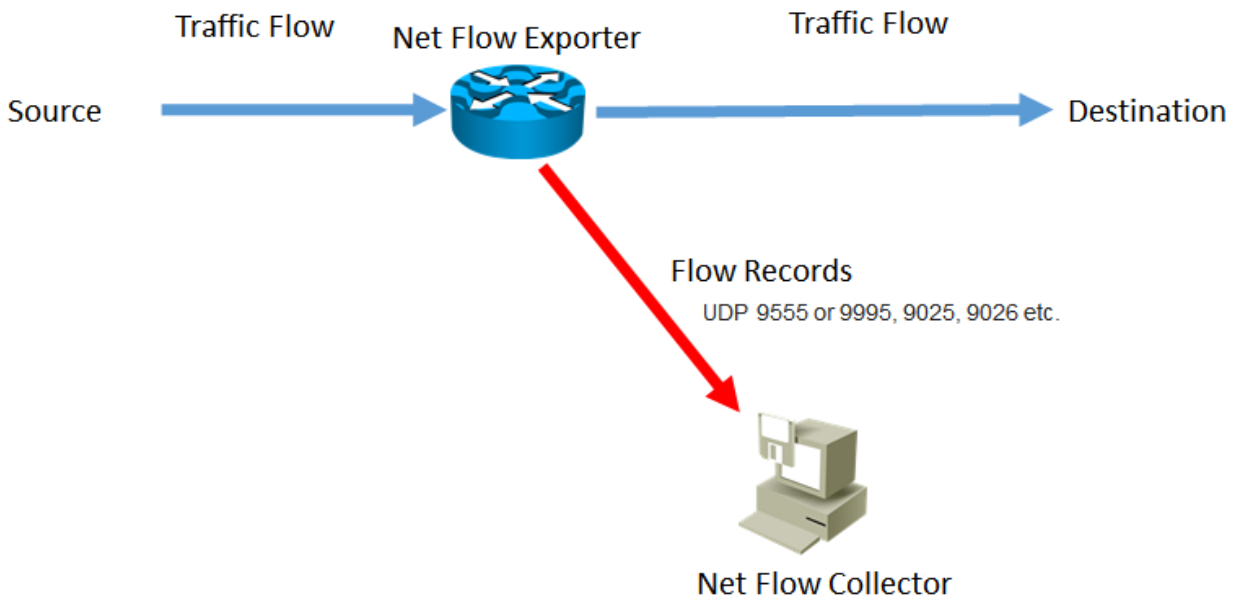
The Big Picture of Net Flow

We all know that Traffic from source to Destination go through Network infrastructure devices such as switches and routers , and normally we need a feature that can tell us some information about these traffics , information such as source / destination IP address/port numbers / Protocol used and more.



lets talk a little bit about above topology , Router will be configured as **Net Flow Exporter** to collect information about traffic going in , out or both to one of his interfaces , he will collect these information according to one or even all of the following 7 criteria (we call it **Net flow Records KEY fields**):

- IP source address
- IP destination address
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- Layer 3 protocol type
- Class of Service (IP Type of Service TOS)
- Router or switch Ingress (Input) interface

With these KEYs you will know the who, what and where of every conversation routed through that device.

Your router will continue to write these records for every conversation that goes through it.

Then he will cache these **IP Flows** information in his **internal cache** , then he will export these **Flows Records** to another device (using UDP port 9995,9555,9025,9026) normally a machine with Net Flow Collector software installed , we call this machine **Net Flow Collector**.

(router used to cahce and wait till session end then send flows collected about this session but nowadays they can even send flows when session still established)
Then Net Flow Collector will organize those flow records into an easy-to-read format and shows you these information in handy dashboard with many features to analysis it or even simply check Top 10 talkers to your router or Top 10 Protocols used…etc.

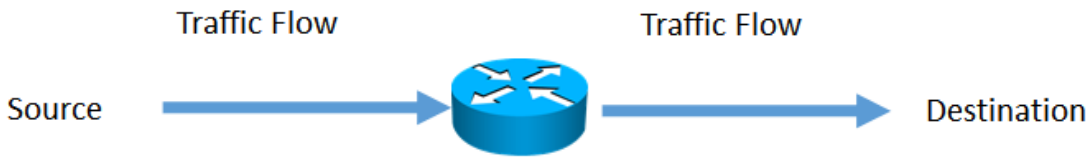
With some solutions , Net Flow Collector may receive the Flow Records then send it to **Analysis Application** (**Flow Sensor**) for deep analysis and monitoring .

With some other solutions , Net Flow Records may send to UDP Director (**Flow Replicator**) then UDP Director send the flows to Flow Collector. WHY? Since most network devices can only send messages to a single log management system, making changes to network devices time consuming and costly.
The UDP Director solves this problem by providing a single destination for all UDP data formats (NetFlow, SNMP, Syslog, etc.). Source IP addresses remain the same, so devices do not need to be reconfigured multiple times.

Now lets talk about Net Flow in Details setp by step.

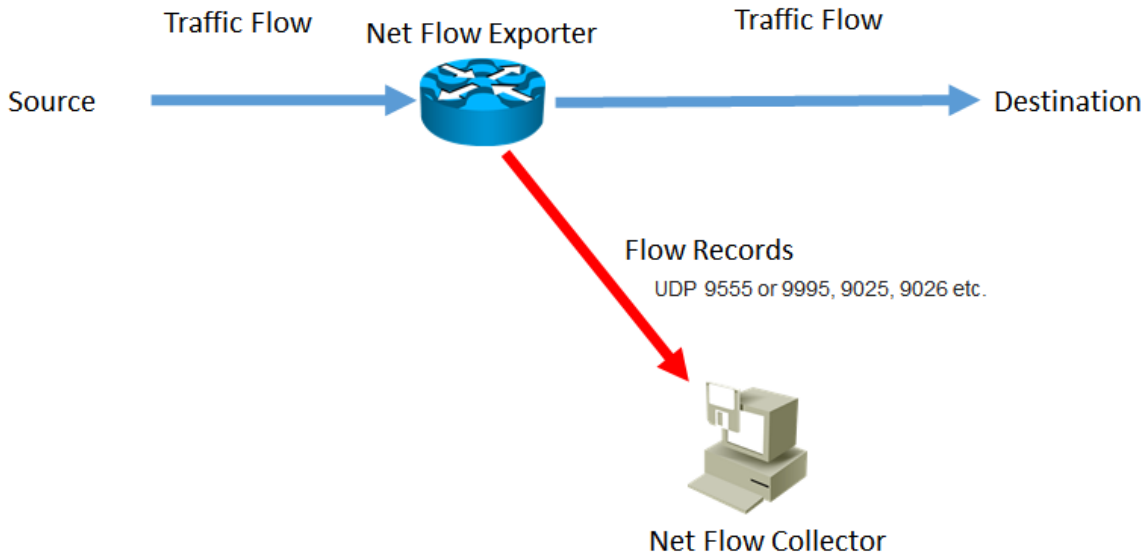
What is Flow?
A flow is a unidirectional series of packets between a given source and destination.
(while Session is bidirectional which means from source to destination and vice versa from destination to source as well)

So what is IP Flow?
Traditionally, an IP Flow is flow based on a set of 5 and up to 7 IP packet attributes.
IP Packet attributes used by NetFlow:
All packets with the same source/destination IP address, source/destination ports, protocol interface and class of service are grouped into a flow and then packets and bytes are tallied.



What is Flow exporter?
Such as your router, switch…etc , it will Aggregates packets into flows and exports flow records towards one or more flow collectors.

So What is Netflow collector?
Responsible for reception, storage and pre-processing of flow data received from a flow exporter.
It is application getting all IP Flow info and show it to us in cool dashboards or even apply some analysis feature on it.



Example for Netflow Collector commercial software:

- Managengine Netflow Analyzer
- Fluke Networks
- IBOM NetFlow Aurora

- Paessler PRTG
- Plixer Scrutinizer
- SolarWinds NetFlow Traffic Analyzer
- Lancope StealthWatch

Example for Netflow Collector Open source software:

- EHNT Platforms: GNU/Linux, Unix
- flowd Platforms: OpenBSD, Linux
- FlowScan Platforms: GNU/Linux, Unix
- fprobe Platforms: Linux, Unix
- ManageEngine NetFlow Analyzer Platforms: Windows, Linux
- nfdump Platforms: Linux, Unix
- NfSen NfSen is a graphical web-based front end for the nfdump netflow tools. Platforms: Linux, Unix
- ntop Platforms: Windows, GNU/Linux, Unix
- Paessler Router Traffic Grapher (PRTG) Platforms: Windows
- Scrutinizer Platforms: Linux, Unix
- SiLK Platforms: Linux, Unix
- Stager Platforms: Linux, Unix

Again what is an IP Flow?

Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets.

Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes ,we call these 5 attributes "**five tuple**" or "**seven tuple**" since nowadays we normally had 7 attributes by adding TOS and ingress interface to the list.

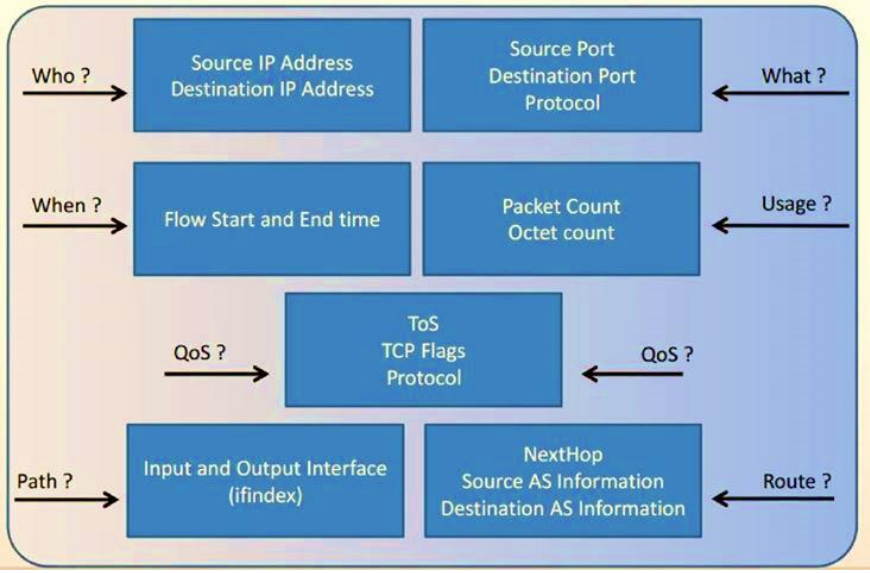
IP Packet attributes used by NetFlow , (Each Flow had these Record KEY Fields) :

1. ● IP source address
2. ● IP destination address
3. ● Source port for UDP or TCP, 0 for other protocols
4. ● Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
5. ● Layer 3 protocol type
6. ● Class of Service (IP Type of Service TOS)
7. ● Router or switch Ingress (Input) interface

Match and Collect

All packets with the same 'matching' attributes (i.e. the same source/destination IP address, source/destination ports, protocol, interface and class of service) are grouped into a flow and then packets and bytes are tallied. The default 7 attributes are the IP packet identity or "**key fields**" for the flow and determine if the packet information is unique or similar to other packets.

Items such as TCP flags, subnet masks, packets, bytes, etc. are "**non key fields**", but are often still 'collected' and exported in NetFlow or IPFIX. In short, **Match = Key** and **Collect = non-key**



This flow information is extremely useful for understanding network behavior which leads to use **Network as Sensor or Enforcer**

NetFlow collected information Stored in a network device called the NetFlow cache.

Non Key Fields are Just Additional information added to a flow includes:
● Flow timestamps to understand the life of a flow; timestamps are useful for calculating packets and bytes per second
● Next hop IP addresses including BGP routing Autonomous Systems (AS)
● Subnet mask for the source and destination addresses to calculate prefixes
● TCP flags to examine TCP handshakes

What is Flows per second (fps) ?
It is a measurement of how many NetFlow records the collector is receiving on a second by second basis.

Every time a packet travels through a NetFlow-capable device a flow is created in the router's memory.

Any subsequent packets that travel through the router that have these same attributes will update the existing NetFlow entry in the router's memory.

Once a flow becomes inactive the information is exported from the router's memory to the NetFlow collector. The rate at which flows are being expired and exported is the "flows per second rate".

Flows Per Second (FPS) Estimator (Calulator)
https://www.lancope.com/fps-estimator

What is NetFlow?

NetFlow was originally a Cisco packet switching technology for Cisco routers, implemented in IOS 11.x around 1996. It was originally a software implementation for the Cisco 7000, 7200 and 7500,[16] where it was thought as an improvement over the then current Cisco Fast Switching. It carries U.S. patent # 6,243,667

NetFlow is a feature that was introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

A typical flow monitoring setup (using NetFlow) consists of three main components:

- **Flow exporter**: aggregates packets into flows and exports flow records towards one or more flow collectors.
- **Flow collector**: responsible for reception, storage and pre-processing of flow data received from a flow exporter.
- **Analysis application**: analyzes received flow data in the context of intrusion detection or traffic profiling, for example.

More about these components later.

NetFlow creating an environment where administrators have the tools to understand who, what, when, where, and how network traffic is flowing.

What is NetFlow Record ?

A NetFlow record can contain a wide variety of information (key and non-key fields) about the traffic in a given flow.

What is telemtery ?

It is an automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

Netflow can provides detailed network telemetry that allows you to :

- see what is actually happening across the entire network
- identify DoS attacks
- identify compromised endpoints and network devices
- monitor employees and any one had access to our organization
- obtain network telemetry during security incident response and forensics
- detect firewall misconfigurations

Typical NetFlow Uses:

- Network Monitoring [provide extensive network monitoring capabilities that can be used to visualize traffic patterns across the network]

- Application Monitoring and Profiling [view time-based application network usage information that can be used to help understand usage patterns]

- User Monitoring and Profiling [view user (or customer) network and application resource usage patterns]

- Network Planning [track the usage (longer term) of the various links across a network]

- Security Analysis [used to identify and classify Denial of Service (DoS), virus and worm attacks in real time]

- Billing and Accounting [provide a very granular picture of the resources being used on a network]

- Data Warehousing and Mining [used to warehouse data for later retrieval and analysis]

NetFlow was initially created for billing and accounting of network traffic and to measure other IP traffic characteristics such as bandwidth utilization and application performance. NetFlow has also been used as a network capacity planning tool and to monitor network availability.

Nowadays, NetFlow is used as a network security tool because its reporting capabilities provide nonrepudiation, anomaly detection, and investigative capabilities.

What is JFlow , Sflow ?

JFlow is a IP traffic flow sampler technology used by Juniper manufactured routers and switches. JFlow is considered a flow sampler technology much like Sflow (from HP) and when enabled on an interface; it allows packets in the input stream to be sampled. As the packets flow through an input stream the router/switch will look at each one, but only records new packets and discards any packets it has already seen.

JFlow is just one of three flow technologies available; among the 3 include Cisco's Net Flow and HP Sflow technologies.

Each having their own strengths; Net flow records all packets while SFlow will only sample incoming traffic based on the packet ratio defined in the router configuration.

How to Access the Data Produced by NetFlow?

The following steps are used to implement NetFlow data reporting:

● NetFlow is configured to capture flows to the NetFlow cache
● NetFlow export is configured to send flows to the collector
● The NetFlow cache is searched for flows that have terminated and these are exported to the NetFlow collector server
● Approximately 30 to 50 flows are bundled together and typically transported in UDP format to the NetFlow collector server
● The NetFlow collector software creates real-time or historical reports from the data

What is NetFlow Versions?

NetFlow Version	Description
Version 1 (v1)	(Obsolete) The first implementation of NetFlow. NetFlow v1 was limited to IPv4 without IP network masks and autonomous system numbers (ASNs).
Version 2 (v2)	Never released.
Version 3 (v3)	Never released.
Version 4 (v4)	Never released.
Version 5 (v5)	Popular NetFlow version on many routers from different vendors. Limited to IPv4 flows.
Version 6 (v6)	(Obsolete) No longer supported by Cisco.
Version 7 (v7)	(Obsolete) Like version 5 with a source router field.
Version 8 (v8)	(Obsolete) Several aggregation form, but only for information that is already present in Version 5 records
Version 9 (v9)	Template-based, available (as of 2009) on some recent routers. Mostly used to report flows like IPv6, Multiprotocol Label Switching (MPLS), or even plain IPv4 with Border Gateway Protocol (BGP) next hop.
IPFIX	IPFIX is an IETF standard based on NetFlow v9 with several extensions. IPFIX was covered in detail in Chapter 1.

Version	Major Advantage	Limits/Weaknesses
V5	Defines 18 exported fields Simple and compact format Most commonly used format	IPv4 only Fixed fields, fixed length fields only Single flow cache
V9	Template-based IPv6 flows transported in IPv4 packets MPLS and BGP nexthop supported Defines 104 fields, including L2 fields Reports flow direction	IPv6 flows transported in IPv4 packets Fixed length fields only Uses more memory Slower performance Single flow cache
Flexible NetFlow (FNF)	Template-based flow format (built on V9 protocol) Supports flow monitors (discrete caches) Supports selectable key fields and IPv6 Supports NBAR data fields	Less common Requires more sophisticated platform to produce Requires more sophisticated system to consume
IP Flow Information Export (IPFIX) AKA NetFlow V10	Standardized – RFC 5101, 5102, 6313 Supports variable length fields, NBAR2 Can export flows via IPv4 and IPv6 packets	Even less common Only supported on a few Cisco platforms
NSEL (ASA only)	Built on NetFlow v9 protocol State-based flow logging (context) Pre and Post NAT reporting	Missing many standard fields Limited support by collectors

What is TNF: Traditional NetFlow & FNF: Flexible NetFlow ?
Flexible NetFlow is an extension of NetFlow v9.
It provides additional functionality that allows you to export more information (even user defined NON key fields) using the same NetFlow v9 datagram. Some Cisco devices support only **Traditional NetFlow (TNF)**, while others support **Flexible NetFlow (FNF)** or both TNF and FNF. Just remember TNF IOS configurations is different than FNF ones.

Here are some of Flexible NetFlow FNF benefits:

- Flexibility and scalability of flow data beyond traditional NetFlow
- Customized traffic identification
- Ability to focus and monitor specific network behavior
- Ability to monitor a wider range of packet information, producing new information about network behavior
- Enhanced network anomaly and security detection
- Convergence of multiple accounting technologies into one accounting mechanism

What is a Flexible NetFlow Key Field?

A Flexible NetFlow (FnF) key field is a field that you want to match on , they are the same whatever we talk about FnF or TnT . **key fields**" are introduced in the CLI via the "**match**" keyword.

Here is how we match on the standard 7 key fields when setting up a Flexible Netflow record:

- match transport tcp destination-port
- match transport tcp source-port
- match ipv4 destination address
- match ipv4 source address
- match ipv4 protocol
- match ipv4 tos
- match interface input

We may only want to match the source IP address and collect the bytes. Also we can dramatically simplify the configuration by using only one match statement:

- match ipv4 source address

The volume of flow cache entries on the router is now dramatically less which means less overhead on the router and less exports to the FnF collector.

You might be asking "What about knowing how much bytes sent or received ?" we can know that using Collect statements.

What is a Flexible NetFlow Non-Key Field?
Additional information can be added to the Flow Record and this information is named non-key fields.

Non-key fields are added to the flow entry in the NetFlow cache and exported.

The non-key fields are not used to create or characterize the flows but are exported and just added to the flow.

In FnF, non-key fields are also configurable by the user. If a field is non-key, normally only the first packet of the flow is used for the value in this field.

Non-key fields" are introduced in the CLI via the "**collect**" keyword such as:

- collect counter bytes
- collect counter packets

Remember Match statements are inherently collect statements. In other words, everything matched is also collected.

Typical non-key NetFlow fields that are often added to the above include:

- collect routing source as
- collect routing destination as
- collect routing next-hop address ipv4
- collect ipv4 dscp
- collect transport tcp flags
- collect interface output ;notice that the input interface was a match statement!!!
- collect counter bytes
- collect counter packets
- collect timestamp sys-uptime first
- collect timestamp sys-uptime last

What is IPFIX?

- IPFIX Internet Protocol Flow Information Export
- IPFIX was created as universal standard of export for flow information from routers , switches , firewalls and other infra devices
- IPFIX defines how flow information should be formatted and transferred from an exporter to a collector
- IPFIX based on IETF standards track RFC 7011 to 7015 and RFC 5103
- Neflow Version 9 is the basis for IPFIX
- The NetFlow protocol itself has been superseded by Internet Protocol Flow Information eXport (IPFIX). IPFIX Based on the NetFlow Version 9 implementation , so we can consider both are the same.
- IPFIX use the concepts of Templates

Simply IPFIX is standard version of Net Flow Version 5 & 9 and later versions

Vendors who did ask the question "What is IPFIX?" and made the switch to export it include but, are not limited to:		
Avaya	Extreme Networks	Solera
Barracuda	Juniper	Saisei Networks
Blue Coat	NetASQ	SonicWall
Cisco	Nortel	VMware
Citrix	nProbe	Xirrus
Ecessa	Open vSwitch	YAF
F5 Networks	Plixer	ZTE

What are the Netflow Components ?

