Cisco Software-Defined WAN (SD-WAN)

**What is the Cisco SD-WAN solution?**

A. Traditional WANs, where the majority of branch office traffic flows within an enterprise’s intranet boundary, have been designed using Multiprotocol Label Switching (MPLS) for connectivity. However, new cloud applications such as Microsoft Office 365 and Salesforce.com, and public cloud services such as Amazon Web Services (AWS) and Azure are changing traffic patterns. Today, the majority of enterprise traffic flows to public clouds and the internet. This change creates new requirements for security, application performance, cloud connectivity, WAN management, and operations.

Cisco® SD-WAN is a cloud-delivered overlay WAN architecture connecting branches to data center and multicloud environments through a single fabric. Cisco SD-WAN helps ensure a predictable user experience for applications; optimizes Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS) connections; and offers integrated security either on-premises or in the cloud. Analytics capabilities deliver the visibility and insights necessary to isolate and resolve issues promptly and deliver intelligent data analysis for planning and what-if scenarios. Cisco SD-WAN provides all of this and is, above all, simple to operate.

- **Predictable application experience:** Increase user productivity by optimizing cloud and on-premises application performance with real-time analytics, visibility, and control.
- **Right security, right place:** Protect users, devices, and applications by deploying embedded or cloud security faster with the best threat intelligence.
- **Simplicity at enterprise scale:** Centralize cloud management to make it easy to deploy SD-WAN and security while maintaining policy across thousands of sites.

**What problems does the Cisco SD-WAN solution help solve?**

The Cisco SD-WAN solution solves many critical enterprise IT problems, including:

- Establishing a transport-independent WAN for lower cost and higher diversity
- Meeting Service-Level Agreements (SLAs) for business-critical and real-time applications on-premises and in the cloud
- Providing complete security from branch to SaaS and internet
- Enabling secure multicloud transformation for enterprises
- Providing centralized management, analytics, and policy across the global WAN

**Who has deployed the Cisco SD-WAN solution?**

Cisco has one of the most widely deployed enterprise-grade SD-WAN solutions in the industry, with large deployments in many sectors in both enterprise and managed service provider infrastructures. The solution is deployed across Fortune 2000 enterprises, with thousands of production sites in every major industry, including healthcare, manufacturing, retail, energy, oil and gas, insurance, finance, government, logistics, distribution, and more.
**How do you manage and operate Cisco SD-WAN?**
Cisco SD-WAN is a centrally managed, orchestrated, and operated solution with a cloud-hosted Cisco vManage GUI management and provisioning platform, vSmart controller, and vBond orchestration layer at the heart of the solution.

**vSmart controllers** are the centralized brain of the solution; they implement policies and connectivity between SD-WAN branches. The centralized policy engine in Cisco vSmart controllers provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.

The entire solution is managed with **Cisco vManage**, Cisco’s GUI-based centralized management and provisioning platform for day 0, day 1, and day n+ for the entire Cisco SD-WAN infrastructure. You can log in to the Cisco vManage dashboard to centrally manage the WAN. Cisco vManage provides the ability to manage all aspects of the WAN, from provisioning, monitoring, and upgrading routers to maintaining application visibility and troubleshooting the WAN.

**What are the SD-WAN security features?**
Cisco SD-WAN offers a full range of integrated security functionality that can be enabled on-premises or by Cisco Umbrella cloud security. Both security architectures provide full protection for enterprises connecting to cloud and internet applications. These security features are:

**Enterprise firewalls**: Granular policy and control of thousands of applications

**Secure web gateway**: Full protection against all kinds of web-based attacks, including SSL inspection

**DNS layer security and URL filtering**: Stops threats at the earliest point, significantly reducing incidents

**IPS**: A built-in intrusion prevention system within an on-premises enterprise firewall based on Snort® and powered by Talos®

**Cloud Access Security Broker (CASB)**: Protects against account compromises, breaches, and other major risks in the cloud application ecosystem

**Malware protection**: An extended security feature across both on-premises and cloud security using Cisco AMP and Threat Grid to prevent and detect malicious files with sandboxing

**How is Cisco SD-WAN deployed at branch offices and data center networks or regional hubs?**
Branch office and regional data center hub sites can be deployed and connected using either virtual or physical secure routers.

Enterprise customers and service providers can gain rich services such as WAN optimization and firewall or basic WAN connectivity for physical or virtual platforms across the branch, WAN, or cloud as follows:

**Physical**
- Branch: Cisco IOS® XE and Viptela OS based devices.
- Branch: Cisco Catalyst 8300 Series Edge Platforms and Cisco 1000, 1100, or 4000 Series Integrated Services Routers (ISR).
- Branch, regional hub, or data center: Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers (ASR).

**Virtual**
- SD-Branch: Cisco 5000 Series Enterprise Network Compute System (ENCS) and Integrated Services Virtual Router (ISRv).
- Network hub, colocation facility, or data center: Cisco Cloud Services Platform 5000 and Cloud Services Router (CSR) 1000V Series (CSR).

