Cisco Cyber Threat Defense Solution 1.1

How-To Guide: Gain Visibility in the Data Center with the Cisco NetFlow Generation Appliance

Guide

May 2013

Introduction

What is the Cisco Cyber Threat Defense Solution?

The network security threat landscape is ever evolving, but always at the cutting edge are custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco® Cyber Threat Defense Solution provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior. These suspicious patterns are then supplemented with contextual information necessary to discern the level of threat associated with the activity.

The Cisco Cyber Threat Defense Solution, jointly developed and offered with Lancope®, leverages Cisco networking technology including NetFlow®, Network Based Application Recognition (NBAR), and the Identity Services Engine to provide visibility and context to allow the identification of suspicious traffic patterns within the network interior. The level of visibility and context provided can allow security analysts to detect targets, potential damage, and threatening behavior such as:

- Network reconnaissance
- Interior network malware proliferation
- Command and control traffic
- Data exfiltration

About This Document

This document describes deployment and implementation best practices in using the Cisco NetFlow Generation Appliance (NGA) as a component in the Cisco Cyber Threat Defense Solution. This document does not describe all possible deployment scenarios, but covers configuration and best practices that have been tested and validated to deliver on stated solution objectives.

This document assumes that the reader has a working familiarity with the Cyber Threat Defense Solution and has at least read the **Introduction to the Cisco Cyber Threat Defense Solution How-To Documents** available at http://www.cisco.com/go/threatdefense.

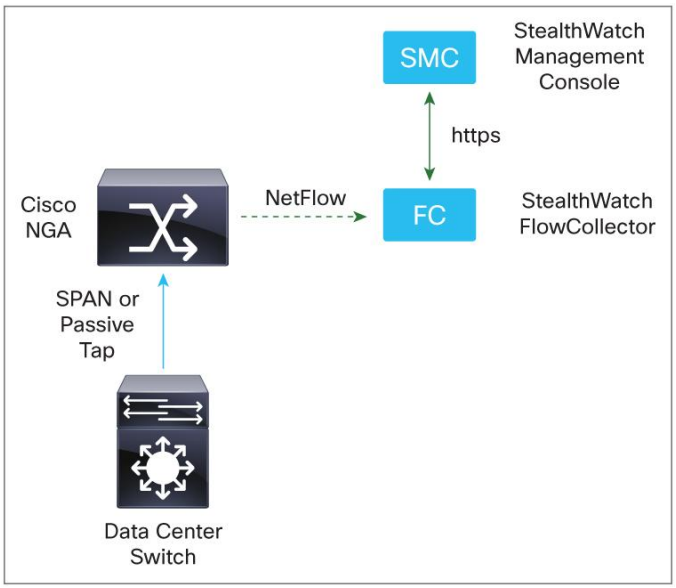
Solution Overview

Modern data centers that serve businesses with a host of applications, services, and solutions have become increasingly difficult for security analysts to monitor. As network and application speeds have increased into the multi-gigabit level, traditional probe-based security monitoring technology has become less and less cost-effective. Cisco NetFlow can provide visibility in these environments; however, in large data centers, generating NetFlow at high rates can be challenging. The Cisco NetFlow Generation Appliance (NGA), a purpose-built, high-performance solution for flow visibility in multi-gigabit datacenters can, as part of the Cisco Cyber Threat Defense Solution, restore flow visibility in these environments in a scalable and affordable manner.

Introduction to the Cisco NGA

The Cisco NGA can be deployed at critical observation points to gather network traffic from data center devices using Switch Port Analyzer (SPAN) and network taps. As illustrated in Figure 1, the Cisco NGA is configured to generate NetFlow records for the traffic it is monitoring, and export these records to the Lancope StealthWatch System for analysis.

