Revised: July 23, 2024

Troubleshoot Inter-VPN Traffic Failing Between Sites in a Hub-and-Spoke Network

Problem

Inter-VPN traffic transmission fails between two sites in a network with a hub-and-spoke topology.

Conditions

This troubleshooting scenario applies when all of these are true:

- Hub-and spoke topology

  Network with a hub-and-spoke topology.

- Cisco NBAR active on hub site routers

  Cisco NBAR is active on the hub site devices, including on the interface handling service insertion traffic. Commonly, a localized policy for the hub site enables Cisco NBAR. Specifically, if you (a) create a localized policy in Cisco SD-WAN Manager, (b) enable application visibility in the policy, and (c) apply the policy to hub site routers, this activates Cisco NBAR on all interfaces of the hub site routers.

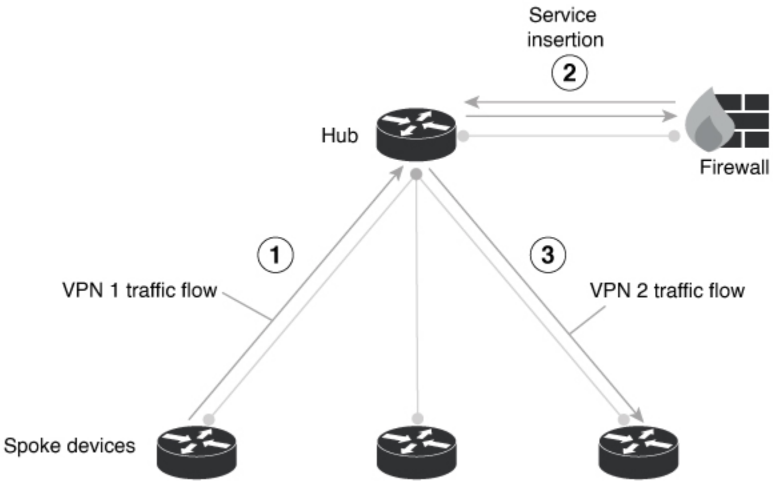
- Inter-VPN traffic routing in the network

  A control policy for spoke sites in the network includes route leaking, meaning that the policy routes specific traffic on a VPN at one spoke site to a different VPN at another site. For example, a policy can route traffic on VPN1 at Site 1 to VPN2 at Site 2. This constitutes inter-VPN traffic routing.

- Data policy providing service insertion

  A data policy for hub devices in the network provides service insertion for some or all traffic. This means that the data policy operating on a router matches specific traffic and routes the traffic to a device providing a service—for example, a firewall service. The service processes the traffic and sends it back to the router. The router then forwards the traffic to its destination. Note that if a service, such as firewall, blocks the traffic, it does not send it back to the router to be forwarded to its destination. This figure shows an example of firewall service insertion.

Figure 1: Service Insertion



Possible Causes

In the scenario described here, Cisco NBAR operating on a hub site device creates separate entries for individual flows in the Cflowd table—one entry for each of the two separate VPNs. This can cause the hub device to drop traffic between spoke sites.

Solutions

1. To check whether a hub device is dropping packets for traffic between spoke sites, use the **show platform hardware qfp active statistics drop** command on the hub device. The output indicates whether packets are being dropped between spoke sites.

2. To check specifically whether an inter-VPN failure is causing a hub device to drop packets, use the **show sdwan statistics** command on the hub device.

   Inter-VPN failure means that a router is failing to forward packets from one VPN to another as configured by route leaking.

   If there is an inter-VPN failure, the command output shows a message containing the string **intervpn-multikey-failed**. This message may suggest that Cisco NBAR is creating multiple Cflowd table entries for individual flows, causing dropped packets.

   Here's an example:

   ```
   Device# show sdwan statistics | exclude 0
   …
   sdwan-statistics-sc-cft-intervpn-multikey-failed
   …
   ```

3. If the preceding steps confirm the possibility that Cisco NBAR is indirectly causing packet loss, disable Cisco NBAR on all interfaces of hub site routers. To do this, follow these steps:

   a. In Cisco SD-WAN Manager, open the localized policy for the hub site devices.

      See Localized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide*.

   b. In the localized policy, uncheck the **Application** and **Netflow** check boxes.

      This disables Cisco NBAR, which disables application and flow visibility.

c. Reapply the policy to the hub site or sites.