Service Chaining

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, see Service Insertion for information about service chaining.

Services in the Network

Services such as firewall, load balancer, and intrusion detection and prevention (IDP) are often run within a virtualized environment, and they may physically be centralized in one location or in several locations for redundancy. Services may be internal, cloud based, or external subscriptions. Networks must be able to reroute traffic from any location in the network through such services.

Customers want the ability to internally spawn or externally subscribe to new services on demand—for capacity, redundancy, or simply to select best-of-breed technologies. For example, if a firewall site exceeds its capacity, a customer can spawn a new firewall service at a new location. Supporting this new firewall would require the configuration of policy-based, weighted load distribution to multiple firewalls.

Following are some of the reasons to reroute a traffic flow through a service or chain of services:

- Traffic flow from a less secure region of a network must pass through a service, such as a firewall, or through a chain of services to ensure that it has not been tampered with.
- For a network that consists of multiple VPNs, each representing a function or an organization, traffic between VPNs must traverse through a service, such as a firewall, or through a chain of services. For example, in a campus, interdepartmental traffic might go through a firewall, while intradepartmental traffic might be routed directly.
- Certain traffic flows must traverse a service, such as a load balancer.

Today, the only way to reroute traffic flow is by provisioning every routing node—from the source to the service node to the systems beyond the service node—with a policy route. This is done either by having an operator manually configure each node or by using a provisioning tool that performs the configuration for each node on behalf of the operator. Either way, the process is operationally complex to provision, maintain, and troubleshoot.

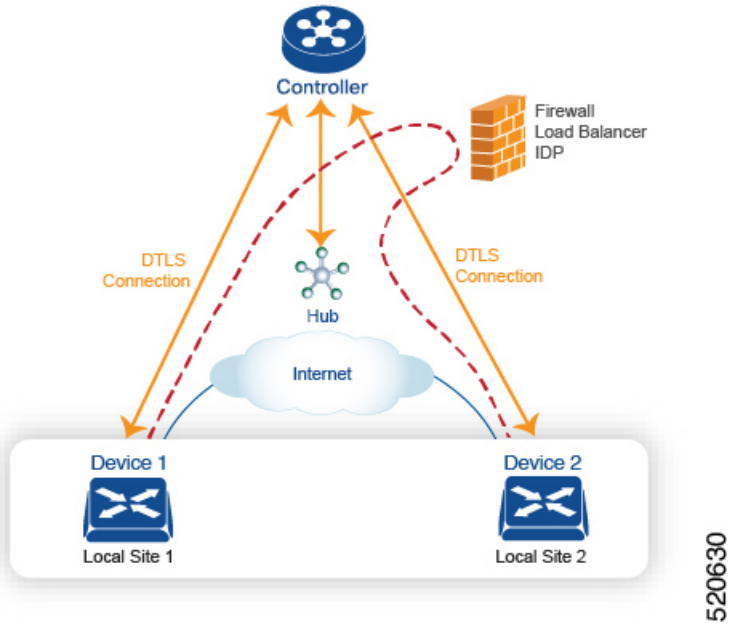
Provisioning Services in the Cisco Catalyst SD-WAN Overlay Network

In the Cisco Catalyst SD-WAN solution, the network operator can enable and orchestrate all service chaining from a central controller, that is, from the Cisco SD-WAN Controller. No configuration or provisioning is required on any of the devices.

The general flow of service chaining in a Cisco Catalyst SD-WAN network is as follows:

- Devices advertise the services available in their branch or campus—such as firewall, IDS, and IDP—to the Cisco SD-WAN Controllers in their domain. Multiple devices can advertise the same services.
- Devices also advertise their OMP routes and TLOCs to the Cisco SD-WAN Controllers.
- For traffic that requires services, the policy on the Cisco SD-WAN Controller changes the next hop for the OMP routes to the service landing point. In this way, the traffic is first processed by the service before being routed to its final destination.

