Cisco SD-AVC User Guide, Release 1.1.0

First Published: 2017-10-22

Last Modified: 2017-10-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Part: Introduction

CHAPTER 1

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

Some of the current features and benefits provided by SD-AVC:

- Network-level application recognition consistent across the network
- Improved application recognition in symmetric and asymmetric routing environments
- Improved first packet recognition
- Protocol Pack update at the network level
- Secure browser-based SD-AVC Dashboard over HTTPS for monitoring SD-AVC functionality and statistics, and for configuring Protocol Pack updates network-wide

For details, see SD-AVC Features and Benefits, on page 7.

No Change to Topology

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

CHAPTER 2

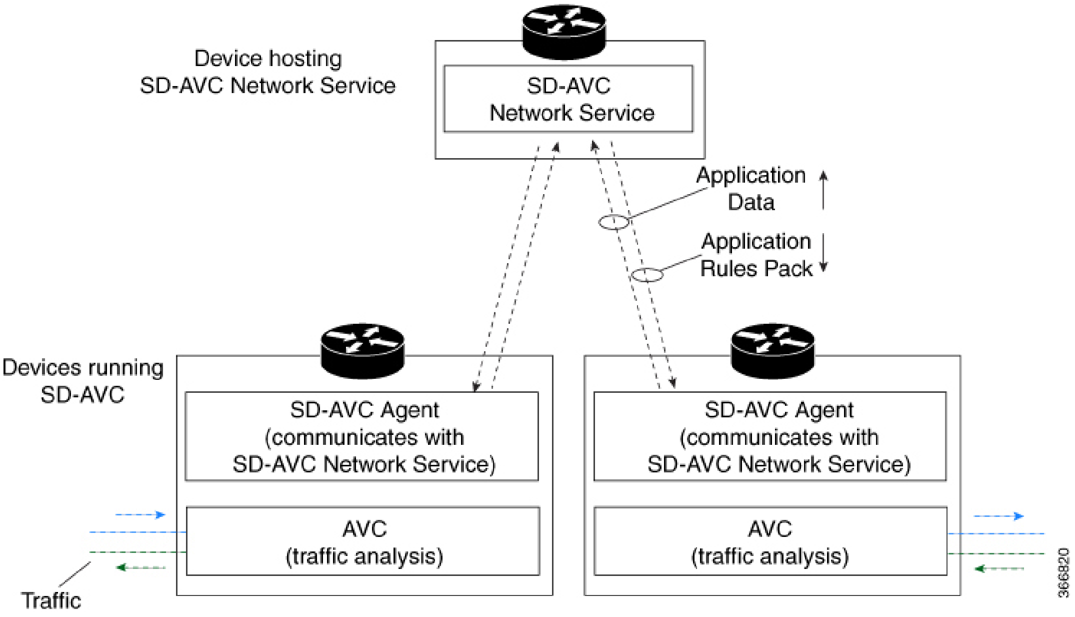
Operation

SD-AVC Architecture

SD-AVC architecture consists of two basic components:

- Centralized SD-AVC Network Service component operating on a host device
- SD-AVC Agent component running on each SD-AVC-enabled device in the network

Figure 1: SD-AVC Network Service and Agents



SD-AVC and Application Recognition

Cisco AVC can recognize 1400+ network applications, providing recognition of most enterprise network traffic. SD-AVC offers a controller-based approach that operates network-wide, aggregating application information collected across the network, and centralized deployment of Protocol Pack updates.

SD-AVC improves application recognition, and offers a solution to challenges posed by complex networks that use a variety of routing devices and routing methods. Such challenges include asymmetric routing, first packet classification, encryption, and so on.

Collecting Application Data

Devices in the network running AVC analyze traffic and generate application data. If a device is connected to SD-AVC, the SD-AVC agent operating on the device receives this application data, and processes and caches the data. Periodically, the SD-AVC agent sends the latest application data to the centralized SD-AVC network service.

As new servers are detected or as server addresses change, the agent continually discovers and validates these servers and updates the SD-AVC network service with the new information. The process of discovery and validation can take several minutes.

Server addresses usually remain constant over time, but when they do change, the SD-AVC agent detects the changes and updates the network service.

Aggregating Application Data

The SD-AVC network service aggregates application data from multiple sources, producing an application rules pack from the composite data. This is made available to network devices using SD-AVC.

Periodically, the network devices using SD-AVC request the application rules pack. Relying on devices to pull (request) the application rules pack on their own schedule improves efficiency and simplifies administration.

The application rules pack contains the following type of information: ID, IP address, port, network protocol, VRF name, application name, and so on.

Example:

```
ID   | IP Address | Port | Protocol | VRF-name | App-Name
=================================================================
0    | 192.0.2.1  | 5901 | TCP      | Mgt      | VNC
```

CHAPTER 3

SD-AVC Features and Benefits

SD-AVC Features and Benefits

The following table describes several SD-AVC features and benefits.

Table 1: 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.
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, on page 6.
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

Feature/Benefit	Description
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 Pack Update Page, on page 37.
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, on page 33

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

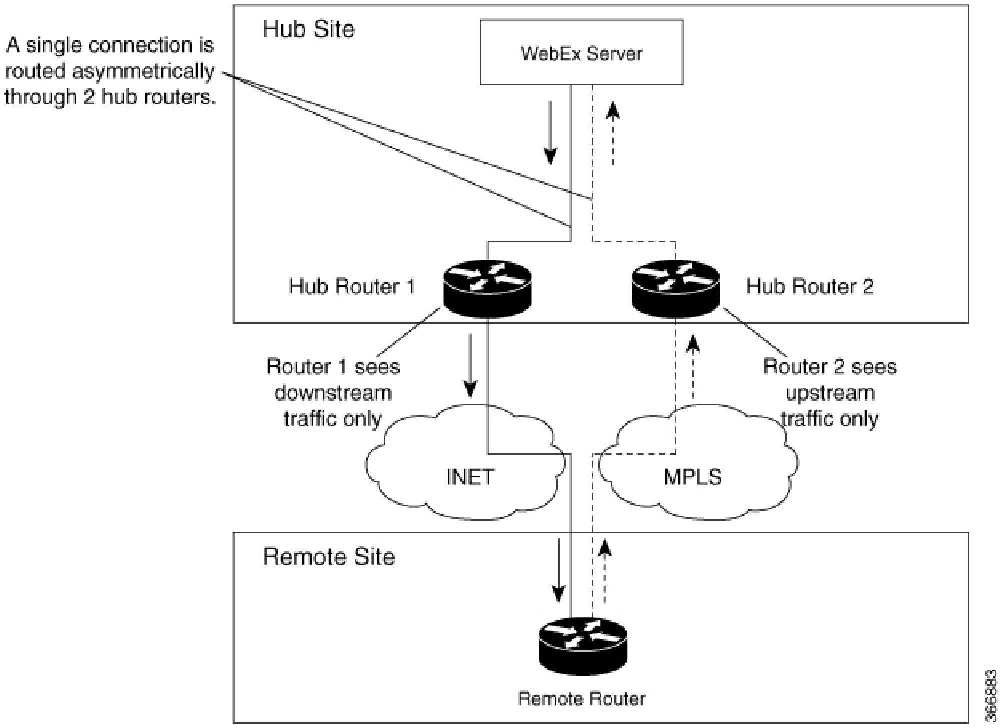
AVC deep packet inspection (DPI) operates best when it sees both directions of traffic. In symmetric routing, AVC operating on a single device that handles both directions of a flow can fully analyze metadata and other traffic attributes to help identify the application creating the flow. By contrast, 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 2: Asymmetric Routing Example