Figure 1. System High Level View



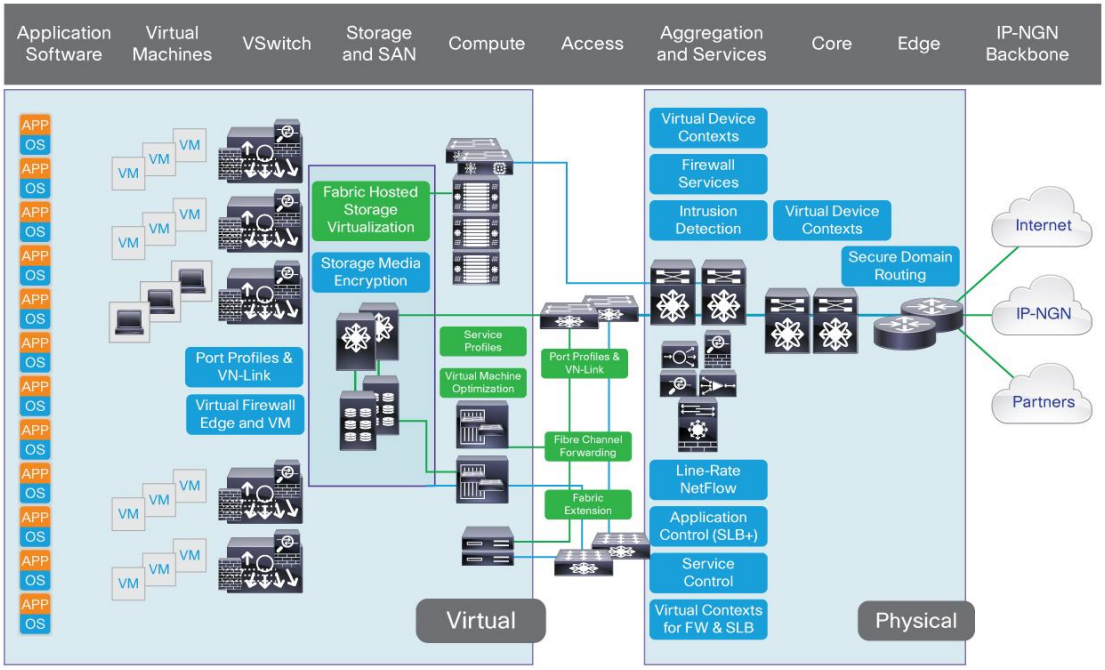
The Cisco NGA can generate and export NetFlow data using version 5, version 9 and/or IPFIX, allowing it to easily integrate with the Lancope StealthWatch System. In fact, the Lancope StealthWatch System will view the NGA just like a normal Cisco NetFlow source, such as a router.

Incorporating the Cisco NGA into the Data Center

The Cisco NGA has four 10G monitoring interfaces and up to four independent flow caches and flow monitors. This means that the Cisco NGA can receive up to 40 gigabits of data and support various combinations of data ports, record templates and export parameters. This is important to consider when placing the NGA inside the data center.

When placing the NGA, take into consideration the Secure Data Center Reference Architecture in the figure below. The NGA can be placed to receive data from the physical access, aggregation, and core layers. The objective is to ensure complete visibility of all traffic within the data center, as well as traffic that is leaving the data center. Traffic within the virtual environment (VM-to-VM traffic) can be monitored using the StealthWatch FlowSensor VE, while traffic entering and leaving the datacenter can be monitored using edge devices such as the ASA. Strategically placing the NGA in the aggregation and core layers will ensure effective monitoring of traffic within the data center, as well as provide additional statistics for traffic leaving the data center. The Cisco NGA is very scalable and can support up to 64 million active flows. Refer to **Quick Start Guide for Cisco NetFlow Generation Appliance 3140** for more detailed information on the installation.

Best Practice: NGA monitoring interfaces should be sourced from choke points to ensure complete visibility into traffic inside the data center.



Note: The Cisco NGA 1.0 release supports SFP+ fiber transceiver modules, but not 1000BASE-T SFP transceiver modules.