The following figure illustrates how service chaining works in the Cisco Catalyst SD-WAN solution. The network shown has a centralized hub router that is connected to two branches, each with a device. The standard network design implements a control policy such that all traffic from branch site 1 to branch site 2 travels through the hub router. Sitting behind the hub router is a firewall device. So now, assume we want all traffic from site 1 to site 2 to first be processed by the firewall. Traffic from the device at site 1 still flows to the hub router, but instead of sending it directly to site 2, the hub router redirects the traffic to the firewall device. When the firewall completes its processing, it returns all cleared traffic to the hub, which then passes it along to the device at site 2.



Service Route SAFI

The hub and local branch devices advertise the services available in their networks to the Cisco SD-WAN Controllers in its domain using service routes, which are sent by way of OMP using the service route Subsequent Address Family Identifier (SAFI) bits of the OMP NLRI. The Cisco SD-WAN Controllers maintain the service routes in their RIB, and they do not propagate these routes to the devices.

Each service route SAFI has the following attributes:

- VPN ID (vpn-id)—Identifies the VPN that the service belongs to.
- Service ID (svc-id)—Identifies the service being advertised by the service node. The Cisco Catalyst SD-WAN software has the following predefined services:
  - FW, for firewall (maps to svc-id 1)
  - IDS, for Intrusion Detection Systems (maps to svc-id 2)
  - IDP, for Identity Providers (maps to svc-id 3)
  - netsvc1, netsvc2, netsvc3, and netsvc4, which are reserved for custom services (they map to svc-id 4, 5, 6, and 7, respectively)
- Label—For traffic that must traverse a service, the Cisco SD-WAN Controller replaces the label in the OMP route with the service label in order to direct the traffic to that service.
- Originator ID (originator-id)—The IP address of the service node that is advertising the service.
- TLOC—The transport location address of the device that is "hosting" the service.
- Path ID (path-id)—An identifier of the OMP path.

Service Chaining Policy

To route traffic through a service, you provision either a control policy or a data policy on the Cisco SD-WAN Controller. You use a control policy if the match criteria are based on a destination prefix or any of its attributes. You use a data policy if the match criteria include the source address, source port, DSCP value, or destination port of the packet or traffic flow. You can provision the policy directly using the CLI, or it can be pushed from Cisco SD-WAN Manager.

The Cisco SD-WAN Controller maintains OMP routes, TLOC routes, and service routes in its route table. A given OMP route carries a TLOC and the label associated with it. On a Cisco SD-WAN Controller, a policy can be applied that changes the TLOC and its associated label to be that of a service.

Tracking the Health of the Service Chain

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, Cisco Catalyst SD-WAN periodically probes devices providing network services to test whether they are operational. Tracking the availability of devices in the service chain helps to prevent a null route, which can occur if a policy routes traffic to a service device which is not available. By default, Cisco Catalyst SD-WAN writes the tracking results to a service log, but this can be disabled.

Limitations

- Service insertion over tunnel interface is not supported on Cisco IOS XE Catalyst SD-WAN devices.
- Control policy based service-chain action on locally hosted service-chain is not supported.
- Configuring service-chain and AppQoE on the same device is not supported irrespective of the data-policy or control-policy based actions.

- Configure Service Chaining, on page 4
- Service Chaining Configuration Examples, on page 5
- Monitor Service Chaining, on page 13

Configure Service Chaining

Here is the workflow for configuring service chaining for a device managed by Cisco Catalyst SD-WAN:

1. Service devices are accessed through a specific VRF. In the VPN template that corresponds to the VRF for a service device, configure service chaining, specifying the service type and device addresses. By default, the tracking feature adds each service device status update to the service log. You can disable this in the VPN template.
2. Attach the VPN template to the device template for the device managed by Cisco Catalyst SD-WAN.
3. Apply the device template to the device.

Configure Service Chaining Using Cisco SD-WAN Manager

To configure service chaining for a device.

1. In Cisco SD-WAN Manager, create a VPN template.
2. Click**Service**.
3. In the **Service** section, click **New Service** and configure the following:
   - **Service Type**: Select the type of service that the service device is providing.
   - **IP Address**: IP Address is the only working option.
   - **IPv4 Address**: Enter between one and four addresses for the device.
   - **Tracking**: Determines whether the periodic health updates of the service device are recorded in the system log. Default: On

Note Maximum number of services: 8

4. Click **Add**. The service appears in the table of configured services.

CLI Equivalent for Cisco IOS XE Catalyst SD-WAN Devices

The following table shows how configuration of service chaining by CLI corresponds to configuration in Cisco SD-WAN Manager. CLI configuration differs between Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices. The CLI example below is for a Cisco IOS XE Catalyst SD-WAN device.