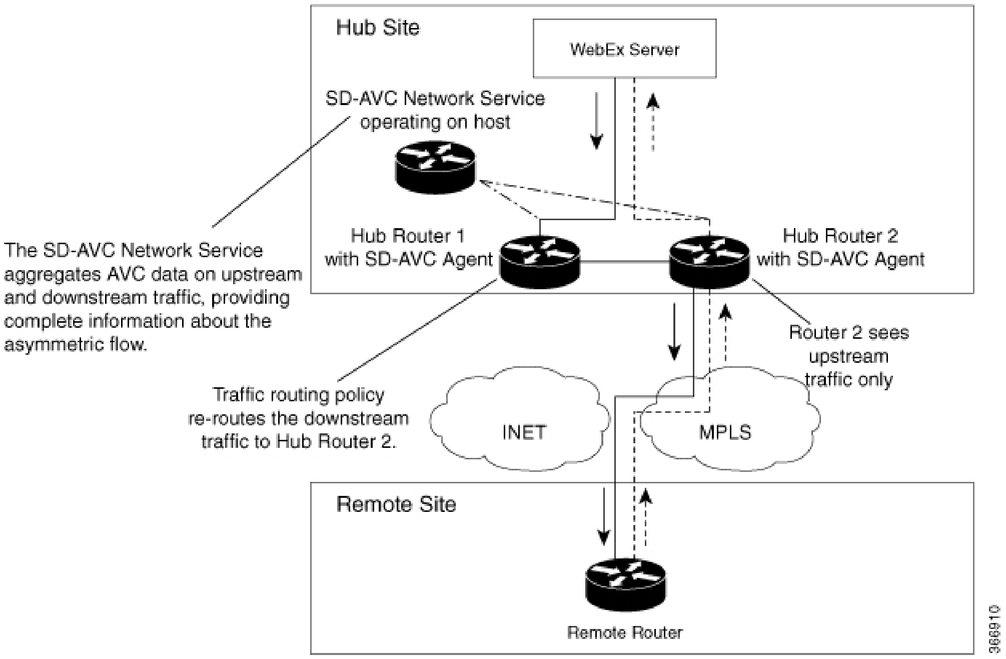

A single connection is routed asymmetrically through 2 hub routers.
Hub Site
WebEx Server
Hub Router 1
Hub Router 2
Router 1 sees downstream traffic only
Router 2 sees upstream traffic only
INET
MPLS
Remote Site
Remote Router
366883

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 3: 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

PART II

Part: Deployment

CHAPTER 4

Installing or Upgrading the SD-AVC Network Service

Installation Overview

SD-AVC operates in a service/agent configuration. For details, see SD-AVC Architecture, on page 5.

- **Network Service**: The SD-AVC Network Service is installed as a virtualized component on a Cisco device service container, and operates on the device as a service. See: System Requirements: SD-AVC Network Service Host, on page 14
- **Agent**: Other devices in the network are enabled as agents, and communicate with the SD-AVC Network Service. See: Configuring Network Devices to Use SD-AVC, on page 25
- **High Availability**: SD-AVC supports a high availability (HA) configuration, using more than one SD-AVC Network Service. See: SD-AVC High Availability, on page 29
- **Connectivity**: Operating SD-AVC requires connectivity between the SD-AVC Network Service and the SD-AVC agents that operate on devices in the network. See: Configuring Connectivity, on page 15

Summary of Setup

The following table briefly describes the steps to set up SD-AVC:

Table 2: Setup

	Setup Task	Section
1	Download the open virtual appliance (OVA) file for the SD-AVC Network Service, and install it on a host device accessible by other devices in the network.	See: Installing the SD-AVC Network Service, on page 16
2	Enable the SD-AVC agent on Cisco devices in the network, pointing them to the SD-AVC Network Service set up in the previous step. (In a high availability setup, include more than one SD-AVC Network Service instance.)	See: Configuring Network Devices, on page 25
3	Configure connectivity, or optionally, secure connectivity.	See: Configuring Connectivity, on page 15, Configuring Secure Connectivity, on page 47

System Requirements: SD-AVC Network Service Host

The following table describes platform requirements for hosting the SD-AVC Network Service.

Table 3: SD-AVC Network Service Host Requirements

Host	Memory	Storage	OS	CPU
Cisco ASR1001-X	M-ASR1001X-16GB	NIM-SSD and SSD-SATA-400G	Cisco IOS XE Everest 16.6.1 or later	—
Cisco ASR1002-X	M-ASR1002X-16GB	MASR1002X-HD-320G	Cisco IOS XE Everest 16.6.1 or later	—
Cisco ISR4431	RAM: MEM-4400-4GU16G Flash: MEM-FLASH-16G	NIM-SSD and SSD-MSATA-400G	Cisco IOS XE Everest 16.6.1 or later	—
Cisco ISR4451	RAM: MEM-4400-4GU16G Flash: MEM-FLASH-16G	NIM-SSD and SSD-MSATA-400G	Cisco IOS XE Everest 16.6.1 or later	—
Cisco Cloud Services Router CSR1000V	Minimum: 8 GB Recommended: 8 GB	20 GB	Cisco IOS XE Everest 16.6.1 or later	4 cores

Configuring Connectivity

Operating SD-AVC requires connectivity between various components.

- SD-AVC network service and host
- SD-AVC network service and agents
- Connectivity to the SD-AVC Dashboard

This section describes the connectivity requirements. If secure connectivity is required, see: Configuring Secure Connectivity, on page 47

SD-AVC Network Service and Host

Connectivity is required between the SD-AVC network service, which operates as a virtualized service, and the device hosting it. The host platform requires connectivity with the service through a virtual interface called VirtualPortGroup. The virtual service communicates with the host over this virtual interface, using SSH on TCP port 22.

SD-AVC Network Service and Agents

Network devices operating with SD-AVC use an SD-AVC agent, which operates in the background on the device, to communicate with the central SD-AVC network service. Connectivity is required between each of these network devices and the SD-AVC network service (more than one network service in SD-AVC high availability configurations).

- **Ports**

  Communication between agent and service uses the following protocols and ports:

  - **UDP**: Port 50000
  - **TCP**: Ports 20, 21, 50000-60000

- **Firewalls and Access Lists**

  Ensure that communication is possible in both directions (agent to SD-AVC Network Service, SD-AVC Network Service to agent) on these ports for the relevant traffic. For example:

  - Firewall policy must enable communication in both directions.
  - If a network device has an access control list (ACL) configured, the ACL must permit communication between the SD-AVC Network Service and SD-AVC agents.

Connectivity to the SD-AVC Dashboard

Connecting to the SD-AVC Dashboard (see Using SD-AVC, on page 33) requires access to the device hosting the SD-AVC Network Service, and involves TCP traffic through port 8443. Ensure that network policy (firewall, ACL, and so on) permits this connectivity for devices requiring access to the SD-AVC Dashboard.