Configuring the Cisco NetFlow Generation Appliance (NGA) 3140

Deploying the Cisco NetFlow Generation Appliance

Procedure 1: Install the NGA appliance.

Step 1. Cable the NGA interfaces. NGA has five interfaces: One management interface with an assigned IP address is used for management and generation of NetFlow; the other four interfaces (known as data ports) are assigned for packet monitoring.

Procedure 2: Run the system configuration on the NGA appliance.

Step 1. Log into the appliance through the console interface.

The system will prompt you to change the password. The default username is **root** with a default password of **root**. The default root user has privileged access to the NGA and can enter command-line interface (CLI) commands.

Note: You are required to change the user root password during the first login session. Use a password that contains at least eight characters and contains numbers, uppercase and lowercase letters, and symbols.

Step 2. Configure the management port.

This is the IP address and subnet information necessary to allow the appliance to connect to the network. This is also the IP address that will be used to access the appliance through the web interface. Enter the information for the NGA's management address using the following CLI command:

```
ip address ip-address subnet-mask
```

Enter the following information for the NGA's default gateway address using the following CLI command:

```
ip gateway ip-address
```

Step 3. (Optional) Enter the following information for your DNS server IP address using the following CLI command:

```
ip nameserver ip-address
```

Step 4. Validate IP configuration.

Enter the following CLI command to verify that you entered the correct network settings.

```
show ip
```

Step 5. Enable the web interface

Best Practice: A significant advantage of the web interface is the ability to allow the NGA to auto-populate NetFlow components by using the 'Quick Setup' functionality. Refer to the **"Configure a Single Set of Components Quickly"** section in the **Cisco NetFlow Generation Appliance (NGA) 3140 User Guide.**

To enable the web interface for standard web access, enter the following CLI command:

```
ip http server enable
```

To enable the web interface for secure web access, enter the following CLI command:

```
ip http secure server enable
```

Press Enter to use the default web administrator username, **admin**. Enter a password for the web administrator, then enter the same password again to ensure accuracy.

Note: The NGA supports only one web user account.

Procedure 3: Configure traffic sources.

Step 1. Configure SPAN or tap connections.

You can direct packets to any of the four data ports on the NGA using either or both of the following methods:

- Enabling SPAN monitoring sessions (also known as port mirroring) from the Cisco Nexus or Catalyst switching platforms.
- Using network taps - A network tap is a hardware device that provides a copy of the packet that flows across a network link.

Refer to your switch device or network tap vendor documentation for details on how to set up these monitoring configurations.

Note: Network taps can intercept packets from any Ethernet link, thus enabling the NGA to support multiple network devices or observation points.

Step 2. Configure managed devices.

If your traffic source is a Nexus 5000 or Nexus 7000 Series switch, the Cisco NGA can export flow records containing the input and output interface of the device (switch) rather than NGA data port interface index. To do this you will need to configure the IP address and login credentials of your traffic source as a managed device. Refer to the **"Configure the IP Address of Your Traffic Source"** section in the **Cisco NetFlow Generation Appliance (NGA) 3140 User.**

Best Practice: Configure the IP address of your traffic source in the Cisco NGA as a managed device.

NGA NetFlow Configuration

When configuring NetFlow on the NGA keep in mind the following supported items:

- Up to ten filters - These define which flows are to be sent to certain collectors. This allows you to use your collector's analysis applications and load balance NetFlow data across collectors.
- Up to four managed devices - Discussed earlier, managed device settings allow you to collect interface information from your traffic sources.
- Up to six collectors - Enabling NetFlow export to up to six different NetFlow collectors, allowing you to load-balance NetFlow data export and to monitor specific applications in your data center.
- Up to four monitors - Up to four independent flow monitors (flow caches) may be active simultaneously. Each monitor supports up to three records. Of those three records, only one IPv4, one IPv6, and one Layer 2 record type is supported.

