Cisco Application Visibility and Control Overview

Introduction

This chapter is an overview of the Cisco Application Visibility and Control solution.

The Cisco Application Visibility and Control solution integrates multiple internal components of the Cisco ASR 1000 Series Aggregation Services Router and external components. This chapter describes both the internal and external components of the solution. It also details the solution process.

- Cisco Application Visibility and Control Components, page 1-2
- Cisco Application Visibility and Control Process, page 1-5
Cisco Application Visibility and Control Components

The core components of the Cisco Application Visibility and Control solution, include:

- Cisco ASR 1000 Series Router, page 1-2
- Cisco Network-Based Application Recognition 2 (NBAR 2), page 1-3
- Cisco Flexible NetFlow, page 1-3
- Cisco NetFlow V9 Export Format, page 1-3
- Cisco Collection Manager, page 1-3
- Cisco Collection Manager Database, page 1-4
- Cisco Insight, page 1-4

Figure 1-1 illustrates the internal and external components of the Cisco Application Visibility and Control solution.

Cisco ASR 1000 Series Router

The Cisco ASR 1000 Series router is Cisco’s midrange routers offering convergence of network services on a scalable routing platform. The Cisco ASR 1000 Series uses the Cisco Quantum Flow Processor (QFP), which offers multiprocessing, advanced memory management, customized quality of service (QoS), and silicon-based service delivery and programmability. The flexibility of this processor allows network services such as packet encryption, packet inspection, application recognition, traffic differentiation, and subscriber management to be integrated on a single routing platform. It does not need to use external network appliances or service modules for this platform. The router delivers the resiliency, intelligent services, and modularity for needed for the future.
Cisco Network-Based Application Recognition 2 (NBAR 2)

Cisco NBAR 2 is an important component of the Cisco Content networking architecture. It acts as a classification engine in Cisco IOS Software and can recognize a wide variety of Layer 7 applications. These applications include Web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that particular application. NBAR 2 can work with quality-of-service (QoS) features to help ensure that the network bandwidth is used efficiently.

Cisco Flexible NetFlow

The original NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. It is the standard for acquiring IP operational data from IP networks. It provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting. Flexible NetFlow improves on the original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export by using reusable configuration components.

Cisco NetFlow V9 Export Format

Flexible NetFlow exports information to reporting servers in various formats including NetFlow version 9. NetFlow version 9 is the format used by the Cisco Application Visibility and Control solution. NetFlow version 9 is a flexible and extensible format. It includes a template to describe what is being exported and the export data. The template is periodically sent to the Flexible NetFlow collector telling it what data to expect from the router or switch. The data is then sent for the reporting system to analyze. Any data available in the device can theoretically be sent in NetFlow version 9 format. Flexible NetFlow allows the user to configure and customize what information is exported using NetFlow version 9. NetFlow version 9 is the basis for the IETF standard IPFIX associated with the IP Flow and Information working group in IETF.

Cisco Collection Manager

The Cisco Collection Manager is a set of software modules that runs on a server. It receives and processes NetFlow Records. The NetFlow Records used by the Cisco Collection Manager are generated by the Cisco ASR 1000 Series router. The process uses Cisco Network-Based Application Recognition (NBAR) and Cisco Flexible NetFlow. The processed records are stored in the Cisco Collection Manager database.

The Cisco Collection Manager also interoperates with the Cisco Service Control Management Suite (SCMS) and the Cisco Service Control Engine (SCE) platform. The Cisco Collection Manager is able to operate with both the Cisco ASR 1000 Series and the Cisco SCE platform at the same time.
Cisco Collection Manager Database

The Cisco Collection Manager database is either a bundled database or an external database. In bundled mode, the Cisco Collection Manager uses the Sybase Adaptive Server Enterprise database. This database is located on the same server as the other Cisco Collection Manager components. It uses a simple schema that includes a group of small, simple tables. The Cisco Collection Manager is also able to use a Java Database Connectivity (JDBC) compliant database. This includes standard databases, such as Oracle or MySQL. The JDBC-compliant database can be located on the same server as the Cisco Collection Manager or hosted on an external server.

Cisco Insight

Cisco Insight is reporting platform software. It processes the formatted data from the Collection Manager database. Cisco Insight presents customizable reports, charts, and statistics about the traffic on the Cisco ASR 1000 Series. It is a web-based application accessed with a browser.
Cisco Application Visibility and Control Process

The Cisco Application Visibility and Control solution provides network visibility and traffic control. This section details the processes and purposes of the various components in the solution.

The Cisco Application Visibility and Control solution processing functions, include:

- Cisco IOS CLI, page 1-5
- NBAR 2, page 1-5
- Quality of Service (QoS), page 1-5
- Bandwidth Control, page 1-6
- Cisco Flexible NetFlow, page 1-6
- Usage Records, page 1-8
- Transaction Records, page 1-8
- Global Usage Records, page 1-8
- Cisco Collection Manager, page 1-8
- Cisco Insight v3, page 1-8

Cisco IOS CLI

The basic interface for the Cisco Application Visibility and Control solution is the standard Cisco IOS CLI. You can configure NBAR 2, Modular Quality of Service (MQC) queues and policers, Flexible NetFlow counters, and the protocols for NetFlow information. In the typical configuration, the user uses the Cisco IOS CLI to configure NetFlow rules. These generate the required records and configure the QoS features on specific interfaces.