CLI (Cisco IOS XE Catalyst SD-WAN device)	Cisco SD-WAN Manager
`service firewall vrf 10`	In Cisco SD-WAN Manager, configure service insertion in the VPN template for a specific VRF—VRF 10 in this example. Select the service type from the drop-down —firewall in this example.

CLI (Cisco IOS XE Catalyst SD-WAN device)	Cisco SD-WAN Manager
`no track-enable` **Note** Default: enabled	When adding a service in the VPN template **Service**, select **On** or **Off** for **Tracking**.
`ipv4 address 10.0.2.1 10.0.2.2`	In the VRF template **Service**, enter one or more IP addresses for the service device providing a specific service.

CLI Example

```
sdwan
  service firewall vrf 10
  ipv4 address 10.0.2.1 10.0.2.2
commit
```

CLI Equivalent for Cisco vEdge Devices

The following table shows how configuration of service chaining by CLI corresponds to configuration in Cisco SD-WAN Manager. CLI configuration differs between Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices. The CLI example below is for a Cisco vEdge device.

CLI (Cisco vEdge device)	Cisco SD-WAN Manager
`vpn 10`	In Cisco SD-WAN Manager, configure service insertion in the VPN template—VPN 10 in this example. Select the service type from the drop-down—firewall in this example.
`service FW address 10.0.2.1`	Select the service type from the drop-down—firewall in this example. Provide one or more addresses for the service device.
`no track-enable` **Note** Default: enabled	When adding a service in the VPN template **Service**, select **On** or **Off** for **Tracking**.

CLI Example

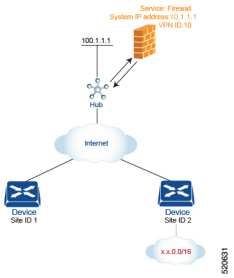
```
vpn 10
  service FW address 10.0.2.1
commit
```

Service Chaining Configuration Examples

Service chaining control policies direct data traffic to service devices that can be located in various places in the network before the traffic is delivered to its destination. For service chaining to work, you configure a centralized control policy on the Cisco SD-WAN Controller, and you configure the service devices themselves on the device collocated in the same site as the device. To ensure that the services are advertised to the Cisco SD-WAN Controller, the IP address of the service device must resolve locally.

This topic provides examples of configuring service chaining.

Route Intersite Traffic through a Service



A simple example is to route data traffic traveling from one site to another through a service. In this example, we route all traffic traveling from the device at Site 1 to the device at Site 2 through a firewall service that sits behind a hub (whose system IP address is 100.1.1.1). To keep things simple, all devices are in the same VPN.

For this scenario, you configure the following:

- On the hub router, you configure the IP address of the firewall device.
- On the Cisco SD-WAN Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall service.
- On the Cisco SD-WAN Controller, you apply the control policy to Site 1.

Here is the configuration procedure:

1. On the hub router, provision the firewall service, specifying the IP address of the firewall device. With this configuration, OMP on the hub router advertises one service route to the Cisco SD-WAN Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the hub router and a service label of svc-id-1, which identifies the service type as a firewall. (As mentioned above, before advertising the route, the device ensures that the firewall's IP address can be resolved locally.)

   ```
   sdwan
   service firewall vrf 10
     ipv4 address 10.1.1.1
   ```

2. On the Cisco SD-WAN Controller, configure a control policy that redirects data traffic traveling from Site 1 to Site 2 through the firewall. Then, also on the Cisco SD-WAN Controller, apply this policy to Site 1.

