

Monitoring Crypto VPN solutions on SD-Routing devices, Release 17.16.x

What's new and changed

Cisco IOS XE Release	Feature Name and Description	Supported Platforms
Cisco IOS XE 17.16.1a	<p>Monitoring Crypto VPN solutions on SD-Routing devices</p> <p>If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts and events.</p>	<ul style="list-style-type: none"> • Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco 1000 Series Integrated Services Routers • Cisco 4461 Integrated Services Router • Cisco Catalyst 1101 Rugged Router • Cisco Catalyst IR1800 Rugged Series Routers

Overview of monitoring crypto VPN solutions

If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts and events.

Having high visibility into the network can help identify errors in real time therefore reducing the network down time.

Before you begin

Ensure that the software version of the SD-Routing devices on which you have deployed the VPN solution is Cisco IOS XE 17.16.1a.

The Cisco DMVPN solution is configurable using [Feature Parcels](#) in Cisco Catalyst SD-WAN Manager. VPN solutions such as FlexVPN or Layer3VPNs are configurable using **Configuration Groups > CLI Add-on Profile** in Cisco Catalyst SD-WAN Manager.

For more information on using commands to form a CLI-Add profile see [FlexVPN documentation](#) and [Layer 3 VPN documentation](#).

Levels of monitoring

In Cisco Catalyst SD-WAN Manager, use the **Monitor** page to monitor SD-Routing devices in a network. The different levels of monitoring are:

Table 1:


Dashlets and bar graph for summary of VPN endpoints and IPsec sessions	On the Cisco Catalyst SD-WAN Manager, choose Monitor > Overview to view VPN endpoint dashlet and IPSec session bar graph
Monitor all the devices in a site or across the network	On the Cisco Catalyst SD-WAN Manager, choose Monitor > Devices to view details such as VPN Role, IPSec session count, VPN Session count, and VPN Peer count.
Monitor a single device in a network	<ol style="list-style-type: none"> 1. On the Cisco Catalyst SD-W AN Manager, choose Monitor > Devices. 2. Select a device from the list. 3. Select Crypto VPN to view general information about all crypto sessions and also details exclusive to specific crypto solutions.
Monitor all events across the network or for a specific site	<ol style="list-style-type: none"> 1. On the Cisco Catalyst SD-WAN Manager, choose Monitor > Logs. 2. Select Events. Select an event, click ..., select Device Details.

Understand monitoring data

The Monitor dashboard in Cisco Catalyst SD-WAN Manager displays various states, stats, charts and events to help you visualize the VPN solution in the network and identify errors in real time.

Table 2:

Parameter	Description
VPN Endpoints	<p>In a network where there are multiple VPN solutions deployed an endpoint means a device that has VPN configuration.</p> <p>For example, if a device is operating as a Hub, the endpoint count is one on the dashlet. But if the device is operating both as Hub and Spoke, the endpoint count is two.</p> <p>In the same manner, if a FlexVPN solution is deployed, the device operating as FlexHeadend is denoted as one on the dashlet and the device operating as FlexClient is also denoted as another endpoint.</p>
Number of IPSec sessions	<p>An IPSec session indicates an encrypted tunnel for the VPN session. The bar graph shows the top 5 devices that have the most number of active IPSec sessions per VPN solution.</p> <p>If the device has two VPN solutions deployed, the bar graph shows the IPSec sessions for each VPN solution.</p>

Parameter	Description
Role of devices in the network	<p>An SD-Routing device can have multiple VPN roles in a network. If a device is acting both as a Hub and Spoke, the role details are displayed accordingly.</p> <p>If a device has multiple VPN solutions deployed, the VPN Role column in Monitor > Devices page displays the details.</p>
Number of VPN sessions	<p>For communication to be established through a VPN channel, Security Association (SA) are used for incoming and outgoing traffic using IKE negotiations.</p> <p>The VPN sessions column displays the number of IKE related SA's per device and not per VPN solution.</p>
Number of VPN Peers	<p>The VPN peer count column displays the number of IKEv1 or IKEv2 peers per VPN solution.</p> <p>Alarms and events are shown for IKEv1 peers but statistics displayed are supported for both IKEv1 and IKEv2 session.</p> <p> The IPsec encryption used in Cisco DMVPN is based on IKEv2.</p> <p>Note</p>
Crypto Information	<p>This option on the Monitor page shows all crypto information per device. The details displayed are:</p> <ul style="list-style-type: none"> • IKEv1 session and peer counts • IKEv2 session and peer counts <p>If the device has DMVPN configuration, details relevant to Hub and Spoke configuration are displayed. The details displayed include:</p> <ul style="list-style-type: none"> • NHRP cache entries. • Spokes connected to NHS. • Next Hop Server IP • Interface Name • Internal VRF • Front Door VRF • Spokes Registered
All events for devices with Crypto VPN configuration	<p>If the device has crypto configuration, alarms and events are generated at specific intervals to alert the network administrator regarding the functioning of the network and take any action if necessary.</p>