NBAR 2

NBAR 2 is a Cisco feature that enables protocol detection for a network. Protocol detection is the process by which the system determines that a particular network flow is from a specific application. This process is done using various techniques including payload signature matching, behavioral classification or classification based on L7 parameters (sometimes called protocol sub-classification). Upon detection, a Protocol-ID is assigned to a flow. The Protocol-ID is then used by the solution to determine the appropriate actions on packets belonging to that flow.

Quality of Service (QoS)

Standard Cisco Modular Quality of Service (MQC) is used for the Cisco Application Visibility and Control solution. Cisco MQC is used to create the application-aware policy of the solution. There are no changes or enhancements to the Cisco QoS framework for the Cisco Application Visibility and Control solution.
Bandwidth Control

The Application Visibility and Control solution provides global bandwidth control by application. This control allows service providers to set acceptable bandwidth consumption policies for different traffic classes. It can ensure better performance for sensitive application flows, for example voice calls, gaming, web browsing, and video. This performance increase is accomplished by lowering the bandwidth priority of less sensitive traffic, for example file downloads or backups. Bandwidth priority is provided by using platform policies.

Cisco Flexible NetFlow

Figure 1-2 illustrates the packet fields used by the Flexible NetFlow Transaction Records and Usage Records.

### Figure 1-2   Packet Fields of Transaction Records and Usage Records

<table>
<thead>
<tr>
<th>Transaction record</th>
<th>Usage Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction ID</td>
<td>Application ID</td>
</tr>
<tr>
<td>Input Interface</td>
<td>Attached Interface (input/output)</td>
</tr>
<tr>
<td>Output Interface</td>
<td>Direction</td>
</tr>
<tr>
<td>Direction</td>
<td>Other interface (input/output)</td>
</tr>
<tr>
<td>Source IP</td>
<td>First timestamp</td>
</tr>
<tr>
<td>Source Port</td>
<td>Last timestamp</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Packets counter</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Bytes counter</td>
</tr>
<tr>
<td>IP Protocol</td>
<td>New-Flows counter</td>
</tr>
<tr>
<td>Application ID</td>
<td>Total Seconds counter</td>
</tr>
<tr>
<td>Connection Initiator</td>
<td>IP Version</td>
</tr>
<tr>
<td>First timestamp</td>
<td>Input VRF ID</td>
</tr>
<tr>
<td>Last timestamp</td>
<td></td>
</tr>
<tr>
<td>Packets counter</td>
<td></td>
</tr>
<tr>
<td>Bytes counter</td>
<td></td>
</tr>
<tr>
<td>Bundle/Flow ID</td>
<td></td>
</tr>
<tr>
<td>Flow close mode</td>
<td></td>
</tr>
<tr>
<td>Sampler ID</td>
<td></td>
</tr>
<tr>
<td>IPv6 Source Address</td>
<td></td>
</tr>
<tr>
<td>IPv6 Destination Address</td>
<td></td>
</tr>
<tr>
<td>IP Version</td>
<td></td>
</tr>
<tr>
<td>Input VRF ID</td>
<td></td>
</tr>
</tbody>
</table>

The following sections describe the two types of Flexible NetFlow records:

- **Usage Records**, page 1-8
- **Transaction Records**, page 1-8
- **Global Usage Records**, page 1-8
Usage Records

Usage Records are records of the different type of applications running over a specific interface. The operator can use Usage records to monitor how much bandwidth the different applications use. The Usage Records can show this application usage over a specific time period, the peak and average usages, and usage for a specific application type.

Usage Records perform periodic aggregation of the category information for the interface. (Example: export information for peer-to-peer or e-mail usage).

Transaction Records

A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow.

The Transaction Record monitors the traffic at transaction levels. Transaction Records provide a detailed analysis of the traffic flows, including extracted Layer 7 fields. Due to the high load of transactions these records are sample or filtered.

Transaction Records are bound to the input and output directions of the network side interfaces. These Transaction Records allow the system to capture each unidirectional flow once.

Global Usage Records

Global usage records are the records of many applications running over an interface. These records monitor the total network traffic. The Global usage records can show the collected application usage over a specific time period, the peak usage, and the average usage.

Cisco Collection Manager

The Cisco Collection Manager is a set of software modules that runs on a server. It receives and processes NetFlow Records and stores the processed records in a database. The Cisco Collection Manager is covered in detail in the Cisco Collection Manager Overview chapter of the Cisco Application Visibility and Control Collection Manager User Guide.

Cisco Insight v3

Cisco Insight v3 is a software platform based on a web 2.0 user experience standard. It accesses information from the database generate by the Cisco Collection Manager. Cisco Insight v3 then collects and presents reports, charts, and statistics about the traffic. Some of the reports you can generate show the active applications on the network in a given time frame. This is according to the estimated amount of bandwidth the applications consume. You can also sort the information as upstream traffic, downstream traffic, or number of sessions.