SD-WAN

This chapter describes the SD-WAN capabilities supported in the management center.

SD-WAN Capabilities

Software-Defined WAN (SD-WAN) solutions replace traditional WAN routers and are agnostic to WAN transport technologies. SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

As organizations expand their operations across multiple branch locations, ensuring secure and streamlined connectivity becomes paramount. Deploying a secure branch network infrastructure involves complex configurations, which can be time-consuming and prone to configuration errors if not handled properly. However, organizations can overcome these challenges by leveraging the Cisco Secure Firewall Management Center (management center) and the Cisco Secure Firewall Threat Defense (threat defense) devices for a simplified and secure branch deployment.

In this guide, we explore the concept of simplifying secure branch deployment using a robust firewall solution. By integrating a secure firewall as a foundational component of the branch network architecture, organizations can establish a strong security baseline while simplifying the deployment process. This approach enables organizations to enforce unified security policies, optimize traffic routing, and ensure resilient connectivity.

Some of the SD-WAN capabilities supported on the Cisco Secure Firewall are:

- **Simplified management:**
  - SASE: Umbrella auto tunnel deployment
  - Dynamic VTI (DVTI) hub spoke topology simplification
- **Application awareness:**
  - Direct Internet Access (DIA) for public cloud and guest user
  - Policy based routing (PBR) using applications as a match criteria

- Local tunnel ID support for Umbrella

- **Increased usable bandwidth:**
  - ECMP support for load balancing across multiple ISPs and VTIs
  - Application-based load balancing using PBR
- **High availability with near zero network downtime:**
  - Dual ISP configuration
  - Optimal path selection based on application-based interface monitoring.
- **Secure Elastic Connectivity:**
  - Route-based (VTI) VPN tunnels between headquarters (hub) and branches (spokes)
  - IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP over VTI
  - DVTI hubs that support spokes with static or dynamic IP

Features

The following table lists some commonly used SD-WAN features:

Feature	Introduced in	More Information
Application monitoring using SD-WAN Summary dashboard	Release 7.4.1	SD-WAN Summary Dashboard, on page 4
SD-WAN Summary Dashboard	Release 7.4	SD-WAN Summary Dashboard, on page 4
Policy-based routing with user identity and SGTs	Release 7.4	Policy Based Routing
Policy-based routing using HTTP path monitoring	Release 7.4	Policy Based Routing
Loopback interface support for VTIs	Release 7.3	About Loopback Interfaces
Support for dynamic VTI (DVTI) with site-to-site VPN	Release 7.3	Dynamic VTI
Umbrella auto tunnel	Release 7.3	Deploy a SASE Tunnel on Umbrella
Support for IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP for VTIs	Release 7.3	BGP OSPF EIGRP

Feature	Introduced in	More Information
Route-based site-to-site VPN with hub and spoke topology	Release 7.2	Create a Route-based Site-to-Site VPN
Policy-based routing with path monitoring	Release 7.2	Policy Based Routing
Site to Site VPN Monitoring Dashboard	Release 7.1	Monitor Site-to-Site VPNs Using Site-to-Site VPN Dashboard
Direct Internet Access/Policy Based Routing	Release 7.1	Policy Based Routing
Equal-Cost-Multi-Path (ECMP) zone with WAN interfaces	Release 7.1	ECMP
ECMP zone with VTI interfaces	Release 7.1	ECMP
Backup VTI for route-based site-to-site VPN	Release 7.0	Route Traffic Through a Backup VTI Tunnel
Support for static VTI (SVTI) with site-to-site VPN	Release 6.7	Static VTI

Use Cases for SD-WAN Capabilities

Use the Cisco Secure Firewall Threat Defense SD-WAN Design and Deployment Guide to design and deploy SD-WAN architectures using Firewall Threat Defense and Firewall Management Center. This guide explains design principles, configuration workflows, and best practices.

Use these guides for detailed instructions for the primary use cases leveraging the SD-WAN capabilities supported by Cisco Secure Firewall.