Using SD-AVC with Cisco IWAN

When operating SD-AVC in a Cisco IWAN environment, the SD-AVC Network Service may be hosted on the hub master controller (MC) or on a router dedicated for the purpose of hosting the service.

In either case, verify that the host device meets the system requirements for hosting the SD-AVC Network Service (see System Requirements: SD-AVC Network Service Host, on page 14). For information about installing the SD-AVC Network Service, see Installing the SD-AVC Network Service, on page 16.

Installing the SD-AVC Network Service

The SD-AVC Network Service operates as a virtualized service on a Cisco router. It is installed as an open virtual appliance (OVA) virtual machine container, and requires a few steps of configuration on the host router. After configuration is complete, you can check service status using the browser-based SD-AVC Dashboard.

Table 4: Overview of Installation Steps

Task	Steps
System requirements	Step 1
Installation	Steps 2 to 4
Configuration	Step 5
Activation	Step 6
Verification	Steps 7 to 10
Connecting to SD-AVC Dashboard	Step 11

Examples follow the steps below.

Installation Procedure

The following procedure installs the SD-AVC Network Service as a virtualized service on a Cisco router.

1. Verify that the intended host device meets the system requirements. See System Requirements: SD-AVC Network Service Host, on page 14.

2. Download the OVA container for the SD-AVC Network Service from Cisco.com, using the Download Software tool. Specify a platform that supports hosting the SD-AVC virtual service, then navigate to software downloads for the platform. Select the "SD AVC Router Virtual Service" option to display available OVA files for SD-AVC.

   Example filename: iosxe-sd-avc.1.1.0.ova

3. Copy the downloaded OVA file onto the device that will host the SD-AVC Network Service. Copy to one of the following locations, depending on the platform type:

- CSR1000V: bootflash
- ASR1000 Series or ISR4000 Series: harddisk

  harddisk refers to the SSD or HD specified in the system requirements for the platform (System Requirements: SD-AVC Network Service Host, on page 14).

4 On the host device, execute the following command to extract the OVA package and install the SD-AVC Network Service. By default, it is installed on the same storage device where the OVA package was saved.

service sd-avc install package *disk-with-OVA*:*OVA-filename* **media** *location-for-OVA-expansion*

Table 5: Command Details

CLI keyword/argument	Description
disk-with-OVA	Specify one of the following, according to the platform type. The location refers to where the OVA was saved in a previous step. • CSR: bootflash • ASR1000 Series or ISR4000 Series: harddisk
OVA-filename	Downloaded OVA file.
location-for-OVA-expansion	Specify one of the following, according to the platform type: • CSR: bootflash • ASR1000 Series or ISR4000 Series: harddisk **Note** On ASR1000 and ISR4000 platforms, the CLI may allow you to incorrectly specify the bootflash for the *disk-with-OVA*, but for these platforms, specifying the bootflash as the location will cause this step to fail. On these platforms, specify only the hard disk for *disk-with-OVA* location.

Examples:

- For CSR1000V router:

```
service sd-avc install package bootflash:iosxe-sd-avc.1.1.0.ova media bootflash
```

- For ASR1000 Series or ISR4000 Series routers:

```
service sd-avc install package harddisk:iosxe-sd-avc.1.1.0.ova media harddisk
```

5 Configure the SD-AVC Network Service.

- Specify the router gateway interface that the virtualized service uses for external access.
- Specify a user-selected external-facing service IP address for the SD-AVC Network Service. This address must be within the same subnet as the gateway interface address.

This step accomplishes the following:

- Enables routers in the network to communicate with the SD-AVC Network Service.
- Enables access to the browser-based SD-AVC Dashboard.

Note Use this command only in scenarios in which the gateway interface is not attached to a VRF. If the gateway interface is attached to a VRF, use the steps described in Operating the SD-AVC Network Service with Host Interface Attached to a VRF, on page 45.

service sd-avc configure gateway interface *interface* **service-ip** *service-ip-address* [**activate** | **preview**]

Table 6: Command Details

CLI keyword/argument	Description
activate	Activates the service immediately. It is not typically recommended to use this option during this configuration step. Execute the `activate` option in a separate step, as shown below.

preview	Preview the configuration without configuring or activating the service. When using this option, the configuration is not sent to the device.
	Note: If the gateway interface is attached to a VRF, see Operating the SD-AVC Network Service with Host Interface Attached to a VRF, on page 45.
	Example output:
	`! Virtual port configuration`
	`interface VirtualPortGroup31`
	`  description automatically created for sd-avc service by 'service sd-avc configure' exec command`
	`  ip unnumbered gigabitEthernet1`
	`end`
	
	`! Virtual service configuration`
	`virtual-service SDAVC`
	`  description automatically created for sd-avc service by 'service sd-avc configure' exec command`
	`  vnic gateway VirtualPortGroup31`
	`    guest ip address 10.56.196.101`
	`  exit`
	`end`
	
	`! Static route configuration`
	`ip route  10.56.196.101 255.255.255.255 VirtualPortGroup31`

interface	Gateway interface: The device interface that the virtualized service uses for external access. **Note**: If the interface is attached to a VRF, see Operating the SD-AVC Network Service with Host Interface Attached to a VRF, on page 45 for instructions for configuring the gateway.

CLI keyword/argument	Description
service-ip-address	External-facing IP address, must be in the same subnet as the IP of the gateway interface. **Example**: Gateway interface: 10.56.196.100 service-ip-address: 10.56.196.101

Example:

```
service sd-avc configure gateway interface gigabitEthernet1 service-ip 10.56.196.146
```

6 Activate the service.

service sd-avc activate

Example:

```
service sd-avc activate
```

7 Verify that the status of the SD-AVC Network Service is activated.

service sd-avc status

If installation and activation were successful, the displayed status is:

```
SDAVC service is installed, configured and activated
```

8 Save the new configuration.

copy running-config startup-config

9 Ping the service IP configured in a previous step to verify that it is reachable.

10 Verify that SSH is enabled on the host device. Details vary according to different scenarios, but the following is a helpful reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html

Example (uses SSH local authentication):

```
aaa new-model
!
aaa authentication login default local
username cisco privilege 15 password cisco
ip domain name cisco.com
crypto key generate rsa
```

11 Wait several minutes for the service to become fully active, then use a Chrome browser to access the browser-based SD-AVC Dashboard, at the following URL, which uses the service-ip configured in an earlier step and port 8443. The SD-AVC Dashboard uses the same authentication as the platform hosting the SD-AVC Network Service.

https://<service-ip>:8443

Note Accessing the SD-AVC Dashboard requires connectivity from the PC you are using to access the SD-AVC interface.

Installation Example for CSR1000V Router

The following is an example of the CLI steps used to install the SD-AVC Network Service on a Cisco CSR1000V Cloud Services Router. For this router, the first step includes “bootflash” as the location for extracting the OVA.

```
service sd-avc install package harddisk:iosxe-sd-avc.1.1.0.ova media bootflash
service sd-avc configure gateway interface gigabitEthernet1 service-ip 10.56.196.146
service sd-avc activate
service sd-avc status
copy running-config startup-config
```

Installation Example for ASR1000 Series or ISR4000 Series Routers

The following is an example of the CLI steps used to install the SD-AVC Network Service on a Cisco ASR1000 Series or ISR4000 Series Router. For these routers, the first step includes “harddisk” as the location for extracting the OVA.

```
service sd-avc install package harddisk:iosxe-sd-avc.1.1.0.ova media harddisk
service sd-avc configure gateway interface gigabitEthernet1 service-ip 10.56.196.146
service sd-avc activate
service sd-avc status
copy running-config startup-config
```

Upgrading the SD-AVC Network Service

Use the following procedure to upgrade the SD-AVC Network Service on the router hosting the service.

