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 directly from Cisco into a repository 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.
Cloud Connector	SD-AVC connects to a cloud service provided by Cisco that improves traffic classification. Cloud Connector uses the latest information available about the server addresses used by public internet sites and services to improve SD-AVC classification of traffic. See Cloud Connector.
Improved Microsoft Office 365 traffic classification	The MS-Office365 Web Service component improves classification for Microsoft Office 365 traffic. The SD-AVC Dashboard displays the status of the component.
REST API	REST API for user-defined applications. See SD-AVC REST API.
Analysis of unclassified traffic	To improve traffic visibility, SD-AVC analyzes unclassified/unidentified traffic and provides server or socket information about unclassified traffic flows that use significant bandwidth. See Unclassified Traffic Analysis and Discovery.

No Change to Topology

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

New Features and Changes, by Release

Table 1: New and Changed Features, SD-AVC Release 4.3

Feature	Description
Installation package for SD-AVC Network Service in tar format	The installation package downloaded from Cisco is in tar format, replacing the earlier OVA format. See Installing the SD-AVC Network Service.
Limit the MS Office 365 Server Domains Sent to Devices in the Network	Added the ability to limit the Microsoft Office 365 server domains that the SD-AVC network service sends to devices in the network, to include only specific service instances. See the **Select Service Instance** option in Cloud Connector.

Table 2: New and Changed Features, SD-AVC Release 4.0.0

Feature	Description
Store Cloud Connector telemetry data in separate locations for each segment	Added the ability to specify a location to store Cloud Connector telemetry data separately for each network segment. This can be done through the REST API. See Configure Cloud Connector Telemetry Data Location.
Configure custom applications in SD-AVC Dashboard	Added the ability to configure user-defined custom applications using the SD-AVC Dashboard. **Note** If you create custom applications using the SD-AVC Dashboard, do not create a new set of custom applications through the REST API using POST. Doing so overwrites the custom applications created through the SD-AVC Dashboard. You can add custom applications through the REST API using PUT. See Creating a Custom Application.
Disable Behavioral Based Classification	Added a control to enable/disable behavioral classification. **Note** Using the Disable option requires that the devices in the network use Cisco IOS XE Amsterdam 17.3.x or later. See Serviceability Page.

Feature	Description
Support for Office 365 Traffic Categories	Added ability to use the Microsoft Office 365 traffic category when creating traffic policy, enabling you to apply policy decisions based on Office 365 traffic category. See Office 365 Traffic Categories.
Clear Traffic Classification Data for a Segment	Added a **Clear State** option, enabling you to clear the collected traffic classification data for a network segment. This resets the application rules pack that the SD-AVC network service sends to devices in the network segment. **Note** This feature requires that the devices in the network use Cisco IOS XE Amsterdam 17.3.x or later. See Application Visibility Page.
SD-AVC REST API: Cloud Connector status API	API added to return Cloud Connector status per segment. See Display Cloud Connector Status.
SD-AVC REST API: Add user-defined application to existing set	API added to add a single user-defined application to an existing set. Add a User-defined Application Rule
SD-AVC REST API: Management of user-defined applications by network segment	Updated the POST API for user-defined applications to enable writing a set of user-defined applications for a specific segment, without affecting other segments. Updated the GET and DELETE APIs to enable displaying or deleting a specific user-defined application for a specific segment, or all of the user-defined applications for a specific network segment. SD-AVC REST API
SD-AVC REST API: For user-defined applications, support for any subnet length for IPv4 or IPv6	Support for an unlimited subnet prefix length, and for IPv6 addresses, when configuring user-defined custom applications. See Custom Applications in SD-AVC (using SD-AVC Dashboard). See User-defined Applications (using SD-AVC REST API).

Table 3: New and Changed Features, SD-AVC Release 3.2.0

Feature	Description
SD-AVC REST API: Enhancement of the L3L4 API	Enhancement of the L3L4 API, extending the supported range of IP addresses. See SD-AVC REST API.
Improved Cloud Connector reliability	Improved Cloud Connector reliability, by improved cloud server connectivity. See Cloud Connector.

Feature	Description
Proxy server configuration from SD-AVC Dashboard	Ability to configure a proxy server from the SD-AVC Dashboard. See Configuring a Proxy Server.

Table 4: New and Changed Features, SD-AVC Release 3.1.0

Feature	Description
Cloud Connector REST APIs	REST APIs added for the Cloud Connector: connect, disable, clear credentials, display configuration, display cloud data See SD-AVC REST API.

