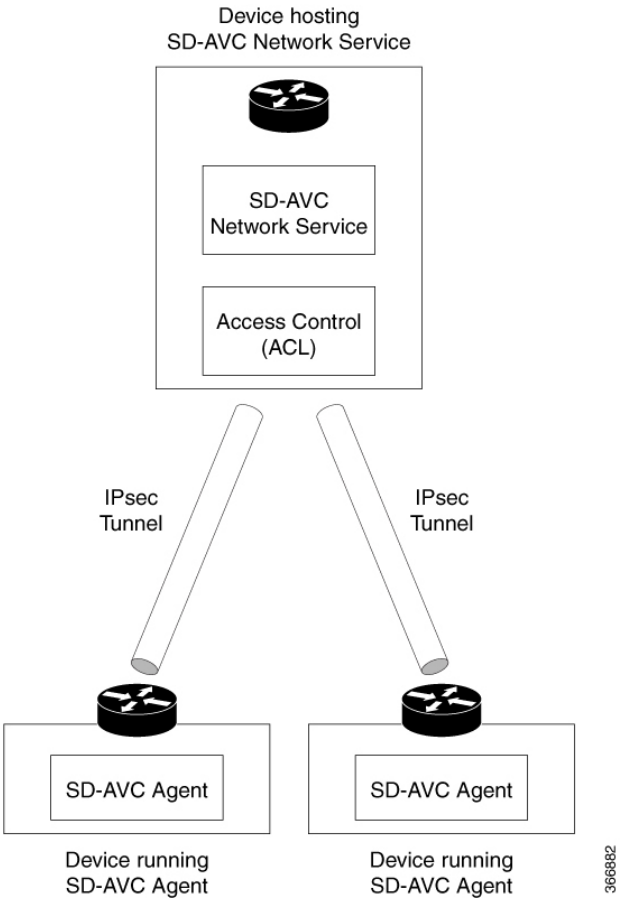
Configuring Secure Connectivity

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 1: 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).

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
```