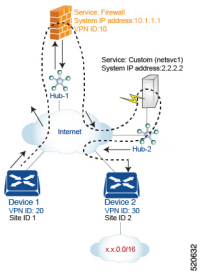
   ```
   policy
     lists
       site-list firewall-sites
         site-id 1
     control-policy firewall-service
       sequence 10
         match route
           site-id 2
         action accept
           set service FW vpn 10
       default-action accept
   apply-policy
     site-list firewall-sites control-policy firewall-service out
   ```

   This policy configuration does the following:

- Create a site list called **firewall-sites** that is referenced in the **apply-policy** command and that enumerates all the sites that this policy applies to. If you later want to scale this policy so that all traffic destined to Site 2 from other sites should also first pass through the firewall, all you need to do is add the additional site IDs to the **firewall-sites** site list. You do not need to change anything in the **control-policy firewall-service** portion of the configuration.
- Define a control policy named **firewall-service**. This policy has one sequence element and the following conditions:
  - Match routes destined for Site 2.
  - If a match occurs, accept the route and redirect it to the firewall service provided by the Hub router, which is located in VPN 10.
  - Accept all nonmatching traffic. That is, accept all traffic not destined for Site 2.
- Apply the policy to the sites listed in **firewall-list**, that is, to Site 1. The Cisco SD-WAN Validator applies the policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:
  - The TLOC is changed from Site 2's TLOC to the hub router's TLOC. This is the TLOC that the Cisco SD-WAN Controller learned from the service route received from the hub router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the hub router
  - The label is changed to svc-id-1, which identifies the firewall service. This label causes the hub router to direct the traffic to the firewall device.

When the hub router receives the traffic, it forwards it to the address 10.1.1.1, which is the system IP address of the firewall. After the firewall has finished processing the traffic, the firewall returns the traffic to the hub router, and this router then forwards it to its final destination, which is Site 2.

Route Inter-VPN Traffic through a Service Chain with One Service per Node



A service chain allows traffic to pass through two or more services before reaching its destination. The example here routes traffic from one VPN to another through services located in a third VPN. The services are located behind different hub routers. Specifically, we want all traffic from device-1 in VPN 20 and that is destined for prefix x.x.0.0/16 in VPN 30 on device-2 to go first through the firewall behind Hub-1 and then through the custom service netsvc1 behind Hub-2 before being sent to its final destination.

For this policy to work:

- VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet
- VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.

- VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
- VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure four things:

- You configure the IP address of the firewall device on the Hub-1 router.
- You configure the IP address of the custom service device on the Hub-2 router.
- On the Cisco SD-WAN Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall device.
- On the Cisco SD-WAN Controller, you configure a second control policy that redirects traffic to the custom service device.

Here is the configuration procedure:

1. Configure the firewall service on Hub-1. With this configuration, OMP on the Hub-1 router advertises a service route to the Cisco SD-WAN Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the hub router and a service label of svc-id-1, which identifies the service type as a firewall.

   ```
   sdwan
   service firewall vrf 10
     ipv4 address 10.1.1.1
   ```

2. Configure the custom service netsvc1 on Hub-2. With this configuration, OMP on the Hub-2 router advertises a service route to the Cisco SD-WAN Controller. The service route contains the TLOC of the Hub-2 and a service label of svc-id-4, which identifies the custom service.

   ```
   sdwan
   service netsvc1 vrf 10
     ipv4 address 2.2.2.2
   ```

3. Create a control policy on the Cisco SD-WAN Controller for first service in the chain—the firewall—and apply it to Site 1, which is the location of the device-1 router:

   ```
   policy
     lists
       site-list firewall-custom-service-sites
         site-id 1
     control-policy firewall-service
       sequence 10
         match route
           vpn 30
           site-id 2
         action accept
           set service FW
       default-action accept
   apply-policy
     site-list firewall-custom-service-sites control-policy firewall-service out
   ```

   This policy configuration does the following:

   - Create a site list called **firewall-custom-service-sites** that is referenced in the **apply-policy** command and that enumerates all the sites that this policy applies to.
   - Define a control policy named **firewall-service** that has one sequence element and the following conditions:
     - Match routes destined for both VPN 30 and Site 2.

- If a match occurs, accept the route and redirect it to a firewall service.
- If a match does not occur, accept the traffic.