Records
These flows are defined by a number of different pieces of traffic information; the information used when using Flexible Netflow can be defined by user records or within standard records.

With the original Netflow, a flow was defined by seven different fields of information that we talked about before in this document .

Traffic with the same values for these seven fields was defined as a flow and individually tracked.

Flexible Netflow provides the ability to either use this original flow definition (“Record”) or to create a new, more specific flow definition.

When creating a user-defined flow definition, the fields that are going to be tracked are selected and then defined as either a key field or as a nonkey field; these key fields are then used by Flexible Netflow to define traffic flows; the fields that are defined as nonkey are captured with the flow but are not used to define specific flows.

Flow Monitor
The Netflow flow monitor component is used to provide the actual traffic monitoring on a configured interface.

When a flow monitor is applied to an interface, a flow monitor cache is created that is used to collect the traffic based on the key and nonkey fields in the configured record.

There are three different modes of flow monitor cache that can be used with each flow monitor:

•**Layer 3**—When in the normal mode, cache entries are aged out according to timeout parameters, based on the activity of a flow. This is the default mode.
•**Immediate**—When in the immediate mode, cache entries are aged out as soon as created. When in this mode, each flow contains only one packet; this is used when traffic information is required immediately at the flow export destination (see next section).
•**Permanent**—When in the permanent mode, cache entries that are newer are aged out. This is useful when long term statistics on a device are required and the number of flows is expected to be low.

Flow Exporter
A flow exporter is used to transfer the contents of the Netflow cache from the device to a remote system.
The Netflow Data Export Format Version 9 is used with Flexible Netflow (as opposed to Version 5) in order to provide additional flexibility.

Multiple flow exporters can be configured and assigned to a variety of different flow monitors if there is a need to export to multiple locations.

Flow Sampler (optional component)
Normally we prefer to use Un-sampled Flow but still we can use Sample Flow if need it.
A flow sampler is used when there is a high volume of traffic to analyze that could potentially affect the performance of the monitored device. In this situation, a flow sampler can be used to limit the number of packets that will be analyzed by the flow monitor.
For example, 1 out of every 2 packets could be captured and analyzed.

Where to collect Net Flow From?
Answer for this question depend on the Use ,Typical Use Cases are listed below:

1. Use case detection of security events –
   a. Only need to account for the packet once.
   b. Collect at the edge **(access)**, if not 100% flow capable then distribution, if not 100% flow capable then core.
   c. Enable flow on any exporter that will provide additional context like ASA FWs (provide NAT and FW actions), and Proxy data (allow visibility into outbound traffic that has been translated)

2. Use case forensics or auditing –
   a. You should be looking to account for all packets.
   b. Deploy as close to the edges of the network as possible (at the access layer).
   c. Enable flow on any exporter that will provide additional context like ASA FWs (provide NAT and FW actions), and Proxy data (allow visibility into outbound traffic that has been translated).

3. Use case networking (performance) –
   a. You need flow from everywhere (access, distribution and core) to help with interface utilization, QoS monitoring, trending and capacity planning and tracking issues back to the source of the problem which could be any interface.

Cisco Devices support Net Flow FNF (v9) –according to CTDv2-

Table 10 Platform Details

Platform	Hardware Details	Software Details	NetFlow Details
Catalyst 3K-X	3560-X/3750-X with SM	IOS 15.0.(2)SE7	FNF (v9)
Catalyst 3850/3650	3850/3650	IOS-XE 3.3.5SE	FNF (v9)
Catalyst 4500	Sup7-E Sup8-E	IOS-XE 3.4.5SG IOS-XE 3.3.2XO	FNF (v9)
Catalyst 6500	Sup2T	IOS 15.0.(1)SY7a	FNF (v9)
Catalyst 2960-X (NetFlow Lite)	2960-X	IOS 15.0.(2)EX	NetFlow Lite (sampled V9)
ISR G2	2901, 2911	IOS 15.(3)M4	FNF (v9)
ASR 1000	ASR 1001/1002F	IOS-XE 3.10.xS	FNF (v9)
ASA 5500	ASA 5505, 5510	ASA 9.0.4	NSEL (v9)
ASA 5500-X with FirePOWER Services	ASA 5515-X, 5545-X	ASA 9.3.2 FirePOWER 5.3.1	NSEL (v9)
NetFlow Generation Appliance (NGA)	NGA 3240	1.0.2	FNF (v9)
UCS VIC	VIC 1240/1280/1225	2.2(2e)	FNF (v9)

Configuring Netflow in Cisco IOS

TNF

```
ip flow-export version 9
ip flow-export destination 10.0.0.1 2055
int f0/0
ip flow ingress
```

FNF (IPFIX)

```
flow record MYRECORD
description Used for basic traffic analysis
match ipv4 destination address
collect interface input

flow exporter MYEXPORTER   < Create and configure a flow exporter
description exports to Netflow Collector
export-protocol netflow-v9
transport udp 9996  < Configure the UDP port used by the flow exporter (by default, UDP / 9995 used)
source g1/0
destination 11.0.0.100 < Configure the exporter destination (net flow collector)  by ip  or hostname

flow monitor MYMONITOR < Create and configure a flow monitor.
description monitor ipv4 internet traffic
record MYRECORD  < Apply the record & Define the record format that will be used by the flow
monitor , can be record name or netflow-original or netflow ipv4 | ipv6
exporter MYEXPORTER  < Apply the exporter
cache entriess 200000
cache timeout active 60   < this is how long a flow can be inactive before removed from cache and
send to Net Flow collector, recommended 15 sec , ALL exporters should have same timeout.
cahce timeout inactive 15  <this is longest amount of time a flow can be in cache without exporting a
Flow Record ,recommended 60 sec , ALL exporters should have same timeout.
int g0/0
ip flow monitor MYMONITOR input   < Apply the flow monitor (during application of a flow monitor,
the flow sampler is also applied).
```

Verifications commands:

```
show flow exporter MYEXPORT
show flow exporter statistics
show flow monitor name MYMONITOR
show flow monitor name MYMONITOR cache
show flow monitor name MYMONITOR cache format record
show flow monitor name MYMONITOR cache format table
```

let's go through these commands in details
let's start with options we can use with **match command**

```
NY-ASR1004(config-flow-record)# match ?
  application  Application fields
  flow         Flow identifying fields
  interface    Interface fields
  ipv4         IPv4 fields
  ipv6         IPv6 fields
  routing      Routing attributes
  transport    Transport layer fields
```

To configure the input and output interfaces as key fields for a Flexible NetFlow flow record, use the **match interface** command in Flexible NetFlow flow record configuration mode

A flow record requires at least one key field before it can be used in a flow monitor.
The key fields differentiate flows, with each flow having a unique set of values for the key fields.
The key fields are defined using the **match** command.

To configure the IPv4 destination address as a key field for a Flexible NetFlow flow record, use the **match ipv4 destination** command in Flexible NetFlow flow record configuration mode.

address	Configures the IPv4 destination address as a key field.
mask	Configures the mask for the IPv4 destination address as a key field.
prefix	Configures the prefix for the IPv4 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range 1 to 32.

let's talk about with options we can use with **collect command**

```
NY-ASR1004(config-flow-record)# collect ?
  application  Application fields
  counter      Counter fields
  flow         Flow identifying fields
  interface    Interface fields
  ipv4         IPv4 fields
  ipv6         IPv6 fields
  routing      Routing attributes
  timestamp    Timestamp fields
  transport    Transport layer fields
```

To configure the input and output interface as a nonkey field for a flow record, use the collect interface command in flow record configuration mode.

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record.
The values in nonkey fields are added to flows to provide additional information about the traffic in the flows.
A change in the value of a nonkey field does not create a new flow.
In most cases the values for nonkey fields are taken from only the first packet in the flow.

let's talk about with options we can use with **record command used in flow monitor**

```
NY-ASR1004(config-flow-monitor)# record ?
  NY-ASR-FLOW-RECORD-1  Used for basic traffic analysis
  netflow               Traditional NetFlow collection schemes
  netflow-original      Traditional IPv4 input NetFlow with origin ASs
```

As you can see you have three options [netflow-orginal | netflow (ipv4 | ipv6) | record name]:

netflow-original Configures the flow monitor to use the Flexible NetFlow implementation of original NetFlow with origin autonomous systems.

netflow ipv4 Configures the flow monitor to use one of the predefined IPv4 records.

netflow ipv6 Configures the flow monitor to use one of the predefined IPv6 records.

record **Name** of the predefined record

let's talk about with options we can use with **Cache commands used in flow monitor**

Each flow monitor has a cache that it uses to store all the flows it monitors.

Each cache has various configurable elements, such as the number of entries and the time that a flow is allowed to remain in it.

When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

The default Flexible NetFlow flow monitor flow cache parameters are used.
The following flow cache parameters for a Flexible NetFlow flow monitor are enabled:

- Cache type: normal
- Maximum number of entries in the flow monitor cache: 4096
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 15 seconds
- Update timeout for a permanent flow cache: 1800 seconds

Remember your Network devices will collect flow and cached internally then send to Flow Collector , So caching parameters are important.

If a cache is already active (that is, you have applied the flow monitor to at least one interface in the router), your changes to the record, cache type, and cache size parameters will not take effect until you either reboot the router or remove the flow monitor from every interface and then reapply it. Therefore whenever possible you should customize the record, cache type, and cache size parameters for the cache before you apply the flow monitor to an interface. You can modify the timers, flow exporters, and statistics parameters for a cache while the cache is active.

entries *number*	Specifies the maximum number of entries in the flow monitor cache. Range: 16 to 1048576. Default: 4096.
timeout active *seconds*	Specifies the active flow timeout in seconds. Range: 1 to 604800 (7 days). Default: 1800.
timeout inactive *seconds*	Specifies the inactive flow timeout in seconds. Range: 1 to 604800 (7 days). Default: 15.
timeout update *seconds*	Specifies the update timeout, in seconds, for a permanent flow cache. Range: 1 to 604800 (7 days). Default: 1800.
timeout event transaction-end	Specifies that the record is generated and exported in the NetFlow cache at the end of a transaction.
type	Specifies the type of the flow cache.
immediate	Configures an immediate cache type. This cache type will age out every record as soon as it is created.
normal	Configures a normal cache type. The entries in the flow cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. This is the default cache type.
permanent	Configures a permanent cache type. This cache type disables flow removal from the flow cache.

cache entries

This command controls the size of the cache.

Cache size should be based on a number of factors, including the number of flows expected, the time the flows are expected to last (based on the configured key fields and the traffic), and the timeout values configured for the cache.

The size should be large enough to minimize emergency expiry.

Emergency expiry is caused by the Flexible NetFlow cache becoming full.

When the Flexible NetFlow cache becomes full, the router performs “emergency expiry” where a number of flows are immediately aged, expired from the Flexible NetFlow cache, and exported in order to free up space for more flows.

For a permanent cache (flows never expire), the number of entries should be large enough to accommodate the number of flows expected for the entire duration of the cache entries.

If more flows occur than there are cache entries, the excess flows are not recorded in the cache.

For an immediate cache (flows expire immediately), the number of entries simply controls the amount of history that is available for previously seen packets.

cache timeout active

This command controls the aging behavior of the normal type of cache.

If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow).

This age out process allows the monitoring application that is receiving the exports to remain up to date.

By default this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements.

A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it.

cache timeout inactive
This command controls the aging behavior of the normal type of cache.
If a flow has not seen any activity or a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected.
If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead.
If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation.

cache timeout update
This command controls the periodic updates sent by the permanent type of cache.
This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache.
By default this timer value is 1800 seconds (30 minutes).

cache timeout event transaction-end
To use this command, you must configure the match connection transaction id command and the match application name command for the flow record.
This command causes the record to be generated and exported in the NetFlow cache at the end of a transaction.
A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow.

cache type immediate
This command specifies the immediate cache type. This type of cache will age out every record as soon as it is created, with the result that every flow contains just one packet.
The commands that display the cache contents will provide a history of the packets seen.
The use of this cache type is appropriate when very small flows are expected and a minimum amount of latency between analyzing a packet and exporting a report is desired.
We recommend using this command when you are sampling packet chunks because the number of packets per flow is typically very low.
This command may result in a large amount of export data that can overload low speed links and overwhelm any systems to which you are exporting. We recommended that you configure sampling to reduce the number of packets seen.
Notice that timeout settings have no effect for the immediate cache type.

cache type normal
This command specifies the normal cache type. This is the default cache type.
The entries in the cache will be aged out according to the timeout active seconds and timeout inactive seconds settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

cache type permanent
This command specifies the permanent cache type. This type of cache never ages out any flows.
This cache type is useful when the number of flows you expect to see has a limit and there is a need to keep long-term statistics on the router.
For example, if the only key field is IP TOS, a limit of 256 flows can be seen, so to monitor the long-term usage of the IP TOS field, a permanent cache can be used.

Update messages are exported via any exporters configured for the monitor associated with this cache in accordance with the timeout update seconds setting.

Note When a cache becomes full, new flows will not be monitored. If this occurs, a “Flows not added” statistic will appear in the cache statistics.
Note A permanent cache uses update counters rather than delta counters. This means that when a flow is exported, the counters represent the totals seen for the full lifetime of the flow and not the additional packets and bytes seen since the last export was sent.

OPTIONAL we can configure also NetFlow Sampler

Sampler MYSAMPLER **< Create and configure a flow sampler.**
Description our custom sampler for netflow
Mode deterministic 1 out-of 10 **< Configure the sampler mode.**

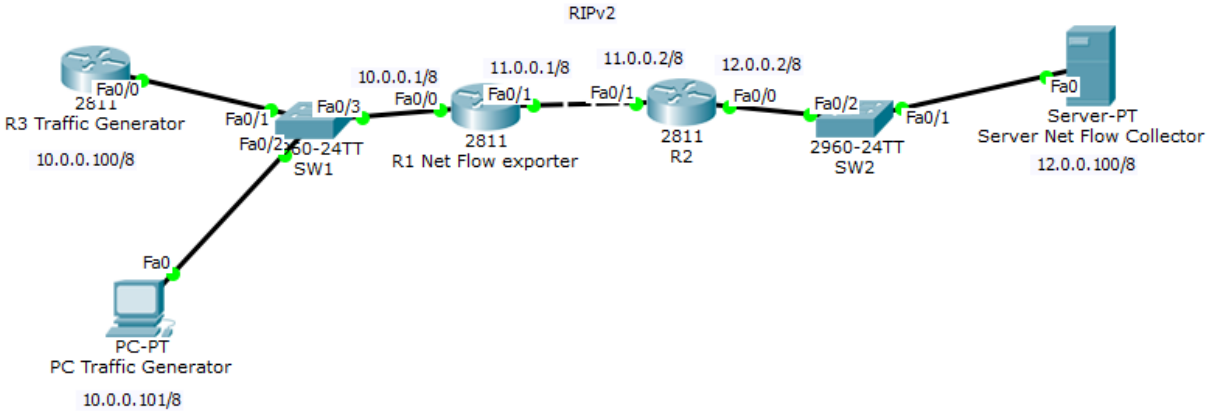
- **Mode can be deterministic or random**
- **Out-of 10 (10 is window-size)**

- **deterministic Enables deterministic mode sampling for the sampler.**
- **random Enables random mode sampling for the sampler.**
- **1 out-of window-size Specifies the window size from which to select packets. Range: 2 to 32768.**

Int f0/0
Ip flow monitor MYMONITOR sampler MYSAMPLER input **< Apply the flow monitor (during application of a flow monitor, the flow sampler is also applied).**

Show sampler MYSAMPLER

Net Flow TNF Lab

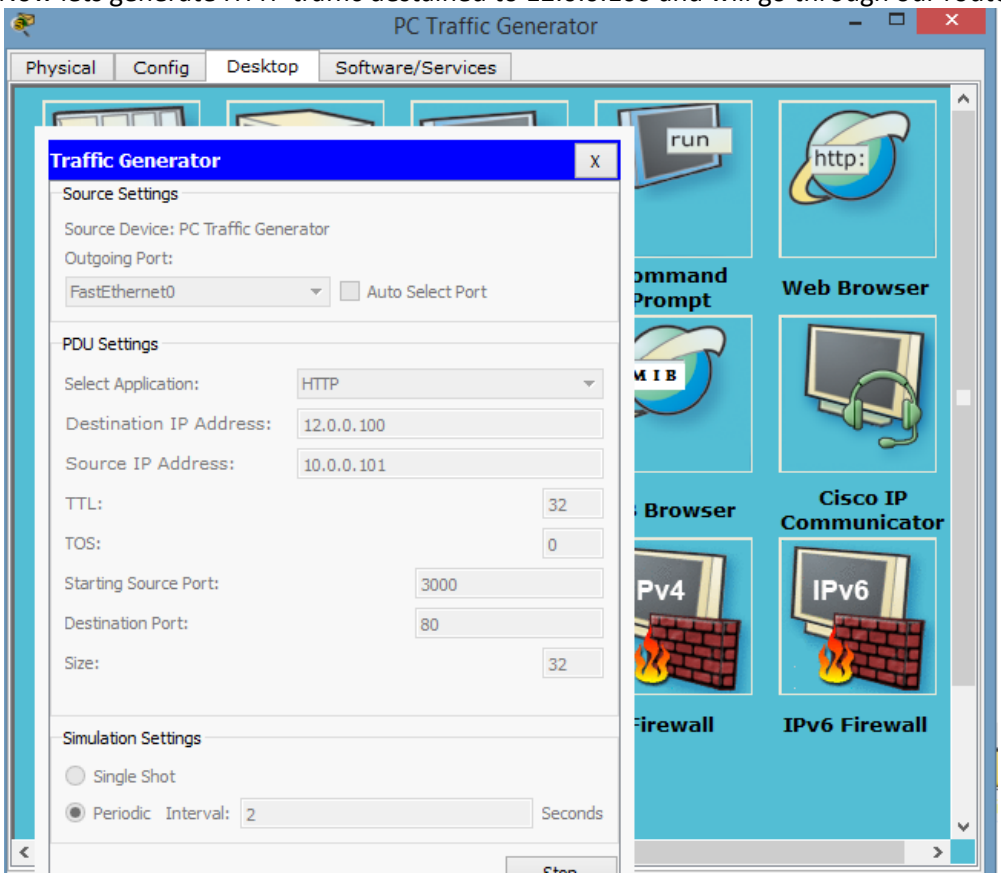


R1 should be configured with TNF for all ingress traffic to interface f0/0 facing network 10.0.0.0 , should collect all Flows Records destained ot going through R1 originated from network 10.0.0.0 devices and then send it to Net Flow Collector server

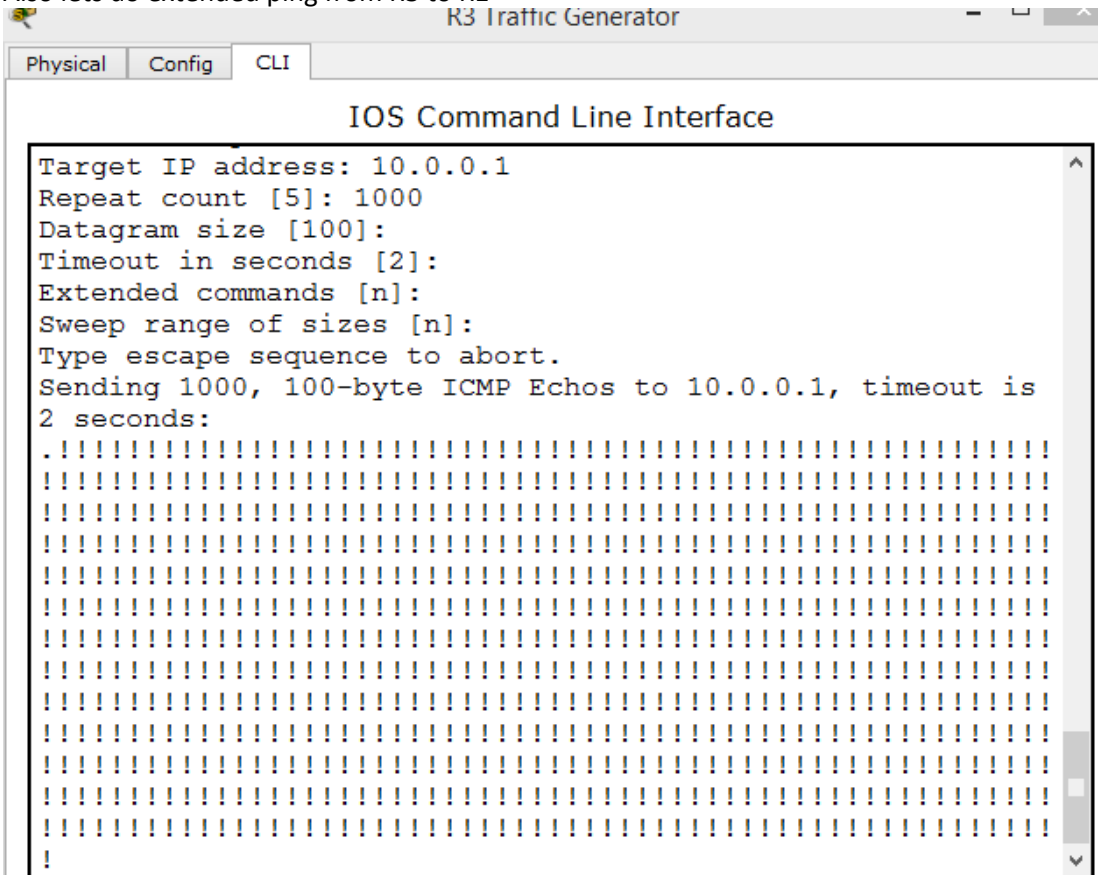
R1

ip flow-export source f0/1
ip flow version 9
ip flow destination 12.0.0.100 9996
int f0/0
ip flow ingress