**Public Cloud (IaaS)**
- Amazon Web Services.
- Microsoft Azure.
- Google Cloud Platform.
**Does the Cisco SD-WAN solution support network segmentation, and what are the benefits?**

Yes, the Cisco SD-WAN solution supports network segmentation. Segmentation provides secure logical isolation on the SD-WAN network, where each segment is defined as a separate VPN and controlled centrally by access-control policies. Some of the benefits of segmentation include:

- Increased security: Isolate your network from outside attackers and create secure separation within multiple application segments.
- Acquisitions can be integrated on the parent network and yet kept separate. Policies control what applications the acquired company can access.

For more information, see the [Segmentation (VPN) Overview](#).

**What are the SD-WAN security capabilities, and which platforms support SD-WAN security?**

Cisco SD-WAN security capabilities include an application-aware enterprise firewall, intrusion prevention, DNS layer enforcement (Cisco Umbrella), and URL filtering. Cisco SD-WAN reduces complexity by having a single management interface (vManage) for both the network and security.

Platform support for SD-WAN security is as follows:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Enterprise firewall</th>
<th>Enterprise firewall application awareness</th>
<th>Intrusion prevention system</th>
<th>URL filtering</th>
<th>Advanced Malware Protection and ThreatGrid</th>
<th>Full cloud security with Cisco Umbrella</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 1000 Series ISRs, vEdge 100, 1000, 2000, and 5000 routers</td>
<td>Yes</td>
<td>DPI using Qosmos</td>
<td>X</td>
<td>X</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco CSR 1000V</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco ISRv, 5000 Series ENCS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 8300-1N1S and 8300-2N2S</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 4451, 4351, 4331, 4321, and 4221 ISRs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 1111X-8P ISR</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco 1111-4P, 1111-8P, 1116-4P, and 1117-4P ISRs</td>
<td>Yes</td>
<td>Yes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Catalyst 8500-12X and 8500-12X4QC</td>
<td>Yes</td>
<td>Yes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco ASR 1001-HX, 1002-HX, 1001-X, and 1002-X</td>
<td>Yes</td>
<td>Yes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Can the Cisco SD-WAN solution provide insight into threats in encrypted traffic, without the need for decryption?

Encrypted Traffic Analytics (ETA) for the Cisco SD-WAN solution is not currently supported but is planned to be introduced in the future. For more information on ETA, see https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html.

Can the Cisco SD-WAN solution provide optimization for IaaS and SaaS platforms such as AWS, Microsoft Azure and Office 365, Google, Salesforce.com, Cisco Webex®, etc.?

The Cisco SD-WAN fabric connects users at the branch to applications in the cloud in a seamless, secure, and reliable fashion. Cisco delivers this comprehensive capability for IaaS and SaaS applications with Cisco Cloud OnRamp, which is currently available with vEdge platform SD-WAN solutions.

With Cloud OnRamp, the SD-WAN fabric continuously measures the performance of a designated application through all permissible paths from a branch (MPLS, internet, 4G LTE, etc.). The Cisco SD-WAN fabric automatically makes real-time decisions to choose the best-performing path between the end users at a remote branch and the cloud application. Enterprises and service providers have the flexibility to deploy this capability in multiple ways and according to business needs and security requirements.


What is the difference between Cisco SD-WAN and Cisco Meraki® SD-WAN?

Cisco SD-WAN can help your business no matter its size with a variety of deployment options. For lean IT operations, Cisco SD-WAN powered by Meraki is preferred, and for full-featured, sophisticated deployments, Cisco SD-WAN powered by Viptela is preferred.

- **Lean IT**: Deploy Cisco SD-WAN powered by the Meraki MX unified threat management hardware, and enjoy a unified, secure SDWAN for businesses with lean IT teams.
- **Branches and campuses**: With both physical and virtual options, you can deploy Cisco SD-WAN on Cisco vEdge, Catalyst 8000V, CSR 1000V, Catalyst 8300 Series, 1000 and 4000 Series ISRs, or with Network Functions Virtualization (NFV) using Cisco SD-Branch with the ISRv on the 5000 Series ENCS and Cisco UCS®-E platforms.
- **Headquarters, data center, and colocation**: With physical or virtual options, deploy Cisco SD-WAN on Cisco Catalyst 8500 Series, ASR 1000 Series routers, or with NFV and network hub solutions on the Cloud Services Platform 5000.

How is the Cisco SD-WAN solution ordered?

Cisco SD-WAN software is included with each vEdge routing device and platform and can be enabled on some Cisco 1000 and 4000 Series ISRs, Catalyst 8300 Series, Catalyst 8500 Series, ASR 1000 Series routers, the ISRv on the 5000 Series ENCS, and the Catalyst 8000V or CSR 1000V on the Cloud Services Platform 5000 Series with the latest Cisco IOS XE software. For a list of SD-WAN-capable Cisco IOS XE platforms, see the SD-WAN Release Notes.

