CISCO VALIDATED DESIGN

Intelligent WAN NetFlow Monitoring Deployment Guide

September 2017

Table of Contents

Deploying the Cisco Intelligent WAN

This guide is one in a series of IWAN advanced deployment guides that focus on how to deploy the advanced features of the Cisco Intelligent WAN (IWAN). These guides build on the configurations deployed in the Intelligent WAN Deployment Guide and are optional components of its base IWAN configurations.

The advanced guides are as follows:

- IWAN High Availability and Scalability Deployment Guide
- IWAN Multiple Data Center Deployment Guide
- IWAN Multiple Transports Deployment Guide
- IWAN Multiple VRF Deployment Guide
- IWAN Public Key Infrastructure Deployment Guide
- IWAN NetFlow Monitoring Deployment Guide (this guide)
- IWAN Remote Site 4G LTE Deployment Guide

For design details, see Intelligent WAN Design Summary.

For configuration details, see Intelligent WAN Configuration Files Guide.

For an automated way to deploy IWAN, use the APIC-EM IWAN Application. For more information, see the Cisco IWAN Application on APIC-EM User Guide.

If want to use TrustSec with your IWAN deployment, see "Configuring SGT Propagation" in the User-to-Data-Center Access Control Using TrustSec Deployment Guide.

DEPLOYMENT DETAILS

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Deploying NetFlow Monitoring

NetFlow operates by creating a NetFlow cache entry that contains information for all active flows on a NetFlow-enabled device. NetFlow builds its cache by processing the first packet of a flow through the standard switching path. It maintains a flow record within the NetFlow cache for all active flows. Each flow record in the NetFlow cache contains key fields, as well as additional non-key fields, that can be used later for exporting data to a collection device. Each flow record is created by identifying packets with similar flow characteristics and counting or tracking the packets and bytes per flow.

Flexible NetFlow (FNF) allows you to customize and focus on specific network information. To define a flow, you can use a subset or superset of the traditional seven key fields. FNF also has multiple additional fields (both key and non-key). This permits an organization to target more specific information so that the total amount of information and the number of flows being exported is reduced, allowing enhanced scalability and aggregation.

PROCESS

Configuring Flexible NetFlow for IWAN Monitoring

1. Create flexible NetFlow flow record
2. Create flow exporter
3. Create a flow monitor
4. Apply flow monitor to router interfaces

These procedures include best practice recommendations for which key fields and non-key fields need to be collected in order to allow for effective IWAN monitoring.

Additional details regarding the deployment of NetFlow with NBAR2 and the usage of a broad range of NetFlow collector/analyzers are covered in the Application Monitoring Using NetFlow Technology Design Guide.

Procedure 1 Create flexible NetFlow flow record

Flexible NetFlow requires the explicit configuration of a flow record that consists of both key fields and non-key fields. This procedure provides guidance on how to configure a user-defined flow record that includes all of the Traditional NetFlow (TNF) fields (key and non-key) as well as additional FNF fields (key and non-key). The resulting flow record includes the full subset of TNF fields used in classic NetFlow deployments.

The examples in this guide are from Cisco Prime Infrastructure and LiveAction LiveNX. Different NetFlow collector applications support different export version formats and you should align your flow record with the type of network management platform used by your organization.

Step 1: Specify key fields. This determines unique flow. Be sure to include a separate match statement for each key field.

```
flow record [record name]
 description [record description]
 match [key field type] [key field value]
```

Table 1 Recommended FNF key fields for IWAN

Key field type	Key field value
flow	direction
interface	input
ipv4	tos protocol source address destination address
transport	source port destination port

Step 2: Specify non-key fields to be collected for each unique flow. Be sure to include a separate **collect** statement for each non-key field.

```
flow record [record name]
 collect [non-key field type] [non-key field value]
```

Table 2 Recommended FNF non-key fields for IWAN

Non-key field type	Non-key field value
application	name
flow	sampler
routing	source as destination as next-hop address ipv4
ipv4	source prefix source mask destination mask dscp id
transport	tcp flags
interface	output
counter	bytes packets
timestamp	sys-uptime first sys-uptime last