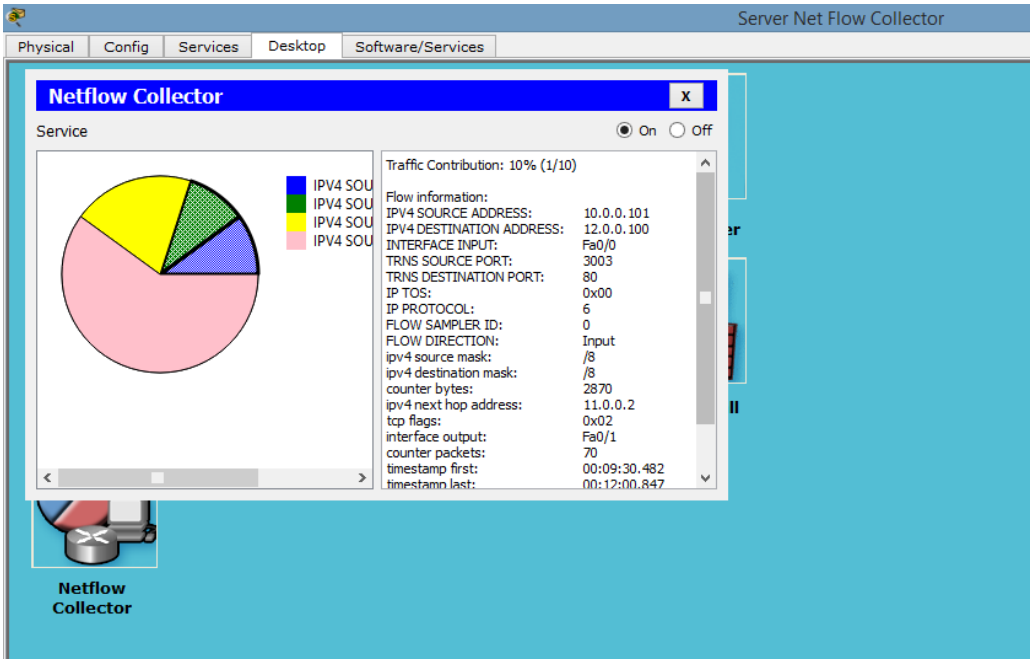
Now lets generate HTTP traffic destained to 12.0.0.100 and will go through our router R1



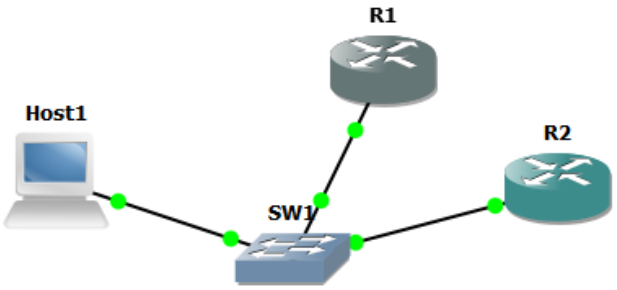
Also lets do extended ping from R3 to R1



Now if we go to our Net flow collector we can see information about what traffic was ingress R1 f0/0 interface.



Net Flow FNF (with Manageengine Flow Collector & Pasessler Net Flow Generator) Lab



R1 (192.168.100.1/24) is the device should send Net Flow data to Host
Host (192.168.100.100/24) is exporter where you installed manageengine netflow collector and Pasessler Net Flow Generator , you will use Pasessler Net Flow Generator to generate some HTTP traffic destined to R1
R2 (192.168.100.2/24) will ping R1 with 2000 packets and also create telnet session to R1 as well.
We should then see some information related to all these traffcis in our manageengine netflow collector

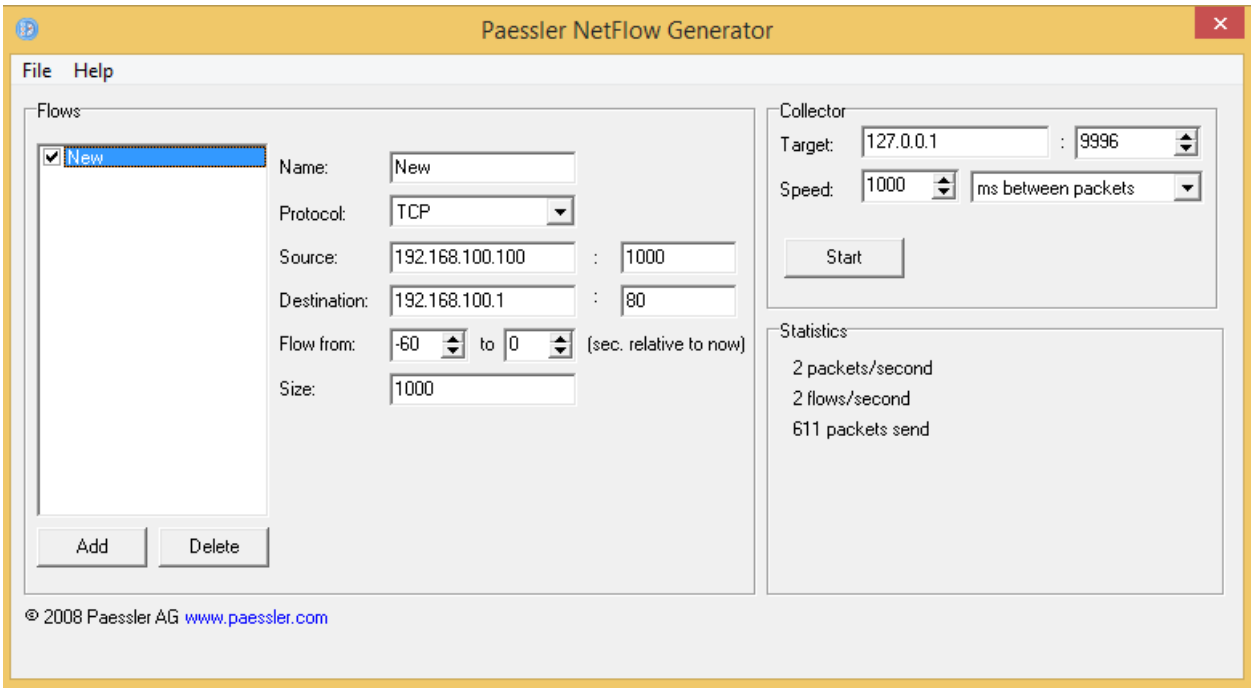
R1

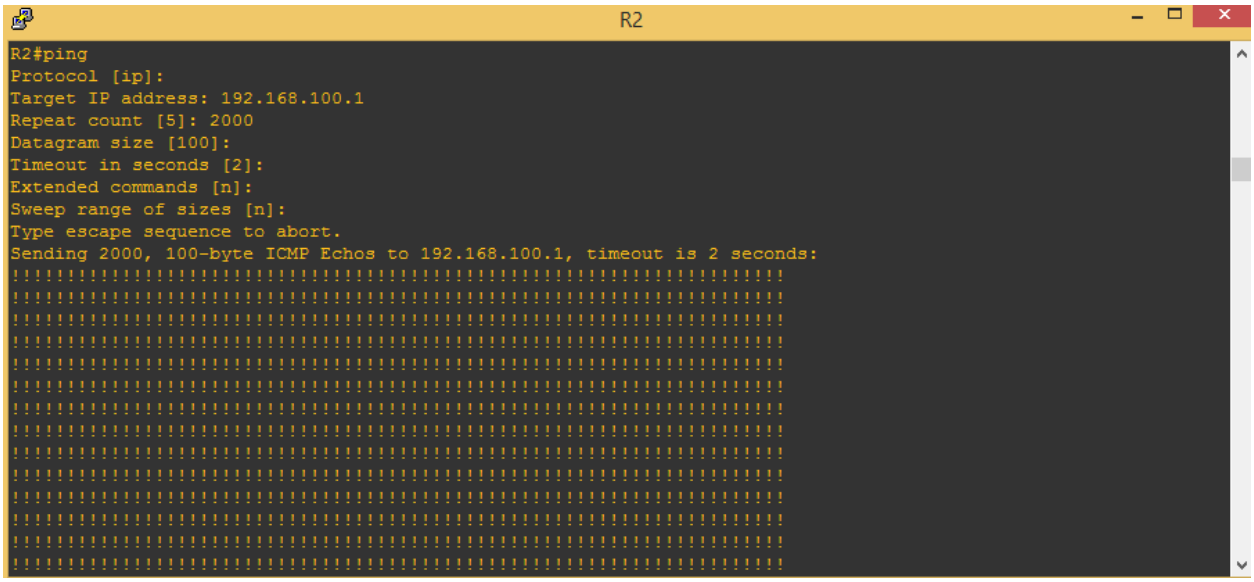
```
FNF
flow exporter MYEXPORTER
 destination 192.168.100.100
source f0/0
export-protocol netflow-v9
 transport udp 9996
!
flow record MYRECORD
 match ipv4 destination address
 match ipv4 protocol
 match ipv4 source address
 match transport destination-port
 match transport source-port
 match flow direction
 match ipv4 tos
 match interface input
 collect routing destination as
 collect routing next-hop address ipv6
 collect transport tcp flags
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
collect application name                    < enable NBAR
```

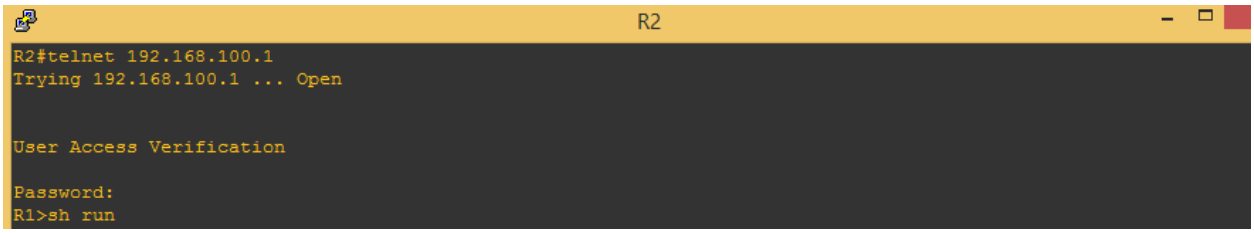
```
!
flow monitor MYMONITOR
 record MYRECORD
 exporter MYEXPORTER

interface f0/0
ip flow monitor MYMONITOR input

R1#show ip cache flow
R1#sh flow monitor MYMONITOR cache
```



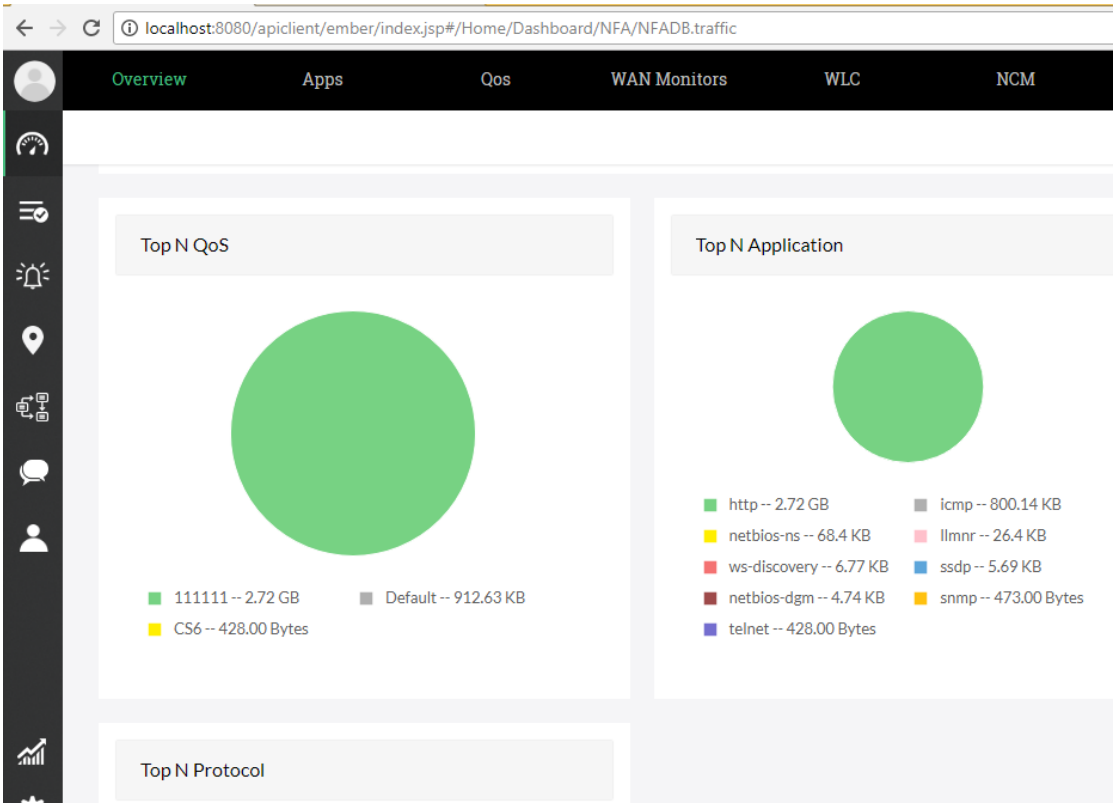


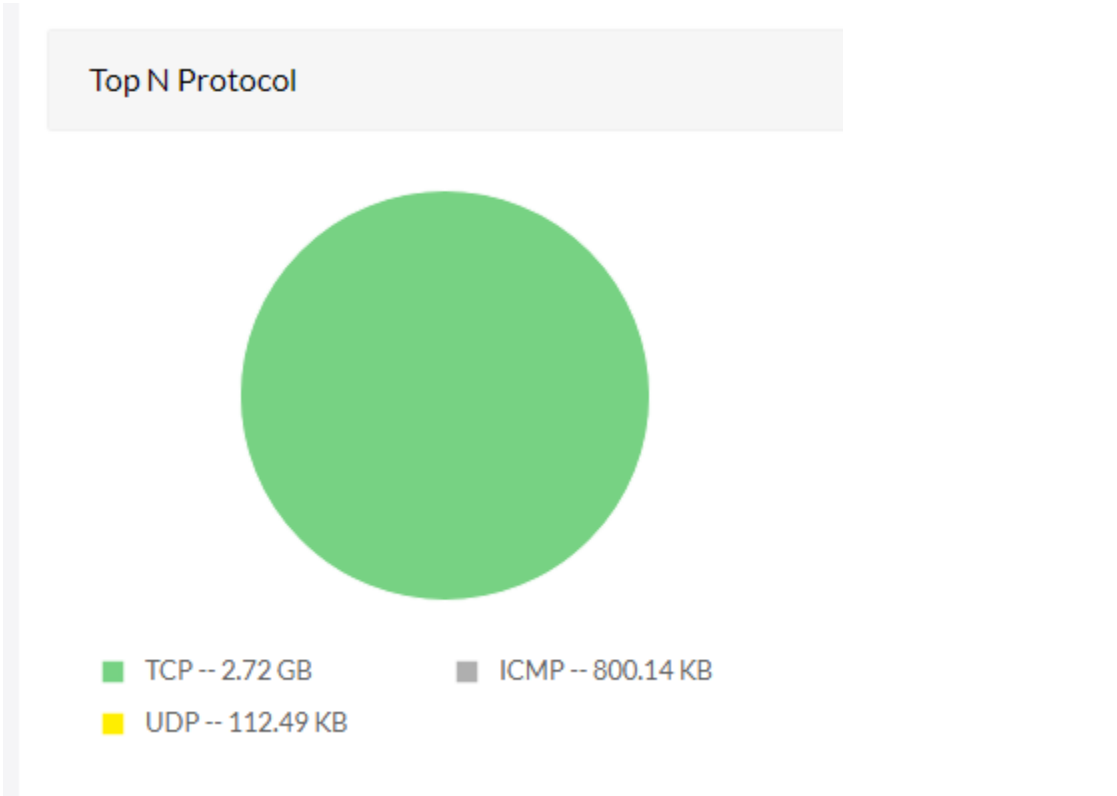


After few minutes you should watch the following flows data in Manageengine Flow Collector

Top N Conversation

Source	Destination	Application	Traffic
192.168.100.100	192.168.100.1	http	2.72 GB
192.168.100.2	192.168.100.1	icmp	799.9 KB
192.168.100.100	192.168.100.255	netbios-ns	68.32 KB
192.168.100.100	224.0.0.252	llmnr	26.4 KB
192.168.100.100	239.255.255.250	ws-discovery	6.77 KB
192.168.100.100	239.255.255.250	ssdp	5.69 KB
192.168.100.100	192.168.100.255	netbios-dgm	4.74 KB
192.168.100.100	192.168.100.1	snmp	473.00 Bytes
192.168.100.2	192.168.100.1	telnet	428.00 Bytes
192.168.100.100	192.168.100.1	icmp	240.00 Bytes


localhost:8080/apiclient/ember/index.jsp#/Home/Dashboard/NFA/NFADB.traffic
Overview
Apps
Qos
WAN Monitors
WLC
NCM
Top N QoS
111111 -- 2.72 GB
Default -- 912.63 KB
CS6 -- 428.00 Bytes
Top N Application
http -- 2.72 GB
icmp -- 800.14 KB
netbios-ns -- 68.4 KB
llmnr -- 26.4 KB
ws-discovery -- 6.77 KB
ssdp -- 5.69 KB
netbios-dgm -- 4.74 KB
snmp -- 473.00 Bytes
telnet -- 428.00 Bytes
Top N Protocol


Top N Protocol
TCP -- 2.72 GB
ICMP -- 800.14 KB
UDP -- 112.49 KB

Using CLI in R1 we can display the status and statistics for a Flexible NetFlow flow monitor
Show flow monitor MYMONITOR cahce format table

```
R1#sh flow monitor MYMONITOR cache format table
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                              20
  High Watermark:                               52

  Flows added:                                1411
  Flows aged:                                 1391
    - Active timeout   (  1800 secs)             0
    - Inactive timeout (    15 secs)          1391
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  INTF INPUT           FLOW DIRN  IP TOS  IP PR
OT  ip dst as  ipv6 next hop addr                                                          tcp flags  intf ou
tput               bytes        pkts  time first   time last
==============  ==============  ============  ============  ====================  =========  ======  =====
==  =========  ========================================================================  =========  =======
============  ==========  ==========  ==========  ==========
192.168.100.100  224.0.0.252              51558          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     49           1     2051776     2051776
192.168.100.100  224.0.0.252              52775          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     51           1     2052740     2052740
192.168.100.100  224.0.0.252              51572          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     51           1     2052748     2052748
192.168.100.100  224.0.0.252              58835          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     96           2     2053828     2054240
192.168.100.100  224.0.0.252              61950          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     96           2     2053828     2054240
192.168.100.100  224.0.0.252              65213          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     96           2     2054676     2055088
192.168.100.100  224.0.0.252              55368          5355  Fa0/0                Input      0x00
17          0  ::                                                                         0x00       Null
                     96           2     2054676     2055088
 --More--
```