Table 5: New and Changed Features, SD-AVC Release 3.0.0

Feature	Description
Cloud Connector	SD-AVC connects to a cloud service provided by Cisco that improves traffic classification. Cloud Connector uses the latest information available about the server addresses used by public internet sites and services to improve SD-AVC classification of traffic. See Cloud Connector.
Protocol Pack import	When Cisco releases a new Protocol Pack, SD-AVC indicates that the new Protocol Pack is available. SD-AVC now provides an option to import the Protocol Pack directly from Cisco to the local SD-AVC repository, without requiring the Software Download tool. The Protocol Pack can then be deployed to devices in the network. See Protocol Packs Page.
System log server	SD-AVC keeps a system log as a local file. Beginning with this release, SD-AVC can also send system messages to an external system log server in real time. See Serviceability Page.
Signed SSL certificate	By default, the browser-based SD-AVC Dashboard provides a self-signed SSL certificate that appears in a browser as untrusted. Optionally, you can register your specific domain and acquire a signed SSL certificate specifically for use with SD-AVC, and import the certificate into SD-AVC. Connecting to the SD-AVC Dashboard is then secure and trusted. See Serviceability Page.

Feature	Description
Changed TCP port range	SD-AVC uses TCP ports for communication between the central SD-AVC network service and the devices in the network running the SD-AVC agent. Port 8080 was added, changing the range from: 21 and 59990-60000 to 21, 8080, and 59990-60000

Table 6: New and Changed Features, SD-AVC Release 2.2.1

Feature	Description
REST API improvements	Several improvements to the SD-AVC REST API.
Optimization of device update time	SD-AVC optimizes the time interval for updating devices in the network, according to the number of devices in the network. For networks containing a relatively small number of devices, updates can occur up to 10 times faster. Updates include the latest aggregated application data, custom applications, and Protocol Pack updates.
Changed TCP port range	SD-AVC uses TCP ports for communication between the central SD-AVC network service and the devices in the network running the SD-AVC agent. The range was simplified from: 21 and 59900-60000 to 21 and 59990-60000
Improved handling of proxy servers	When a network includes a proxy server, SD-AVC recognizes the proxy server IP and synchronizes the IP as a proxy, thereby preventing the SD-AVC agent from caching the IP. This prevents errors in flow classification.

Table 7: New and Changed Features, SD-AVC Release 2.2.0

Feature	Description
Improved scale	SD-AVC supports 1 segment with 6000 devices, or up to 12 segments with 1000 devices in each.
MS-Office365 Connector updates	The MS-Office 365 Connector (external source for SD-AVC) has been updated to incorporate the new Microsoft Office 365 web API. Recent changes that Microsoft has made to the Microsoft Office 365 web API have blocked the SD-AVC Microsoft Office 365 Connector, breaking its functionality in previous releases of SD-AVC.

Table 8: New and Changed Features, SD-AVC Release 2.1.1

Feature	Description
Memory and CPU allocation	Smart allocation of memory and CPU resources used for tracking sockets and L3 incoming entries.
Application rules pack distribution by network segment	For improved control, you can assign application rules pack distribution by network segment.
User-defined applications by network segment	For improved control, user-defined applications can be defined by network segment.
Debugging by device or network segment	SD-AVC **Dashboard** > **Serviceability** page > **Vertical Debug**: Can track traffic for a specific device or network segment.
Unclassified Traffic Visibility	Ability to enable or disable the Unclassified Traffic Visibility feature. See Serviceability Page.
User Interface improvements	Numerous improvements to usability.

Table 9: New and Changed Features, SD-AVC Release 2.1.0

Feature	Description
REST API	The REST API enables configuring user-defined applications, providing classification of applications not covered by the standard Protocol Pack. See SD-AVC REST API.
Unclassified traffic discovery	To improve traffic visibility, SD-AVC analyzes unclassified/unidentified traffic and provides server or socket information about unclassified traffic flows that use significant bandwidth. See Unclassified Traffic Analysis and Discovery.
Source interface configuration	On network devices operating with SD-AVC, you can specify the interface that will appear as the source address for all SD-AVC traffic between the network device and the SD-AVC network service. See Source Interface Configuration Overview.
Ability to configure proxy 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.

Table 10: 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.

