NBAR2 Auto-learn

Important Beginning with Cisco IOS XE Fuji 16.9.1, this feature has been deprecated. The functionality has moved to Cisco Software-Defined AVC (SD-AVC).

NBAR2 Auto-learn improves classification of traffic not otherwise recognized by NBAR2 protocols. For generic HTTP or SSL traffic, NBAR2 can identify the hostname from packet header fields. For unknown traffic, it can track top-occurring server-side ports and sockets. These mechanisms facilitate creating custom protocols to better classify the otherwise generic or unknown traffic.

Note NBAR2 Auto-learn was previously called "NBAR Customized Assistance Based on SSL or HTTP."

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

NBAR2 Auto-learn Overview

A portion of network traffic may be difficult for NBAR2 mechanisms to identify specifically. Such traffic may be classified either as **generic** HTTP or SSL, or as **unknown**. This provides very little useful information about the traffic.

NBAR2 Auto-learn analyzes traffic classified as generic HTTP/SSL or unknown.

- For generic HTTP/SSL traffic, it derives hostnames from packet header fields in the traffic and tracks the "top hosts" that occur in generic traffic. This refers to the hosts with the highest traffic volume. The list of top hosts is arranged in order of traffic volume; hosts with the highest traffic volume are at the top of the list.
- For unknown traffic, it identifies server-side ports and tracks the "top ports" and "top sockets" that occur in unknown traffic. This refers to the ports and sockets with the highest traffic volume. The lists of top ports and sockets are arranged in order of traffic volume; ports and sockets with the highest traffic volume are at the top of the lists.

The lists of "top hosts" for generic and "top ports"/"top sockets" for unknown traffic can then be used to assist the custom protocol mechanism in creating protocols to better identify and classify the traffic. For example, top hosts provide "candidate" hosts to use in creating custom protocols.

Mechanism Details

NBAR supports the creation of custom protocols to identify traffic that built-in NBAR2 protocols do not recognize.

- For **generic** HTTP or SSL traffic, the NBAR2 Auto-learn can derive the relevant hostname from one of the following:
  - Server Name field in the Client Hello extensions
  - Common Name field in the digital certificate that a client sends to a server
- For **unknown** traffic, it can derive the server-side port number.

Example

For example, if NBAR2 is unable to classify traffic of an enterprise mail server, the traffic may be be classified only as SSL. This feature can assist in creating a custom protocol to identify the traffic more definitively, improving reporting of the mail server traffic.

How to Configure NBAR2 Auto-learn

Configuring NBAR2 Auto-learn

- For generic HTTP or SSL traffic, NBAR2 Auto-learn collects a list of the most often occurring hosts ("top hosts"). For unknown traffic, the feature collects a list of most often occurring server-side ports ("top ports") and sockets ("top sockets"). This information may be fed into the auto-custom mechanism to facilitate creating custom protocols.

- To optimize performance, the system does not track all flows of generic and unknown traffic. It samples flows using a specific sample rate. By default, for analyzing top hosts, NBAR2 sets the sample rate dynamically based on traffic. For information on configuring the sample rate, see Configuring NBAR2 Auto-learn, on page 2.
- By default, tracking top hosts is enabled; tracking top ports and top sockets is disabled.
- Auto-learn for "top sockets" is automatically enabled or disabled when "top ports" is enabled or disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nbar classification auto-learn** { **top-hosts** | **top-ports** }
4. **ip nbar classification auto-learn** { **top-hosts** | **top-ports** } **sample-rate** *rate*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter a password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**ip nbar classification auto-learn** { **top-hosts**	**top-ports** }
		Example:
		`Device (config)# ip nbar classification auto-learn top-hosts`
		`Device (config)# ip nbar classification auto-learn top-ports`
			top-hosts: Enables analyzing traffic classified as generic to generate a list of top hosts for the generic traffic.
			top-ports: Enables analyzing traffic classified as unknown to generate a list of server-side top ports and top sockets occurring in the unknown traffic.

Step 4	**ip nbar classification auto-learn** { **top-hosts**	**top-ports** } **sample-rate** *rate* **Example:** `Device (config)# ip nbar classification auto-learn top-ports sample-rate 5`	(Optional) Sets the flow sampling rate for the feature. To optimize performance, the mechanism does not track all generic and unknown traffic. It samples flows using a specific sample-rate. A smaller number improves accuracy, but requires more router resources. A *rate* value of 1 means that the mechanism samples all flows of generic (for **top-hosts**) or unknown (for **top-ports**) traffic. **top-hosts** default: NBAR2 sets the rate dynamically based on traffic.

