Configuring Secure Connectivity

Securing Connections to the SD-AVC Network Service

The SD-AVC Network Service, operating on a host device, communicates with:

One or more PC-type devices running the SD-AVC Dashboard
Network devices running the SD-AVC Agent

Enable Connectivity

To enable connectivity, ensure that ports, firewall policy, and so on, are configured to enable communication between the SD-AVC Network Service and the other relevant devices. See Configuring Connectivity.

Secure Connectivity

You can optionally use the mechanisms described below to secure the connections between the SD-AVC Network Service and other devices.

Method	Information
Access control list (ACL)	Configure an ACL on the device hosting the SD-AVC Network Service to define a white list of devices authorized to communicate with the SD-AVC Network Service. The ACL may be applied on a physical interface of the host device, or on the virtual interface between the host device and the SD-AVC Network Service. **Note** When using ACLs, only configured addresses will have access to the device hosting the SD-AVC Network Service.
IPsec tunnels	For network scenarios that require a secure connection between the SD-AVC Network Service and network devices running the SD-AVC agent, you can use IPsec tunnels to encrypt the SD-AVC communication. For information about configuring Cisco IOS IPsec VPN connections, see Cisco IOS IPsec.

Figure 1: Apply ACL to Physical Interface or Virtual Interface

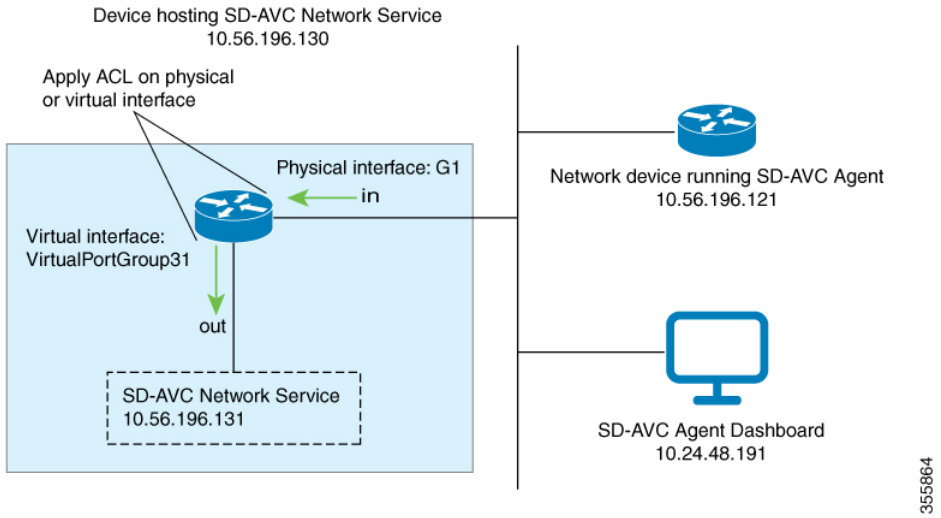
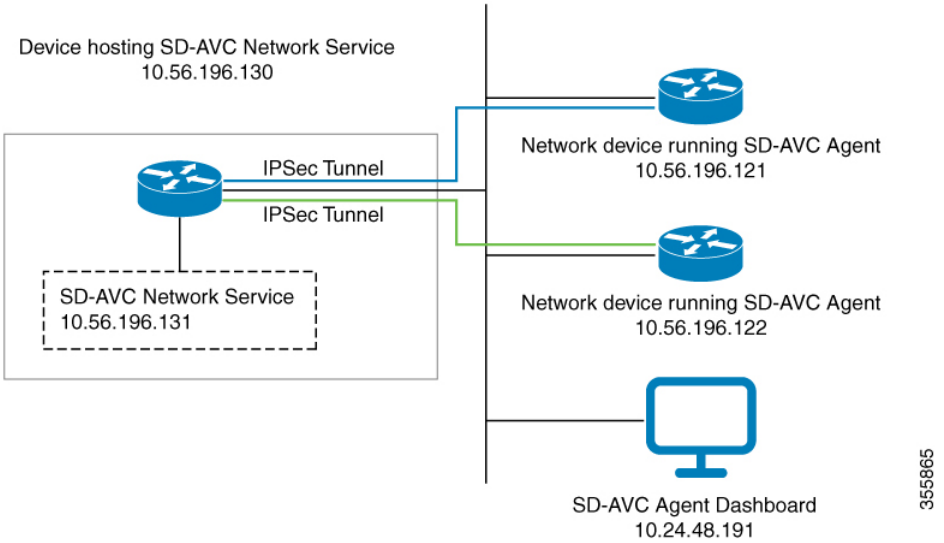


