SD-AVC Overview

SD-AVC Overview

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.

As an SDN solution operating network-wide, Cisco SD-AVC complements solutions such as:

- Cisco Intelligent WAN (IWAN)

- Cisco EasyQoS

- Application Assurance

Features and Benefits

Feature/Benefit	Description
Network-level application recognition consistent across the network	The SD-AVC network service aggregates application data from multiple devices and sources, and provides that composite application information in return. Because SD-AVC operates at the network level, any application rule created by SD-AVC based on aggregated application data is shared and applied consistently across all participating network devices.

Feature/Benefit	Description
Improved application recognition in symmetric and asymmetric routing environments	Cisco SD-AVC further refines application recognition accuracy by helping numerous devices in a network
	SD-AVC aggregates application data shared by participating devices in the network, and analyzes the shared application data. It then provides this composite application information (in the form of an application rules pack) to the participating routers, improving application recognition. Because SD-AVC shares application rules across numerous network devices, devices that see only one direction of a flow can benefit from the information collected on the other direction of the same flow.
	See SD-AVC and Application Recognition
Improved first packet recognition	SD-AVC application rules are based on flow tuple (address and port) information. After a learning phase and sharing tuples among participating devices, the devices are able to identify new flows on the first packet, based on the tuple information
Protocol Pack update at the network level	SD-AVC can assist in deploying Protocol Packs to numerous routers in the network. Download the Protocol Packs to deploy, store them on the centralized SD-AVC network service, then use the SD-AVC Dashboard to select which devices in the network will receive the Protocol Packs.
	See: Protocol Packs Page
SD-AVC Dashboard	Secure browser-based SD-AVC Dashboard over HTTPS for monitoring SD-AVC functionality and statistics, and for configuring Protocol Pack updates network-wide.
	See: Using SD-AVC
Improved Microsoft Office 365 traffic classification	The MS-Office365 Connector component improves classification for Microsoft Office 365 traffic. The SD-AVC Dashboard displays the status of the component.
	See: MS-Office365 Connector

No Change to Topology

Deploying SD-AVC within an existing network does not require any changes to the network topology.

New Features and Changes in 2.0.x

Table 1: New and Changed Features, SD-AVC Release 2.0.1

Feature	Description
SD-AVC system time and displayed times	Improved display of times in the SD-AVC Dashboard. Internally, the SD-AVC network service uses standard UTC. The Dashboard displays times according to the internal SD-AVC system time, adjusted by the local time zone offset of the PC that is accessing the Dashboard. See SD-AVC System Time and Displayed Times.
Improved ability to configure and view DNS servers for the MS-Office365 Connector	By default, SD-AVC has two Cisco OpenDNS DNS servers configured. Improved ability to add additional DNS servers. See MS-Office365 Connector.

Table 2: New and Changed Features, SD-AVC Release 2.0.0

Feature	Description
Updated user interface	• Improved interactive display of traffic data • Improved presentation of warnings and errors affecting devices
Improved control of Protocol Pack deployment	• Can update Protocol Packs for individual devices, for segments, or for all devices in the network • Ability to revert to the Protocol Pack built into the Cisco IOS release See: Protocol Packs Page
Improved Microsoft Office 365 traffic classification	MS-Office365 Connector is a component introduced in this release that improves classification for Microsoft Office 365 traffic. The SD-AVC Dashboard displays the status of the component. This feature requires connectivity to a DNS server. By default, SD-AVC uses Cisco OpenDNS servers: 208.67.222.222 and 208.67.220.220 See: MS-Office365 Connector
Support for more devices	Support for 4000 network devices operating with SD-AVC

Using SD-AVC in an Asymmetric Routing Scenario

The Challenge of Asymmetric Routing

One of the challenges that SD-AVC addresses well is application recognition in asymmetric routing scenarios. While it is not the only situation in which SD-AVC offers improved results, asymmetric routing demonstrates one of the advantages of aggregating application data from many sources.