There are many other useful show commands
show flow exporter
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1359026
show flow interface
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1349520
show flow monitor
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1360126
show flow monitor cache aggregate
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1350309
show flow monitor cache filter
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1350687
show flow monitor cache sort
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1351162
show flow record
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1363297
show sampler
http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_02.html#wp1351668

```
R1#sh flow monitor MYMONITOR cache
  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                              18
  High Watermark:                               52

  Flows added:                                1443
  Flows aged:                                 1425
    - Active timeout    (  1800 secs)            0
    - Inactive timeout (    15 secs)         1425
    - Event aged                                0
    - Watermark aged                            0
    - Emergency aged                            0

IPV4 SOURCE ADDRESS:        192.168.100.100
IPV4 DESTINATION ADDRESS:   192.168.100.255
TRNS SOURCE PORT:           137
TRNS DESTINATION PORT:      137
INTERFACE INPUT:            Fa0/0
FLOW DIRECTION:             Input
IP TOS:                     0x00
IP PROTOCOL:                17
ip destination as:          0
ipv6 next hop address:      ::
tcp flags:                  0x00
interface output:           Null
counter bytes:              4914
counter packets:            63
timestamp first:            2057740
timestamp last:             2087028

IPV4 SOURCE ADDRESS:        192.168.100.100
IPV4 DESTINATION ADDRESS:   239.255.255.250
TRNS SOURCE PORT:           54945
TRNS DESTINATION PORT:      1900
INTERFACE INPUT:            Fa0/0
FLOW DIRECTION:             Input
IP TOS:                     0x00
IP PROTOCOL:                17
ip destination as:          0
ipv6 next hop address:      ::
tcp flags:                  0x00
interface output:           Null
```

```
R1#show flow record
flow record MYRECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  58 bytes
  Fields:
    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 destination as
    collect routing next-hop address ipv6
    collect transport tcp flags
    collect interface output
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

R1#show flow exporter
Flow Exporter MYEXPORTER:
  Description:              User defined
  Tranport Configuration:
    Destination IP address: 192.168.100.100
    Source IP address:      192.168.100.1
    Source Interface:       FastEthernet0/0
    Transport Protocol:     UDP
    Destination Port:       9996
    Source Port:            59502
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used
```

```
R1#sh flow interface
Interface FastEthernet0/0
  FNF:  monitor:          MYMONITOR
        direction:        Input
        traffic(ip):      on

R1#show flow record
flow record MYRECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  58 bytes
  Fields:
    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 destination as
    collect routing next-hop address ipv6
    collect transport tcp flags
    collect interface output
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last

R1#show flow exporter
Flow Exporter MYEXPORTER:
  Description:              User defined
  Tranport Configuration:
    Destination IP address: 192.168.100.100
    Source IP address:      192.168.100.1
    Source Interface:       FastEthernet0/0
    Transport Protocol:     UDP
    Destination Port:       9996
    Source Port:            59502
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used
```

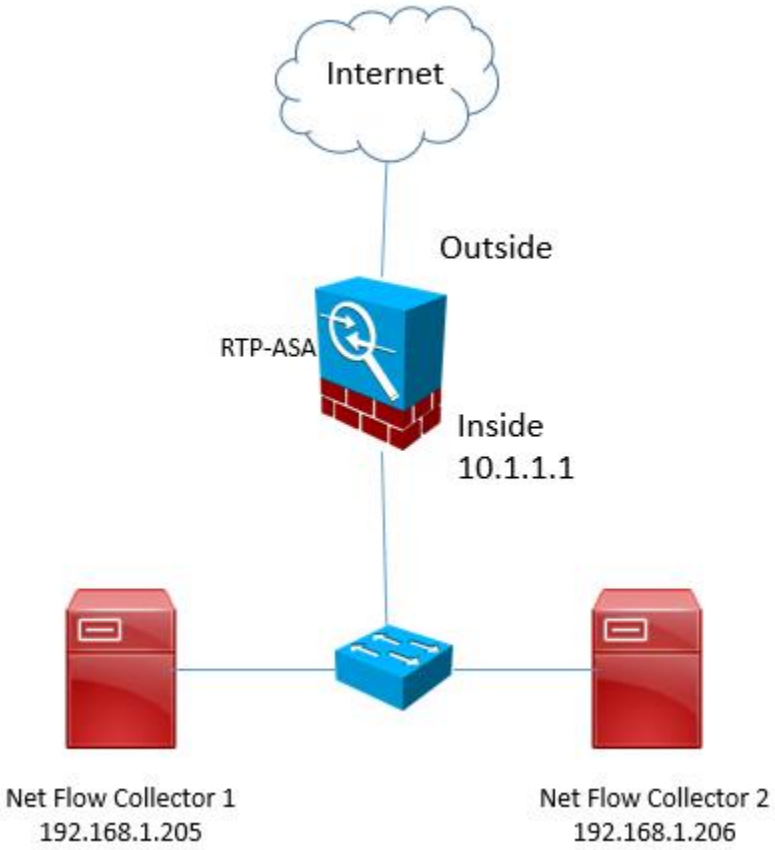
Configuring NSEL in the Cisco ASA [ASDM/CLI]
Cisco ASA used its own term when it comes to NetFlow , ASA call it NetFlow Secure Event Logging (NSEL)
Cisco ASA support version 9 of NetFlow

NSEL provides a stateful IP flow tracking method that exports only those records that indicate significant events in a flow.

The following are the significant flow events that are tracked:

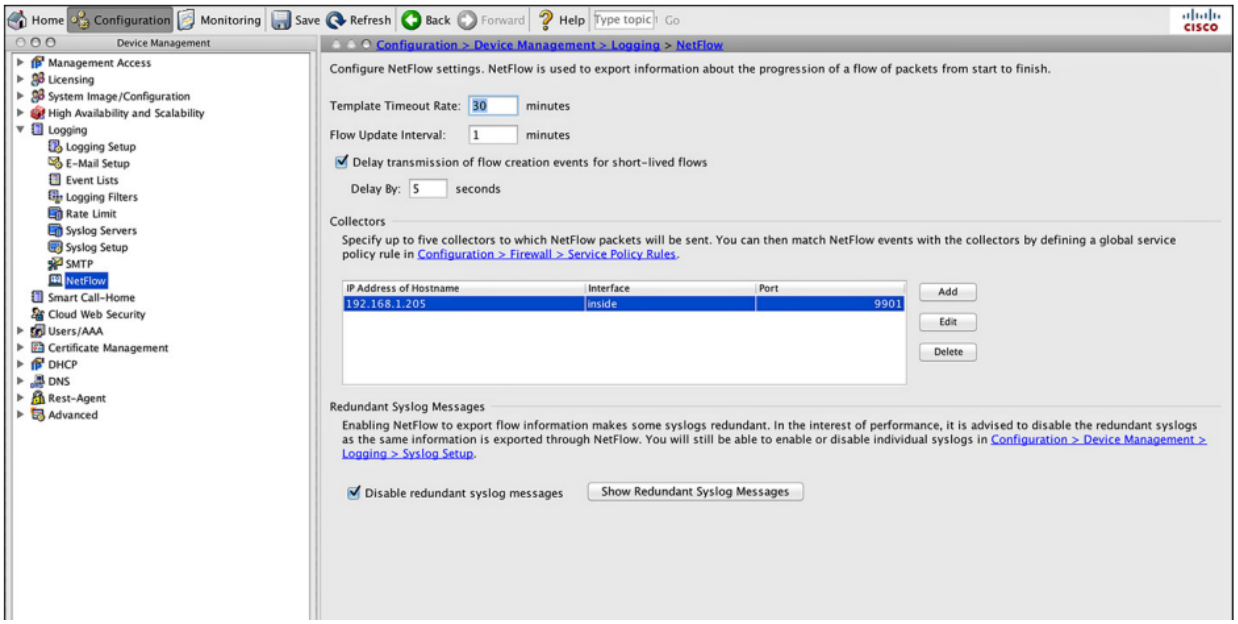
- Flow create
- Flow teardown
- Flow denied
- Flow update (provide periodic byte counters over the duration of the flow)

Let's assume we had the following topology



Configuring NSEL in the Cisco ASA Using ASDM

Log in to ASDM and navigate to **Configuration > Device Management > Logging > NetFlow**



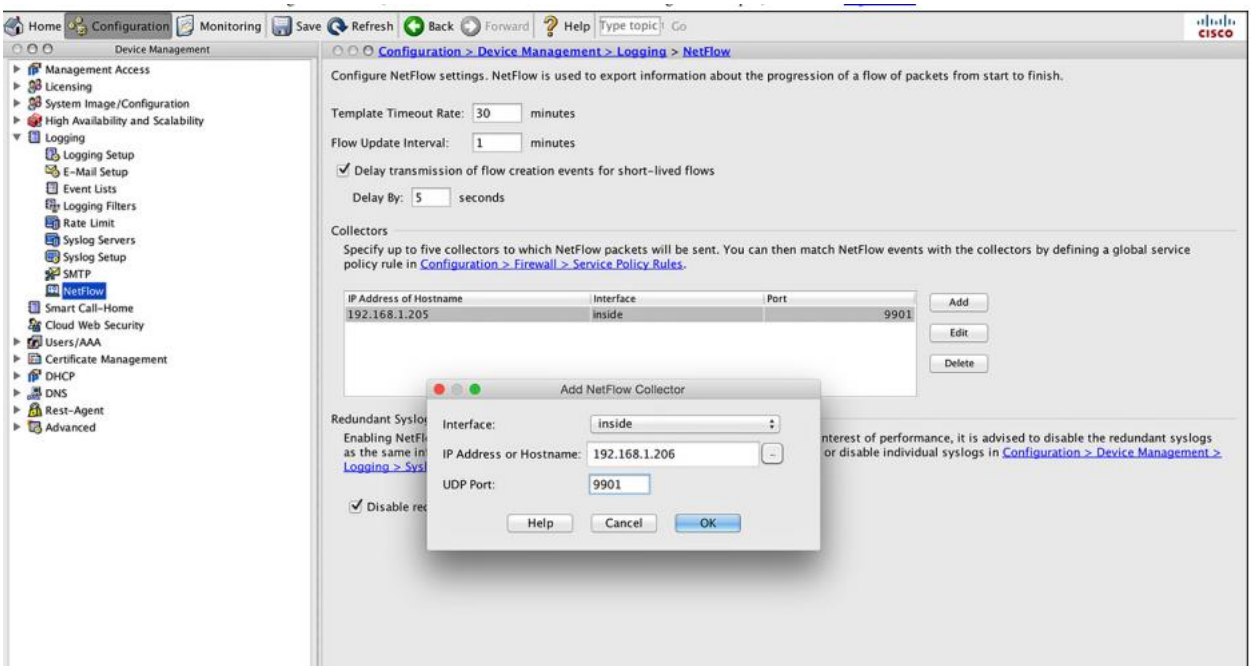
Enter the **template timeout rate** (in minutes). This is the time at which template records are sent to all configured collectors. In this example, the default value is configured (30 minutes).

Enter the **flow update interval**, which is the time interval between flow-update events.
You can configure the flow update interval from 1 to 60 minutes. In this example, the default value is configured (1 minute).

You can configure the Cisco ASA to delay the export of flow-creation events and process a single flow-teardown event instead of a flow-creation event and a flow-teardown event. To do so, check the **Delay Export of Flow Creation Events for Short-Lived Flows** checkbox.
In this example, the number of seconds for the delay in the Delay By field is configured to 5 seconds.

You can configure a maximum of five NetFlow collectors.
In this example, a NetFlow collector with the IP address 192.168.1.205 is already configured in the inside interface and using UDP port 9901.

Let's add a second collector. To configure a collector, click **Add**.
The Add NetFlow Collector dialog box will open, as shown in next page.



From the drop-down menu, **choose the interface to which NetFlow packets will be sent.**
The inside interface is selected in this example.

Enter the IP address or hostname and the UDP port number in the respective fields.
The IP address of the new collector is 192.168.1.206 and the UDP port is 9901.

Step 8. Click **OK** , Click **Apply ,** Click **Save**

Configuring NSEL in the Cisco ASA Using the CLI

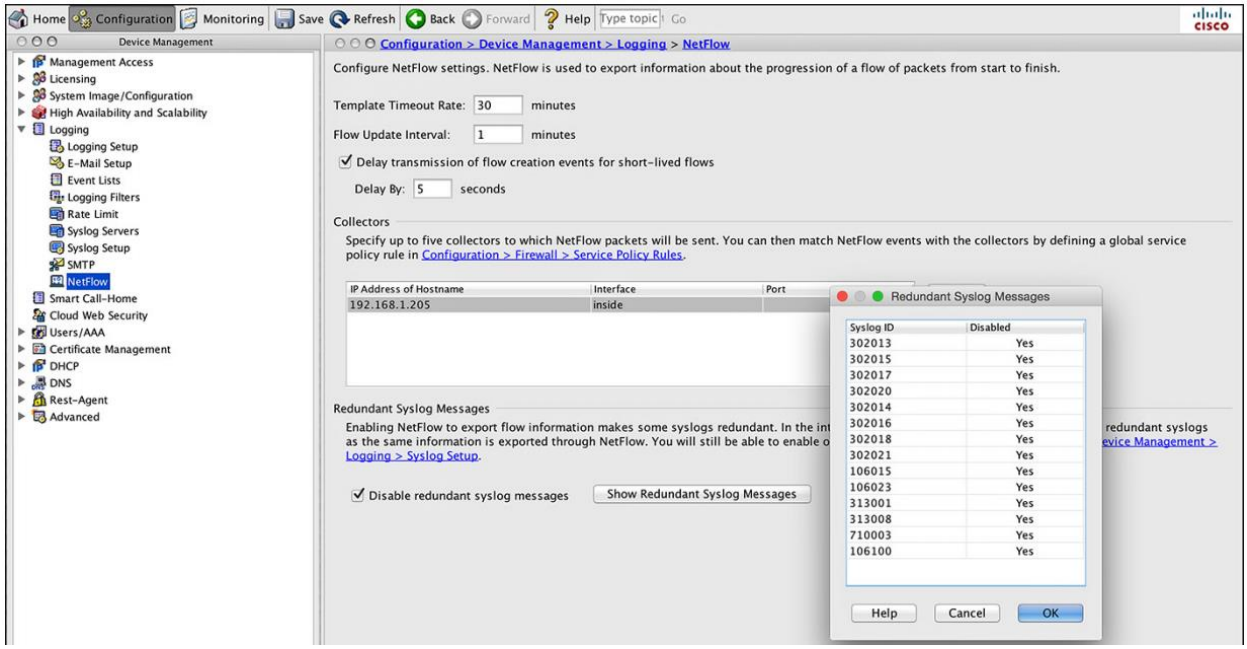
RTP-ASA
enable
configure terminal
flow-export destination inside 192.168.1.205 9001
flow-export delay flow-create 5

NSEL and Syslog

When you configure NSEL in the Cisco ASA, several syslog messages become redundant.
It is recommended that you disable all redundant syslog messages.

Disabling Redundant Syslog Messages Using the ASDM

To disable all redundant syslog messages, navigate to
Configuration > Device Management > Logging > NetFlow and check the Disable Redundant Syslog Messages check box.



Disabling Redundant Syslog Messages Using the CLI

```
rtp-asa(config)# no logging message 106015
rtp-asa(config)# no logging message 313001
rtp-asa(config)# no logging message 313008
rtp-asa(config)# no logging message 106023
rtp-asa(config)# no logging message 710003
rtp-asa(config)# no logging message 106100
rtp-asa(config)# no logging message 302015
rtp-asa(config)# no logging message 302014
rtp-asa(config)# no logging message 302013
rtp-asa(config)# no logging message 302018
rtp-asa(config)# no logging message 302017
rtp-asa(config)# no logging message 302016
rtp-asa(config)# no logging message 302021
rtp-asa(config)# no logging message 302020
```

Defining the NSEL Export Policy
The Cisco ASA does not send NetFlow (NSEL) packets to any configured collectors until you classify the traffic type it should be monitoring to generate the NetFlow events.

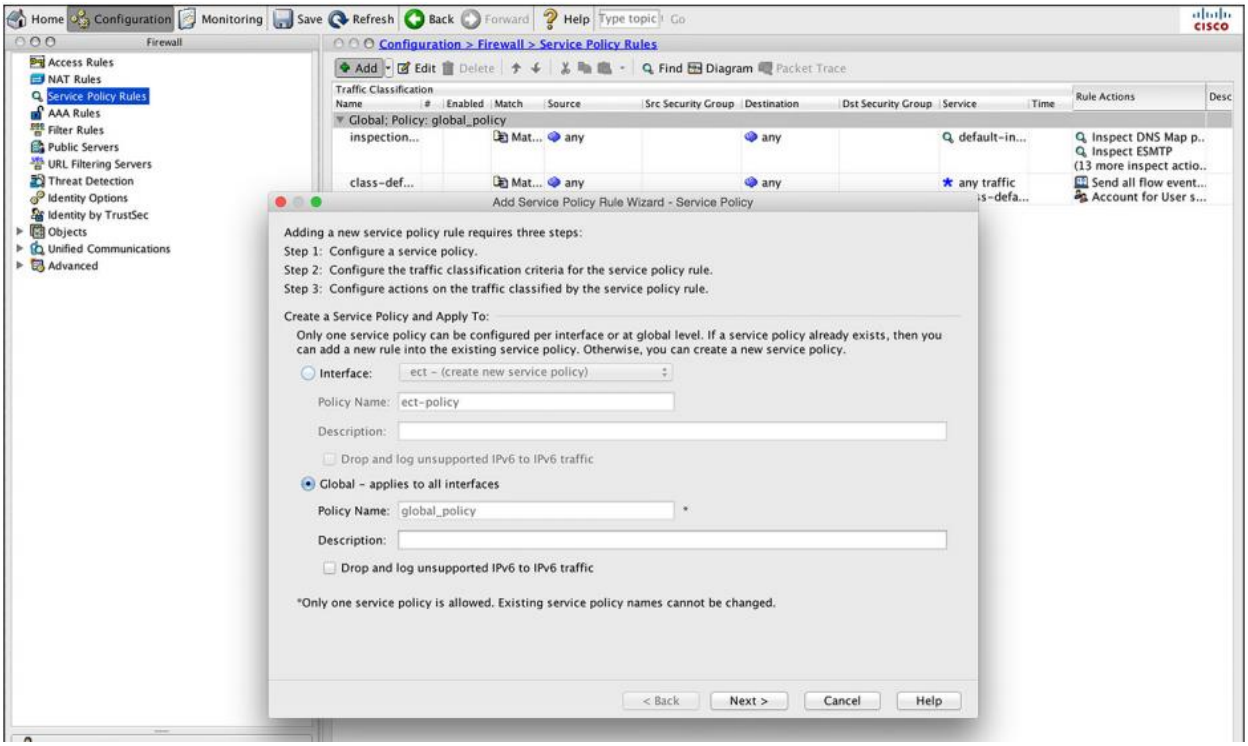
For example, if you want it to monitor all traffic for NetFlow exports, specify a global policy that analyzes all traffic.

NetFlow export policy is constructed via the MPF.

Define the NSEL export policy using the ASDM.

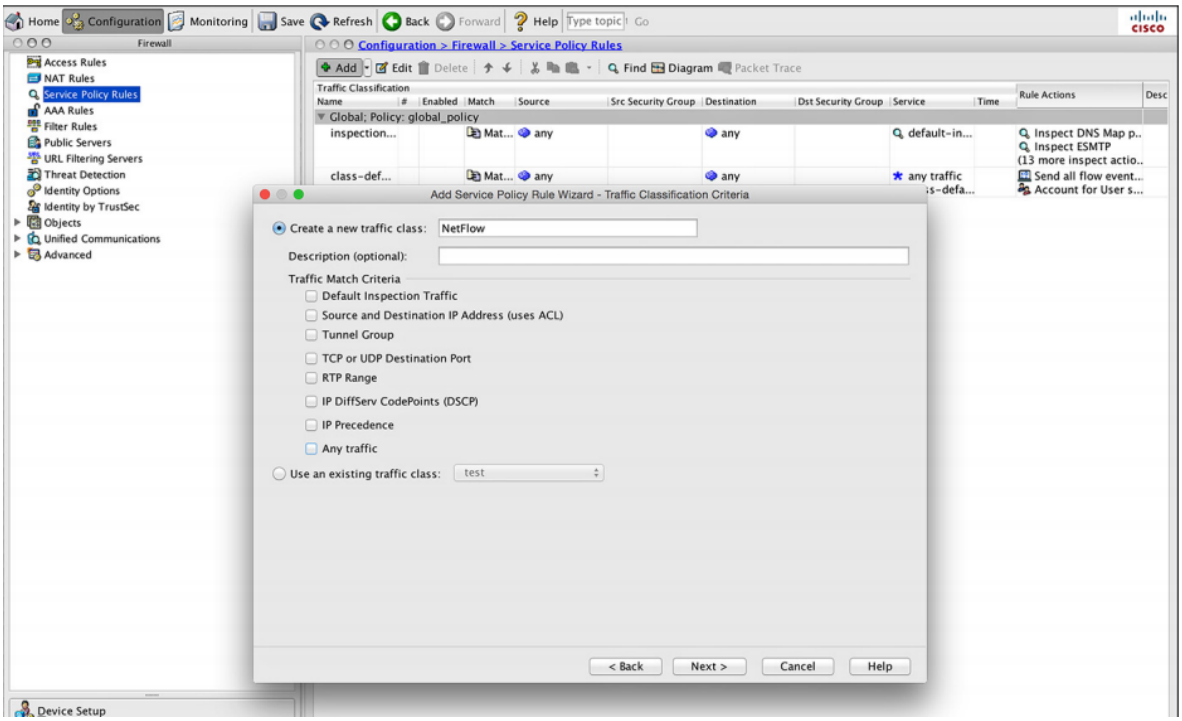
Navigate to **Configuration > Firewall > Service Policy Rules, select the inspection_default policy, and then choose Add > Insert After**. ASDM launches an Add Service Policy Rule Wizard.

