

Custom Applications

Table 1: Feature History

Feature Name	Release Information	Description
Support for Defining Custom Applications	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature adds support for defining custom applications.

- Information about custom applications , on page 1
- Configure Custom Applications Using Cisco SD-WAN Manager, on page 6
- Verify Custom Applications, on page 8

Information about custom applications

Cisco Network-Based Application Recognition (NBAR) is a Cisco technology that performs the SD-WAN Application Intelligence Engine (SAIE) flow on network traffic to identify network applications according to their traffic characteristics.

Note In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

The specific traffic characteristics of a network application are called an application signatures. Cisco packages the signature for an application, together with other information, as a protocol. Cisco packages a large set of protocols, covering numerous commonly occurring network applications, as a Protocol Pack. Cisco updates and distributes Protocol Packs regularly. They provide a database of network application signatures for NBAR to use to identify network application traffic.

The term network applications is defined broadly, and may include all of the following, and more:

- Social media websites
- Voice over IP (VoIP) applications
- Streaming audio and video, such as Cisco Webex
- Cloud applications, such as for cloud storage

- SaaS applications
- Custom network applications specific to an organization

Identifying applications is useful for monitoring network traffic, configuring application-aware traffic policy, and more.

To summarize network application signatures, protocols, and Protocol Packs, and how NBAR uses them:

- The traffic of a network application has unique characteristics that can be used to identify the traffic as belonging to that specific application. These characteristics are called application signatures.
- Cisco packages the signature for a specific network application as a protocol.
- Cisco packages a large set of protocols, covering commonly occurring internet applications, as Protocol Packs.
- Cisco NBAR performs the SAIE flow on traffic to gather the information required to identify the sources of the traffic, and uses protocols, such as those provided in Protocol Packs, to match that information to specific network applications. The result is that NBAR identifies the network applications producing traffic in the network.

Cisco Software-Defined Application Visibility and Control (SD-AVC) uses Cisco NBAR application identification to provide information about application usage within a network.

Custom applications

In addition to the standard protocols provided in a Protocol Pack, you can define protocols, called custom applications, to identify internet traffic, often for uncommon network applications that are of specific interest to their organization. Custom applications augment the protocols provided in a Protocol Pack.

You can use custom applications in the same way as any other protocol when configuring:

- Cisco Catalyst SD-WAN policies
- Application Quality of Experience (AppQoE) policies, such as application-aware routing, TCP acceleration, and Quality of Service (QoS)



Note The following terms are used in the documentation of related technologies, and are equivalent: custom applications, custom protocols, user-defined applications

Custom applications in Cisco Catalyst SD-WAN

Cisco Software-Defined AVC (SD-AVC) is a component of Cisco Application Visibility and Control (AVC). It functions as a centralized network service, operating with specific participating devices in a network. One function of Cisco SD-AVC, which is included as a component of Cisco Catalyst SD-WAN, is to create and manage custom applications. Cisco Catalyst SD-WAN uses this Cisco SD-AVC functionality, through SD-AVC REST APIs, to enable you to define custom applications within Cisco Catalyst SD-WAN.

As a Cisco Catalyst SD-WAN user, you can use Cisco SD-WAN Manager to define custom applications. Cisco SD-AVC then pushes the custom applications to devices in the network. The devices in the network use the custom applications and other application protocols to analyze traffic traversing the devices.

The process of defining a custom protocol includes choosing criteria to identify network traffic as coming from a specific network application. The criteria can include characteristics of hosts originating the traffic, such as server names, IP addresses, and so on.

Priority of protocols and custom applications

It is possible to define custom applications that match some of the same traffic as a protocol included in the Protocol Pack operating with Cisco NBAR. When matching traffic, custom applications have priority over Protocol Pack protocols. Deploying SD-AVC within an existing network does not require any changes to the network topology.

Custom application functionality

- Releases earlier than Cisco vManage Release 20.5.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

  Creating a custom application has the following effect:

  A custom application does not affect visibility functionality (monitoring traffic) or control functionality (traffic policy) until a policy that makes use of the custom application is applied.