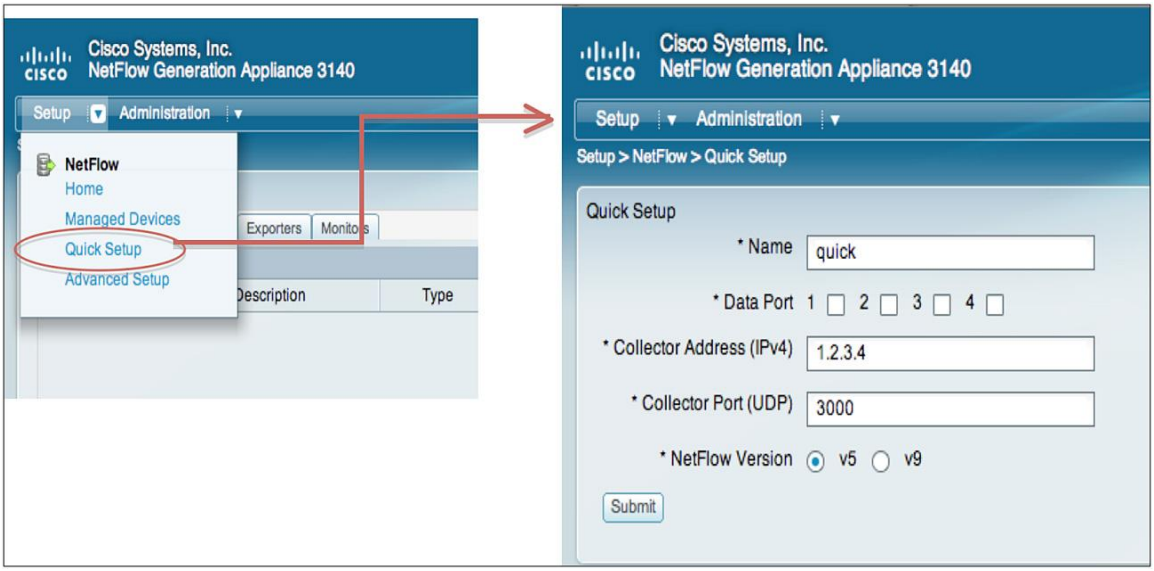
NGA NetFlow Configuration from the Web Interface

The Cisco NGA offers both CLI and web interface as methods of configuring NetFlow components. This section describes configuration of the NGA through the web interface; for details on how to configure the NGA from the CLI, see Appendix A.

Procedure 1: Perform Quick Setup NetFlow configuration.

This is the easiest and simplest configuration to export v5 or v9 NetFlow packets to a collector.

Step 1. Click Setup → Quick Setup.



Step 2. Define a name.

Enter a unique name to identify this configuration.

Step 3. Define one or more data ports.

Check the check box for each appliance data port that will accept incoming packets.

Step 4. Define a collector address.

Enter the IP address for the collector in the Collector Address field.

Step 5. Define a UDP collector port.