Click the **Global – Applies to All Interfaces** radio button

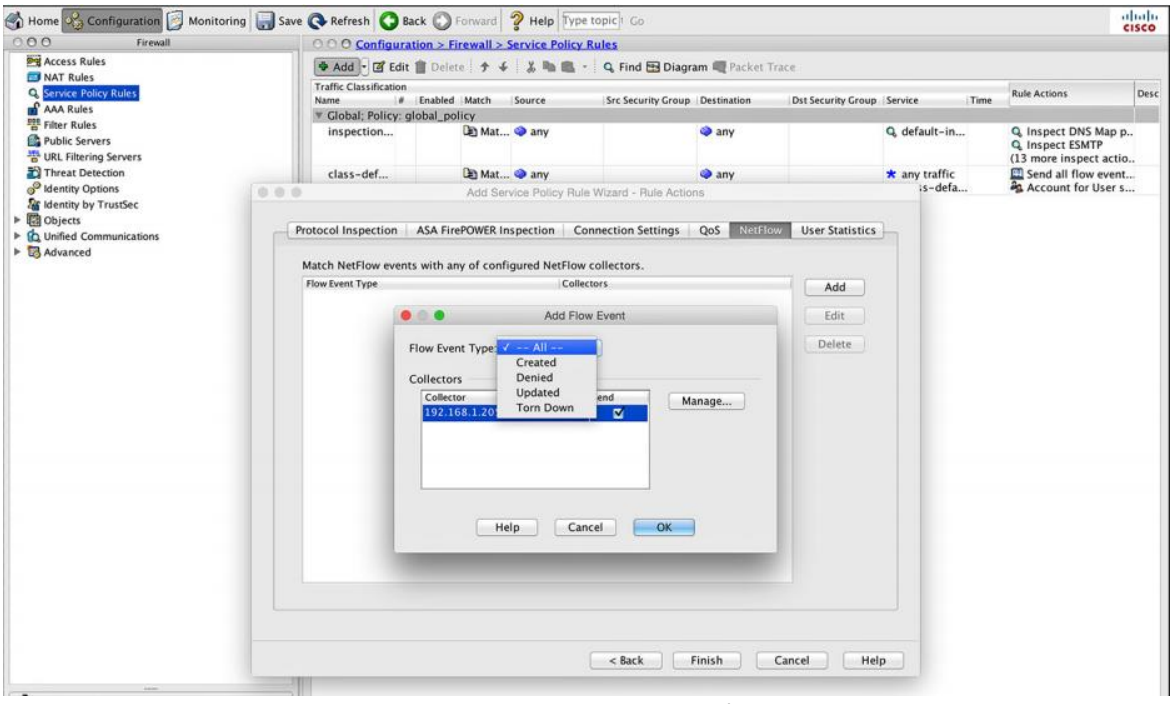


Click **Next**.

Under Create a New Traffic Class, specify a traffic class name of NetFlow.
Check the Any Traffic check box as the traffic match criteria,



Click **Next**.
Under Rule Actions, navigate to the **NetFlow tab** and click **Add**.
A new window opens where you can specify the flow event type



Select **All** and check the Send check box next to the collector's IP address.
The collector that was previously configured is displayed.

Click **OK** and then click **Finish** to complete defining a NetFlow export policy.

Define the NSEL export policy using the CLI.
enable
configure terminal
class-map NetFlow
match any
policy-map global_policy
class NetFlow
flow-export event-type all destination 192.168.1.205

Note to Remember about Net Flow
Net Flow **NOT Impacts performance** , HW implemented Net Flow has zero performance impact , SW implementation is typically significantly <15% processing overhead.

Net Flow has **NO bandwidth overhead** , since Net Flow is a summary protocol , Traffic overhead is typically significantly <1% of total traffic per exporting device

Now before we try to understand Lancope Stealth Watch system, let me explain two important things, first the concept of THE BIG DATA , second the Cisco Cyber Threat Defense CTD

What is Big Data?

It is a too large set of data [unstructured data,] complex to query or analysis with standard tools, such as Facebook data (billions of FB users' pictures, videos, notes and posts).

The size of data that can be classified as big data can range from a few terabytes to yottabytes of data in a single data set.
A petabyte is 1000 terabytes.
An exabyte is 1000 petabytes.
A zettabyte is 1000 exabytes.
A yoyabyte is 1000 zettabytes

Not only Facebook but also in networks we can see the existence of Big data .
In the world of cyber security, a lot of the network traffic can be also categorized as unstructured data:

- Syslog messages [from Routers,Switches,Firewall]
- IPS/FirePOWER logs
- AAA,SNMP logs [from Routers,Switches,Firewall , ACS , ISE]
- Netflow data [from Routers,Switches,Firewall in R&S,DC or SP environments]
- Routing Information
- Management access logs
- Configuration changes
- Packet captures

Industry experts estimate that the majority of the data in any organization is unstructured, and the amount of unstructured data is growing significantly. There are numerous, disparate data sources. There is an industry concept called Not-Only SQL (NoSQL), which is the name given to several databases that do not require SQL to process data. However, some of these databases support both SQL and non-SQL forms of data processing.

Big data analytics can be done in combination of advanced analytics and data mining, they get all data then extract it according to set of rules then take the output and apply set of filtration based of specific criteria to finally got a useful meaningful output of data.

Introduction to Cisco Cyber Threat Defense CTD v2.0

According to Cisco Cyber Threat Defense v2.0 Design Guide , which you can download for free from below link
http://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

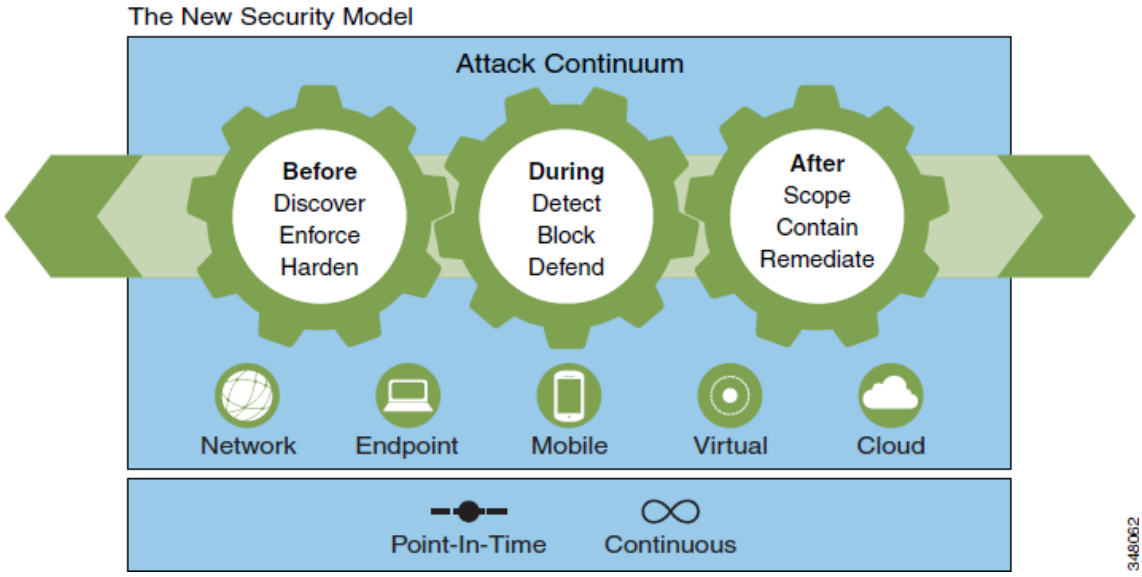
The goal of the Cyber Threat Defense solution is to introduce a design and architecture that can help facilitate the discovery, containment, and remediation of threats once they have penetrated into the network interior.

Indicators of compromise IoC is an artifact observed on a network or in OS that with high confidence indicates a computer intrusion.

The nature of the APT and the modern threat leads to think about having advanced **indicators of compromise (IOC)** that answer many important questions such as
•What is this attack (such as a known type or category)?
•What are the attack specifics, such as how it is/was executed? What may have changed on the target endpoint, and so on?
•Where did the attack originate?
•How was hostility determined?
•What is the target? Host? User?
•What other systems/users has this device contacted?
•What is the targeted application or data?
•Does the target have a chance to be impacted by this event?
•Is this a new issue or was it delivered via an outside source, such as bring-your-own-device (BYOD)?
•Is the attacking host currently in the network or outside the network?
•What was/is the root cause?
•Can the system identify immediately how many hosts or network devices may be vulnerable to this threat?
•If this attack is blocked, how can the system determine whether it is a false positive or true positive?

There are many IoCs from the network which we need to piece together to solve the case we are facing: IPS/IDS Alert ,IP Address , File Hashes ,Log Analysis SIEM , Raw flow analysis, Outside notification, Anomaly detection, Behavioral analysis, Activity monitoring
To achieve an advanced indication of compromise capability, events must be correlated from the following:
•Malware activities
•Intrusion detections
•Network connections
•Network file trajectories
•Device trajectories
•Device network flows, including but not limited to lateral movements, parent-child relationship, or context

All This lead Cisco to create New Security Model



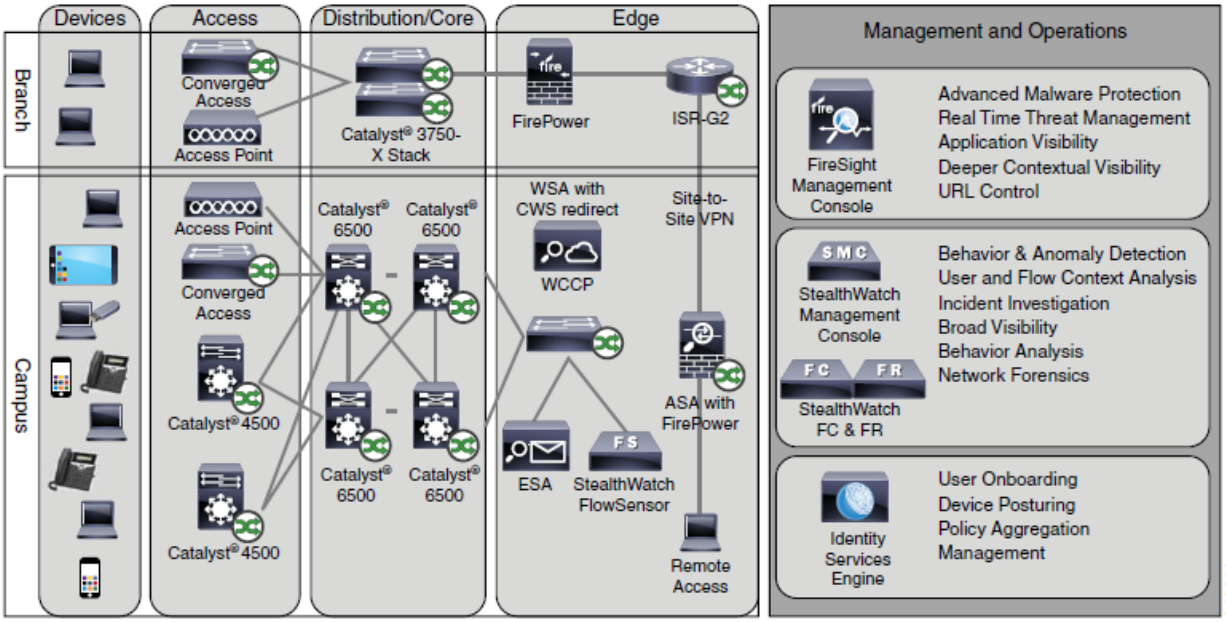
This model addresses the threat problem by looking at the actions you must take **before**, **during**, and **after** an attack, as well as across the broad range of attack vectors such as endpoints, mobile devices, data center assets, virtual machines, and even in the cloud. Where most security solutions tend to address the threat at a point in time, it is important to look at it as a continuous cycle.

The Cyber Threat Defense 2.0 Solution's primary focus is on the "During" and "After" stages of the Attack Continuum. Additional security solutions can be found on the Cisco DesignZone website.

The Cyber Threat Defense advice you to use many Security Products from Cisco to Protect your network in the three stages **before**, **during**, and **after** an attack.

It worth to mention that NetFlow is a key element of the original version of the Cisco Cyber Threat Defense solution.

Figure 1 High-Level Architecture of the Cisco Cyber Threat Defense Solution



Cisco Cyber Threat Defense version 2.0 makes use of several solutions to accomplish its objectives:

- NetFlow and the Lancope StealthWatch System
  - Broad visibility
  - User and flow context analysis
  - Network behavior and anomaly detection
  - Incident response and network forensics
- Cisco FirePOWER and FireSIGHT
  - Real-time threat management
  - Deeper contextual visibility for threats bypassing the perimeters
  - URL control
- Advanced Malware Protection (AMP)
  - Endpoint control with AMP for Endpoints
  - Malware control with AMP for networks and content

- Content Security Appliances and Services
  - Cisco Web Security Appliance (WSA) and Cloud Web Security (CWS)
    - Dynamic threat control for web traffic
    - Outbound URL analysis and data transfer controls
    - Detection of suspicious web activity
  - Cisco Email Security Appliance (ESA)
    - Dynamic threat control for email traffic
    - Detection of suspicious email activity
- Cisco Identity Services Engine (ISE)
  - User and device identity integration with Lancope StealthWatch
  - Remediation policy actions using pxGrid

For more info about CTD 2.0
https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

Introduction to Cisco Lancope Stealth Watch

- Cisco has acquired Lancope, a privately held company headquartered in Alpharetta, GA.
- Lancope helps customers monitor, detect, analyze and respond to modern threats on enterprise networks through continuous network visibility and specialized threat analysis and protection.

- Lancope's StealthWatch system provides visibility into suspicious traffic patterns inside the network to quickly detect a wide range of attacks. This helps enterprises reduce time to detection, respond to incidents faster, improve forensic investigations, and reduce risks for the company.

- Lancope's StealthWatch solution is a key component of the Cisco Cyber Threat Defense (CTD) Solution.

- The Lancope StealthWatch System aggregates and normalizes considerable amounts of NetFlow data to apply security analytics to detect malicious and suspicious activity.

- The Lancope StealthWatch System, is a purpose-built, high-performance network visibility and security intelligence solution.

- Through the collection, aggregation, and analysis of NetFlow data, along with other contextual data sources such as identity data from Cisco ISE, system-specific data such as syslog and Simple Network Management Protocol (SNMP), and application data via NBAR2 and Cisco AVC, the StealthWatch system helps security operations staff gain real-time situational awareness of all users, devices, and traffic on the network.

- With stealthwatch you can discover if internal/external user trying to copy inside data to outside of your organization , if he try to practice in DDoS attack or if he bring malware by mistake or in purpose to his organization.

- With stealthwatch you can discover network performance , investigate malware activities inside your organization.

StealthWatch Mandatory Components

- **Stealthwatch FlowCollector FC**

  Serves as a central collector for flow data generated by NetFlow-enabled devices.
  The StealthWatch FlowCollector monitors, categorizes, and analyzes network traffic to create comprehensive security intelligence at both the network and host level.

- **Stealthwatch Managmenet Console SMC**

  Manages, coordinates, and configures all StealthWatch appliances to correlate security and network intelligence across the enterprise.
  Retrieves authenticated session information from the Cisco ISE to correlate flow and identity.
- **Flow licenses**

StealthWatch optional Components

- **Stealthwatch FlowSensor FS**

  Passively monitors all host and server communications and network traffic statistics, translating them into flow records, which are sent to FlowCollectors. The main benefit about it is providing Layer 7 visibility by doing deep packet inspection which means adding more valuable information in Flow records.

- **Stealthwatch Flow Replicator (UDP Director) FR**

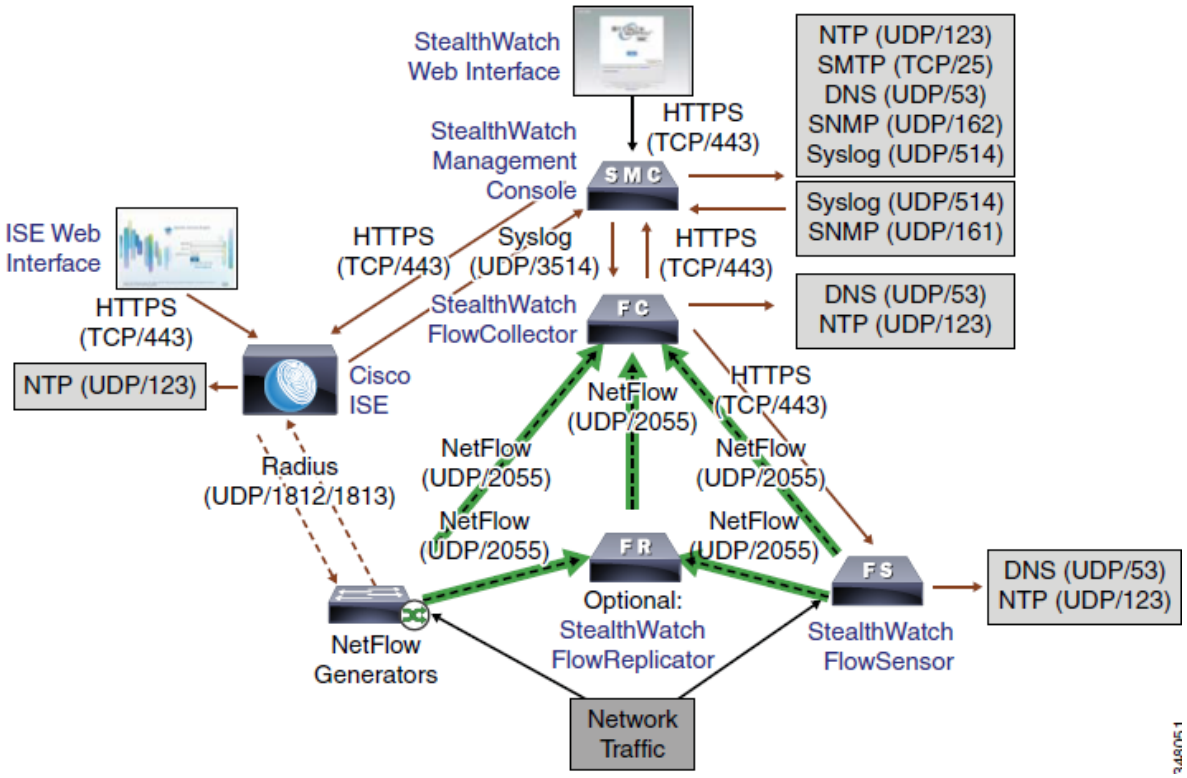
  Aggregates NetFlow, syslog, and SNMP information in a single, high-speed appliance. This high-speed UDP packet replicator gathers essential network optimization and security information from multiple locations, and then forwards this information in a single data stream to one or more StealthWatch FlowCollector appliances.

- **StealthWatch IDentity**
- **Stealthwatch Endpoint License**
- **Stealthwatch Flow Cloud license**

Many of these components comes as

- **Physical Appliance**
- **Virtual Appliances [also known as** virtual edition VE **]**

Figure 4 Lancope StealthWatch System



You need to install and configure your virtual appliances [virtual edition (VE)] in the following order:

1. UDP Director VE (also known as FlowReplicator VE)
2. FlowSensor VE
3. FlowCollector VE
4. SMC VE

If you do not follow this recommended order, when you set up the StealthWatch system, the SMC VE may not properly collect data from the appliances and you will have to set up each one separately.

The following are the Primary components of the Lancope StealthWatch System:

1-FlowCollector [FC]

- It is a physical or virtual appliance that collects NetFlow data from infrastructure devices.
- It is just netflow collector , it will gather data from Stealthwatch FlowSensors and other devices , data came from cFlow,J-Flow , Net Flow , IPFIX , NSEL , NetStream and NetFLOW with NBAR.
- Then it will monitor , analyzes , categorizes and store the data (records) and create a baseline of typical network activity , if unusual activity occurs it will send alarm to setalthwatch Management Console
- Can collect flows from 4000 exporters and sources , up to sustained 240,000 fps
- The FlowCollector uses flow-based anomaly detection to zoom in on any unusual behavior and immediately sends an alarm with actionable intelligence that allows personnel to take quick, decisive steps to mitigate any issues.
- Operators can use the Stealthwatch System's unique drill-down features to identify and isolate the root cause within seconds, enhancing operational efficiency, decreasing costs and dramatically reducing the time from problem onset to resolution.