1. Deactivate the service. This step stops the service but does not erase the database of compiled application data.

   service sd-avc deactivate

2. Verify that the service has been deactivated.

   service sd-avc status

   The following output confirms that the service has been deactivated:

   ```
   Service SDAVC is installed, configured and deactivated
   ```

3. On the host router, execute the following command to extract and install the OVA package. By default, it is installed on the same storage device where the OVA package is stored.

   service sd-avc upgrade package *disk-with-OVA*:*OVA-filename* **media** *location-for-OVA-expansion*

   Table 7: Command Details

CLI keyword/argument	Description
disk-with-OVA	Specify one of the following, according to the platform type. The location refers to where the OVA was stored in a previous step. • CSR: bootflash • ASR1000 Series or ISR4000 Series: harddisk
OVA-filename	Downloaded OVA file.

CLI keyword/argument	Description
location-for-OVA-expansion	Specify one of the following, according to the platform type: • CSR: bootflash • ASR1000 Series or ISR4000 Series: harddisk **Note** On ASR1000 and ISR4000 platforms, the CLI may allow you to specify the bootflash for the *disk-with-OVA*, but on these platforms, specifying the bootflash as the location will cause this step to fail. On these platforms, specify only the hard disk for *disk-with-OVA* location.

Examples:

- For Cisco CSR1000V router:

  ```
  service sd-avc upgrade package bootflash:iosxe-sd-avc.1.1.0.ova media bootflash
  ```

- For Cisco ASR1000 Series or ISR4000 Series routers:

  ```
  service sd-avc upgrade package harddisk:iosxe-sd-avc.1.1.0.ova media harddisk
  ```

4 (Optional) During the upgrade process, view the service status.

service sd-avc status

During the upgrade, the following output indicates that the service is being installed:

```
Service SDAVC is installing..., configured and deactivated
```

The following output indicates that the upgrade is complete:

```
Service SDAVC is installed, configured and deactivated
```

5 Activate the service.

service sd-avc activate

Example:

```
service sd-avc activate
```

6 Verify that the status of the SD-AVC Network Service is activated.

service sd-avc status

If upgrade and activation were successful, the displayed status is:

```
SDAVC service is installed, configured and activated
```

CHAPTER 5

Unconfiguring or Uninstalling the SD-AVC Network Service

Unconfiguring the SD-AVC Network Service

Use the following procedure to unconfigure the SD-AVC Network Service on the router hosting the service. Unconfiguring the service is necessary before changing the SD-AVC Network Service configuration.

1 Deactivate the service. This step stops the service but does not erase the database of compiled application data.

  service sd-avc deactivate

2 Verify that the service has been deactivated.

  service sd-avc status

  The following output confirms that the service has been deactivated:

```
Service SDAVC is installed, configured and deactivated
```

3 Unconfigure the service.

  service sd-avc unconfigure

4 Verify that the service has been unconfigured.

  service sd-avc status

  The following output confirms that the service has been unconfigured:

```
Service SDAVC is installed, not configured and deactivated
```

Uninstalling the SD-AVC Network Service

Use the following procedure to uninstall the SD-AVC Network Service on the router hosting the service.

1 Deactivate and unconfigure the SD-AVC Network Service. Follow the full procedure in: Unconfiguring the SD-AVC Network Service, on page 23

2 Uninstall the service. This step deletes all information from the SD-AVC database for this SD-AVC Network Service.

service sd-avc uninstall

3 Verify that the service has been uninstalled.

service sd-avc status

The following output confirms that the service has been uninstalled:

```
Service SDAVC is uninstalled, not configured and deactivated
```

CHAPTER 6

Configuring Network Devices

Configuring Network Devices to Use SD-AVC

After the SD-AVC Network Service has been set up, use the information in this section to check the prerequisites for Cisco devices in the network to operate with the SD-AVC Network Service. Then activate and configure SD-AVC on the devices. This activates an SD-AVC agent that operates on the devices to communicate with the SD-AVC Network Service.

After configuration is complete, verify the status of each device using the SD-AVC Dashboard. The SD-AVC Dashboard is a tool provided by the SD-AVC Network Service, and displays the details of participating devices, among other things (see Using SD-AVC, on page 33).

For High Availability SD-AVC, which employs more than one SD-AVC Network Service, see SD-AVC High Availability, on page 29.

System Requirements: Network Devices Using SD-AVC

The following table describes the supported platforms and requirements for network devices to operate with SD-AVC. When operating with SD-AVC, network devices run the SD-AVC agent, which manages communication between the devices and the SD-AVC Network Service.

Table 8: Network Device Requirements

Platform	OS
Cisco ASR1001-X	Cisco IOS XE Everest 16.6.1 or later
Cisco ASR1002-X	Cisco IOS XE Everest 16.6.1 or later

Platform	OS
Cisco ASR1001-HX	Cisco IOS XE Everest 16.6.1 or later
Cisco ASR1002-HX	Cisco IOS XE Everest 16.6.1 or later
Cisco ISR4000 Series: 4451, 4321, 4431	Cisco IOS XE Everest 16.6.1 or later
Cisco Cloud Services Router CSR1000V	Cisco IOS XE Everest 16.6.1 or later
Cisco Route Processor RP2, operating on Cisco ASR1004, ASR1006, or ASR1013	Cisco IOS XE Everest 16.6.1 or later
Cisco Route Processor RP3, operating on Cisco ASR1004, ASR1006, or ASR1013	Cisco IOS XE Everest 16.6.1 or later

Connectivity

For connectivity requirements and procedures, see Configuring Connectivity, on page 15.

Configuration Prerequisites: Network Devices Using SD-AVC

Network devices participating with SD-AVC run an SD-AVC agent (see SD-AVC Architecture, on page 5).

SD-AVC functionality depends on receiving application statistics from each participating network device. Application statistics are collected on each interface (on participating devices) on which one of the following is enabled: Cisco Performance Monitor, Easy Performance Monitor (ezPM), PfR policy, or Protocol Discovery

Depending on the Cisco solution in place, application statistics must be collected as follows:

- **IWAN solution**: (No additional user configuration required) Collection of application statistics is enabled by the use of Easy Performance Monitor (ezPM) and PfR policy.
- **Application Assurance solution**: (No additional user configuration required) Collection of application statistics is enabled by the use of Performance Monitor or Easy Performance Monitor (ezPM), and PfR policy.
- **EasyQoS**: (Requires user configuration) Configure Protocol Discovery on WAN-side interfaces.

Activating the SD-AVC Agent

Use the following procedure on a device in the network to activate the SD-AVC agent, enabling the device to communicate with the SD-AVC Network Service.

Note See System Requirements for network devices operating with SD-AVC .