Table 11: 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
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

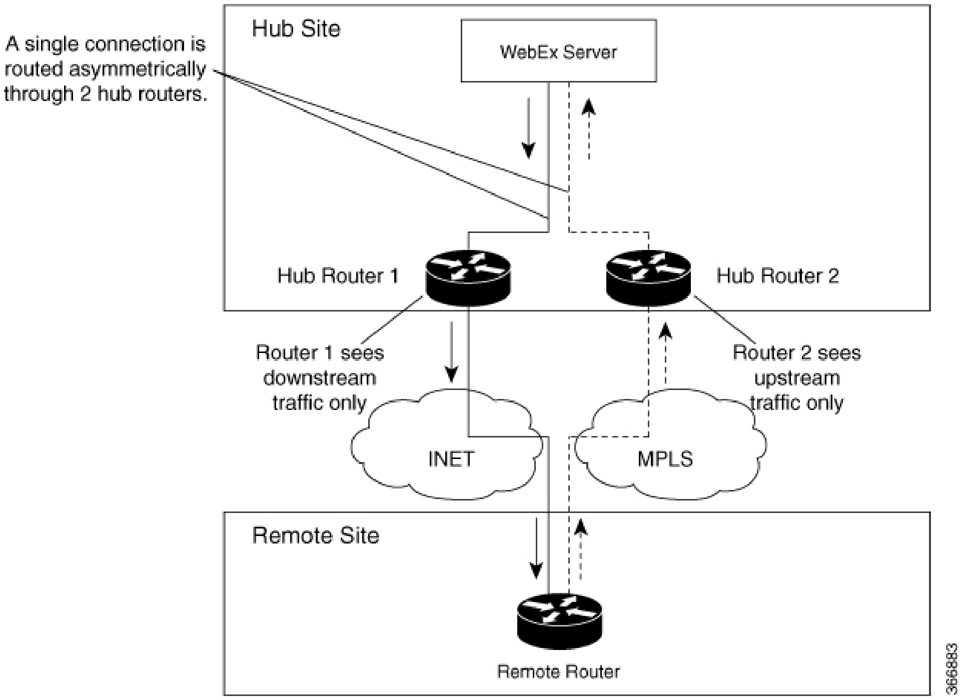
AVC deep packet inspection (DPI) operates best when it sees both directions of traffic. In symmetric routing, AVC operating on a single device that handles both directions of a flow can fully analyze metadata and other traffic attributes to help identify the application creating the flow. By contrast, 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

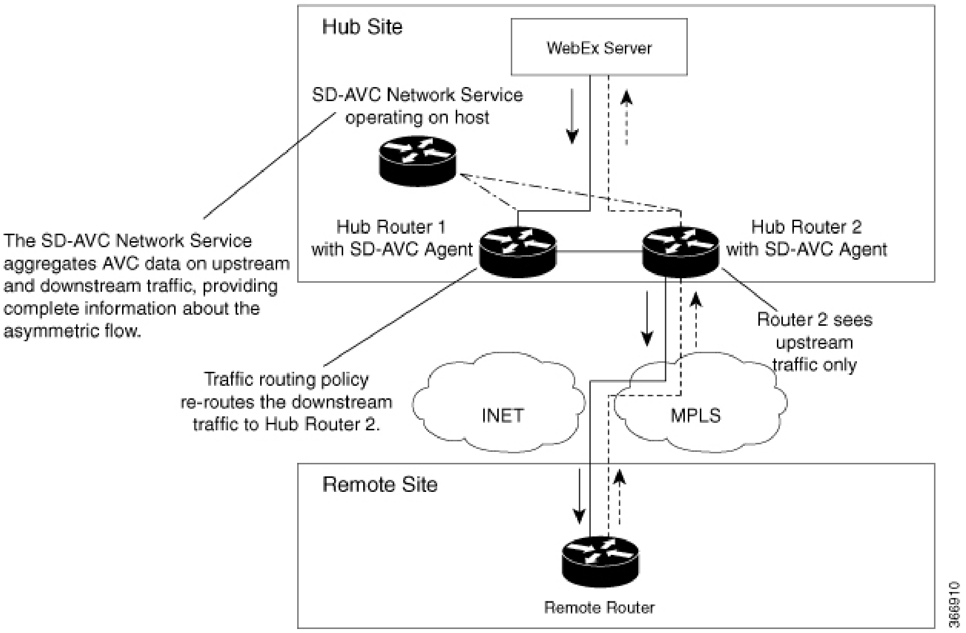

Hub Site
A single connection is routed asymmetrically through 2 hub routers.
WebEx Server
Hub Router 1
Hub Router 2
Router 1 sees downstream traffic only
Router 2 sees upstream traffic only
INET
MPLS
Remote Site
Remote Router
366883

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



Hub Site
WebEx Server
SD-AVC Network Service operating on host
The SD-AVC Network Service aggregates AVC data on upstream and downstream traffic, providing complete information about the asymmetric flow.
Hub Router 1 with SD-AVC Agent
Hub Router 2 with SD-AVC Agent
Router 2 sees upstream traffic only
Traffic routing policy re-routes the downstream traffic to Hub Router 2.
INET
MPLS
Remote Site
Remote Router
366910