FC provides :

- Baseline of all IP traffic
- Anomaly detection in traffic/host behavior
- Layer 7 anomaly detection
- Appliance or virtual deployment options
- NAT stitching
- P2P file sharing detection
- Host and service profiling
- Index-based prioritization technology
- OS fingerprinting
- Support for application-aware flows such as NBAR2
- Support for custom applications
- Closest interface determination and tracking
- De-duplication of flows
- Virtual environment monitoring
- Host Group tracking and reporting
- Router interface tracking and reporting
- Bandwidth accounting and reporting
- Packet-level performance metrics
- QoS (DSCP) monitoring
- Interface utilization alarming
- Unauthorized host access detection
- Unauthorized Web server detection

- Misconfigured firewall detection
- Combined internal and external monitoring
- Full flow logging
- Worm detection
- Botnet detection
- DoS/DDoS detection (SYN, ICMP, or UDP flood)
- Fragmentation attack detection
- Network scanning and reconnaissance detection
- Large file transfer detection
- Rogue server detection
- Long term flow retention

> "...a **single** FlowCollector can store and analyze data from as many as **4,000 flow sources** at up to **240,000 flows per second.**"

StealthWatch FlowCollector Features Matrix

Features	Network	Security
Automatic baselining of all IP traffic	✓	✓
Automatic anomaly detection in traffic/host behavior	✓	✓
Layer 7 anomaly detection*	✓	✓
Massive scalability	✓	✓
Flexible deployment options, including virtual	✓	✓
NAT stitching	✓	✓
Peer-to-Peer (P2P) file sharing detection	✓	✓
Host and service profiling	✓	✓
Index-based prioritization technology	✓	✓
OS fingerprinting**	✓	✓
Support for application-aware flows such as NBAR2	✓	✓
Support for custom applications	✓	✓
Closest interface determination and tracking	✓	✓
Deduplication of flows	✓	✓
Virtual environment monitoring*	✓	✓

Host Group tracking and reporting	✓	✓
Unauthorized host access detection*	✓	✓
Unauthorized web server detection	✓	✓
Misconfigured firewalls detection*	✓	✓
Combined internal and external monitoring	✓	✓
Router interface tracking and reporting	✓	
Bandwidth accounting and reporting	✓	
Packet-level performance metrics*	✓	
QoS (DSCP) monitoring	✓	
Interface utilization alarming	✓	
Full flow logging		✓
Worm detection		✓
Botnet detection*		✓
DoS/DDoS detection (SYN, ICMP or UDP flood)		✓
Fragmentation attack detection**		✓
Network scanning and reconnaissance detection		✓
Large file transfer detection		✓
Rogue server detection		✓

Each StealthWatch FlowCollector can support a minimum guaranteed flow volume, as listed below.

However, also consider the following factors in the selection of a StealthWatch FlowCollector for the Cisco Cyber Threat Defense solution version 2.0:

•**Exporter count**—Number of NetFlow generation devices that each StealthWatch FlowCollector can accept.

•**Data rate**—Rate of fps that the StealthWatch FlowCollector is receiving.

•**Host count**—Number of hosts (both inside and outside the network) for which the StealthWatch FlowCollector can maintain state. Cisco recommends that the number of inside hosts not exceed 60 percent of the host count value.

•**Flow storage**—Amount of granular flow data required for a particular location on the network.

Table 5 StealthWatch FlowCollector Appliance Specifications

Model	Flows per Second	Exporters	Hosts	Storage
StealthWatch FlowCollector 1000	Up to 30,000	Up to 500	Up to 250,000	1.0 TB
StealthWatch FlowCollector 2000	Up to 60,000	Up to 1000	Up to 500,000	2.0 TB
StealthWatch FlowCollector 4000	Up to 120,000	Up to 2000	Up to 1,000,000	4.0 TB

Table 6 StealthWatch FlowCollector VE Specifications

Flows per second	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 4500	Up to 250	Up to 125,000	4 GB	2
Up to 15,000	Up to 500	Up to 250,000	8 GB	3
Up to 22,500	Up to 1000	Up to 500,000	16 GB	4
Up to 30,000	Up to 1000	Up to 500,000	32 GB	5

2-StealthWatch Management Console [SMC]

- Comes in two different form factors (just like the StealthWatch FlowCollectors) , appliances and virtual edition (VE).
- Used for reporting and to manage the rest of the Lancope StealthWatch solution.
- Can manage up to 25 Flow Collectors and up to 6 million fps globally
- SMC provides a rich graphical unit interface (GUI) with many visualizations and telemetry information.

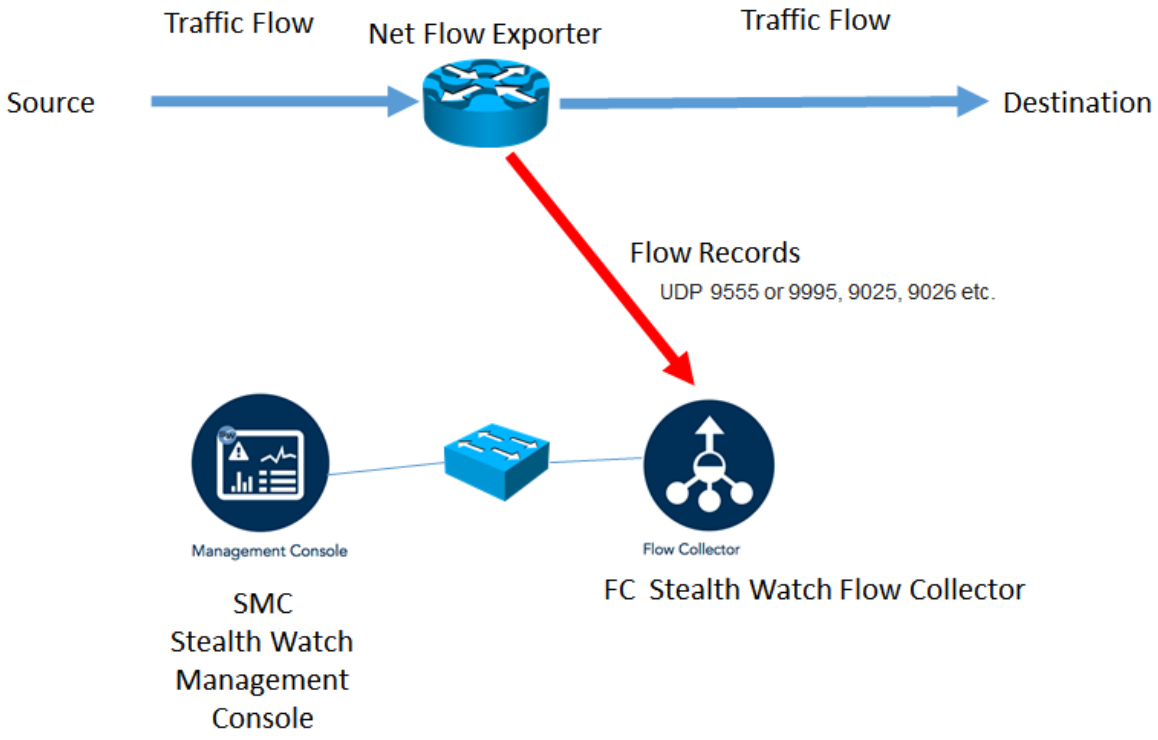


Table 7 SMC Appliance Specifications

SMC Model	Maximum FlowCollectors	Size	Storage	Memory
SMC 1000	5	1 RU	1.0 TB	8 GB
SMC 2000	25	2 RU	2.0 TB	16 GB

Table 8 SMC VE Specifications

FlowCollectors	Concurrent Users	Reserved Memory	Reserved CPUs
1	2	4 GB	2
3	5	8 GB	3
5	10	16 GB	4

SMC provides the following features:

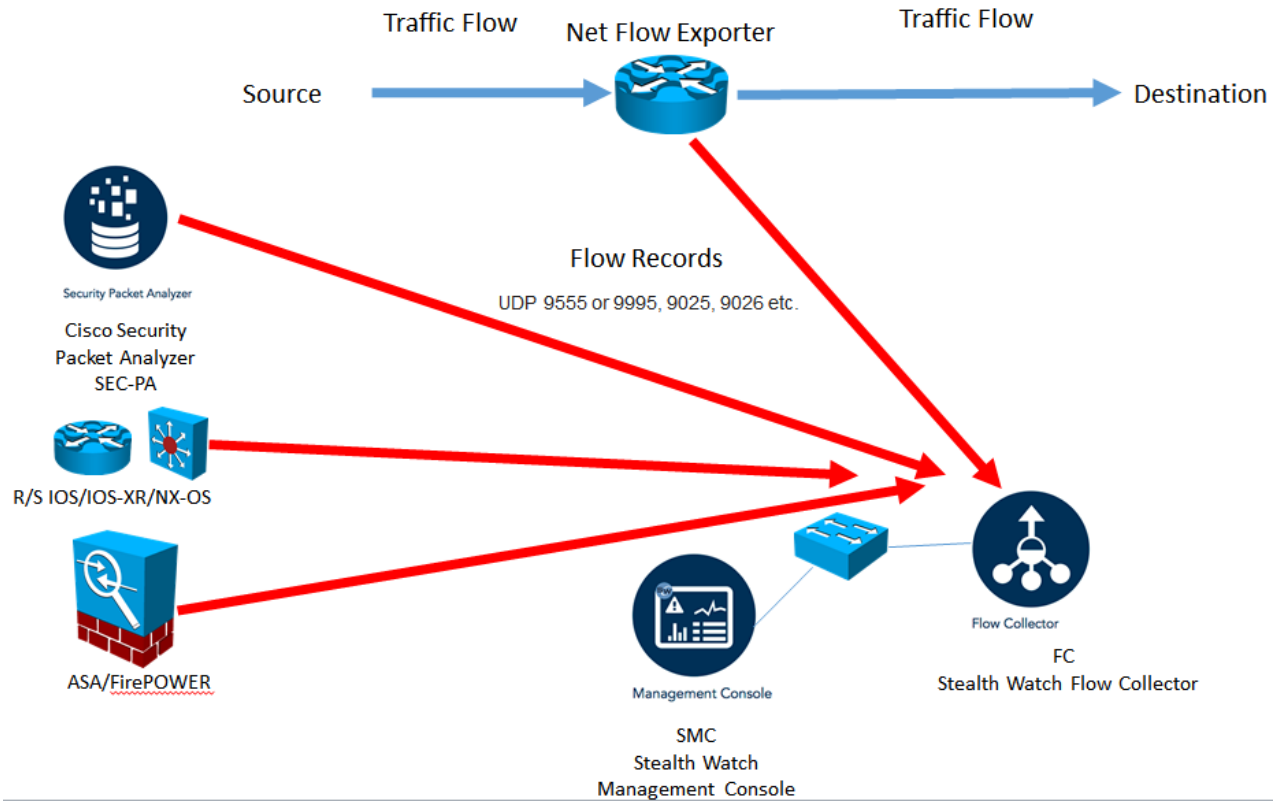
- User identity tracking
- Appliance and virtual deployment options
- Root-cause analysis and troubleshooting
- Relational flow maps
- NAT stitching
- Custom dashboards
- Custom reporting
- Blocking, remediation or rate limiting
- Top N reports for applications, services, ports, protocols, hosts, peers and conversations
- Traffic composition breakdown
- Customizable user interface based on Point-of-View technology
- Advanced flow visualization
- Internal and external monitoring
- Capacity planning and historical traffic trending
- WAN optimization reporting
- DSCP bandwidth utilization
- Worm propagation visualization
- Internal security for high-speed networks

3-Flow licenses, which are required to aggregate flows at the StealthWatch Management Console. (Flow licenses define the volume of flows that may be collected.)

What is Cisco Security Packet Analyzer 2400 Appliance ?

In below picture you can see another appliance from Cisco **(this product is not part of lancope stealthwatch system but it can be a useful part for our Solution)**

- The Cisco Security Packet Analyzer provides tools that help you investigate security events and anomalous network activity.
- It works in conjunction with Cisco Stealthwatch to speed incident response and network forensics.
- It is packet capture solutions. These can collect and store all of the information that traverses the network.
- Cisco Security Packet Analyzer uses Stealthwatch flow data analysis to locate specific points in the data stream. It then generates a detailed search query to locate those packets.
- The Cisco Security Packet Analyzer enhances "detect and respond" capabilities to help defend your network. Dive deep into anomalous network activity and security events to get the complete status of your network.



The following are optional components of the Lancope StealthWatch System:

1-FlowSensor [FS]

- A physical or virtual appliance that can generate NetFlow data when legacy Cisco network infrastructure components are not capable of producing line-rate, un-sampled NetFlow data.

- Alternatively, you can use the Cisco NGA instead of Stealthwatch Flow Sensor .
(Will talk about NGA later)

Table 3 StealthWatch FlowSensor Appliance Specifications

Model	Processing Capacity	Interface	Speed	Physical Layer	Form Factor	Power
250	100 Mbps	2	10/100/100	Copper	1 RU-short	Non-redundant
1000	1 Gbps	3	10/100/1000	Copper	1 RU-short	Non-redundant
2000	60,000	5	10/100/1000	Copper or Fibre	1 RU	Redundant
3000	120,000	1 or 2	1GB	Fibre	1 RU	Redundant

- The Stealthwatch FlowSensor uses a combination of **deep packet inspection (DPI)** and behavioral analysis to identify Layer 7 applications and protocols in use across the network – no matter if they are plain text or use advanced encryption and obfuscation techniques.

- It also gathers packet-level performance statistics at a fraction of the cost of traditional probe-based devices, playing a key role in troubleshooting both security incidents and application performance problems.

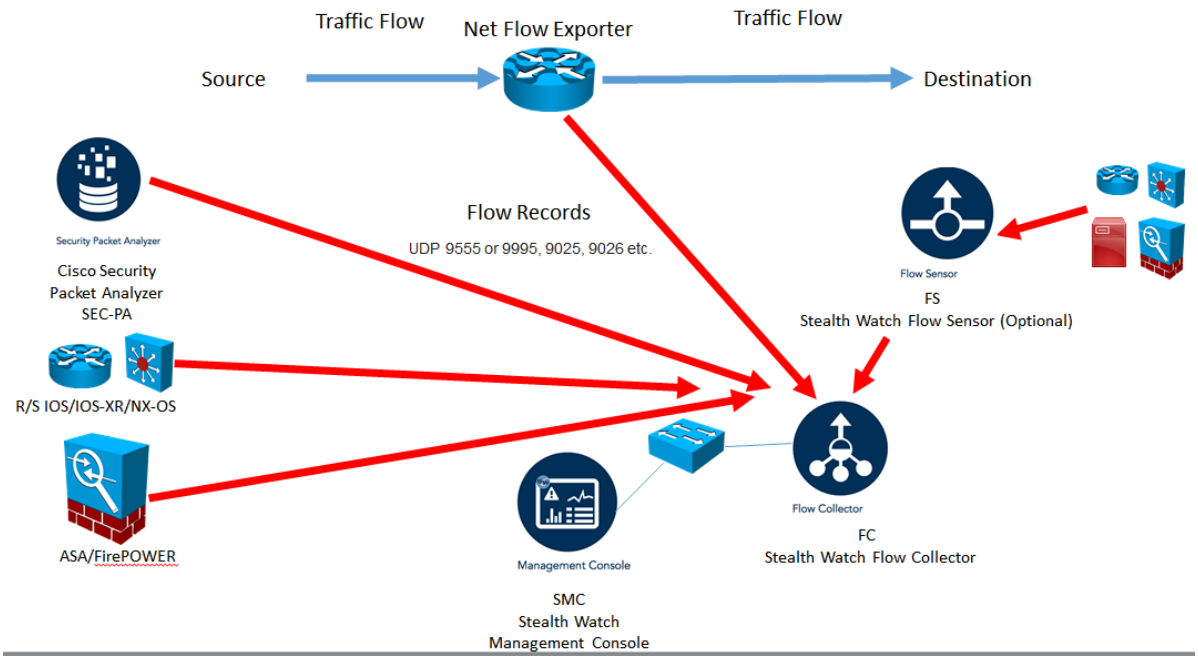
- Additionally, the FlowSensor VE (Virtual Edition) enables operators to see the same detailed traffic statistics for their virtual networks as they can for their physical environments, eliminating dangerous network blind spots.

Table 4 StealthWatch FlowSensor VE Specifications

Disk Space Requirement	Flow Export Format	Minimum CPU Requirements	Minimum Memory Requirement	Interfaces
1.4 GB	NetFlow v9	2 GHz Processor	512 MB 1024 MB for application inspection	Up to 16 vNICs

- FlowSensor appliance connect to your infrastructure using SPAN or TAP or any port mirroring mechanism.

- FlowSensor will start capture frames and observe it while same time it will calculates various performance statistics (such as round trip time RTT , server response time SRT and packet loss for TCP sessions) for each flow and export them with these performance statistics data to FlowCollector appliance .



FS provides:

- Identifies applications and protocols regards of whether they are:
- ✓ Plain text
- ✓ Advanced encryption
- ✓ Obfuscation techniques
- Provides application including SRT, RTT, MTTK
- Packet-level metrics such as HTTP/HTTPS Header Data and packet paylod
- Able to create Netflow data in environments where it is not enabled

What is [NGA]Cisco NetFlow Generation 3000 Series Appliances ?

(This product is not part of lancope stealthwatch system but it can be a useful part for our Solution)

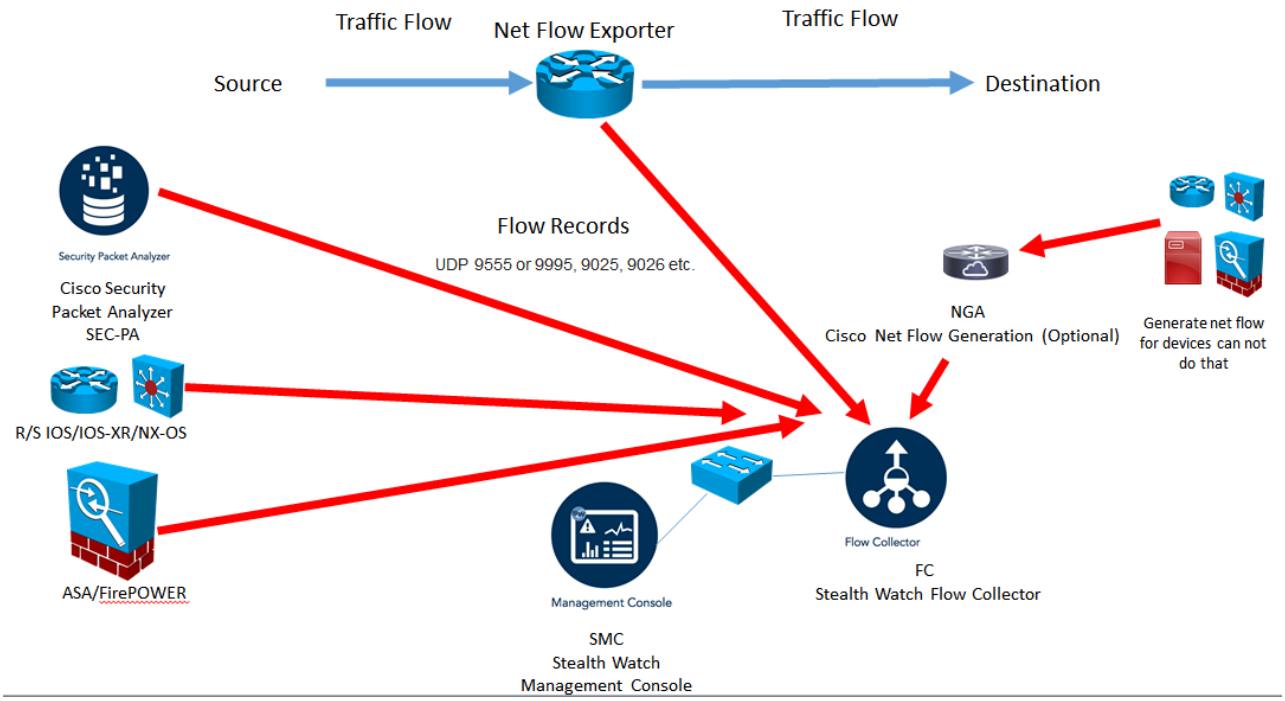
Cisco NGA consumes raw network data from platforms such as Cisco Nexus ® 7000, Cisco Nexus 5000, Cisco Nexus 3000, and Catalyst ® 6500 Series Switches to create and export NetFlow Data Export (NDE) records (Version 5 [v5], Version 9 [v9], IPFIX) for traffic analysis and other management needs.

Built-on best-in-class Cisco UCS C220 M4 hardware, the NGA 3340 generates, unifies, and exports flow data, empowering network operations, engineering, and security teams to:

- Achieve operational efficiencies
- Improve services delivery
- Assure billing accuracy
- Harden network security

The NGA can export NetFlow records to multiple collectors concurrently, providing a single flow source for business-critical management applications such as security, billing, capacity planning, and more.

The NGA is a part of the Cisco Application Centric Infrastructure [ACI]. It integrates with Cisco Nexus switches, including the new Cisco Nexus 9000 Series, to simplify manageability in the data center by helping enable unified flow visibility across the L2 and L3 domains. The NGA is also a component of the Cisco Prime for IT portfolio.