Figure 2: IPsec Tunnels between SD-AVC Network Service and Network Devices



Configuring ACL Access

Prerequisites

Ports, firewall policy, and so on, have been configured to enable communication between the SD-AVC Network Service and:

- Network devices running the SD-AVC Agent
- PC-type devices that connect to the SD-AVC Network Service to display the SD-AVC Dashboard

Configuring ACL

1. Create the ACL.

   ip access-list extended sdavc-acl

2. Configure access for a PC-type device that will connect to run the SD-AVC Dashboard.

   permit tcp host *dashboard-access-device-address* **host** *sdavc-network-service-address* **eq 8443**

   Example:

   ```
   permit tcp host 10.24.48.191 host 10.56.196.131 eq 8443
   ```

3. Configure access for one or more network devices running the SD-AVC Agent. For each network device, permit these ports:

   UDP: 50000
   TCP: 21, 8080, 59990-60000

   The complete syntax options for ACL configuration, such as address wildcards, are beyond the scope of this document. For complete information about configuring ACL, see the documentation for your platform.

   permit udp host *sdavc-agent-address* **host** *sdavc-network-service-address* **eq 50000**

   permit tcp host *sdavc-agent-address* **host** *sdavc-network-service-address* **eq 21**

   permit tcp host *sdavc-agent-address* **host** *sdavc-network-service-address* **eq 8080**

   permit tcp host *sdavc-agent-address* **host** *sdavc-network-service-address* **range 59990 60000**

   Example:

   ```
   permit udp host 10.56.196.121 host 10.56.196.131 eq 50000
   permit tcp host 10.56.196.121 host 10.56.196.131 eq 21
   permit tcp host 10.56.196.121 host 10.56.196.131 eq 8080
   permit tcp host 10.56.196.121 host 10.56.196.131 range 59990 60000
   ```

4. Apply the ACL to a physical interface of the host device or to the virtual interface between the host device and the SD-AVC Network Service. Use one of the following:

   - Physical interface (note the **in** keyword):

     interface *interface*

     ip access-group sdavc-acl in

     Example:

     ```
     interface GigabitEthernet1
       ip access-group sdavc-acl in
     ```

   - Virtual interface (note the **out** keyword):

     interface *virtual-interface*

     ip access-group sdavc-acl out

     Example:

     ```
     interface VirtualPortGroup31
        ip access-group sdavc-acl out
     ```

Examples

Complete example, configuring a single device for Dashboard access and a single network device. This example uses the virtual interface option:

```
ip access-list extended sdavc-acl
     permit tcp host 10.24.48.191 host 10.56.196.131 eq 8443
     permit udp host 10.56.196.121 host 10.56.196.131 eq 50000
     permit tcp  host 10.56.196.121 host 10.56.196.131 eq 21
     permit tcp  host 10.56.196.121 host 10.56.196.131 range 59990 60000

interface VirtualPortGroup31
   ip access-group sdavc-acl out
```

Complete example, configuring a single device for Dashboard access, and a range of devices (10.56.0.0 to 255). This example uses the physical interface option.

```
ip access-list extended sdavc-acl
     permit tcp host 10.24.48.191 host 10.56.196.131 eq 8443
     permit udp 10.56.0.0 0.0.255.255 host 10.56.196.131 eq 50000
     permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.131 eq 21
     permit tcp 10.56.0.0 0.0.255.255 host 10.56.196.131 range 59990 60000

interface GigabitEthernet1
  ip access-group sdavc-acl in
```