	Command or Action	Purpose
		top-ports default: 128
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Displaying Auto-learn Top Hosts or Ports

SUMMARY STEPS

1. **show ip nbar classification auto-learn** { **top-hosts** | **top-ports** } *number_of_entries* [**detailed**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show ip nbar classification auto-learn** { **top-hosts** | **top-ports** } *number_of_entries* [**detailed**]
	Example:
	`Device (config)# show ip nbar classification auto-learn top-hosts 10 detailed`
	
	`Device (config)# show ip nbar classification auto-learn top-ports 25`
		Displays statistics for the top hosts in generic traffic or top server-side ports occurring in unknown traffic.
		number_of_entries: Maximum number of entries to display. Possible values: 1 to 100
		detailed: Provides additional information, such as the byte, flow, and packet counts for each.

Displaying Auto-learn Top Sockets

In the context of auto-learn, sockets refer to server-side socket addresses (IP address and port).

Note The auto-learn top-sockets functionality is enabled or disabled automatically when top-ports is enabled or disabled.

SUMMARY STEPS

1. **show ip nbar classification auto-learn top-sockets** *number_of_entries* [**detailed**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip nbar classification auto-learn top-sockets** *number_of_entries* [**detailed**] **Example:**	Displays statistics for the top sockets in unknown traffic. *number_of_entries*: Maximum number of entries to display. Possible values: 1 to 100

	Command or Action	Purpose
	`Device (config)# show ip nbar classification auto-learn top-sockets 100 detailed`	**detailed**: Provides additional information, such as the byte, flow, and packet counts for each.

Clearing Host/Port Statistics for NBAR2 Auto-learn

This procedure operates on the list of hosts, ports, and sockets that the NBAR2 Auto-learn feature creates for traffic classified as generic or unknown.

This command clears the statistical data (bytes, packets, flows, and so on) collected for the hosts (**top-hosts** option) or ports and sockets (**top-ports** option), but does not clear old hosts/ports/sockets for which no recent traffic has been detected. Compare this with **clear ip nbar classification auto-learn top-hosts restart**, which clears the statistics and also clears old hosts/ports/sockets.

SUMMARY STEPS

1. **clear ip nbar classification auto-learn** { **top-hosts** | **top-ports** } **statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear ip nbar classification auto-learn** { **top-hosts** | **top-ports** } **statistics** **Example:** `Device# clear ip nbar classification auto-learn top-hosts statistics`	Clears the statistical data collected for hosts (**top-hosts** option), or ports and sockets (**top-ports** option).

Clearing Host/Port Statistics and Inactive Hosts/Ports for NBAR2 Auto-learn

This procedure operates on the list of hosts, ports, and sockets that the NBAR2 Auto-learn feature creates for traffic classified as generic or unknown.

The procedure clears the statistical data (bytes, packets, flows, and so on) collected for the hosts (**top-hosts** option), or ports and sockets (**top-ports** option), and also clears the old hosts/ports/sockets for which no recent traffic has been detected. Compare this with **clear ip nbar classification auto-learn top-hosts statistics**, which clears the statistics, but does not clear old hosts/ports/sockets.

SUMMARY STEPS

1. **clear ip nbar classification auto-learn** { **top-hosts** | **top-ports** } **restart**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**clear ip nbar classification auto-learn** { **top-hosts** | **top-ports** } **restart** **Example:**	Clears the statistical data collected for hosts (**top-hosts** option) or ports (**top-ports** option), and also clears the old hosts/ports/sockets for which no recent traffic has been detected.

	Command or Action	Purpose
	`Device# clear ip nbar classification auto-learn top-hosts restart`	

Configuration Examples for NBAR2 Auto-learn

Example: Configuring Auto-learn for Hosts

```
Device> enable
Device# configuration terminal
Device (config)# ip nbar classification auto-learn top-hosts
Device (config)# exit
```