- Releases Cisco vManage Release 20.5.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later

  Creating a custom application has the following effect:

  - A custom application affects application visibility functionality only (monitoring traffic), such as for protocol-discovery counters and Flexible NetFlow (FNF), and does not affect traffic policy.
  - When the custom application is used by a policy, it affects control functionality (traffic policy) also.

Packet trace and Network-wide Path Insights

From Cisco vManage Release 20.5.1, packet trace output includes these terms:

- Classification name: This is the application classification of traffic for policy purposes.
- Classification visibility name: This is the application classification of the traffic for traffic visibility purposes, such as for protocol-discovery counters and Flexible NetFlow (FNF).

The **NBAR** section of the Network-wide Path Insights (NWPI) **Insight advanced** views uses the same terms. In Cisco SD-WAN Manager, see this in **Tools** > **Network-wide Path Insights**.

In this example, the Classification name and Classification visibility name are different because custom applications are enabled only for visibility functionality (monitoring traffic).

```
Packet number in flow: 12
Classification state: Final
Classification name: ssl
Classification ID: 1312 [CANA-L7:453]
Candidate classification sources:
N/A
Early cls priority: 255
Permit apps list id: 0
Sdavc Early prioirty as app: 0
Classification visibility name: cisco_com
Classification visibility ID: 3714 [21:3714]
Number of matched sub-classifications: 0
Number of extracted fields: 0
Is PA (split) packet: False
Is FIF (first in flow) packet: False
```

```
TPH-MQC bitmask value: 0x4
Source MAC address: 00-00-5E-00-53-00
Destination MAC address: 00-00-5E-00-53-01
Traffic Categories: N/A
```

In this example, the Classification name and Classification visibility name match because custom applications are enabled for visibility functionality (monitoring traffic) and control functionality (traffic policy).

```
Packet number in flow: 12
Classification state: Final
Classification name: cisco_com
Classification ID: 1312 [CANA-L7:453]
Candidate classification sources:
N/A
Early cls priority: 255
Permit apps list id: 0
Sdavc Early prioirty as app: 0
Classification visibility name: cisco_com
Classification visibility ID: 3714 [21:3714]
Number of matched sub-classifications: 0
Number of extracted fields: 0
Is PA (split) packet: False
Is FIF (first in flow) packet: False
TPH-MQC bitmask value: 0x4
Source MAC address: 00-00-5E-00-53-00
Destination MAC address: 00-00-5E-00-53-01
Traffic Categories: N/A
```

Custom application names

From Cisco Catalyst SD-WAN Manager Release 20.16.1, when you create a new custom application and provide a name for the application, Cisco SD-WAN Manager appends "-Custom" to the name. This ensures that the name does not conflict with other application types, such as those from Protocol Packs, or cloud-sourced applications.

Restrictions for custom applications

Ensure that the following restrictions are adhered to when configuring custom applications:

- Maximum number of applications

  Maximum number of custom applications: 1100

- Maximum number of rules

  Maximum number of L3/L4 rules: 20000 and maximum number of server names: 50000

- Wildcards
  - Wildcard followed by a period

    For server names, maximum instances of wildcard followed by a period (.): 50000

    Example: ***.cisco.com** matches www.cisco.com, developer.cisco.com

Note ***.cisco.com**: Configuring the custom application server name as *.cisco.com (including the dot) results in an exact suffix match. The rule matches any domain ending in .**cisco.com**, regardless of the subdomains. Consequently, both **www.cisco.com** and **developer.cisco.com** match, whereas **www.cisco.com.test.org.us** does not match.

- Prefix wildcard

  For server names, maximum instances of prefix wildcard as part of server name: 256

  Example: *ample.com matches www.example.com

Note ***cisco.com**: Configuring the custom application server name as *cisco.com (omitting the dot) results in a substring match. Consequently, any domain string containing ***cisco.com**, such as **www.cisco.com** or **www.cisco.com.test.org.us**, will be matched.

- One domain, two applications

  Mapping the same domain to two different custom applications is not supported.

- First-packet classification

  To enable first-packet classification with SD-AVC, unencrypted DNS traffic must be redirected through the router running on Cisco IOS XE Catalyst SD-WAN devices and must be visible within the same VRF as the application traffic.