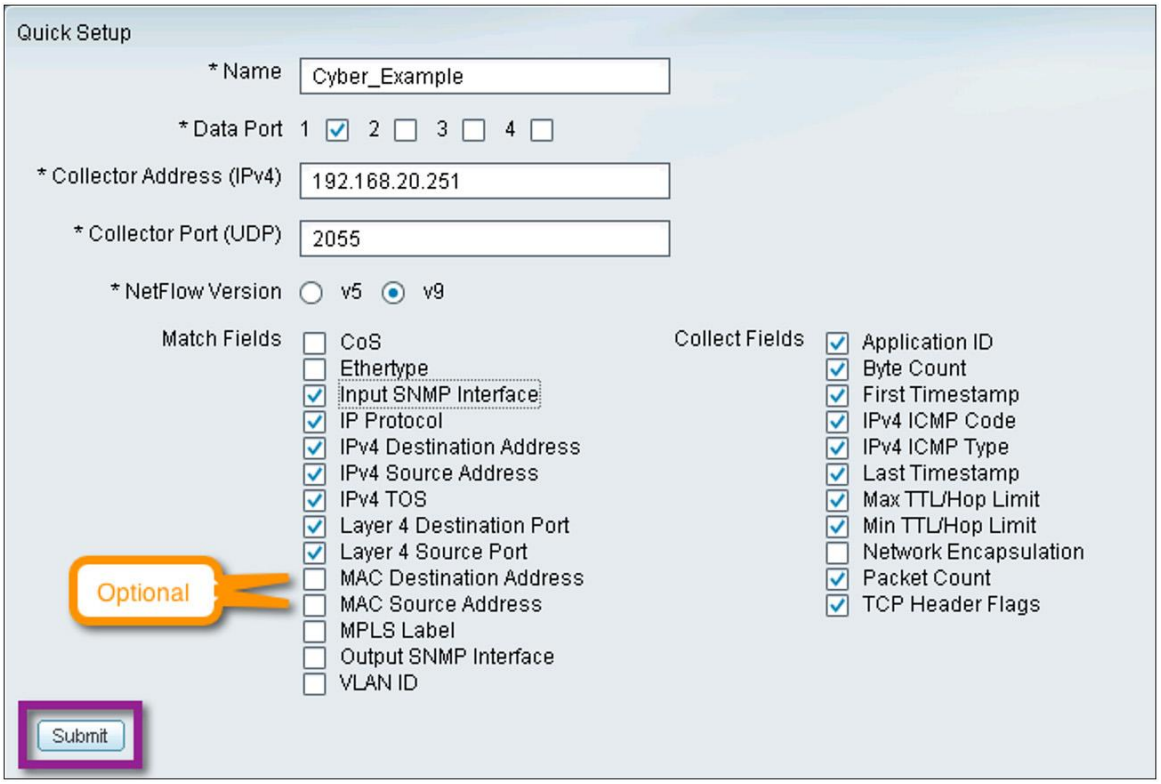
Enter the port on which the collector device is listening. This is typically configurable on the collector device. StealthWatch by default expects NetFlow on UDP port 2055.

Step 6. Define the NetFlow version.

Select version 5 to configure the appliance to perform standard NetFlow version 5 monitoring and export. You do not need to select individual record fields since they are predetermined by the NetFlow version 5 standard.

Select which version 9 fields you want to include in your monitoring/collecting.

Best Practice: Use version 9 and select the fields as illustrated in the following figure.



Note: The MAC fields are optional, based on whether Managed Device settings are configured or not. If Managed Device settings are configured, then the MAC fields should be selected; if Managed Device settings are not configured, then the MAC fields should not be selected.

Step 7. Click Submit. The following components are created:

For V5:

- A collector named **Cyber_Example_collector**
- An exporter named **Cyber_Example_exporter**
- A monitor named **Cyber_Example _monitor**

For V9:

- A collector named **Cyber_Example_collector**

- An exporter named **Cyber_Example_exporter**
- A monitor named **Cyber_Example_monitor**
- A record named **Cyber_Example_record**

Step 8. Select **Cyber_Example_monitor** in the Monitor tab and click **Activate/Inactivate**

This will enable the newly created flow monitor to generate NetFlow information for the input traffic and send it to the StealthWatch FlowCollector.

Refer to **Cisco NetFlow Generation Appliance (NGA) 3140 User Guide** under section **Setting Up Multiple NetFlow Monitor Instances** for advanced information on creating filters, setting up multiple collectors, records, exporters and monitors.