- Simplify Branch to Hub Communication using Dynamic Virtual Tunnel Interface (DVTI)
- Route Application Traffic from the Branch to the Internet Using Direct Internet Access (DIA)
- Secure Internet Traffic Using Umbrella Auto Tunnel
- Empower Remote Workers with Secure Connectivity: DIA, Umbrella Auto Tunnel, and DVTI in Action
- Set Up SD-WAN Branch Office with Dual ISPs Using Registration Key and Device Templates
- Set Up SD-WAN Branch Office with Dual ISPs Using Serial Numbers and Device Template

Monitoring SD-WAN Topologies

-

SD-WAN Summary Dashboard

The SD-WAN Summary dashboard (**Overview** > **Dashboards** > **SD-WAN Summary**) provides a snapshot of your WAN devices and their interfaces. This dashboard helps you to:

- Identify issues with the underlay and overlay (VPN) topologies.
- Troubleshoot VPN issues using the existing **Health Monitoring**, **Device Management**, and **Site-to-Site Monitoring** pages.
- Monitor application performance metrics of WAN interfaces. The threat defense steers application traffic based on these metrics.

A WAN device must meet one of the following criteria:

- The device must be a VPN peer.
- The device must have WAN interface.

A WAN interface must meet one of the following criteria:

- The interface has IP address-based path monitoring enabled on it.
- The interface has a Policy Based Routing (PBR) policy with at least one application configured to monitor it.

For more information about PBR policy and path monitoring, see Policy Based Routing.

Click **Uplink Decisions** to view the **VPN Troubleshooting** page. You can view syslogs with ID: 880001. These syslogs show the threat defense interfaces through which it steers traffic based on the configured PBR policy.

To view the above syslogs and to view the data on this dashboard, ensure that you review Prerequisites for Using SD-WAN Summary Dashboard, on page 4.

For clusters, this dashboard displays application performance metrics of only the control node and not the data nodes.

Prerequisites for Using SD-WAN Summary Dashboard

- You must be an Admin, Security Analyst, or Maintenance user to view this dashboard.
- Threat defense devices must be Version 7.2 or later.
- Enable IP-based path monitoring and HTTP-based application monitoring on the WAN interfaces.
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click the edit icon adjacent to the interface that you want to edit.
  4. Click the **Path Monitoring** tab.
  5. Check the **Enable IP based Monitoring** check box.
  6. Check the **Enable HTTP based Application Monitoring** check box.
  7. Click **OK**.

- Configure a PBR policy with at least one application configured to monitor it:
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **Policy Based Routing**.
  5. Click **Add**.
  6. From the **Ingress Interface** drop-down list, choose an interface.
  7. Click **Add** to configure a forwarding action.
  8. Configure the parameters.
  9. Click **Save**.

- To view the application performance metrics for the WAN interfaces, you must:
  - Threat defense devices must be Version 7.4.1.
  - Enable data collection from the SD-WAN module in the health policy.
    1. Choose **System** (⚙) > **Health** > **Policy**.
    2. Click the **Edit health policy** icon.
    3. In the **Health Modules** tab, under **SD-WAN**, click the **SD-WAN Monitoring** toggle button.
  - Configure applications for the PBR policies.
    1. Choose **Objects** > **Object Management** > **Access List** > **Extended**.
    2. Click the edit icon adjacent to the access list and add the applications for the PBR policy.
  - Configure the forwarding action for the policy with one of the four application metrics.
    1. Choose **Devices** > **Device Management**.
    2. Click the edit icon adjacent to the device that you want to edit.
    3. Click **Routing**.
    4. In the left pane, click **Policy Based Routing**.
    5. Click the edit icon adjacent to the policy that you want to edit.
    6. In the **Edit Policy Based Route** dialog box, click the edit icon adjacent to the corresponding ACL.
    7. In the **Edit Forwarding Actions** dialog box, from the **Interface Ordering** drop-down list, choose one of the following options:
       - **Minimal Jitter**
       - **Maximum Mean Opinion Score**
       - **Minimal Round-Trip Time**

- **Minimal Packet Loss**

If you choose **Interface Priority** or **Order**, application monitoring is not enabled on the interface.