Example: Displaying Auto-learn Data

Top Hosts

Output of **show ip nbar classification auto-learn top-hosts** command without **detailed** option:

```
Device#show ip nbar classification auto-learn top-hosts 10

Total bytes:         23.236 M
Total packets:       31.816 K
Total flows:         229
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
-------------------------------------------------------------------------------
  #|Host                                |Byte%|Flow%|Pkt% |Type |Field
-------------------------------------------------------------------------------
  1|images1.xyz.com                     | 37% | 34% | 38% |http |host
  2|res.cloudinary.com                  | 34% |  3% | 25% |http |host
  3|mail.cisco.com                      | 27% | 62% | 35% |ssl  |host
  4|10.210.20.19                        | <1% | <1% | <1% |http |host
```

Top Hosts - Detailed

Output of **show ip nbar classification auto-learn top-hosts** command with **detailed** option:

```
Device# show ip nbar classification auto-learn top-hosts 10 detailed
Total bytes:         23.236 M
Total packets:       31.816 K
Total flows:         229
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
-----------------------------------------------------------------------------------------------

  #|Host                |Byte count |Byte%|Flow count |Flow%|Pkt count  |Pkt% |Type |Field
-----------------------------------------------------------------------------------------------
```

```
  1|site.xyz.com          |8.707 M    | 37% |79         | 34% |12.239 K   | 38% |http |host

  2|res.cloudinary.com    |8.045 M    | 34% |7          |  3% |8.162 K    | 25% |http |host

  3|mail.cisco.com        |6.363 M    | 27% |142        | 62% |11.315 K   | 35% |ssl  |host

  4|10.210.20.19          |120.111 K  | <1% |1          | <1% |100        | <1% |http |host
```

Top Sockets

In the context of auto-learn, sockets refer to server-side socket addresses (IP address and port).

Note The auto-learn top-sockets functionality is enabled or disabled automatically when top-ports is enabled or disabled.

Output of **show ip nbar classification auto-learn top-sockets** command (modified to fit more clearly):

```
Device#show ip nbar classification auto-learn top-sockets 100 detailed
Total bytes:  398.747 K
Total packets:         1.611 K
Total flows:           1.109 K
Sample rate last:    1
Sample rate average: 1
Sample rate min:     1
Sample rate max:     1
-------------------------------------------------------------------------------------------
 #|Port  |IP              |Byte count |Byte%|Flow |Flow%|Pkt   |Pkt% |Traffic |Asymmetric
  |      |                |           |     |count|     |count |     |Type    |byte
  |      |                |           |     |     |     |      |     |        |count
-------------------------------------------------------------------------------------------
 1|80    |173.38.201.172  | 81.776 K  | 20% |  4  | <1% | 90   |  5% |TCP     |0
 2|80    |173.38.201.174  | 74.555 K  | 18% |  4  | <1% | 84   |  5% |TCP     |0
 3|123   |10.56.129.33    | 42.672 K  | 10% |889  | 80% |889   | 55% |UDP     |N/A
 4|443   |47.88.68.98     |  1.472 K  | <1% |  3  | <1% | 10   | <1% |TCP     |0
 5|1080  |10.56.217.8     |  1     K  | <1% |  1  | <1% |  1   | <1% |TCP     |0
 6|63699 |10.210.20.123   | 213       | <1% |  1  | <1% |  1   | <1% |TCP     |0
 7|443   |171.70.124.118  | 37        | <1% |  1  | <1% |  1   | <1% |TCP     |0
 8|37814 |10.210.20.122   | 14        | <1% |  1  | <1% |  2   | <1% |TCP     |0
 9|443   |140.205.195.83  | 12        | <1% |  1  | <1% |  2   | <1% |TCP     |0
10|443   |10.61.25.91     |  7        | <1% |  1  | <1% |  1   | <1% |TCP     |0
```

Additional References for NBAR2 Auto-learn

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NBAR2 Auto-learn

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for NBAR Customization Assistance Based on SSL or HTTP

Feature Name	Releases	Feature Information
NBAR2 Auto-learn (previously called "NBAR Customization Assistance based on SSL or HTTP")	Cisco IOS XE Release 3.16S, Cisco IOS Release 15.5(3)T	Assists in creating custom protocols to improve classification of generic or unknown traffic. The following commands were introduced or modified: **ip nbar classification auto-learn top-hosts**, **ip nbar classification auto-learn top-ports**, **ip nbar classification auto-learn top-ports sample-rate**, **show ip nbar classification auto-learn top-hosts**, **show ip nbar classification auto-learn top-ports**, **clear ip nbar classification auto-learn top-ports restart**, **clear ip nbar classification auto-learn top-hosts**, **clear ip nbar classification auto-learn top-ports statistics**