- Apply the policy to the sites in the **firewall-custom-service-sites** site list, that is, to Site 1. The Cisco SD-WAN Controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:
  - The TLOC is changed from Site 2's TLOC to the Hub-1 router's TLOC. This is the TLOC that the Cisco SD-WAN Controller learned from the service route received from the hub. It is because of the change of TLOC that traffic destined for Site 2 is directed to the Hub-1 router.
  - The label is changed to svc-id-1, which identifies the firewall service. This label causes the Hub-1 router to direct the traffic to the firewall device.

When the Hub-1 router receives the traffic, it forwards it to the address 10.1.1.1, which is the system IP address of the firewall. After the firewall completes processing the traffic, it returns the traffic to the Hub-1 router, which, because of the policy defined in the next step, forwards it to the Hub-2 router.

4. Create a control policy on the Cisco SD-WAN Controller for the second service in the chain, which is the custom service, and apply it to the site of the Hub-1 router:

```
policy
  site-list custom-service
    site-id 3
  control-policy netsvc1-service
    sequence 10
      match route
        vpn 30
        site-id 2
      action accept
        set service netsvc1
    default-action accept
apply-policy
  site-list custom-service control-policy netsvc1-service out
```

This policy configuration does the following:

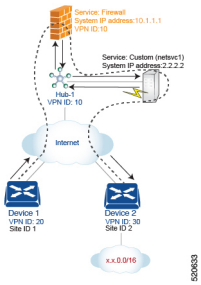
- Create a site list called **custom-service** that is referenced in the **apply-policy** command and that enumerates all the sites that this policy applies to.
- Define a control policy named **netsvc1-service** that has one sequence element and the following conditions:
  - Match routes destined for both VPN 30 and Site 2.
  - If a match occurs, accept the route and redirect it to the custom service.
  - If a match does not occur, accept the traffic.

- Apply the policy to the sites in the **custom-service** list, that is, to Site 3. The Cisco SD-WAN Controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 3. In these routes:
  - The TLOC is changed from Site 2's TLOC to the Hub-2 router's TLOC. This is the TLOC that the Cisco SD-WAN Controller learned from the service route received from the Hub-2 router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the Hub-2 router.

- The label is changed to svc-id-4, which identifies the custom service. This label causes the Hub-2 to direct the traffic to the device that is hosting the custom service

When the Hub-2 routers receives the traffic, it forwards it to the address 2.2.2.2, which is the system IP address of the device hosting the custom service. After the traffic has been processed, it is returned to the Hub-2 router, which then forwards it to its final destination, Site 2.

Route Inter-VPN Traffic through a Service Chain with Multiple Services per Node



If a service chain has more than one service that is connected to the same node, that is, both services are behind the same device, you use a combination of control policy and data policy to create the desired service chain. The example here is similar to the one in the previous section, but instead has a firewall and a custom service (netsvc-1) behind a single hub router. Here, we want all data traffic from device-1 in VPN 20 destined for prefix x.x.0.0/16 on device-2 in VPN 30 to first go through the firewall at Hub-1, then through the custom service netsvc1, also at Hub-1, and then to its final destination.

For this policy to work:

- VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet.
- VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.
- VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
- VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure the following:

- On the hub router, you configure the firewall and custom services.
- On the Cisco SD-WAN Controller, you configure a control policy that redirects data traffic from Site 1 that is destined to Site 2 through the firewall.
- On the Cisco SD-WAN Controller, you configure a data policy that redirects data traffic to the custom service.

Here is the configuration procedure:

1. On the hub router, configure the firewall and custom services:

```
sdwan
service firewall vrf 10
  ipv4 address 10.1.1.1
service netsvc1 vrf 10
  ipv4 address 2.2.2.2
```

With this configuration, OMP on the hub router advertises two service routes to the Cisco SD-WAN Controller, one for the firewall and the second for the custom service netsvc1. Both service routes contain the TLOC of the Hub-1 router and a service label that identifies the type of service. For the firewall service, the label is svc-id-1, and for the custom service, the label is svc-id-4.

