Introduction to Cisco Catalyst SD-WAN for Government

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst Controller**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Cisco Catalyst SD-WAN for Government Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing.

FedRAMP, the Federal Risk and Authorization Management Program, is a U.S.-government program that establishes a standardized approach for assessing, authorizing, and monitoring cloud service providers.

Cisco Catalyst SD-WAN for government incorporates encryption and security at its core:

- Creates a restricted space called the federal boundary within the AWS GovCloud (U.S.).
- Restricts access to federally cleared personnel.

- Runs in Federal Information Processing Standard (FIPS) mode for all controllers.
- Ensures that all data and control connections are Secure Hash Algorithm 2 (SHA-2) compliant.
- Provides enhanced user session management.
- Performs a real-time audit at the controller level.
- Provides an automated Plan of Actions and Milestones (POA&M) report.
- Enables customers to have their own dedicated Amazon Virtual Private Cloud (Amazon VPC) that automatically denies all HTTP requests unless specifically authorized.
- Ensures protection by AWS services such as AWS Application Load Balancer (ALB), AWS Web Application Firewall (WAF), and AWS Shield. All the web services are behind the ALB and WAF for protection. They are also protected from distributed denial of service (DDoS) attacks by the AWS Shield.
- Uses a role-based access without local users for Cisco Federal Operations, a Cisco team that maintains and monitors the environment.

Cisco Catalyst SD-WAN for government conducts monthly penetration testing through Third-Party Assessment Organizations (3PAOs). In addition to this, Qualys performs daily penetration scanning. Qualys is a component of the management Amazon VPC. For more information, see the Cisco Catalyst SD-WAN for Government Components, on page 3 section.

For more information on the general Cisco Catalyst SD-WAN security configuration, see the Security Configuration Guide, Cisco IOS XE Release 17.x.

Supported Platforms

For a complete list of the supported platforms for Cisco Catalyst SD-WAN for government, see the Supported Devices section of the Release Notes document for Cisco IOS XE Catalyst SD-WAN devices.

To be FedRAMP-compliant, ensure that you run Cisco vManage Release 20.3.1 and Cisco IOS XE Catalyst SD-WAN Release 17.3.1a or later releases.

Note If you are using a hardware router, your device must be TAA-compliant. When ordering a device, ensure that the device's SKU is appended with ++. This indicates that the device is TAA-compliant. For more information, contact your Cisco sales representative.

Intended Audience

There are two types of users for Cisco Catalyst SD-WAN for government:

- Customers, such as service providers, partners, and other end users.
- Cisco Federal Operations (FedOps): A Cisco team that maintains and monitors Cisco Catalyst SD-WAN for government.

Note Cisco FedOps cannot access the customers' Amazon VPCs.

Cisco Catalyst SD-WAN for Government Components

The Cisco Catalyst SD-WAN for government cloud boundary has a customer Amazon VPC and a management Amazon VPC. Individual customers have their own exclusive Amazon customer VPCs.

VPC	Components	User Access
Customer	Cisco Catalyst SD-WAN solution includes: Cisco SD-WAN Manager, Cisco SD-WAN Validator, Cisco SD-WAN Controller, Cisco IOS XE Catalyst SD-WAN devices, and other applications.	Customers
Management	Cisco Catalyst SD-WAN Portal (SSP): Sets up and monitors Cisco Catalyst SD-WAN overlay networks. Cisco vMonitor: Monitors the system for vulnerabilities and system failures. Cisco vOrchestrator: Assists in creating the customer VPC. Wazuh server: Monitors data from the Wazuh (FIM server client). Qualys: Scans for penetration testing. Cisco Data Management Service (DMS): Provides data storage location services for Cisco SD-WAN Manager to send customer telemetry data. Cisco Data Collection Agent (DCA): Collects data regarding the health of the system. Pushes data to the Data Collection Service (DCS). Cisco Data Collection Service (DCS): Acts as the entry point for all telemetry data in the system. Jira (Atlassian): Refers to a hardened instance of Jira that automatically creates incidents for vulnerabilities found in the system. Amazon Web Services (AWS) Bastion host: Provides a secure login mechanism for Cisco FedOps.	Cisco FedOps **Note**: To manage their overlay networks, customers can access the Cisco Catalyst SD-WAN Portal that is hosted in the management VPC.