Verify NetFlow Collection by the StealthWatch System

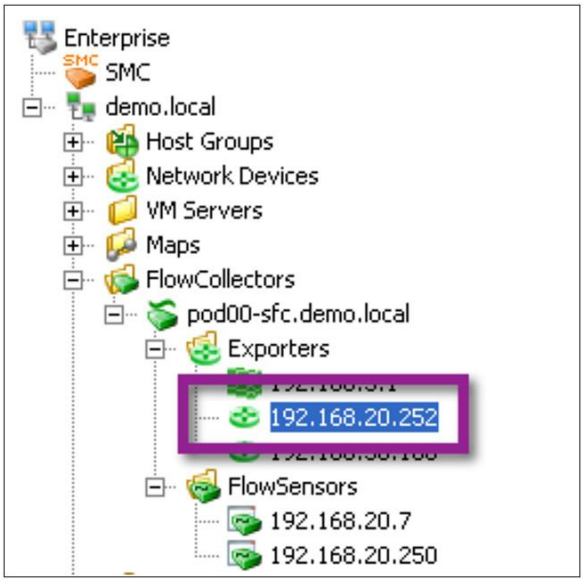
Once the Cisco NGA has been fully configured and NetFlow collection has been verified it is necessary to verify the collection of the NetFlow records by the Lancope FlowCollector. This verification is done through the Lancope SMC.

Procedure 1: Verify NetFlow collection by StealthWatch.

Step 1. Log into the Lancope SMC.

Step 2. Expand the FlowCollectors and Exporters in the Enterprise Tree.

Step 3. Verify that the IP address of the recently configured Cisco NGA is appearing in the expanded tree.



Note: The Cisco NGA will appear with the generic Router icon inside StealthWatch

Step 4. Right-click the IP address of the NGA and click Flows → Flow Table.

Step 5. Ensure that the expected flow records appear in the Flow Table.

Summary

This guide describes the deployment and implementation of the Cisco NGA inside the data center as part of the Cisco Cyber Threat Defense Solution. Leveraging the Cisco NGA and the Cyber Threat Defense Solution can restore visibility to high-performance data centers in a cost-effective and scalable manner, allowing for the monitoring and detection of suspicious and malicious activity inside the data center. For more information on how to use the Cyber Threat Defense Solution to detect advanced threats, refer to the other guides in the Cyber Threat Defense How-To series available at http://www.cisco.com/go/threatdefense.

Appendix A: Flexible NetFlow Configuration from the NGA CLI

Procedure 1: Configure the flow record.

Step 1. Create a IPv4 flow record using the following key and non-key fields.

```
root@nga.cisco.com#flow record IPv4 CTD_Example_record
root@nga.cisco.com(sub-record)#match input-interface
root@nga.cisco.com(sub-record)#match ip protocol
root@nga.cisco.com(sub-record)#match destination
root@nga.cisco.com(sub-record)#match source
root@nga.cisco.com(sub-record)#match ip tos
root@nga.cisco.com(sub-record)#match transport destination-port
root@nga.cisco.com(sub-record)#match transport source-port
root@nga.cisco.com(sub-record)#match datalink mac-destination
root@nga.cisco.com(sub-record)#match datalink mac-source
root@nga.cisco.com(sub-record)#collect classification application-id
root@nga.cisco.com(sub-record)#collect counter bytes
root@nga.cisco.com(sub-record)#collect timestamp sys-uptime first
root@nga.cisco.com(sub-record)#collect icmp code
root@nga.cisco.com(sub-record)#collect icmp type
root@nga.cisco.com(sub-record)#collect timestamp sys-uptime last
root@nga.cisco.com(sub-record)#collect ip max-ttl
root@nga.cisco.com(sub-record)#collect ip min-ttl
root@nga.cisco.com(sub-record)#collect counter packets
root@nga.cisco.com(sub-record)#collect transport tcp flags
```

Note: Refer to the **Command Reference Guide for Cisco NetFlow Generation Appliance** for guidance on creating IPv6 and Layer 2 flow records.

Procedure 2: Configure the flow collector.

