Auto Traffic Analysis and Protocol Generation

NBAR includes an **auto-learn** feature that analyzes generic and unknown network traffic to determine the most frequently used hosts and ports. Using this data, the **auto-custom** feature can automatically generate NBAR protocols provisionally to improve identification of traffic.

Prerequisites for auto-custom

The auto-custom feature requires auto-learn to be active.

See NBAR2 auto-learn.

Limitations of auto-custom

Default

The auto-custom feature is disabled by default.

Environments Supported

The auto-custom feature supports the following environments:

- A single router with a single collector, or
- A single router with no collector

The feature does not support environments with multiple routers operating with a single collector.

Background: Auto Traffic Analysis Using NBAR2 Auto-learn

The NBAR2 **auto-learn** (see NBAR2 Auto-learn) and **auto-custom** features work together. 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. For unknown traffic, it identifies server-side ports and tracks the "top ports" and "top sockets" that occur in unknown traffic.

The results produced by **auto-learn** can be used by the **auto-custom** feature to automatically create custom NBAR protocols that improve classification of the traffic to improve application visibility for this difficult-to-classify traffic. For example, top hosts provide "candidate" hosts to use in creating custom protocols.

Auto Generation of Custom Protocols Using auto-custom

The **auto-custom** feature uses the results of **auto-learn** to improve NBAR classification of generic and unknown network traffic, automatically generating custom NBAR protocols.

Format for Reporting of Traffic Classified by Auto-generated NBAR Protocols

Auto-generated NBAR protocols report traffic according to hostname or port number:

- For **generic** traffic, protocols are generated for the most frequently occurring **hosts**, and are named according to the hostname. For traffic that contains only a host address and not a hostname, where possible, NBAR uses DNS lookup to provide the corresponding hostname.

  Examples: abcd.com, efgh.net

- For **unknown** traffic, protocols are generated for the most frequently occurring ports, and are named according to the **port number or socket** (server-side IP + port), and the traffic type: TCP or UDP.

  Examples for port: Port_80_TCP, Port_443_UDP

  Example for socket: 72.163.4.162:256_TCP

Auto-generation Is Based on Sampling of Traffic Flows

The **auto-learn** mechanism collects data about generic and unknown traffic by sampling traffic flows for analysis. Not every flow is analyzed. Using sampling rather than analyzing each flow is necessary due to the constraints of hardware resources. The availability of hardware resources for auto-learn analysis depends mostly on the network traffic volume that a device is handling.

For **generic** traffic, the sampling rate is dynamic, adjusting automatically according to system load. For **unknown** traffic, the default sampling rate is 128, meaning that the mechanism samples 1 flow for every 128 of unknown traffic. This value can be configured manually.

Because the **auto-custom** feature relies on data collected by **auto-learn**, the flow sampling performed by auto-learn can influence the automatic generation of protocols by auto-custom. In most use cases, however, sampling accurately reflects the makeup of network traffic.

Use of Auto-generated NBAR Protocols By Other Features

The NBAR application protocols auto-generated by auto-custom improve network traffic reporting, improving application visibility. However, the auto-generated protocols present at any given time are determined by the makeup of recent network traffic, making them inherently dynamic and impermanent.

Because of this dynamic nature, auto-custom protocols are applicable to some features, but not to others. In general, auto-custom protocols improve application **visibility**, but do not affect **security** (firewall) or **QoS** policies.

Features affected by auto-custom protocols:

- NBAR protocol discovery
- Application visibility (FNF, performance-monitor, ezPM, MACE, ...)

Features not affected by auto-custom protocols:

- MQC/QoS
- WAAS
- Performance Routing (PfR)
- NAT

Enabling and Disabling auto-custom

Enables or disables one or both of the auto-custom modes:

- top-hosts
- top-ports

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **ip nbar auto-custom** {**top-ports** | **top-hosts**}
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	[**no**] **ip nbar auto-custom** {**top-ports**	**top-hosts**} **Example:** `Device(config)# ip nbar auto-custom top-hosts`	Enables or disables auto-custom. The **top-ports** and **top-hosts** options apply the command to those respective modes of auto-custom.

	Command or Action	Purpose
Step 3	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring the Maximum Number of Auto-generated NBAR Protocols to Create

Configures the maximum number of protocols automatically generated by **auto-custom**. The auto-generated protocols present at any given time are determined by the makeup of recent network traffic, making them inherently dynamic and impermanent.