Note The term, SD-AVC Network Service, refers to the virtual service that operates on a host device and performs SD-AVC functions, such as aggregating application data. The **avc sd-service** command used in this procedure does not refer to the SD-AVC Network Service.

1 Activate SD-AVC.

avc sd-service
Example:

```
conft#avc sd-service
```

2 Configure the segment (group of devices that share the same purpose, such as routers within the same hub).

segment cisco
Example:

```
(config-sd-service)#segment cisco
```

3 Enter controller mode to configure the agent to use the SD-AVC Network Service (not related to the **avc sd-service** command used in an earlier step).

controller
Example:

```
(config-sd-service)#controller
```

4 Enter the service-IP used when the SD-AVC Network Service (running on a host device) was set up.

address *service-ip*

Note For a high availability (HA) configuration, more than one SD-AVC Network Service is specified in this step. See SD-AVC High Availability, on page 29 for details.

Example:

```
(config-sd-service-controller)#address 10.56.196.146
```

5 Configure VRF.

vrf vrf_mgmt
Example:

```
(config-sd-service-controller)#vrf vrf_mgmt
```

The device is now configured to operate with SD-AVC, and begins:

- Sending collected application data to the SD-AVC Network Service
- Receiving application rules packs periodically from the SD-AVC Network Service

6 Using the SD-AVC Dashboard, in the Connectivity tab, confirm that the router appears in the hostname list, and that the “Exporter Health” column shows a green checkmark.

Note If the tabs are hidden, click the menu button ☰ to display them.

Configuration Example

The following is an example of the CLI steps used to configure the SD-AVC agent on a device.

```
conft#avc sd-service
(config-sd-service)#segment cisco
(config-sd-service)#controller
(config-sd-service-controller)#address 10.56.196.146
(config-sd-service-controller)#vrf vrf_mgmt
```

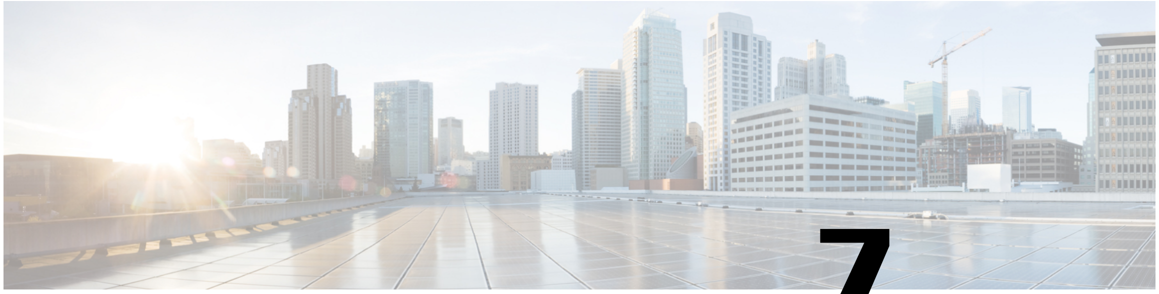
Deactivating the SD-AVC Agent

Use the following procedure on a device in the network to deactivate the SD-AVC agent and clear any SD-AVC agent configuration details that have been entered. This stops SD-AVC functionality on the device, and the device stops communicating with the SD-AVC network service.

1 Deactivate SD-AVC and remove SD-AVC agent configuration.

no avc sd-service
Example:

```
conft#no avc sd-service
```



CHAPTER 7

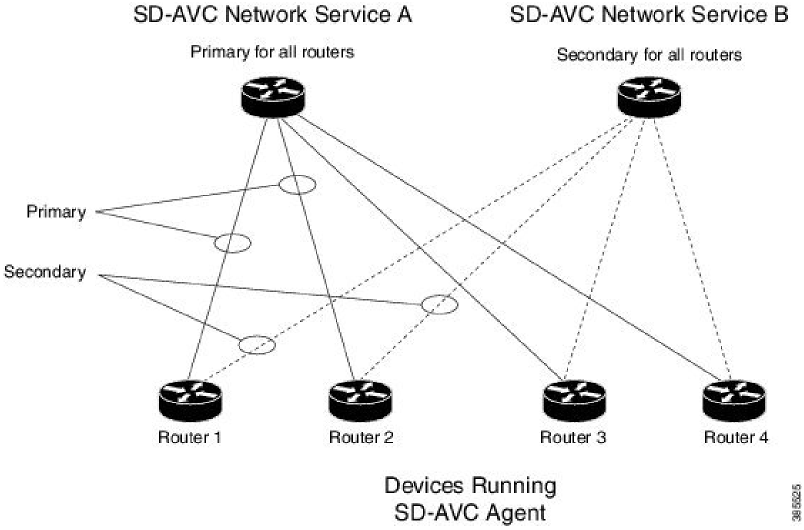
SD-AVC High Availability

SD-AVC supports a high availability (HA) configuration, using more than one SD-AVC network service. Each network device operating with SD-AVC, and consequently running the SD-AVC agent, designates a primary and secondary SD-AVC network service. If the primary SD-AVC network service becomes unavailable, the device fails over to the secondary service.

In the event of failover, the secondary SD-AVC network service receives the application data (state) maintained by the SD-AVC agents on participating network devices. This provides SD-AVC a degree of resilience, enabling the secondary network service to receive previously aggregated data and resume operation where the primary network service left off. In addition, because each SD-AVC agent maintains its state locally, classification of traffic on each device continues seamlessly during the failover from primary to secondary network service.

For all devices in the network that are operating with SD-AVC, it is recommended to use the same primary SD-AVC network service.

Figure 4: Primary and Secondary SD-AVC Network Services in High Availability Configuration



SD-AVC Network Services Collect Application Data Separately

Each SD-AVC network service collects application data from the devices that are using it as their active service. Multiple SD-AVC network services do not share application data with each other directly. So if the primary service becomes unavailable, the agents that were using it fail over to the secondary service, and that service begins collecting application data from the agents.

- Configuring High Availability SD-AVC, page 30

Configuring High Availability SD-AVC

Setting up SD-AVC in a high availability configuration requires two steps that differ from a non-HA configuration.

1. Set up more than one SD-AVC Network Service. For information about setting up an SD-AVC Network Service, see Installation Overview, on page 13.

2. When configuring a device to use SD-AVC, specify primary and secondary SD-AVC Network Services with the **address** command. In other respects, configuring the device is identical to a non-HA configuration. For information about setting up a device, see Configuring Network Devices to Use SD-AVC, on page 25. The configuration commands are shown below.

```
avc sd-service
segment cisco
controller
address primary-network-service-ip secondary-network-service-ip
vrf vrf_mgmt
```

Example:

```
conft#avc sd-service
(config-sd-service)#segment cisco
(config-sd-service)#controller
(config-sd-service-controller)#address 10.56.196.146 10.56.196.150
(config-sd-service-controller)#vrf vrf_mgmt
```

PART III

Part: Usage

CHAPTER 8

Using SD-AVC

Using SD-AVC

Use the SD-AVC Dashboard to monitor and control SD-AVC functionality and statistics, and to configure Protocol Pack updates. Specifically, the Dashboard:

- Provides information about devices operating with SD-AVC
- Provides detailed traffic analytics
- Enables setting up Protocol Pack deployment

Connecting

Using a Chrome browser with access to the device hosting the SD-AVC Network Service, open the SD-AVC Dashboard. The Dashboard is accessible using the service IP configured when setting up the SD-AVC Network Service, and port 8443, in the format:

https://<service-ip>:8443

Example:

```
https://10.56.196.153:8443
```

Note The SD-AVC Dashboard uses the same authentication as the platform hosting the SD-AVC Network Service. The host platform may use locally configured usernames and passwords, or it may use other methods, such as an Authentication, Authorization, and Accounting (AAA) server.