- CLI

  Creating custom applications though CLI is not supported in Cisco Catalyst SD-WAN policy.

- Disaster recovery

  SD-AVC state replication in disaster recovery (DR) is not supported in Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier. DR switchover resets SD-AVC state for Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier releases. Post switchover, custom applications will not be present in SD-AVC.

- DNS traffic unencrypted

  For NBAR to correctly categorize traffic based on domain name, the DNS traffic needs to pass unencrypted through the router.

- Custom application name restriction

  Cisco Catalyst SD-WAN does not support creating a custom application with "test" as part of the name, such as test, test1, test2, and so on. SD-WAN Manager permits you to create the application, but it does not deploy correctly to the devices in the network.

Configure Custom Applications Using Cisco SD-WAN Manager

Prerequisites

Install Cisco SD-AVC as a component of Cisco Catalyst SD-WAN. For information on how to enable SD-AVC on Cisco SD-WAN Manager, see Information on how to enable SD-AVC for Cisco SD-WAN devices.

Perform the following steps to configure custom applications:

1. From Cisco SD-WAN Manager, select **Configuration** > **Application Catalog**.
2. Click **Applications**.
3. Select **Custom Application**.



Note For Cisco IOS XE Catalyst SD-WAN Release 17.14.x and earlier, do the following:

a. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.

b. Select **Centralized Policy**.

c. Click **Custom Options** and select **Centralized Policy** > **Lists**.

d. Click **Custom Applications**.

4. Click **New Custom Application**.
5. To define the application, provide an application name and enter match criteria. The match criteria can include one or more of the attributes provided: server names, IP addresses, and so on. You do not need to enter match criteria for all fields.

   The match logic follows these rules:

   - Between all L3/L4 attributes, there is a logical AND. Traffic must match all conditions.
   - Between L3/L4 and Server Names, there is a logical OR. Traffic must match either the server name or the L3/L4 attributes.

Field	Description
Application Name	(mandatory) Enter a name for the custom application. From Cisco Catalyst SD-WAN Manager Release 20.16.1, Cisco SD-WAN Manager appends "-Custom" to the name. This ensures that the name does not conflict with other application types, such as those from Protocol Packs, or cloud-sourced applications.

Field	Description
Server Names	One or more server names, separated by commas. You can include an asterisk wildcard match character (*) only at the beginning of the server name. Examples: *cisco.com, *.cisco.com (match www.cisco.com, developer.cisco.com, …)
L3/L4 Attributes	
IP Address	Enter one or more IPv4 addresses, separated by commas. Example: 10.0.1.1, 10.0.1.2 **Note** The subnet prefix range is 24 to 32.
Ports	Enter one or more ports or port ranges, separated by space. Example: 30, 45-47
L4 Protocol	Select one of the following: TCP, UDP, TCP-UDP

6. Click **Add**. The new custom application appears in the table of custom applications.



Note To check the progress of creating the new custom application, click **Tasks** (clipboard icon). A panel opens, showing active and completed processes.

Result

See the custom application functionality section in Information about custom applications , on page 1.

Example Custom Application Criteria

Criteria	How to configure fields
Domain name	**Server Names**: Custom
Set of IP addresses, set of ports, and L4 protocol	**IP Address**: 10.0.1.1, 10.0.1.2 **Ports**: 20 25-37 **L4 Protocol**: TCP-UDP

Criteria	How to configure fields
Set of ports and L4 protocol	**Ports**: 30 45-47 **L4 Protocol**: TCP

Verify Custom Applications

Verify Custom Applications in Cisco SD-WAN Manager

After you define a custom application, it appears in the **Custom Application List**, which shows all available protocols and custom applications. The **Custom Application List** is available here:

Configuration > **Policies** > **Centralized Policy** > **Add Policy** > **Custom Applications**.

Verify Protocols and Custom Applications on a Device

Use the **show ip nbar protocol-id** command to display all protocols and custom applications that are loaded on the router. It is helpful to filter the results. For example, to display all protocols and custom applications with "custom" in the name, use this:

```
vm5#show ip nbar protocol-id | include custom
custom_amazon                    3899          PPDK LOCAL
custom_facebook                  3284          PPDK LOCAL
```

See show ip nbar protocol-id.