- Configure ECMP on the WAN interfaces:
  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon adjacent to the device that you want to edit.
  3. Click **Routing**.
  4. In the left pane, click **ECMP**.
  5. Click **Add** and specify a name for the ECMP zone.
  6. Click **Add** to move interfaces from **Available Interfaces** to **Selected Interfaces**.
  7. Click **OK**.
- Ensure that traffic passes through the interface.
- Enable DNS inspection on each WAN device so that the threat defense device can do DNS snooping, and configure the trusted DNS servers:
  1. Choose **Devices** > **Platform Settings**.
  2. Click the edit icon adjacent to the threat defense policy that you want to edit.
  3. In the left pane, click **DNS**.
  4. Click the **DNS Settings** tab.
  5. Check the **Enable DNS name resolution by device** check box.
  6. Click the **Trusted DNS Servers** tab.
  7. Do one of the following:
     - Click the **Trust Any DNS server** toggle button.
     - Under **Specify DNS Servers**, click **Edit** to add trusted DNS servers.

- To view syslogs when you click **Uplink Decisions**, you must:
  - Choose **Devices** > **Platform Settings** and create or edit a threat defense policy.
  - In the left pane, click **Syslog**.
  - Click the **Logging Setup** tab.
  - Check the **Enable Logging** check box to turn on the data plane system logging for the threat defense device.
  - Click the **All Logs** radio button to enable logging of all the troubleshooting syslog messages.

    or

    Click the **VPN Logs** radio button to enable logging of only the VPN troubleshooting messages.

- Click **Save**.

Monitor WAN Devices and Interfaces Using the SD-WAN Summary Dashboard

The SD-WAN Summary dashboard has the following widgets under the **Overview** tab:

Top Applications

This widget displays the top 10 applications ranked according to throughput.

You can choose a time range for the widget data from the **Show Last** drop-down list. The range is 15 minutes to two weeks.

WAN Connectivity

This widget provides a summary of the WAN interfaces statuses. It shows the number of WAN interfaces that are in the **Online**, **Offline** or **No Data** states. Note that you cannot monitor subinterfaces using this widget.

Click **View All Interfaces** to view more details about the interfaces in the health monitor page.

If a WAN interface is in the **Offline** or **No Data** state, you can troubleshoot it from the health monitor page:

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click the **Interface** tab to view the interface status and aggregate traffic statistics for a specific time.

   Alternatively, you can click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

VPN Topology

This widget provides a summary of the site-to-site VPN tunnel statuses. It shows the number of **Active**, **Inactive**, and **No Active Data** VPN tunnels.

Click **View All Connections** to view the VPN tunnel details in the **Site-to-site VPN Monitoring** dashboard.

If the tunnels are in the **Inactive** or **No Active Data** state, you can troubleshoot using the **Site-to-site VPN Monitoring** dashboard. In the **Tunnel Status** widget, hover your cursor over a topology, click **View** ( ) and do one of the following:

- Click the **CLI Details** tab to view the details of the VPN tunnels.
- Click the **Packet Tracer** tab to use the packet tracer tool for the topology.

Interface Throughput

This widget monitors the average throughput of the WAN interfaces during the chosen time period.

The interface throughput is classified into four bands. These details aid in cost planning and resourcing. You can choose a time range for the widget data from the **Show Last** drop-down list. The range is from 15 minutes to two weeks.

Click **View Health Monitoring** to view more details about the interface in the health monitor page.

Device Inventory

This widget lists all the managed WAN devices and groups them according to the model.

Click **View Device Management** to view more details about the device in the **Device Management** page.

WAN Device Health

This widget displays the device count according to the health of the WAN devices. You can view the number of devices with errors, warnings, or those that are in **Disabled** state.

Click **View Health Monitoring** to view the alarms, and quickly identify, isolate, and resolve issues.

If the health of a device is affected, you can troubleshoot it from the health monitor page.

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

A device can be in **Disabled** state for multiple reasons, including the following:

- Management interface is disabled.
- Device is powered off.
- Device is being upgraded.

Monitor Application Performance Metrics of WAN Interfaces Using the SD-WAN Summary Dashboard

Under the **Application Monitoring** tab, you can select a WAN device and view the application performance metrics for the corresponding WAN interfaces. These metrics include Jitter, Round Trip Time (RTT), Mean Opinion Score (MOS), and Packet Loss.

By default, the metrics data is refreshed every 5 minutes. You can change the refresh time; the range is from 5 to 30 minutes. You can view the metrics in tabular and graphical formats. For each WAN interface, the latest metric value appears in the table. For graphical data, you can choose a time interval of up to 24 hours to view the metrics data for the corresponding WAN interfaces.