If prompted, enter the username and password used on the host platform.

Connectivity Page

The Connectivity page lists the devices in the network that are operating with the SD-AVC Network Service, and indicates the connectivity and health status for each device.

Table 9: User Controls

Control	Description
Menu button ☰	Display web interface tabs.
Search field	Enter a string in the Search field to filter the display of devices.
Home button ⌂	Open the main dashboard page.
Refresh button ⟳	Refresh display.
Time button 🕒	Display system time.

Table 10: Information Provided in the SD-AVC Connectivity Page

Field	Description
Hostname	Device hostname
IP	Device IP
Segment	Network segment: A group of devices that share the same purpose, such as routers within the same hub.

Field	Description
Connectivity	Device connectivity with the SD-AVC Network Service. Connectivity messages are sent over UDP port 50000. • **Green** checkmark: All connectivity messages are being received. • **Orange** caution: Some connectivity messages have not been received. SD-AVC will monitor the device for restoration of connectivity. Wait a few minutes for the issue to resolve or escalate to red X. • **Red** X: No messages are being received. **Troubleshooting**: • Check connectivity on UDP port 50000. If no problem is found with connectivity, contact Cisco TAC.
Update Health	Status of updates from the SD-AVC Network Service to the device. Updates include application and configuration data, and are made by standard FTP connection. • **Green** checkmark: The device has successfully accessed the SD-AVC Network Service and has installed any application data updates. • **Orange** caution: Some messages are being received; some are missing. Wait a few minutes for the issue to resolve or escalate to red X. • **Red** X: One of the following may have occurred: (a) No messages are being received. (b) The device has failed to install an application data update from the SD-AVC Network Service. **Troubleshooting**: • Verfiy FTP connectivity on ports 20, 21. • On the device, execute **show tech-support nbar platform** to display NBAR data useful for troubleshooting. Save the output for use by TAC if the problem persists.
Exporter Health	Status of device data export to the SD-AVC Network Service. • **Green** checkmark: All messages are being received. • **Orange** caution: Some messages are being received; some are missing. Wait a few minutes for the issue to resolve or escalate to red X. • **Red** X: No messages are being received. **Troubleshooting**: • Check FTP connectivity on UDP port 50000. If no problem is found with connectivity, contact Cisco TAC.

Field	Description
Traffic Health	Traffic health status in the network – indicates whether the device is processing traffic. • **Green** checkmark: The NBAR2 component on the device is processing traffic. **Requires**: ◦ Connectivity between the SD-AVC Network Service and device ◦ NBAR2 is enabled. ◦ Device is processing traffic. • **Orange** caution: The SD-AVC Network Service has not received some expected application data from the device. Wait a few minutes for the issue to resolve or escalate to red X. • **Red** X: No application data is being received. **Possible causes**: ◦ Connection error. ◦ NBAR is not enabled. ◦ The device is not processing traffic. **Troubleshooting**: • Check FTP connectivity on UDP port 50000. If no problem is found with connectivity, contact Cisco TAC.
Classification Score	Last measured classification quality score for the device. This indicates the degree of classification quality (specificity), calculated according to traffic volume. Higher score indicates better quality.
Asymmetric Index	Last measured degree of asymmetry seen by device. This is the ratio of asymmetric flows to total flows for TCP and DNS traffic. 0 is least asymmetry, and 10 is highest asymmetry.

Application Visibility Page

The Application Visibility page provides high-level information regarding the classification score of devices, and applications providing network traffic. Use the controls at the top to clear the statistics, filter by device, or select a time period (hours). The metrics and graphs displayed on the page are an average over the span of time indicated by the selected period.

Table 11: Application Visibility page

Metric	Description
Classification (over time) score	Degree of classification quality (specificity), calculated according to traffic volume.
First Packet classification ratio	Ratio of flows classified on the first packet, to total TCP/UDP flows.
SD-AVC Coverage Ratio	Ratio of flows covered by the SD-AVC application rules pack, to the total number of TCP/UDP flows.
Business Relevancy chart	Traffic business relevance, over the period selected in the Period menu.

Application Rules Page

The Application Rules page lists application data compiled by SD-AVC, organized into rules ready for export to participating devices in the network. The information is sent when the devices request an Application Rules Pack from the SD-AVC Network Service.

Asymmetric Sockets Page

The Asymmetric Sockets page lists the asymmetric flows currently being tracked by SD-AVC. In networks that do not employ asymmetric routing, the list may be empty.

Protocol Pack Update Page

The Protocol Pack Update page enables deploying Protocol Packs to devices in the network that are are using SD-AVC. The page contains tabs for loading and scheduling deployment of Protocol Pack files, and checking status.

Understanding Protocol Pack Files

Cisco releases Protocol Packs on an ongoing basis. Each Protocol Pack release provides updates that expand and improve AVC application recognition. Typically, it is recommended to use the latest Protocol Pack compatible with the OS running on a device. The Protocol Library page indicates the latest Protocol Pack and provides compatibility information.

Protocol Packs are available using the Cisco Download Software tool. When using the tool, specify a platform and then navigate to software downloads for the platform.

Protocol Pack filenames have the following format:

pp-adv-<platform-type>-<OS>-<engine-id>-<protocol-pack-version>.pack

Platform type may be, for example, asr1k, csr1000v, or isr4000. However, a Protocol Pack may be installed on any compatible device, even if that device is not indicated by the filename.

How SD-AVC Determines which Devices are Compatible with a Protocol Pack

The SD-AVC network service contains a Protocol Pack repository that stores specific Protocol Packs uploaded to the repository for deployment to devices in the network. The SD-AVC network service deploys a Protocol Pack in the repository to all compatible devices, at the time scheduled.

To determine compatibility, the SD-AVC network service compares the IOS version and engine ID of a Protocol Pack in the repository to the IOS version and engine running on devices in the network. If a Protocol Pack in the repository is compatible with a device, then the SD-AVC network service deploys the Protocol Pack from the repository to the device.

Deploying Protocol Packs Using SD-AVC

Use the SD-AVC network service to deploy Protocol Packs to devices operating with the service, as follows:

1. Determine the Protocol Pack to deploy. The Protocol Library page provides compatibility information.
2. Download the Protocol Pack using the Cisco Download Software tool. In the filename of the downloaded Protocol Pack, note the engine ID.
3. In the SD-AVC Dashboard, use the Protocol Pack Update page to upload the Protocol Pack file into the Protocol Pack repository on the SD-AVC network service. SD-AVC determines which devices are compatible with the Protocol Packs in the repository.
4. On the Protocol Pack Update page, open the Deployment Status tab. The SD-AVC network service indicates the Protocol Packs ready for deployment to compatible devices.
5. On the Protocol Pack Update page, open the Deploy tab and schedule a time for deployment. At the specified time, the SD-AVC network service deploys the Protocol Pack to any compatible devices. If no time is scheduled, and if the Immediate option is not selected, then Protocol Pack deployment does not occur.