2. On the Cisco SD-WAN Controller, configure a control policy controller to reroute traffic destined for VPN 30 (at Site 2) to firewall service that is connected to Hub-1 (at Site 3), and apply this policy to Site 1:

```
policy
  lists
    site-list device-1
      site-id 1
  control-policy firewall-service
    sequence 10
      match route
        vpn 30
      action accept
        set service FW
apply-policy
  site-list device-1 control-policy firewall-service out
```

3. On the Cisco SD-WAN Controller, configure a data policy that redirects, or chains, the data traffic received from the firewall device to the custom service netsvc1. Then apply this policy to Hub-1. This data policy routes packets headed for destinations in the network x.x.0.0/16 to the IP address 2.2.2.2, which is the system IP address of the device hosting the custom service.

```
policy
  lists
    site-list device-2
      site-id 2
    site-list Hub-1
      site-id 3
    prefix-list svc-chain
      ip-prefix x.x.0.0/16
    vpn-list vpn-10
      vpn 10
  data-policy netsvc1-policy
    vpn-list vpn-10
      sequence 1
        match
          ip-destination x.x.0.0/16
        action accept
          set next-hop 2.2.2.2
apply-policy
  site-list Hub-1 data-policy netsvc1-policy from-service
```

Active or Backup Scenario with Service Chaining

When using **set service** action to configure active or backup control policy with **set service** action for service chaining, if total number of available paths (summary of active and standby paths) is more than configured **send-path-limit**, do not set preference directly to routes. Ensure to use **set tloc-list** action to set preferences together with **set service** action. Otherwise, you may see cases where either only active or only backup paths are advertised to a particular spoke router.

For example, in the Cisco SD-WAN Controller OMP table, there are eight active and backup paths. Based on the best-path calculation, the paths are sorted in the following order:

backup1, backup2, backup3, backup4, active1, active2, active3, active4

When **send-path-limit 4** is configured, if you apply the first policy, only the four backup paths are sent. If you apply the second policy, two active and two backup paths are sent.

Example of policy susceptible for failures if **send-path-limit** is lower than total number of active and backup paths:

```
control-policy SET_SERVICE_ACTIVE-BACKUP
  sequence 10
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_PRIMARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     preference 200
     service FW vpn 10
    !
   !
  !
  sequence 20
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_SECONDARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     preference 100
     service FW vpn 10
    !
   !
  !
  default-action accept
!
!
```

Example of the same policy but fixed according to recommendations:

```
policy
lists
  tloc-list HUBS_PRIMARY_INTERNET_TLOCS
   tloc 10.0.0.0 color biz-internet encap ipsec preference 200
   tloc 10.0.0.1 color biz-internet encap ipsec preference 200
  !
  tloc-list HUBS_SECONDARY_INTERNET_TLOCS
   tloc 10.255.255.254 color biz-internet encap ipsec preference 100
   tloc 10.255.255.255 color biz-internet encap ipsec preference 100
  !
!
control-policy SET_SERVICE_ACTIVE-BACKUP_FIXED
  sequence 10
   match route
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_PRIMARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     service FW vpn 10 tloc-list HUBS_PRIMARY_INTERNET_TLOCS
    !
   !
  !
  sequence 20
   match route
```

```
    prefix-list _AnyIpv4PrefixList
    site-list   HUBS_SECONDARY
    tloc-list   INTERNET_TLOCS
   !
   action accept
    set
     service FW vpn 10 tloc-list HUBS_SECONDARY_INTERNET_TLOCS
    !
   !
  !
  default-action accept
!
!
```

Monitor Service Chaining

You can monitor different aspects of service chaining on hub and spoke devices.

Note Configuring a service device to operate as part of the service chain is called service insertion.

- On a hub device, view the configured services.
  - From the Cisco SD-WAN Manager menu:

    View the configured services on the **Real Time** monitoring page (**Monitor** > **Devices** > *hub-device* > **Real Time**). For **Device Options**, select **OMP Services**.

    Cisco vManage Release 20.6.x and earlier: View the configured services on the **Real Time** monitoring page (**Monitor** > **Network** > *hub-device* > **Real Time**). For **Device Options**, select **OMP Services**.

- On a spoke device, view the details of the service chain path.
  - **Using Cisco SD-WAN Manager**:

    View the service chain path on the **Traceroute** page (**Monitor** > **Devices** > *spoke-device* > **Troubleshooting** > **Connectivity** > **Trace Route**). Enter the destination IP, VPN, and source interface for the desired path.