Example

```
flow record Record-FNF-IWAN
 description Flexible NetFlow for IWAN Monitoring
 match flow direction
 match interface input
 match ipv4 destination address
 match ipv4 protocol
 match ipv4 source address
 match ipv4 tos
 match transport destination-port
 match transport source-port
 collect application name
 collect counter bytes
 collect counter packets
 collect flow sampler
 collect interface output
 collect ipv4 destination mask
 collect ipv4 dscp
 collect ipv4 id
 collect ipv4 source mask
 collect ipv4 source prefix
 collect routing destination as
 collect routing next-hop address ipv4
 collect routing source as
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
 collect transport tcp flags
```

Procedure 2 Create flow exporter

The NetFlow data that is stored in the cache of the network device can be more effectively analyzed when exported to an external collector.

Creating a flow exporter is only required when exporting data to an external collector. If data is analyzed only on the network device, you can skip this procedure.

Reader Tip

Most external collectors use SNMP to retrieve the interface table from the network device. Ensure that you have completed the relevant SNMP procedures for your platform.

Different NetFlow collector applications support different export version formats (v5, v9, IPFIX) and expect to receive the exported data on a particular UDP or TCP port (ports 2055, 9991, 9995, 9996 are popular). The NetFlow RFC 3954 does not specify a specific port for collectors to receive NetFlow data. In this deployment, the collector applications used for testing use the parameters designated in the following table.

Table 3 NetFlow collector parameters

Vendor	Application	Version	Export capability	NetFlow destination port
Cisco	Prime Infrastructure	3.2	Flexible NetFlow v9	UDP 9991
LiveAction	LiveNX	6.2	Flexible NetFlow v9	UDP 2055

Step 1: Configure a basic flow exporter by using NetFlow v9.

```
flow exporter [exporter name]
 description [exporter description]
 destination [NetFlow collector IP address]
 source Loopback0
 transport [UDP or TCP] [port number]
 export-protocol netflow
```

Step 2: For FNF records, export the interface table for FNF. The **option interface-table** command enables the periodic sending of an options table. This provides interface names through the NetFlow export.

```
flow exporter [exporter name]
 option interface-table
 template data timeout 600
```

Step 3: If you are using an NBAR flow record, export the NBAR application table. The **option application-table** command enables the periodic sending of an options table that allows the collector to map the NBAR application IDs provided in the flow records to application names.

```
flow exporter [exporter name]
 option application-table
```

Step 4: If you are using an NBAR flow record, export the NBAR application attributes. The **option application-attributes** command causes the periodic sending of NBAR application attributes to the collector.

```
flow exporter [exporter name]
 option application-attributes
```

Step 5: If you are using the Cisco ISR-G2 series routers, enable **output-features**. Otherwise, NetFlow traffic that originates from a WAN remote-site router will not be encrypted or tagged using QoS.

```
flow exporter [exporter name]
 output-features
```

Example: LiveAction LiveNX

```
flow exporter Export-FNF-Monitor-1
 description FNFv9 NBAR2 with LiveAction
 destination 10.4.48.178
 source Loopback0
 output-features    ! this command is not required on IOS-XE routers
 transport udp 2055
 template data timeout 600
 option interface-table
 option application-table
 option application-attributes
```

Example: Prime Infrastructure

```
flow exporter Export-FNF-Monitor-2
 description FNFv9 NBAR2 with Prime
 destination 10.4.48.36
 source Loopback0
 output-features    ! this command is not required on IOS-XE routers
 transport udp 9991
 template data timeout 600
 option interface-table
 option application-table
 option application-attributes
```

Step 6: Verify the NetFlow exporter configuration using the **show flow exporter** command.

```
show flow exporter Export-FNF-Monitor-2


Flow Exporter Export-FNF-Monitor-2:
  Description:              FNFv9 NBAR2 with Prime
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.4.48.36
    Source IP address:      10.255.241.41
    Source Interface:       Loopback0
    Transport Protocol:     UDP
    Destination Port:       9991
    Source Port:            64254
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
  Options Configuration:
    interface-table (timeout 600 seconds)
    application-table (timeout 600 seconds)
    application-attributes (timeout 600 seconds)
```

Procedure 3 Create a flow monitor

The network device must be configured to monitor the flows through the device on a per-interface basis. The flow monitor must include a flow record and optionally one or more flow exporters if data is to be collected and analyzed. After the flow monitor is created, it is applied to device interfaces. The flow monitor stores flow information in a cache, and the timer values for this cache are modified within the flow monitor configuration. It is recommended that you set the timeout active timer to 60 seconds, which exports flow data on existing long-lived flows.