Protocol Pack Repository Tab

The Protocol Pack Repository is a collection of Protocol Pack files stored with the SD-AVC Network Service, for deployment to devices managed by the SD-AVC Network Service. The Protocol Pack Repository tab:

- Displays Protocol Pack files in the repository.
- Enables loading Protocol Pack files into the repository.
- Enables removal of Protocol Pack files from the repository.

Table 12: Information in the Protocol Pack Repository Tab

Column	Description
Name	Protocol Pack filename.
Engine-ID	The engine ID is determined by the version of Cisco IOS XE. Protocol Pack files are compatible with specific engine ID versions.

Column	Description
Latest	A **green** checkmark in this column indicates that the Protocol Pack file is ready for deployment. To downgrade from a later Protocol Pack to an earlier Protocol Pack (for example 31.0.0 to 30.0.0), delete the later Protocol Pack from the repository, upload the earlier version (30.0.0), and then deploy. SD-AVC deploys the Protocol Pack to all compatible devices managed by the SD-AVC Network Service.
Action	Enables deleting a Protocol Pack file from the repository.

Deploy Tab

The Deploy tab enables scheduling a deployment time or selecting Immediate for immediate deployment.

If no time is scheduled, the SD-AVC Network Service does not deploy any Protocol Packs.

Deployment Status Tab

The Deployment Status tab displays information about each device managed by the SD-AVC Network Service, as described in the following table. It indicates the current Protocol Pack, and any compatible Protocol Pack in the repository, if there is one.

If a Protocol Pack file is listed in the Candidate column, and if it differs from the Active Protocol Pack, then the Candidate Protocol Pack will be deployed at the scheduled deployment time.

Table 13: Information in the Deployment Status Tab

Column	Description
Hostname	Device hostname.
IP	Device IP.
Segment	Network segment: A group of devices that share the same purpose, such as routers within the same hub.
Active Pack	Protocol Pack currently installed on the device.
Candidate	A compatible Protocol Pack in the repository. **Note**: The latest Protocol Pack file in the repository compatible with the device may be an older Protocol Pack version, especially if the repository has not been kept up to date.

Column	Description
Current Status	**Green**: The active Protocol Pack and the candidate are the same, so no Protocol Pack will be deployed to the device. **Yellow/Orange**: The candidate Protocol Pack is different from the active one, and it will be deployed at the scheduled time. **Red**: The candidate Protocol Pack is different from the active one, and a recent attempt to deploy a Protocol Pack failed. In this case the Last Status column indicates that a deployment failed.
Last Status	Indicates the status of the most recent attempt, if any, to deploy a Protocol Pack to the device.

Module Statistics Page

The Module Statistics page displays statistics for various types of packets, for each device. Each device reports raw data about packet handling to the SD-AVC Network Service, which compiles statistics for each device. The statistics may be useful for monitoring or troubleshooting.

Click the **X**-icon to clear the module statistics.

CHAPTER 9

SD-AVC Notes and Limitations

The following are limitations of SD-AVC:

- For the SD-AVC Network Service, running on a host device, if the host interface that is used as a gateway interface is attached to a VRF, see Operating the SD-AVC Network Service with Host Interface Attached to a VRF, on page 45 for configuration details.
- SD-AVC requires a few minutes to learn from the network traffic before the application data is sent to the SD-AVC Network Service and compiled at the network level. See SD-AVC and Application Recognition, on page 6.
- SD-AVC provides application classification for server-based applications. The SD-AVC application rules pack is less relevant for client-to-client traffic, which is more granular and dynamic. Client-to-client traffic is classified by NBAR running on each network element.
- In the case of a proxy or content delivery network (CDN), multiple applications may use the same IP/port combination. The network devices themselves classify such traffic fully. However, for these applications, the SD-AVC agent operating on a device may report application data to the SD-AVC network service with a lesser degree of detail: they may be reported with less detailed classification granularity or not at all.

CHAPTER 10

Troubleshooting SD-AVC

This section provides information for troubleshooting SD-AVC problems. If this information does not provide a solution, contact Cisco TAC for assistance.

Communication with Devices by TCP

The SD-AVC Network Service uses TCP to communicate with the devices that it manages, over port 50000. In the SD-AVC Dashboard, if the Connectivity Page page shows any type of connectivity warning, check FTP connectivity on UDP port 50000. If no problem is found with connectivity, contact Cisco TAC.

NBAR Activation on Interfaces

On devices in the network that are using SD-AVC, the NBAR2 component must be active on any interface that processes network traffic, in order to report on traffic handled by the interface. For details, see Configuration Prerequisites: Network Devices Using SD-AVC, on page 26.

Without this, the device will not report on any traffic on that interface. This can cause a **red X** icon warning in the SD-AVC Dashboard, on the Connectivity Page page, in the Traffic Health column.

APPENDIX A

Operating the SD-AVC Network Service with Host Interface Attached to a VRF

In specific use cases, it may be necessary to operate the SD-AVC Network Service on a host device on which the host interface that is used by SD-AVC as its gateway interface may be attached to a VRF. In this case, the typical installation command described in Installing the SD-AVC Network Service, on page 16 cannot be used, and manual configuration is required, using the following guidelines:

- Ensure that the virtual port group and gateway interface(s) are not on the same subnet.
- Assign the virtual port group and gateway interface(s) to a VRF.
- Ensure that the IP address of the SD-AVC network service (**guest IP** in the configuration steps below) is on the virtual port group subnet.

Example:

```
ip vrf Mgt
!
interface VirtualPortGroup31
ip vrf forwarding Mgt
ip address 10.56.197.221 255.255.255.0
!
interface GigabitEthernet1
ip vrf forwarding Mgt
ip address 10.56.196.169 255.255.255.0
!
virtual-service SDAVC
vnic gateway VirtualPortGroup31
  guest ip address 10.56.197.222
activate
!
```

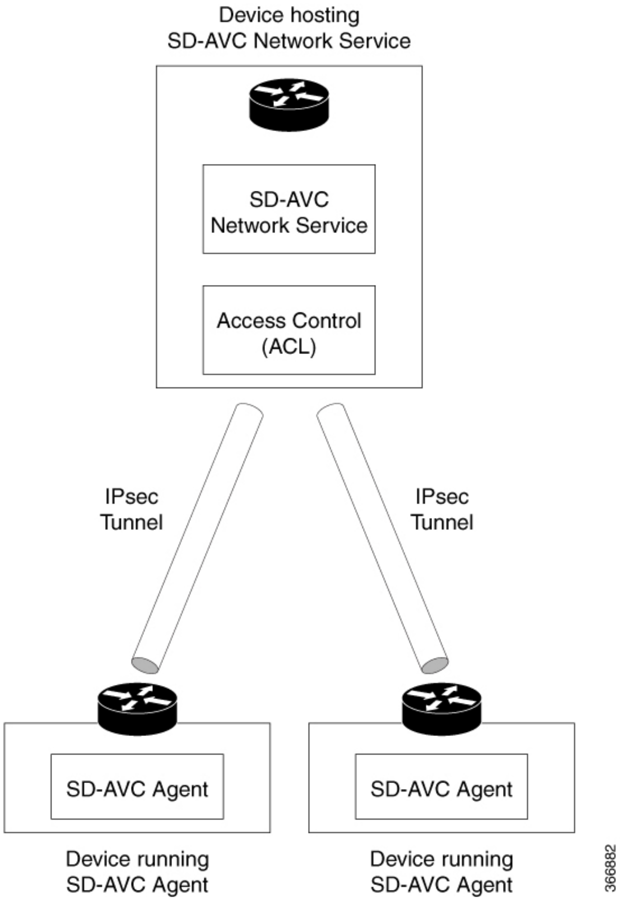
APPENDIX B

Configuring Secure Connectivity

Scenarios Requiring a Secure Connection

For network scenarios that require a secure connection between a network device running the SD-AVC agent, and the SD-AVC Network Service, you can optionally encrypt the SD-AVC communication between agent and Network Service using IPsec tunnels, and control device access using access control lists (ACL), as described in the sections that follow.