Step 1. Define a flow collector.

```
root@nga.cisco.com#flow collector CTD_Example_collector
```

Step 2. Define the destination IP address.

```
root@nga.cisco.com(sub-collector)#address 192.168.20.251
```

Step 3. Define the transport protocol.

```
root@nga.cisco.com(sub-collector)#transport udp destination-port 2055
```

Best Practice: NetFlow is usually sent over UDP port 2055.

Procedure 3: Configure the flow exporter.

Step 1. Define a flow exporter.

```
root@nga.cisco.com#flow exporter CTD_Example_exporter
```

Step 2. Define the format of the NetFlow packets that are sent to collector.

```
root@nga.cisco.com(sub-exporter)#version v9
```

Note: Other options include v5 and IPFIX.

Step 3. Define how frequently (in minutes) the exporter will send NetFlow data templates to collectors.

```
root@nga.cisco.com(sub-exporter)#template-period 1
```

Step 4. Define how frequently (in minutes) the exporter will send option templates and option data to collectors.

```
root@nga.cisco.com(sub-exporter)#option-period 1
```

Step 5. Define the exporting policy. With multi-destination policy, the exporter will send the same NetFlow packet to all collectors set in the exporter.

```
root@nga.cisco.com(sub-exporter)#policy multi-destination
```

Note: Other options include weighted-round-robin.

Step 6. Select a previously-defined collector to be used in this exporter.

```
root@nga.cisco.com(sub-exporter)#destination CTD_Example_collector
```

Procedure 4: Create the flow monitor.

The flow monitor represents the device's NetFlow database and links together the flow record and the flow exporter with any or all of the four data ports on the NGA.

Step 1. Define the flow monitor.

```
root@nga.cisco.com#flow monitor CTD_Example_monitor
```

Step 2. Configure the flow record.

```
root@nga.cisco.com(sub-monitor)#record CTD_Example_record
```

Step 3. Configure the exporter.

```
root@nga.cisco.com(sub-monitor)#exporter CTD_Example_exporter
```

Step 4. Define the data port(s) on which this flow monitor will receive packets and populate flow records.

```
root@nga.cisco.com(sub-monitor)#dataport 1
```

Step 5. Configure the flow monitor to track the innermost IP addresses.

```
root@nga.cisco.com(sub-monitor)#tunnel inner
```

Note: Use this command to instruct the flow monitor how to handle network packets that are tunneled and have more than one set of IP addresses. The other option is to track the outermost IP addresses.

Step 6. Define the percentage of total cache memory space to allocate for this monitor instance, before flows are aged out of the cache and forwarded to the exporter.

```
root@nga.cisco.com(sub-monitor)#cache size 100
```

Step 7. Define the cache mode.

```
root@nga.cisco.com(sub-monitor)#cache type standard
```

Note: In standard cache mode, inactive flows will be completely removed from the cache, and the memory space made available for a new flow to use. In the other option, permanent cache mode, flows are never deleted from the cache to free space for new flows.

Step 8. Define the active timeout.

The active timeout refers to how often NetFlow records are generated for flows that are still active.

```
root@nga.cisco.com(sub-monitor)#cache timeout active 60
```

Best Practice: The active timeout should be set to 60 seconds

Step 9. Define the inactive timeout.

The inactive timeout refers to the time period in which flows that are inactive (not transmitting data) but still resident in the cache are timed out of the cache.

```
root@nga.cisco.com(sub-monitor)#cache timeout inactive 15
```

Best Practice: The inactive timeout should be set to 15 seconds

Procedure 5: Validate NetFlow export.

Step 1. Verify the rate that raw flow data is being processed.

```
root@nga.cisco.com#show cache statistics rates monitor_name
```

This command displays the rate of raw traffic being processed and the number of flows being created and forwarded to the exporter engine. If flows are being processed expect to see counters greater than zero.

Step 2. Verify that flow data is being exported.

```
root@nga.cisco.com#show collector statistics collector_name
```

This displays the information about NetFlow packets being sent to the collector; if NetFlow data is being exported expect to see counters and statistics greater than zero.