Step 1: Create the flow monitor, and then set the cache timers.

```
flow monitor [monitor name]
 description [monitor description]
 cache timeout active 60
 cache timeout inactive 10
```

Step 2: Associate the flow record to the flow monitor. You can use either a custom or a built-in flow record.

```
flow monitor [monitor name]
 record [record name]
```

Step 3: If you are using an external NetFlow collector, associate the exporters to the flow monitor. If you are using multiple exporters, add additional lines.

```
flow monitor [monitor name]
 exporter [exporter name]
```

Example: Prime Infrastructure and LiveAction LiveNX

```
flow monitor Monitor-FNF-IWAN
 description IWAN Traffic Analysis
 record Record-FNF-IWAN
 exporter Export-FNF-Monitor-1
 exporter Export-FNF-Monitor-2
 cache timeout active 60
 cache timeout inactive 10
```

Step 4: Verify the flow monitor configuration by using the **show flow monitor** command.

```
show flow monitor
Flow Monitor Monitor-FNF-IWAN:
  Description:       IWAN Traffic Analysis
  Flow Record:       Record-FNF-IWAN
  Flow Exporter:     Export-FNF-Monitor-1
                     Export-FNF-Monitor-2
  Cache:
    Type:                 normal
    Status:               not allocated
    Size:                 4096 entries/0 bytes
    Inactive Timeout:     10 secs
    Active Timeout:       60 secs
    Update Timeout:       1800 secs
    Synchronized Timeout: 600 secs
    Status:             allocated
    Size:               4096 entries/376856 bytes
    Inactive Timeout:   15 secs
    Active Timeout:     60 secs
    Update Timeout:     1800 secs
```

Procedure 4 Apply flow monitor to router interfaces

A best practice for NetFlow in an IWAN deployment is to monitor all inbound and outbound traffic on the DMVPN tunnel interfaces.

Step 1: Apply the flow monitor to the tunnel interface(s).

```
interface [name]
 ip flow monitor [monitor name] input
 ip flow monitor [monitor name] output
```

Example: Single-router remote site with dual-link for hybrid

```
interface Tunnel100
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output


interface Tunnel200
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output
```

Step 2: Verify the proper interfaces are configured for NetFlow monitoring using the **show flow interface** command.

```
show flow interface
Interface Tunnel100
  FNF:  monitor:          Monitor-FNF-IWAN
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          Monitor-FNF-IWAN
        direction:        Output
        traffic(ip):      on
Interface Tunnel200
  FNF:  monitor:          Monitor-FNF-IWAN
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          Monitor-FNF-IWAN
        direction:        Output
        traffic(ip):      on
```

Step 3: At dual-router sites with a distribution layer, also apply the flow monitor to the interfaces that connect to the distribution layer switch. This ensures that you capture all possible traffic flows.

Example: First router of a dual-router dual-link remote site

```
interface Port-channel1.50
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output
```

Example: Second router of a dual-router dual-link remote site

```
interface Port-channel2.54
 ip flow monitor Monitor-FNF-IWAN input
 ip flow monitor Monitor-FNF-IWAN output
```

Step 4: Verify the dscp used in the network by displaying the NetFlow cache on the WAN aggregation routers. Use the **show flow monitor** command.

```
show flow monitor Monitor-FNF-IWAN cache format table
```

Appendix A: Product List

To view the full list of IWAN-supported routers for this version of the CVD, see Supported Cisco Platforms and Software Releases. All master controllers and border router devices at a common site must use the same version of software.

This guide was validated using the software detailed in this appendix. When deploying, you should always use the Cisco IOS Software Checker tool to see if there are software vulnerabilities applicable for your environment. This tool is available at the following location:

https://tools.cisco.com/security/center/selectIOSVersion.x

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- Routing update:
  - Updated the tunnel interface numbering to match other guides

You can use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.