2-FlowReplicator (aka UDP Director) [FR]

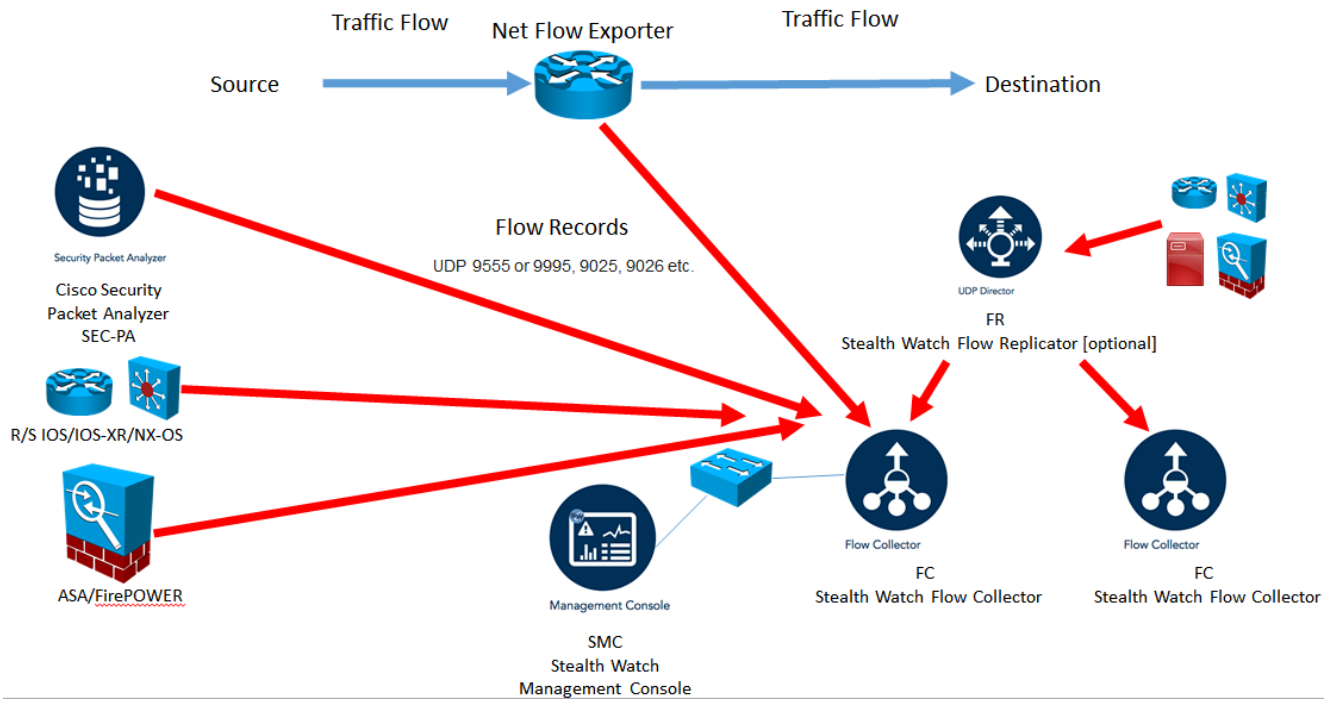
- A physical appliance used to forward NetFlow data as a single data stream to other devices.
- The StealthWatch FlowReplicator supports Cisco NetFlow, IPFIX, and other vendors' flow data.
- It combines multiple capabilities into a single device to streamline the collection and distribution of network and security data across the corporate network.
- The StealthWatch FR can receive data from any connectionless UDP application and syslog messages and then replicate those to network analysis systems.
- In addition, StealthWatch FR can process Simple Network Management Protocol (SNMP) traps from network infrastructure devices and distribute them to several different SNMP management stations.
- Each FlowReplicator comes with two active interfaces: one is assigned an IP address for management, monitoring, and generation of packet copies; and the other can be put into promiscuous mode for monitoring.
- Each FlowReplicator is rated for a certain volume of input and output in terms of packets per second (pps).
- Each is tested against a generation of two to three copies per packet, but can support more destinations if required.

Table 9 StealthWatch FlowReplicator Appliance Specifications

FlowReplicator Model	Processing Capacity	Physical Layer	Form Factor	Power	Fault Tolerant
1000	10,000 pps input 20,000 pps output	Copper	1 RU-short	Non-redundant	No
2000	20,000 pps input 60,000 pps output	Copper or Fiber	1 RU	Redundant	Yes

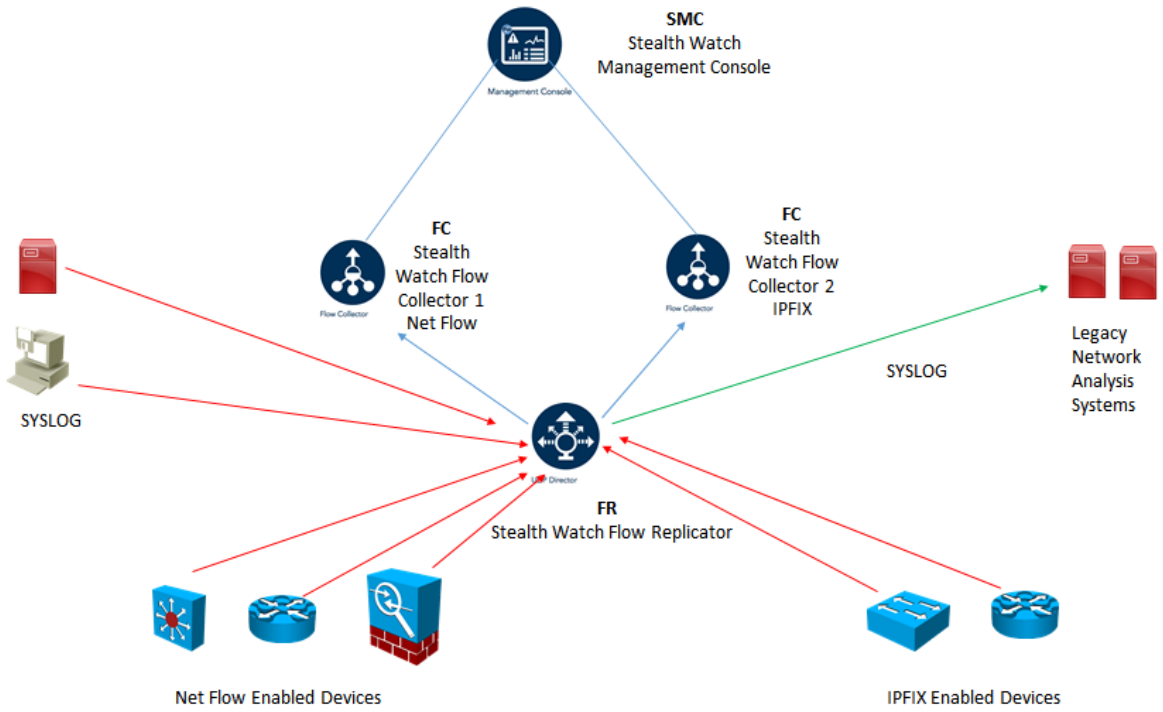
FR provides:

•Simplifies collection of network and security data
•Reduces points of failure on your network
•Provides a single destination for all UDP formats on the network including Netflow, SNMP, syslog, etc
•Reduces network congestion for optimum network performance



CTD Best Practice: All NetFlow records belonging to a flow should be sent to the same StealthWatch FlowCollector.

In below picture, the StealthWatch FR sends all NetFlow data to the StealthWatch FlowCollector 1 and all IPFIX data to the StealthWatch FlowCollector 2.



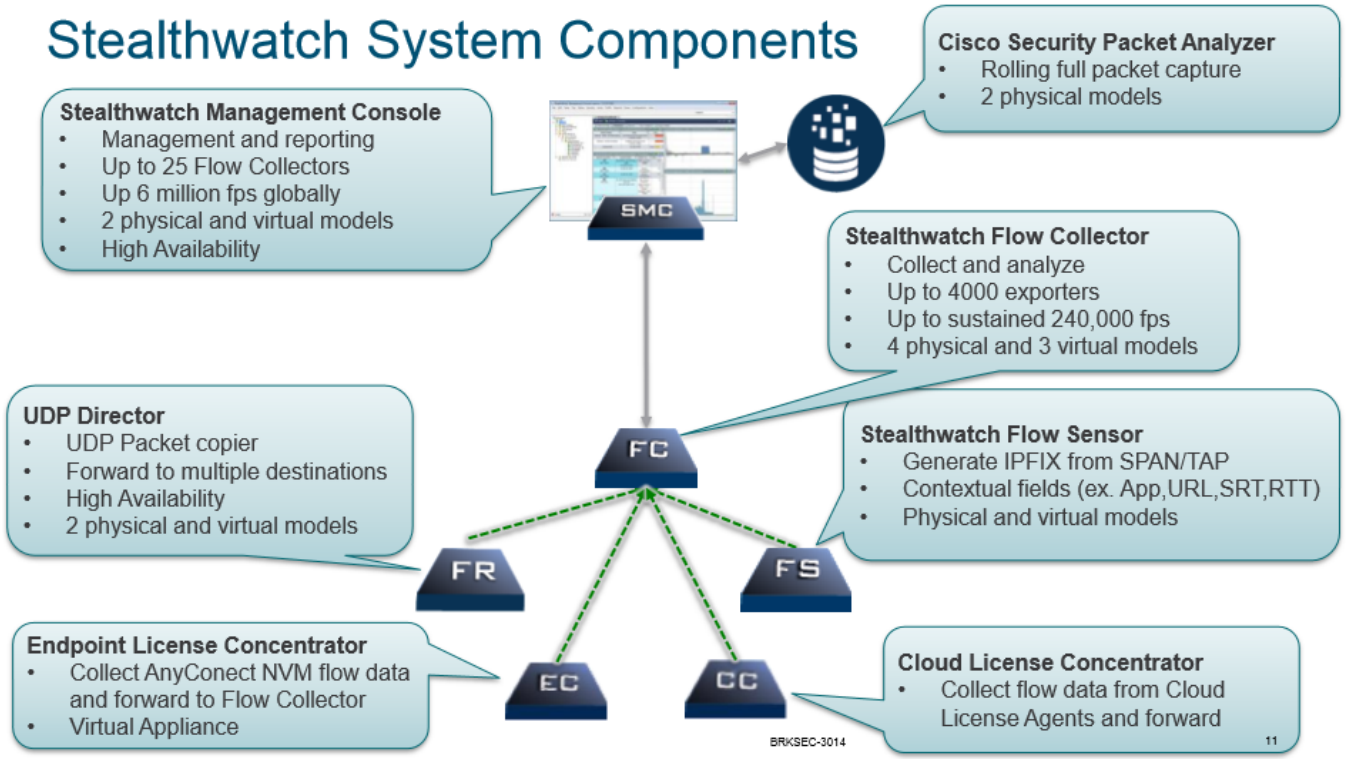
3-StealthWatch IDentity

- Provides user identity monitoring capabilities. Administrators can search on user names to obtain a specific user network activity.

- Identity data can be obtained from the StealthWatch IDentity appliance or through integration with the Cisco ISE.

- One of the key benefits of Lancope's StealthWatch is its capability to scale in large enterprises.
- It also provides integration with the Cisco Identity Services Engine (ISE) for user identity information.

- Cisco ISE is a security policy management and control system that you can use for access control and security compliance for wired, wireless, and virtual private network (VPN) connections.



Deploying the Lancope StealthWatch System

Deploying StealthWatch Management Console SMC

The StealthWatch Management Console manages, coordinates, and configures all StealthWatch appliances, including the StealthWatch FlowCollector and the StealthWatch FlowReplicator.

It is designed to correlate network intelligence across the corporate network primarily using NetFlow. The StealthWatch Management Console can also be configured with the Cisco ISE to receive authenticated session information to correlate flow and identity.

Following table lists the different StealthWatch Management Console appliances and high-level specifications.

Model	Storage cabaibility	Memory	Number of FlowCollectors supported
StealthWatch Managmenet Console 1000	1TB	8GB	5
StealthWatch Managmenet Console 2000	2TB	16GB	25

Lancope recommends 8 GB for reserved memory. Less than 4 GB of memory is not supported. If less than 4 GB is allocated, a Low Memory alarm will be triggered and no flows will be stored in the database.

To determine the minimum resource allocations for the SMC VE, you should determine the number of FlowCollectors and users expected to log in to the SMC.

Refer to the following specifications to determine your resource allocations:

FlowCollectors	Concurrent Users*	Reserved Memory	Reserved CPUs
1	2	4 GB	2
3	5	8 GB	3
5	10	16 GB	4

Concurrent users include scheduled reports and people using the SMC client at the same time.

To determine your resource allocations for the FlowCollector VE, you should determine the flows per second expected on the network, and the number of exporters and hosts it is expected to monitor.

Refer to the following specifications to determine our resource allocations:

Flows per second	Exporters	Hosts	Reserved Memory	Reserved CPUs
Up to 4,500	Up to 250	Up to 125,000	4 GB	2
Up to 15,000	Up to 500	Up to 250,000	8 GB	3
Up to 22,500	Up to 1000	Up to 500,000	16 GB	4
Up to 30,000	Up to 1000	Up to 500,000	32 GB	5
Up to 60,000	Up to 1500	Up to 750,000	64GB	6
Up to 120,000	Up to 2000	Up to 1,000,000	128GB	7

The maximum amount of data storage allowed on either the FlowCollector VE or the SMC VE is 1 TB. The maximum disk space is 1.4 TB.

The virtual appliance uses approximately 75% of the disk for data storage, leaving 25% for the operating system and cache.

Therefore, always expand the disk to 40% more than the desired disk amount. If you expand the disk to more than 1.4 TB, the virtual appliance will not use the additional space for storage.

Lancope recommends allocating a minimum of 1 GB of disk storage for each day every 1,000 flows per second (FPS) your system averages daily multiplied by the number of days you want to store the flows. For example, If your system averages 2,000 FPS and you want to store flows for 30 days, allocate a minimum of 60 GB (2 X 30) of disk storage space.

FPS calculator https://www.lancope.com/fps-estimator
Bandwidth calculator https://www.lancope.com/bandwidth-calculator

Some other things to note when deploying StealthWatch:
•You can deploy the SMC in an HA failover pair for redundancy
•You can deploy the UDP Directors in an HA failover pair for redundancy or if you have a large environment, you could place them behind a load balancer
•When it comes to asymmetric routing, make sure the flow is going to the same FlowCollector
•If you place the FlowCollector outside a firewall, turn off the setting of "accept traffic from any exporter" or you may be flooded with sources you don't want to be flooded with

Depending on the services and if there is a firewall in the way, here are the ports that the appliances may utilize:

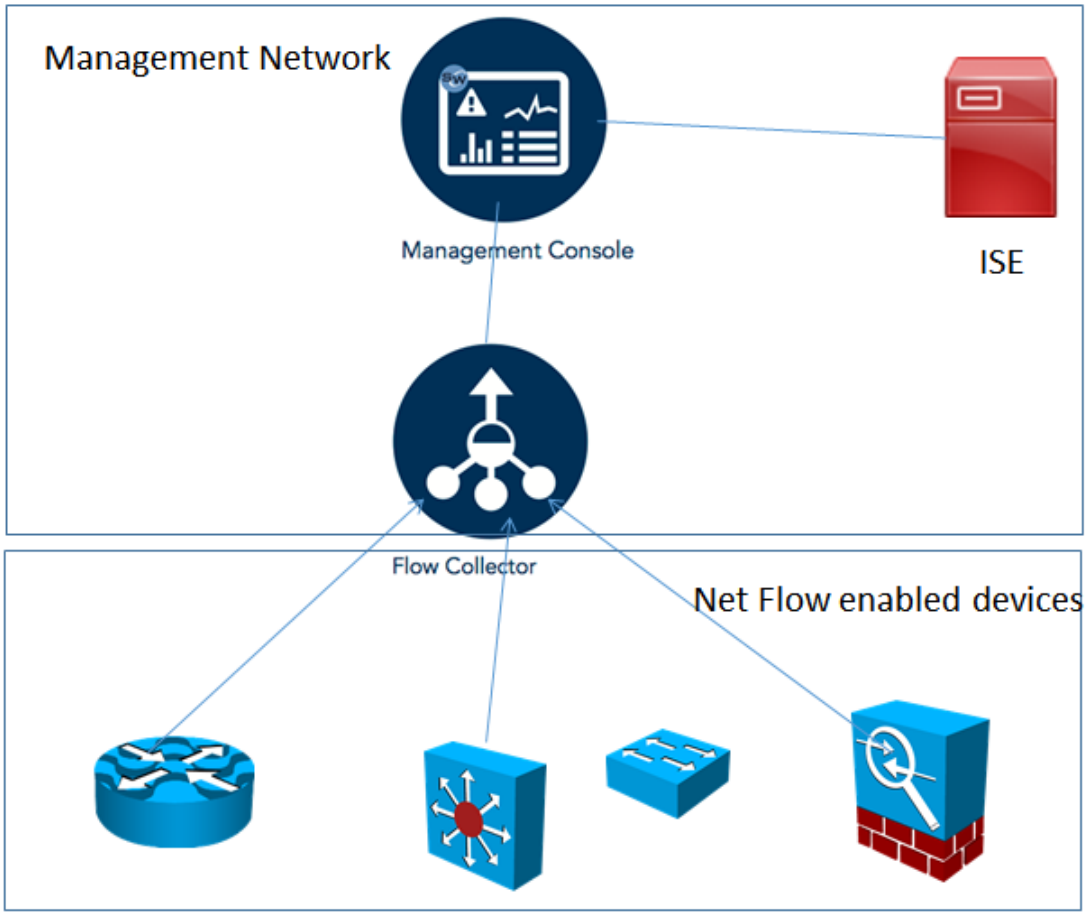
From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	SMC	TCP/389, UDP/389	LDAP
Cisco ISE	SMC	TCP/443	HTTPS
Cisco ISE	SMC	UDP/3514	SYSLOG
External log sources	SMC	UDP/514	SYSLOG
FlowCollector	SMC	TCP/443	HTTPS
SLIC	SMC	TCP/443 or proxied connection	HTTPS
UDP Director (also known as FlowReplicator)	FlowCollector - sFlow	UDP/6343	sFlow
UDP Director (also known as FlowReplicator)	FlowCollector - NetFlow	UDP/2055*	NetFlow
UDP Director (also known as FlowReplicator)	3rd Party event management systems	UDP/514	SYSLOG
FlowSensor	SMC	TCP/443	HTTPS
FlowSensor	FlowCollector - NetFlow	UDP/2055	NetFlow
IDentity	SMC	TCP/2393	SSL
NetFlow Exporters	FlowCollector - NetFlow	UDP/2055*	NetFlow
sFlow Exporters	FlowCollector - sFlow	UDP/6343*	sFlow
SMC	Cisco ISE	TCP/443	HTTPS
SMC	DNS	UDP/53	DNS
SMC	FlowCollector	TCP/443	HTTPS
SMC	FlowSensor	TCP/443	HTTPS
SMC	IDentity	TCP/2393	SSL
SMC	Flow Exporters	UDP/161	SNMP
User PC	SMC	TCP/443	HTTPS

*This is the default NetFlow port, but any UDP port could be configured on the exporter.