Certain network configurations may produce "asymmetric routing" as an unintended effect. In asymmetric routing, the packets of a single two-way connection travel by different paths between network nodes. For example the downstream traffic from a server to a client might be routed through one path, while the upstream traffic from the client to the server might be through a different path. When this occurs, AVC operating on a hub router may see only a single direction of the traffic for that connection, posing a challenge to application recognition.

Deep Packet Inspection and Asymmetry

AVC deep packet inspection (DPI) operates best when it sees both directions of traffic. In symmetric routing, AVC operating on a single device that handles both directions of a flow can fully analyze metadata and other traffic attributes to help identify the application creating the flow. By contrast, an asymmetric scenario can limit the ability to recognize some types of traffic. This is especially true when AVC sees only to the downstream traffic for a particular flow.

Asymmetric routing may occur for various reasons, including from intelligent path selection by Cisco IWAN. The issue particularly affects hub routers within an enterprise network with a hub/branch topology.

Effects of Limited Application Recognition

Limiting AVC application recognition can affect classification of traffic for QoS policy, visibility, and other functionality. Consequently, a solution that overcomes the limitations caused by asymmetric routing is especially helpful for maximum network efficiency.

Figure 1: Asymmetric Routing Example
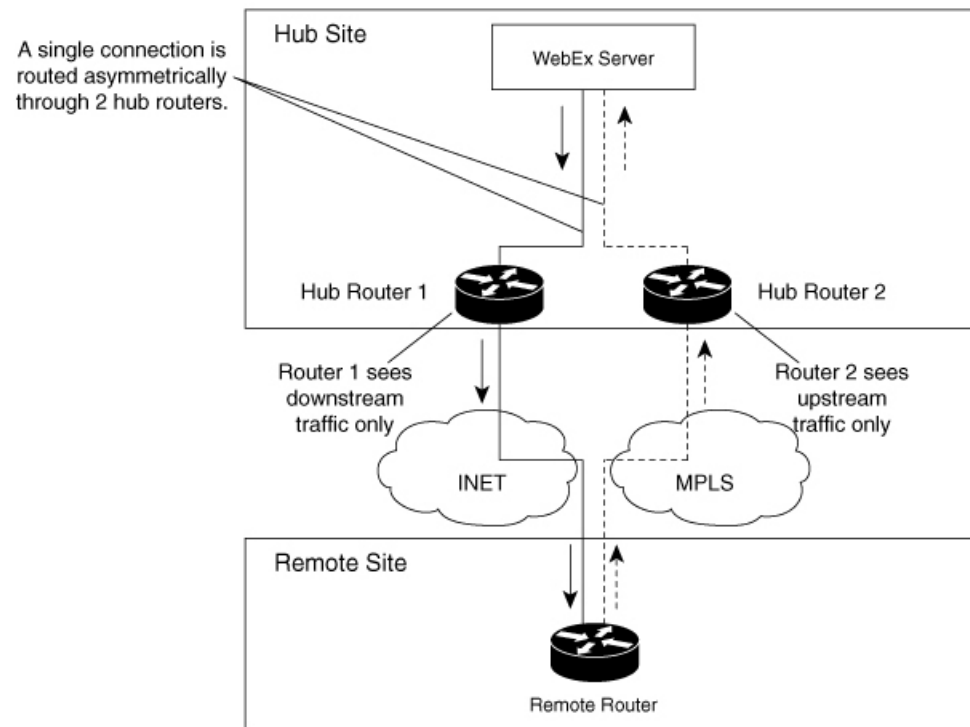
Centralized Server Aggregating Application Data

SD-AVC compiles and analyzes application data from multiple devices within the network, including devices that separately handle the downstream and upstream traffic for a single flow. Using data from multiple sources, SD-AVC synchronizes application information network-wide, overcoming the challenges of asymmetric routing. This strategy provides a major improvement to application recognition within networks, improving the effectiveness of application-based solutions.

With the improved application recognition, AVC can apply application-based policies, such as QoS, path selection, and visibility more accurately. For example, with complete information about both streams of a flow, a path selection policy can direct the downstream path through the same route as the upstream.

Figure 2: Asymmetric Routing and SD-AVC