In addition to the components listed in the table, to assist with the flow of data, the Cisco Catalyst SD-WAN for government solution uses Amazon Web Services' (AWS) Simple Queue Service (SQS), AWS Application Load Balancer (ALB), AWS Web Application Firewall (WAF), and the Amazon Aurora MySQL database. The network access control list (ACL) of the management Amazon VPC is managed using a Cisco Catalyst SD-WAN for government-approved instance of Okta.

Federal Boundary

The federal boundary for Cisco Catalyst SD-WAN for government contains a customer Amazon VPC and an Amazon management VPC. Individual customers have their own Amazon VPC.

The Cisco Catalyst SD-WAN for government's federal boundary is a restrictive environment that has only two entry points for each customer:

- Customer Amazon VPC
- Management Amazon VPC

Customer Access to the Amazon Virtual Private Cloud

Only customers can access their customer Amazon VPC.

When customers set up their overlay network, it includes the following Cisco Catalyst SD-WAN components:

- Cisco SD-WAN Manager
- Cisco SD-WAN Controller
- Cisco SD-WAN Validator

How Customers Access their Customer Amazon VPC

To access their customer Amazon VPC, customers must allow the Cisco Catalyst SD-WAN Portal to allow trusted IP addresses to access their overlay network.

Management Access to the Amazon Virtual Private Cloud

The management Amazon VPC provides secure monitoring and end-to-end auditing of the Cisco Catalyst SD-WAN for government solution. An Amazon VPC is a secure location within the Amazon cloud with a set of allowed IP addresses and port numbers.

The only component customers can access in the management Amazon VPC is the Cisco Catalyst SD-WAN Portal. The other components in the Cisco Catalyst SD-WAN Portal are only accessible to Cisco FedOps.

How Can Cisco FedOps Access the Management Amazon VPC

1. Connect to the Cisco network using the Cisco AnyConnect Secure Mobility Client.
2. Log in to the Cisco Catalyst SD-WAN Portal.

   When a Cisco FedOps user logs in, the request goes through an AWS bastion host, which provides Secure Shell (SSH) access to the management Amazon VPC.
3. Use the Okta Advanced Server for multi-factor authentication (MFA).

Note Only authorized users who belong to the specified group in the Okta Identity Provider (IdP) can access the AWS bastion host.

4. After the log in is authenticated, Cisco FedOps can connect to any device in the management Amazon VPC.

Data Flow

In the Cisco Catalyst SD-WAN for government solution, Cisco vMonitor collects data and logs from a variety of systems to check the health of the system and identify issues. Cisco vMonitor uses the following sources:

- Cisco Data Collection Agents (DCA): These agents are used to collect health data from Cisco Catalyst SD-WAN for government. Data from all these Cisco DCAs is then sent to the Cisco Data Collection Service (DCS).
- Wazuh server: Monitors data from the Wazuh File Integrity Monitoring (FIM) server client. The controllers for the Cisco Catalyst SD-WAN for government solution have a built-in FIM server that collects audit logs and syslog changes. These changes are monitored by the Wazuh server for vulnerability vectors. All the data that is collected by the Cisco vMonitor server, and the vulnerabilities, are tagged and provided as POA&M reports.
- Okta: Cisco vMonitor polls the external Okta server that is used for MFA for Okta's logs on authentication and access attempts.
- Qualys: Qualys performs vulnerability and compliance scans. This scanning is done on all the data in the customer Amazon VPC, and on every component in the management Amazon VPC, on a daily basis. The results of the scans are recorded in the Cisco vMonitor database.

Every connection, the location where data is stored, and file incident management events are pushed to the Cisco vMonitor database. If a critical issue is detected, the Cisco vMonitor database files a JIRA ticket and a POA&M alert. For more information on the JIRA tickets and POA&M alerts, see Plan of Action and Milestones.