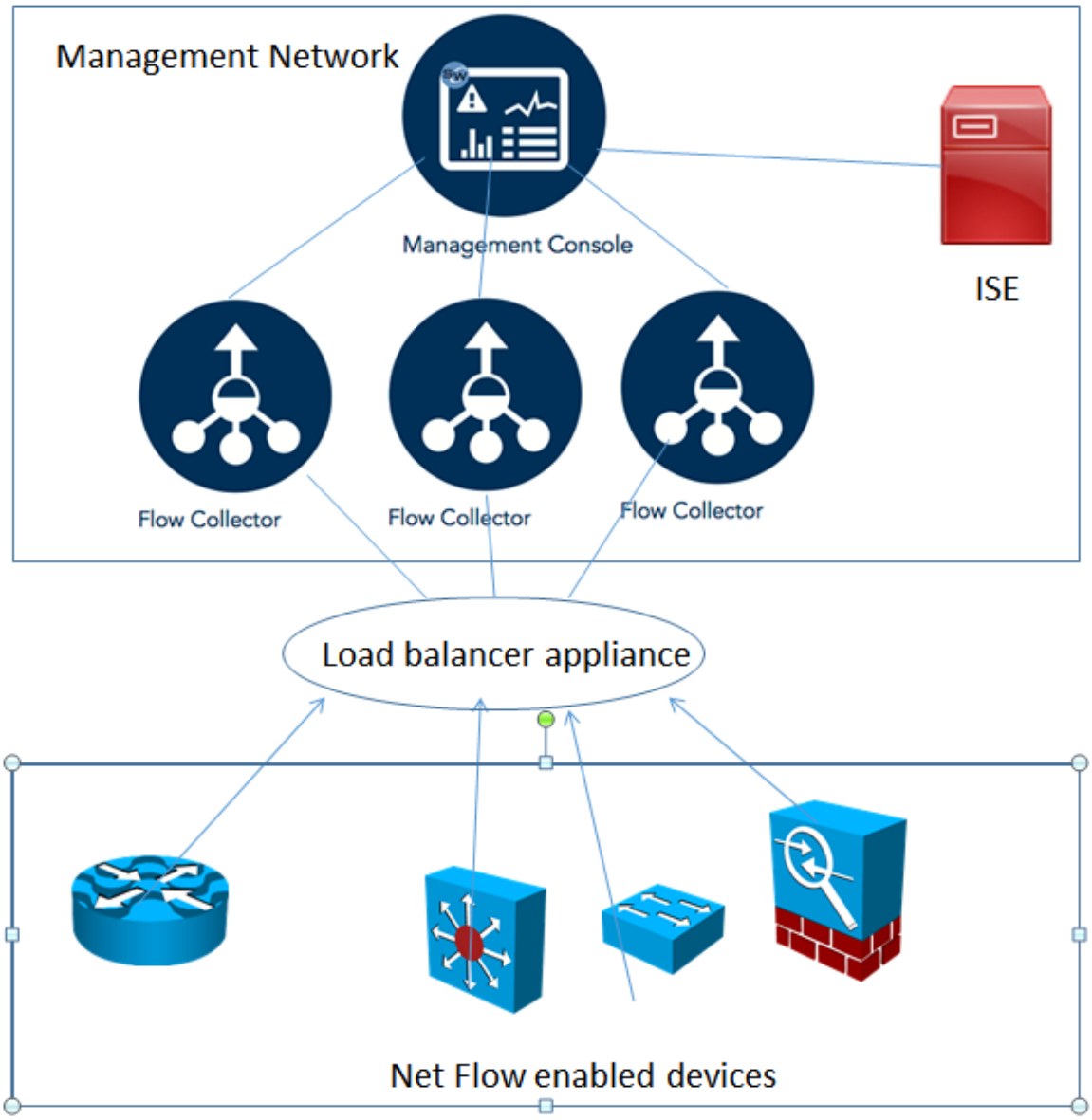
Deploying StealthWatch Flow Collectors FC

The StealthWatch FlowCollector can be deployed in the corporate network in several ways:

1. A single StealthWatch FlowCollector collecting all NetFlow data in a centralized location
2. Multiple StealthWatch FlowCollector behind a load balancer in a centralized location
3. Multiple StealthWatch FlowCollectors at multiple sites (usually placed close to the source producing the highest number of NetFlow records)



A single StealthWatch FlowCollector collecting all NetFlow data in a centralized location

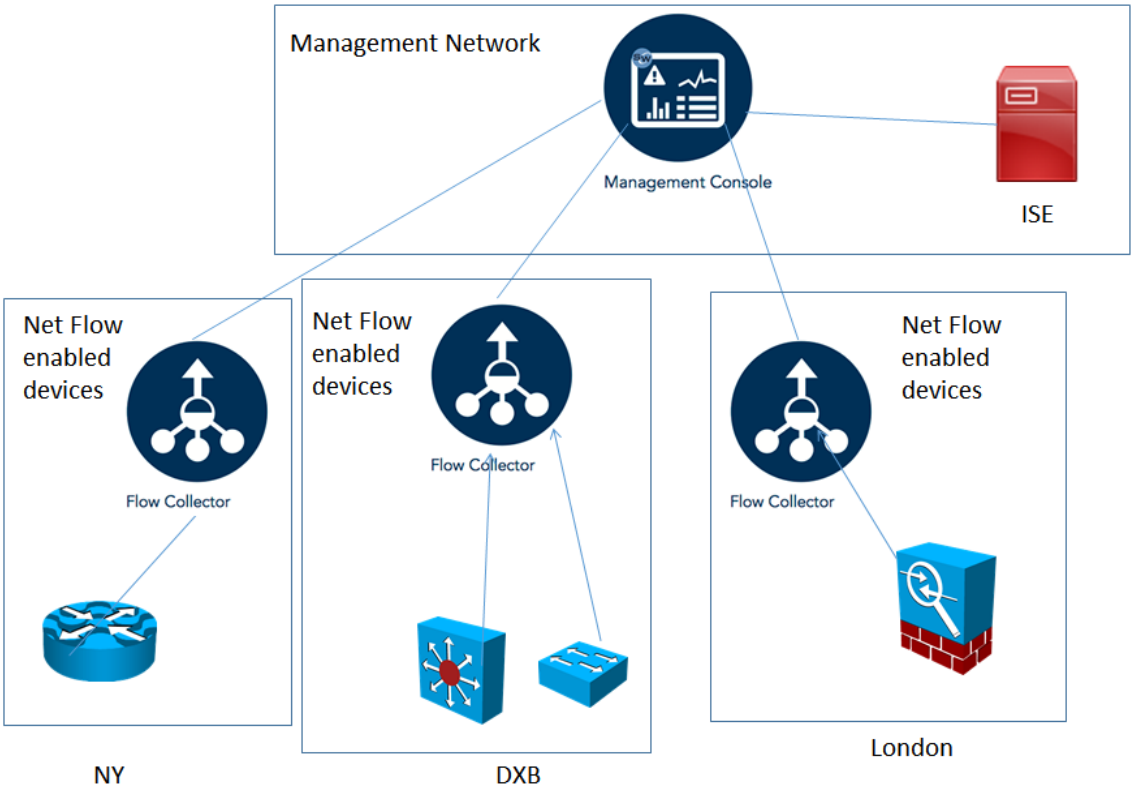


Multiple StealthWatch FlowCollector behind a load balancer in a centralized location

As you can see above three StealthWatch FlowCollectors are deployed behind a load balancer.

For example, you can deploy the Citrix NetScaler 1000V on demand, anywhere in the data center, using the Cisco Nexus 1100 Series Cloud Services Platform (CSP) or running as a virtual appliance on VMWare ESXi or KVM.

This load-balancing solution will help you scale your StealthWatch FlowCollectors (or any other collectors) more efficiently in your environment.



Multiple StealthWatch FlowCollectors at multiple sites

As you can see three StealthWatch FlowCollectors are deployed in a distributed way, with one StealthWatch FlowCollector at each site (NY,DXB,London).

This deployment has the advantage of limiting the overhead introduced by NetFlow.

If you have multiple geographically located sites, pay attention to bandwidth limitations between sites.

As a best practice, a single FlowCollector should be used for as much related traffic as possible. However, the benefits of centralized collection diminish when the traffic is not similar.
Another best practice is that all NetFlow records belonging to a flow should be sent to the same StealthWatch FlowCollector.

Duplicate NetFlow records can be a problem when trying to respond to an incident or analyze traffic patterns.

StealthWatch FlowCollectors have a de-duplication feature where it guarantees that the flow data is stored properly, while preserving the details about each flow exporter and eliminating the reporting of inflated traffic volumes.

When deploying StealthWatch FlowCollectors, you should consider several factors:

- The number of NetFlow generation devices (exporter count).
- The rate of flows per second (fps) that is expected to be received.
- The number of hosts (both inside and outside the network) for which the collector can maintain state. As a best practice, the number of inside hosts should not exceed 60 percent of the host count value.
- The amount of flow data to be stored.

StealthWatch Flow Collectors come in two different form factors as we said before:
Physical Appliances and virtual edition (VE).

These are the Flow Collector VE models and their capacities:

FC VE Model	Flows per second	Exporters	Hosts	Reserved Memory	Reserved CPUs	Maximum Disk Storage
1000	Up to 30,000	Up to 1,000	Up to 500,000	32 GB	5	1 TB
2000	Up to 60,000	Up to 1,500	Up to 750,000	64 GB	6	2 TB
4000	Up to 120,500	Up to 2,000	Up to 1,000,000	128 GB	7	4 TB

For the **Flow Collector FC VM**, the following resources are recommended:

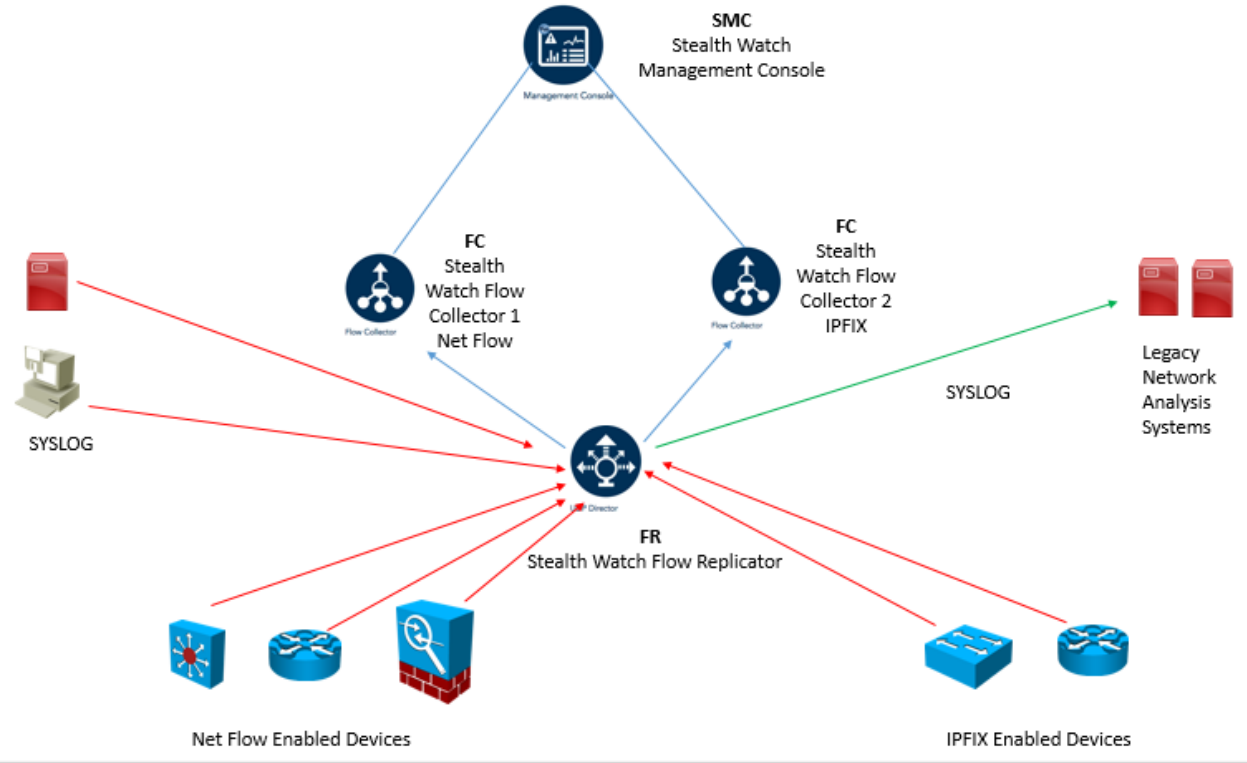
Number of CPUs	Memory	Exporters	Hosts	Flows per Second
2	4 GB	Up to 250	Up to 125,000	Up to 4500
3	8 GB	Up to 500	Up to 250,000	Up to 15,000
4	16 GB	Up to 1000	Up to 500,000	Up to 22,500
5	32 GB	Up to 1000	Up to 500,000	Up to 30,000

Deploying StealthWatch Flow Replicators FR

The StealthWatch Flow Replicator is an optional component of the Cisco CTD Solution.

The StealthWatch FlowReplicator supports Cisco NetFlow, IPFIX, and other vendors' flow data.
It combines multiple capabilities into a single device to streamline the collection and distribution of network and security data across the corporate network.

Topology below shows an example topology where the StealthWatch FlowReplicator (FR) is deployed collecting NetFlow, IPFIX, and syslog data from multiple devices in the network.



StealthWatch FlowReplicator Deployment Example

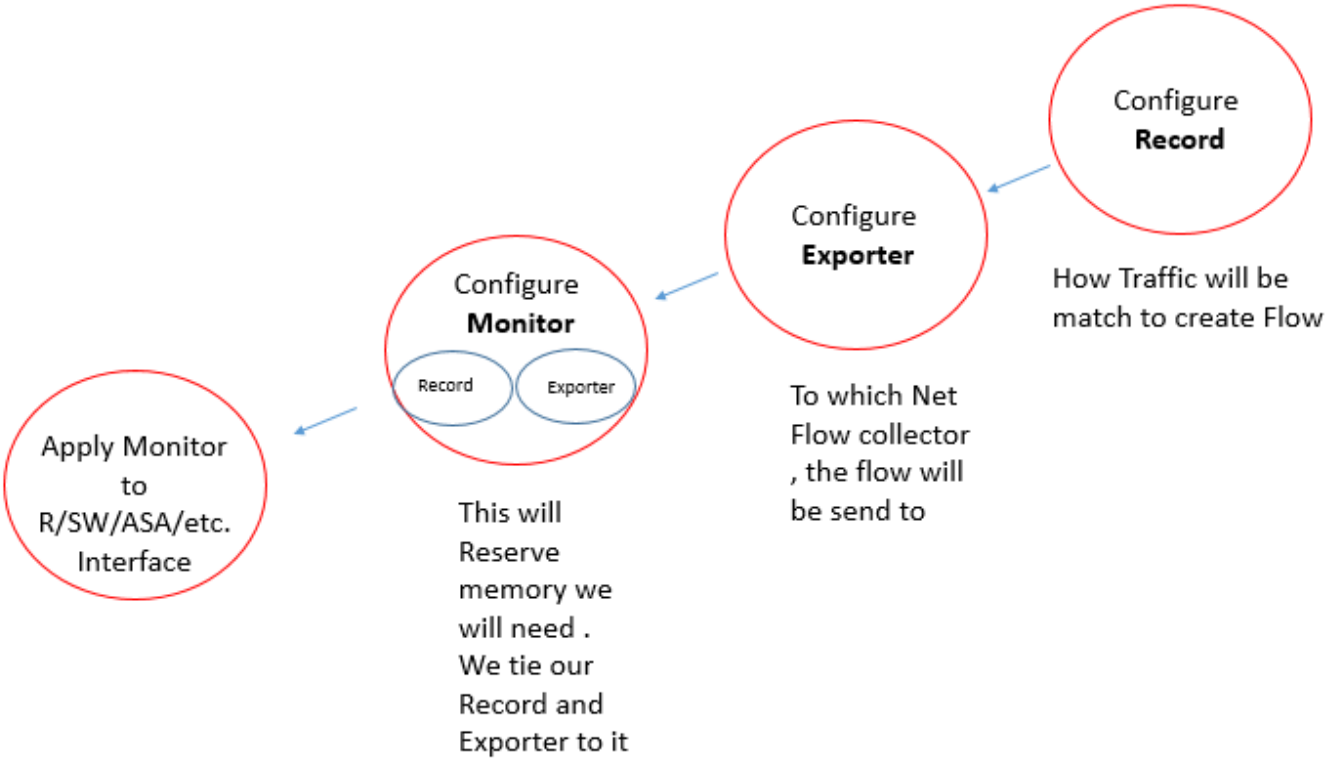
In above picture, the StealthWatch FR sends all NetFlow data to the StealthWatch FlowCollector 1 and all IPFIX data to the StealthWatch FlowCollector 2.

The StealthWatch FR can receive data from any connectionless UDP application and syslog messages and then replicate those to network analysis systems.

In addition, StealthWatch FR can process Simple Network Management Protocol (SNMP) traps from network infrastructure devices and distribute them to several different SNMP management stations.

Configuring Cisco's IOS Flexible Net Flow for use with Stealth Watch

Remember in the middle of this documents we go through Net Flow four steps configuration , the Figure below will summarize these four steps



1. Configure a *record*.

In this step we're setting up the actual NetFlow record format and key/non-key fields. We have to specify a series of "match" and "collect" commands that tell the router which 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 collector for reporting and analysis.

You don't really want to modify the "match" fields much.

The seven match entries shown below should always be included in your FnF 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 all StealthWatch installations.

```
flow record LANCOPE1
 match ipv4 tos required; key field
 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
 collect routing destination as optional; enable if you use BGP
 collect routing next-hop address ipv4 required;
 collect ipv4 dscp optional; used to generate QoS reports
 collect ipv4 ttl minimum optional; provides pathing info
 collect ipv4 ttl maximum optional; provides pathing info
 collect transport tcp flags optional; security anaysis
 collect interface output required; used for computing bps rates
 collect counter bytes required; used for bps calculation
 collect counter packets required; used for pps calculation
 collect timestamp sys-uptime first required; for calculating duration
 collect timestamp sys-uptime last required; for calculating duration
!
```

2. Configure one or more *exporters*.

The “exporter” is the FnF configuration section that describes how and where the flows are sent.

This terminology is somewhat confusing since most NetFlow users (including the StealthWatch system) refer to an “exporter” as the router itself. In the context of FnF “exporter” to describes the collector.

Anyway, we use this section to set up the destination IP and port of the StealthWatch flow collector. You can create multiple exporters if you have multiple StealthWatch flow collectors.

```
!
flow exporter EXPORTER1
 description StealthWatch Xe
 source loopback0 ensures all NetFlow packets source from same IP
 destination 10.202.1.62  specify the IP of the NetFlow collector
 transport udp 2055 specify the UDP port number
!
!
```

3. Configure a *monitor*.

The “monitor” represents the router's memory-resident NetFlow database.

FnF allows you to create multiple independent monitors. While this can be useful in some select situations, most users will create a single main cache for collecting and exporting NetFlow.

Configuring multiple monitor will use a significant amount of memory in the exporter so be aware.

Here we assume a single monitor called “MONITOR1”

```
!
flow monitor MONITOR1
 description Main Cache
 record lancope1 associate the record to the monitor
 exporter exporter1 associate the exporter to the monitor
 cache timeout active 60 set the active timeout to 1 minute
```

4. Apply the *monitor* to each layer-3-enabled interface.

It’s very important that NetFlow be enabled at each entry point to the router.

In almost all causes you’ll want to use “input” monitoring.

This ensures that both sides of all communications through the router are captured by FnF and sent to the flow collector.

```
!
interface FastEthernet0/0
 ip address 10.209.9.19 255.255.255.248
 ip flow monitor MONITOR1 input        apply this command to each interface

interface FastEthernet0/1
 ip address 10.209.10.1 255.255.255.0
 ip flow monitor MONITOR1 input        apply this command to each interface
```

More about NetFlow Configuration for Catalyst 3650,4500x,6500, ISR , ASR , ASA,Nexus 7000 Series ...etc. https://www.lancope.com/wiki/netflow-configuration

Resources:

StealthWatch Management Console VE and FlowCollector VE Installation and Configuration Guide pdf (includes step by step with rich pictures taken from SMC & FC GUI)
http://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/virtual/installation/guide/SW_6_9_0_SMC_VE_and_Flow_Collector_VE_Installation_and_Configuration_DV_1_4.pdf

FlowSensor Virtual Edition Installation and Configuration Guide pdf
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/flow_sensor/virtual/installation/guide/SW_6_9_0_Flow_Sensor_VE_Installation_and_Configuration_DV_1_0.pdf

StealthWatch System Hardware Configuration Guide pdf
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/configuration/SW_6_9_0_Hardware_Configuration_Guide_DV_1_2.pdf

StealthWatch System Hardware Installation Guide pdf
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/hardware/installation/SW_6_9_0_Hardware_Installation_DV_1_1.pdf

UDP Director (Flow Replicator) Virtual Edition Installation and Configuration Guide pdf
http://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/udp_director/virtual/installation/guide/SW_6_9_0_UDP_Director_VE_Installation_and_Configuration_DV_1_0.pdf

StealthWatch Identity Appliance Installation and Configuration Guide pdf
https://cisco-marketing.hosted.jivesoftware.com/servlet/JiveServlet/previewBody/69004-102-1-127989/StealthWatch%20Identity%20Appliance%20Installation%20and%20Configuration%20Guide.pdf

NetFlow Configuration Guide, Cisco IOS Release 15M&
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book.html

Cisco NetFlow LiveLessons: Big Data Analytics for Cyber Security by Omar Santos (commercial)
http://www.ciscopress.com/store/cisco-netflow-livelessons-big-data-analytics-for-cyber-9780134469850

Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security by Omar Santos (commercial)
https://www.amazon.com/Network-Security-NetFlow-IPFIX-Information/dp/1587144387

Net Flow Configuration for Loncope
https://www.lancope.com/wiki/netflow-configuration

How to Configure NetFlow on Cisco Routers for Loncope
https://www.lancope.com/blog/how-to-configure-netflow-on-cisco-ios-devices

Stealthwatch Free Videos from Lancope
https://www.lancope.com/wiki/stealthwatch-videos

Cisco NetFlow Generation 3000 Series Appliances
http://www.cisco.com/c/en/us/products/cloud-systems-management/netflow-generation-3000-series-appliances/index.html

Cisco Security Packet Analyzer 2400
http://www.cisco.com/c/en/us/support/security/security-packet-analyzer-2400/model.html

Good Luck
CCIE & CCSI: Yasser Auda
https://www.facebook.com/YasserRamzyAuda
https://learningnetwork.cisco.com/people/yasserramzy
https://www.youtube.com/user/yasserramzyauda