SUMMARY STEPS

1. **configure terminal**
2. **ip nbar auto-custom** {**top-hosts** | **top-ports**} **max-protocols** *number*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip nbar auto-custom** {**top-hosts** | **top-ports**} **max-protocols** *number* **Example:** `ip nbar auto-custom top-hosts max-protocols 30`	Configures the maximum number of auto-custom protocols to generate from the lists of top-hosts or top-ports collected by the auto-learn mechanism. **top-hosts** default: 10 **top-ports** default: 10
Step 3	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring the Time Interval for Re-generating the auto-custom Protocols

Configures the time interval at which auto-custom reloads the lists of "top-hosts" for generic traffic and "top-ports" for unknown data. The lists are provided by the **auto-learn** mechanism. After reloading the lists, the **auto-custom** mechanism generates a new set of custom protocols based on the data, which reflects the

most recent network traffic. Because of this mechanism, the list of auto-custom protocols is dynamic, changing with the makeup of generic and unknown network traffic.

SUMMARY STEPS

1. **configure terminal**
2. **ip nbar auto-custom** {**top-hosts** | **top-ports**} **time-interval** *minutes*
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip nbar auto-custom** {**top-hosts**	**top-ports**} **time-interval** *minutes* **Example:** `ip nbar auto-custom top-hosts time-interval 10`	Configures the time interval at which auto-custom reloads the lists of "top-hosts" for generic traffic and "top-ports" for unknown data. Default: 30 minutes
Step 3	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Clearing auto-custom Data

SUMMARY STEPS

1. **configure terminal**
2. **clear ip nbar auto-custom** {**top-hosts** | **top-ports**} {**stats** | **restart**}
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**clear ip nbar auto-custom** {**top-hosts**	**top-ports**} {**stats**	**restart**} **Example:** `clear ip nbar auto-custom top-ports restart`	Clears auto-custom data. The **top-ports** and **top-hosts** options apply the command to those respective modes of auto-custom. **stats**: Clears only counters

	Command or Action	Purpose
		restart: Clears counters and removes all current auto-custom protocols.
Step 3	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Displaying Auto-generated NBAR Protocols Created by auto-custom

SUMMARY STEPS

1. **show ip nbar auto-custom** [**top-hosts** | **top-ports**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip nbar auto-custom** [**top-hosts**	**top-ports**] **Example:** `show ip nbar auto-custom`	Displays the auto-generated NBAR protocols created by the auto-custom mechanism. Optionally, can specify only protocols for **top-hosts** or **top-ports**. • The first part of the output shows the protocols based on hostnames, from **generic** traffic. • The second part of the output shows the protocols based on port numbers + traffic type (TCP or UDP), from **unknown** traffic.

Example

```
# show ip nbar auto-custom
Top-hosts:
 Max number of protocols   :10
 Interval (min)            :30
 ---------------------------------------------------------------------------------------------------
 | Id  | Protocol name          | Underlying | Auto-learn value               | Age (min) | Status |
 |     |                        | protocol   |                                |           |        |
 ---------------------------------------------------------------------------------------------------
 |    1|m.abc-demo.com          |http        |m.abc-demo.com                  |         80|Dynamic |
 |    2|hwcdn.def-demo.com      |http        |hwcdn.def-demo.com              |         80|Dynamic |
 |    3|ec.def-demo.com         |http        |ec.def-demo.com                 |         80|Dynamic |
 |    4|payroll.demo.com        |ssl         |payroll.demo.com                |         80|Dynamic |
 |    5|ec-media.demo.com       |http        |ec-media.demo.com               |         50|Dynamic |
 |    6|TrustedSourceServer_IMQ |ssl         |TrustedSourceServer_IMQA01      |         20|Dynamic |
 |    7|go.microsoft.com        |http        |go.microsoft.com                |         20|Dynamic |
 |    8|ping.chartbeat.net      |http        |ping.chartbeat.net              |         20|Dynamic |
 ---------------------------------------------------------------------------------------------------

Top-ports:
 Max number of protocols   :40
 Interval (min)            :1
 ---------------------------------------------------------------------------------------------------
 | Id  | Protocol name          |             Auto-learn value                  | Age (min) | Status |
 ---------------------------------------------------------------------------------------------------
 |    1|Port_256_TCP            |Port_256_TCP                                   |          0|Dynamic |
```

```
|    2|72.163.4.162:256_TCP    |72.163.4.162:256_TCP                          |          0|Dynamic |
-------------------------------------------------------------------------------------------------------
```

Displaying NBAR Protocol Discovery Information for auto-custom Protocols

SUMMARY STEPS

1. **show ip nbar protocol-discovery stat auto-custom**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip nbar protocol-discovery stat auto-custom** **Example:** `show ip nbar protocol-discovery stats auto-custom`	Displays the auto-custom protocol discovery statistics.

Example

```
# show ip nbar protocol-discovery stats auto-custom

 Ethernet0/0

 Last clearing of "show ip nbar protocol-discovery" counters 1d05h


                            Input                    Output
                            -----                    ------
   ------------------------ ------------------------ ------------------------
www.abcdef-demo.com          152         0
Total                        152                      0
```