To ensure that data is secure, it is stored in AWS S3 buckets. All the data (at rest and in transit) and control connections are SHA-2 compliant. The following types of data are stored:

- Personal Identifiable Information (PII)
- Domains accessed
- Private IP addresses
- Customers that have accessed the solution
- Any sniffing that occurs on the network

Data Collection Agent Configuration and Monitoring

The Cisco DCA is an agent that runs inside Cisco SD-WAN Manager, which can be hosted either on-premises or in the cloud. This Cisco DCA agent is used to report statistics, monitor, and provide telemetry data to Cisco Catalyst SD-WAN as long as the appropriate configurations are enabled.

To achieve this, the Cisco DCA contacts a service known as the Cisco DMS, which has relevant information regarding a customer's overlay network, for example, which region the network is located in, what are the data storage preferences, and so on. The Cisco DCA authenticates itself with the Cisco DMS using the custom oAuth credentials that are generated per customer overlay network (and communicated out of band to the customer). If the Cisco DMS is able to authenticate the Cisco DCA, the former gives the latter an authentication token and redirects the Cisco DCA to the appropriate Cisco DCS.

The Cisco DCS is the entry point for all telemetry data to get into Cisco Catalyst SD-WAN. There may be many instances of the Cisco DCS service depending on the public cloud, region, and so on. The Cisco DCA uses the token obtained in the prior flow to authenticate itself with the Cisco DCS and exchanges it for a regional Cisco DCS token. Thereafter, this token is used by the Cisco DCA when pushing all kinds of data to the Cisco DCS.

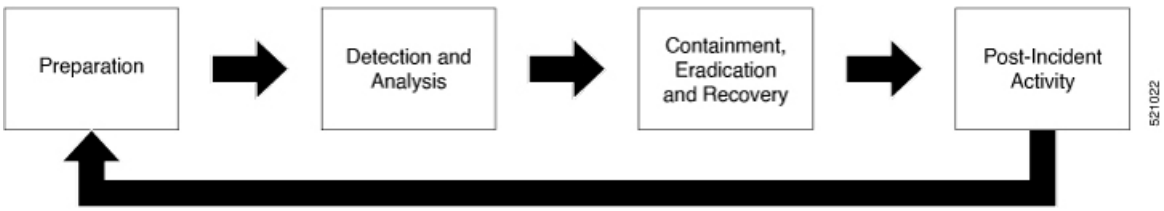
The Cisco DCA periodically collects data from its Cisco Catalyst SD-WAN localhost and pushes that data to the Cisco DCS. The Cisco DCS in turn, saves the data as JSON files in the S3 bucket. For every new JSON file that the S3 bucket receives, a new-object-created event is sent to an AWS Simple Notification Service (SNS) topic. Since Cisco vMonitor has already subscribed the topic with an HTTPS endpoint, Cisco vMonitor servers receive HTTPS requests from an AWS SNS for all the S3 new-object-created events. Cisco vMonitor servers validate the HTTPS request and use the metadata inside to fetch the actual files on S3 and update the database.

Incident Response

Incident response provides a consistently effective means of responding to and reporting on security incidents of the system. It encompasses all the actions taken to quickly restore normal information technology (IT) services and to minimize adverse impacts on business operations. Cisco Catalyst SD-WAN follows the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Rev 2 definitions of an incident in determining when to activate the incident response team. The incident response plan coordinates with Cisco resources on an ongoing basis to remain prepared to identify, contain, eradicate, and recover from any incidents, if any, to the offering.

Responding to a security incident is not a single action, but an entire approach. This approach ensures that issues are detected and mitigated. The approach also has a step to recover from issues, if any, that were detected. It encompasses the following phases:

Figure 1: Incident Response Phases



Workflow for Using Cisco Catalyst SD-WAN for Government

To use Cisco Catalyst SD-WAN for government, you must do the following:

1. Log in to the Cisco Catalyst SD-WAN Portal.
2. Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric
3. Configure Cisco SD-WAN Manager.
4. Set up additional security features.
5. Monitor and manage your environment.