    Cisco vManage Release 20.6.x and earlier: View the service chain path on the **Traceroute** page (**Monitor** > **Network** > *spoke-device* > **Troubleshooting** > **Connectivity** > **Trace Route**). Enter the destination IP, VPN, and source interface for the desired path.

  - **Using the CLI**:

    Use the **traceroute** command. For information, see the Cisco Catalyst SD-WAN Command Reference.

Example: View a Service Chain Path Between Two Spoke Devices

The following example shows how to view the path between two spokes before and after adding a service chain between them, using Cisco SD-WAN Manager or the CLI.

For clarity, the example presents a scenario of two spoke devices, a hub device, and a service device providing a firewall service, and shows how to configure the firewall service chain.

Here are the details for each device in the scenario:

Device	Address
Hub, through interface ge0/4	10.20.24.15
Spoke 1	10.0.3.1
Spoke 2	10.0.4.1
Service device (firewall service)	10.20.24.17

Configuration of the three devices:

```
Hub
====
vm5# show running-config  vpn 1
vpn 1
 name ospf_and_bgp_configs
 service FW
  address 10.20.24.17
 exit
 router
  ospf
   router-id 10.100.0.1
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
    exit
   exit
  !
 !
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
 !
 interface ge0/5
  ip address 10.30.24.15/24
  no shutdown
 !
!


Spoke 1
=======
vpn 1
 name ospf_and_bgp_configs
 interface ge0/1
  ip address 10.0.3.1/24
  no shutdown
 !
!


Spoke2
======
vpn 1
 interface ge0/1
  ip address 10.0.4.1/24
  no shutdown
```

```
 !
!
```

1. **Without Service Insertion**:

   At this point, no service insertion policy has been configured, so executing **traceroute** on Spoke 1 to display the path details to Spoke 2 (10.0.4.1) shows a simple path to Spoke 2:

   → Spoke 2 (10.0.4.1)

   ```
   vm4# traceroute vpn 1 10.0.4.1
   Traceroute  10.0.4.1 in VPN 1
   traceroute to 10.0.4.1 (10.0.4.1), 30 hops max, 60 byte packets
    1  10.0.4.1 (10.0.4.1)  7.447 ms  8.097 ms  8.127 ms
   ```

   Similarly, viewing the Traceroute page in Cisco SD-WAN Manager shows a simple path from Spoke 1 to Spoke 2.

2. **With Service Insertion**:

   The following Cisco SD-WAN Controller policy configures service insertion for a firewall service, using the firewall service device described above.

   ```
   vm9# show running-config policy
   policy
    lists
     site-list firewall-sites
      site-id 400
     !
    !
    control-policy firewall-services
     sequence 10
      match route
       site-id 600
      !
      action accept
       set
        service FW vpn 1
       !
      !
     !
     default-action accept
    !
   !
   vm9# show running-config apply-policy
   apply-policy
    site-list firewall-sites
     control-policy firewall-services out
    !
   !
   ```

   After configuring the service insertion, executing **traceroute** on Spoke 1 (10.0.3.1) to display the path details to Spoke 2 (10.0.4.1) shows this path:

   → Hub (10.20.24.15) → Firewall service device (10.20.24.17) → Hub (10.20.24.15) → Spoke 2 (10.0.4.1)

   ```
   Traceroute -m 15 -w 1 -s 10.0.3.1 10.0.4.1 in VPN 1
   traceroute to 10.0.4.1 (10.0.4.1), 15 hops max, 60 byte packets
   1 10.20.24.15 (10.20.24.15) 2.187 ms 2.175 ms 2.240 ms
   2 10.20.24.17 (10.20.24.17) 2.244 ms 2.868 ms 2.873 ms
   3 10.20.24.15 (10.20.24.15) 2.959 ms 4.910 ms 4.996 ms
   4 10.0.4.1 (10.0.4.1) 5.045 ms 5.213 ms 5.247 ms
   ```

Similarly, viewing the **Traceroute** page in Cisco SD-WAN Manager shows each step of the path from Spoke 1 to Spoke 2, through the hub and firewall service device.