Each device requires a subscription license (3 or 5 years) for Cisco SD-WAN software. The license fee is charged per branch device and is dependent on service bandwidth and feature content, with a single set of software licenses that includes security and access to ongoing innovation and the latest threat intelligence. License bundles include:
FAQ
Cisco public

- **Cisco DNA Essentials**: Includes basic connectivity, security, and application visibility.
- **Cisco DNA Advantage**: Includes everything in Cisco DNA Essentials plus application optimization, multicloud, on-premises security, etc.
- **Cisco DNA Premier (replaces Cisco ONE™)**: Includes everything in Cisco DNA Essentials and Cisco DNA Advantage plus the Cisco Umbrella SIG Essentials package.


The subscription price of SD-WAN software includes cloud-hosted vManage, vSmart, and vBond devices, 24-hour daily Cisco SD-WAN support, next-day hardware replacement for Cisco SD-WAN platforms, software upgrades on all components, and the cost of hosting Cisco SD-WAN controllers in the Cisco SD-WAN cloud.


**Are the Cisco DNA subscription licenses portable and able to be moved to another hardware platform?**

Yes, the Cisco DNA software licenses are portable and can be moved across routing platforms, including 1000 and 4000 Series ISR, Catalyst 8300 Series, Catalyst 8500 Series, ASR 1000 Series, 5000 Series ENCS, and Cisco vEdge routers. With software portability you have investment protection for your licenses, regardless of which Cisco routing platform you choose now or upgrade to in the future.


**Does the Cisco SD-WAN solution support multitenancy?**

Yes, a service provider can manage multiple customers, called tenants, from vManage that is running in multitenant mode. All tenants share a single vBond orchestrator. All tenants share the service provider’s domain name, with each tenant having a subdomain name to identify the tenant. For example, the service provider fruit.com might manage the tenants mango (mango.fruit.com) and plum (plum.fruit.com). For each tenant, you configure one or more vSmart controllers and vEdge routers in the same way that you configure these devices on a single-tenant vManage Network Management System (NMS).

For more information, see [https://sdwan-docs.cisco.com/Product_Documentation/Getting_STARTED/Viptela_Overlay_Network_Bringup/03Deploy_the_vManage_NMS/07Create_a_Multitenant_vManage_NMS](https://sdwan-docs.cisco.com/Product_Documentation/Getting_STARTED/Viptela_Overlay_Network_Bringup/03Deploy_the_vManage_NMS/07Create_a_Multitenant_vManage_NMS).

**Is Cisco’s SD-WAN solution programmable, and does it support APIs?**

Yes, the Cisco SD-WAN solution is open and programmable, with open APIs. Cisco SD-WAN provides service providers and partners the opportunity to create new and unique services, including operational and business support systems. With Cisco SD-WAN you can access the available Representational State Transfer (REST) APIs, create API calls, obtain device and interface information using code, pass parameters and write applications, and work on innovative solutions.

As part of the SD-WAN developer resources and learning content, there are two additional resources that are great value-added services for developers:

- **DevNet Ecosystem Exchange** makes it easy to find and share an application or solution built for Cisco platforms. Business leaders and developers alike can use this online portal to discover partner solutions that span all Cisco platforms and products. Currently, this central repository for developers contains over 1300 solutions.
DevNet Code Exchange gives developers a place to access and share software to quickly build next-generation applications and workflow integrations. It offers a curated list of sample code, adapters, tools, and SDKs available on GitHub and written by Cisco and the DevNet community. Code Exchange spans Cisco’s entire portfolio and is organized according to Cisco platform and product areas.

For more information, see the SD-WAN Developer Center at https://developer.cisco.com/sdwan.

**Where can I find more information on Cisco SD-WAN?**

For more information about Cisco SD-WAN, visit [https://www.cisco.com/go/sd-wan](https://www.cisco.com/go/sd-wan).

**What are the voice and application optimization features that Cisco SD-WAN supports?**

- Cisco has the only SD-WAN solution with full integrated unified communications support.
- On voice optimization, Cisco SD-WAN supports FEC and packet duplication.
- On internet optimization, Cisco SD-WAN supports TCP optimization.
- For on-premises applications, Cisco SD-WAN support SLA-based dynamic routing based on real-time network telemetry.
- For SaaS applications, Cisco provides dynamic routing based on cloud and internet telemetry.

**Are there any services available to support my SD-WAN solution?**

Regardless of where you are in your journey, Cisco Services offers a full lifecycle of services to support your transition. Our portfolio allows you to create a roadmap for success, speed deployment, and maximize network performance, security, uptime, and efficiency. Cisco experts will help you build your in-house IT expertise and effectively migrate and manage your SD-WAN solution to achieve high service levels at lower costs. [Learn more.](https://developer.cisco.com/sdwan)

**How is Cisco SD-WAN integrated with Cisco Umbrella cloud security?**

Cisco SD-WAN provides complete integration with Cisco Umbrella cloud security. Using Cisco vManage, auto registration and auto setup of tunnels to the Cisco Umbrella cloud can be executed within a few minutes, such that the enterprise is completely protected.