Figure 5: IPsec Tunnels between Network Devices and SD-AVC Network Service



Securing Connection between Host and SD-AVC Network Service

The SD-AVC Network Service runs as a virtual service on a Cisco device serving as a host platform. The host platform requires connectivity with the service through a virtual interface called VirtualPortGroup. The virtual service communicates with the host over this virtual interface, using SSH on TCP port 22.

Using ACL to Secure Connectivity between Host and SD-AVC Network Service

The SD-AVC network service operates as a virtualized component on a host device. To secure the connection between the host device and the SD-AVC network service, use the following:

interface VirtualPortGroup31

ip unnumbered GigabitEthernet1

ip access-group sd-avc-acl in

ip access-list extended *acl-name*

permit tcp host *SD-AVC-virtual-service-IP* **host** *host-router-IP* **eq** 22

permit tcp host *host-router-IP* **eq 22** *SD-AVC-virtual-service-IP*

Example using ACL:

```
interface VirtualPortGroup31
ip unnumbered GigabitEthernet1
ip access-group sd-avc-acl in
ip access-list extended sd-avc-acl
!! Configure SSH connection between the sd-avc-network-service to the hosted router
    permit tcp host 10.56.196.232 host 10.56.196.231 eq 22
    permit tcp host 10.56.196.231 eq 22 host 10.56.196.231
```

Securing Connection between Agents and Network Service

Network devices operating with SD-AVC communicate with a central SD-AVC Network Service. Ensure that ports, firewall policy, and so on, are configured to enable communication between the SD-AVC agents and SD-AVC Network Service(s) (see Configuring Connectivity, on page 15).

Using ACL to Secure Connection between Agent and Network Service

On the device hosting the SD-AVC Network Service, configure the UDP and TCP access control lists, as follows.

Note When using ACLs, only configured addresses will have access to the device hosting the SD-AVC Network Service.

- UDP

  The following syntax is presented for reference. For complete information about configuring ACL, see the documentation for your platform.

  permit udp [**host** *source-agent-ip* | *source-agent-network source-wildcard*] **host** *sd-avc-network-service-ip* **eq** 50000

  Example: Configuring port 50000 for UDP traffic for a range of devices (10.56.0.0 to 255).

  ```
  permit udp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 50000
  permit udp host 10.56.196.232 eq 50000 10.56.0.0 0.0.255.255
  ```

- TCP

  The following syntax is presented for reference. For complete information about configuring ACL, see the documentation for your platform.

  permit tcp [**host** *source-agent-ip* | *source-agent-network source-wildcard*] **host** *sd-avc-network-service-ip* [**eq** *port* | **range** *port-range-start port-range-end*]

  Example: Configuring required ports (20, 21, 50000-60000) for TCP traffic for a range of devices (10.56.0.0 to 255).

  ```
  permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 20
  permit tcp host 10.56.196.232 eq 20 10.56.0.0 0.0.255.255

  permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 21
  permit tcp host 10.56.196.232 eq 21 10.56.0.0 0.0.255.255
  ```

```
    permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 range 50000 60000
    permit tcp host 10.56.196.232 range 50000 60000 10.56.0.0 0.0.255.255
```

Using IPsec Tunnels to Secure Connection between Agent and Network Service

For network scenarios that require an encrypted connection between a network device running the SD-AVC agent, and the SD-AVC Network Service, set up IPsec tunnels to handle this communication.

For information about configuring Cisco IOS IPsec VPN connections, see Cisco IOS IPsec.

Connectivity to the SD-AVC Dashboard

Access to the SD-AVC Dashboard requires access to the device hosting the SD-AVC Network Service, and involves TCP traffic through port 8443. Ensure that network policty (firewall, ACL, and so on) permits this connectivity for devices requiring access to the SD-AVC Dashboard.

Using ACL to Secure Device Access to the SD-AVC Dashboard

On the device hosting the SD-AVC Network Service, configure the access control list as follows, to enable specific devices to connect to the SD-AVC Dashboard.

The following syntax is presented for reference. For complete information about configuring ACL, see the documentation for your platform.

ip access-list extended sd-avc-acl

permit tcp any host *sd-avc-network-service-ip* **eq 8443**

permit tcp host *source-agent-ip* **eq 8443 any**

Example: Configure PC access to SD-AVC Dashboard.

```
ip access-list extended sd-avc-acl
permit tcp any host 10.56.196.232 eq 8443
permit tcp host 10.56.196.232 eq 8443 any
```

Connectivity: Complete Example

The following example configures connectivity for a newly installed SD-AVC Network Service, hosted on a platform with the address 10.56.196.232, and a range of devices in the network that are operating with SD-AVC.

- Because the SD-AVC Network Service is newly installed, the first section of the example configures connectivity between the host and the SD-AVC virtual service.
- Platform hosting the SD-AVC virtual service: 10.56.196.232
- Network devices operating with SD-AVC, connecting to the SD-AVC Network Service: Address range 10.56.0.0 0.0.255.255
- In this example, any PC may be used to connect to the SD-AVC Dashboard.

```
!! Enables extended ACL
    ip access-list extended sd-avc-acl

!! Configure SSH connection between the sd-avc-network-service to the hosted router
    permit tcp host 10.56.196.232 host 10.56.196.231 eq 22
    permit tcp host 10.56.196.231 eq 22 host 10.56.196.231
```

```
!! Configure access to the SD-AVC Dashboard
    permit tcp any host 10.56.196.232 eq 8443
    permit tcp host 10.56.196.232 eq 8443 any

!! Configure access between SD-AVC Network Service and Agents - UDP
    permit udp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 50000
    permit udp host 10.56.196.232 eq 50000 10.56.0.0 0.0.255.255

!! Configure access between SD-AVC Network Service and Agents - TCP
    permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 20
    permit tcp host 10.56.196.232 eq 20 10.56.0.0 0.0.255.255

    permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 eq 21
    permit tcp host 10.56.196.232 eq 21 10.56.0.0 0.0.255.255

    permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.232 range 50000 60000
    permit tcp host 10.56.196.232 range 50000 60000 10.56.0.0 0.0.255.255

!! Configure connectivity between host and SD-AVC Network Service (virtual service)
    interface VirtualPortGroup31
    ip access-group  sd-avc-acl in
```