The bridge to possible

Cisco Catalyst SD-WAN Service Insertion

The bridge to possible

Overview

Q: How can I insert security services with Cisco Catalyst™ SD-WAN?

A: Cisco Catalyst SD-WAN provides a choice of security capabilities that include:

- Next-generation firewall embedded within the SD-WAN routers.

- Security Service Edge (SSE) integrations with Cisco and third-party vendors – Cisco Umbrella®, Zscaler, Netskope, etc.

- Automated service insertion (new): Customers will also have a choice of inserting Cisco® or third-party physical or virtual services.

Q: What is Cisco Catalyst SD-WAN Service Insertion?

A: Cisco Catalyst SD-WAN Service Insertion abstracts and automates the on-demand chaining and insertion of services into the SD-WAN fabric. It has the capability to attach any service (physical or virtual, Cisco or third party) to physical or virtual SD-WAN routers anywhere (on-premises, in the cloud, or in a colocation facility). The automation provides intent-based workflows to chain multiple services and enable traffic steering through service-chain policy. This capability also offers the mechanisms to

implement bidirectional traffic symmetry, as well as multiple ways to attach services, including IPv4, IPv6, dual-stack, and tunneling.

Q: When is the solution available?

A: The solution is available beginning with Cisco IOS® XE SD-WAN Release 17.13 and Cisco Catalyst SD-WAN Release 20.13, scheduled for the end of 2023.

Q: What problems does Cisco Catalyst SD-WAN Service Insertion help solve?

A: SD-WAN Service Insertion helps solve problems inherent to the traditional style of service insertion, such as complexities around orchestrating service chaining and traffic steering, as well as restrictions to the types, form factors, and locations of services. It also helps to solve issues that arise when defining policies, classifying specific traffic, and routing to service nodes. Additionally, it overcomes common problems such as service scaling, load balancing, building resiliency, asymmetric routing, and suboptimal pathing.

Q: What are benefits of Cisco Catalyst SD-WAN Service Insertion?

A: Benefits include:

- **Simplified IT:** Simplify configuration and management of service chains across the network.

- **Reduced operations:** Reduce operation cycles via automated service insertion and visibility of one or more services on any router located anywhere.

- **Enhanced security:** Bring your own service and enhance network security posture with consistent policy across multicloud and on-premises environments.

Q: What are the key capabilities of SD-WAN Service Insertion?

A: Key capabilities include:

- **On-demand services insertion:** Automation to easily insert services into the Catalyst SD-WAN fabric.

- **Intent-based automation:** Orchestration workflows capture and execute on the service insertion intent to build and attach the service chain.

- **Service Chaining:** Chain up to four different services without the need to manually stitch them together.

- **Any service:** Bring any Cisco or third-party services to be inserted.

- **Any location:** Services can be located anywhere – on-premises, in colocation facilities, or in the cloud.

- **Any form factor:** Services can be virtual or physical in nature. Similarly, the SD-WAN router acting as the service chain hub can have a virtual or physical form factor.

- **Flexible traffic selection for service application:** Use control policy, data policy, and/or interface ACL to match traffic and steer it towards a service chain.

- **Define once, deploy multiple times:** Different service chain definitions and configurations can be created and used repeatedly to deploy the appropriate service chain at the desired location at the desired time.

Q: What are the key features of SD-WAN Service Insertion?

A: Key features include:

- Service chaining for inter- and intra-VPN, transit, branch-to-branch, branch-to-internet, branch-to-cloud, and cloud-to-cloud traffic.

- Automatic forwarding through all services in a chain.

- Multiple ways to attach services: IPv4, IPv6, dual-stack, and tunneled.

- Built-in load balancing and high availability across instances of a single service.

- Path preference and symmetric routing.

- Advanced service tracking.

- Ability to share a service chain across multiple user VPNs.

- Powerful traffic steering methods that use control policy, data policy, and interface Access Control Lists (ACLs) and all supported match conditions.

- Fail-open, fail-close behavior: configurable option to block or allow traffic, in case of service failure.

- Special features for security services: To- and from-service transports, trusted and untrusted postures, firewall between devices.

- Serviceability: Periodic, on-demand, and state notifications.

- Orchestration via Catalyst SD-WAN Manager: Workflow-based service chaining, traffic policy configuration.

Q: What are the key terms when discussing SD-WAN Service Insertion?

A: The key terms used when discussing Service Insertion include:

- **Service chain definition:** Ordered sequence of services defined by the operator.

- **Service chain instance:** An actual instance of the services defined in the service chain definition. Services in the chain can be physical or virtual.

- **Service chain policy:** Traffic policy to identify what types of traffic are to be subjected to what specific service chains.

- **Service chain hub:** A Catalyst SD-WAN router where the service chain is attached. The hub forwards traffic toward a service chain based on the service chain policy and then sends it onward to the destination.

- **Service chain advertisement:** An advertisement from a service chain hub that identifies which particular service chain is reachable through it.

Q: What improvements have been made compared to previous versions of service insertion?

A: The new SD-WAN Service Insertion feature is a complete architectural revamp of the earlier feature. It consists of innovations across all aspects of service insertion networking. It offers:

- Native support for multiple services in a chain.

- Selective service chaining using a rich set of match criteria in data, control, and interface ACL policies.

- The ability to attach to services in multiple ways (IPv4, IPv6, dual stack, and tunneling).

- A rich set of high-availability and load-balancing features.

- Advanced tracking of the chain.

- Deployment anywhere (on-premises, in the cloud, in a colocation facility).

Deployment and management

Q: What are the key steps in deploying SD-WAN Service Insertion?

A: Key steps for deploying SD-WAN Service Insertion are:

1. Define the service chain: Define the services in the chain and their sequence.

2. Attach it to the hub router: Configure the service chain parameters and attach it to the desired Catalyst SD-WAN router (service chain hub). Service chain reachability is thus advertised by the hub to the Catalyst SD-WAN controller.

3. Define the service chain policy: Define the policy to match traffic or routes and apply it to all traffic origin sites.

Once the above steps are completed, traffic is steered through the service chain hub and associated service chain in accordance with the service chain policy.
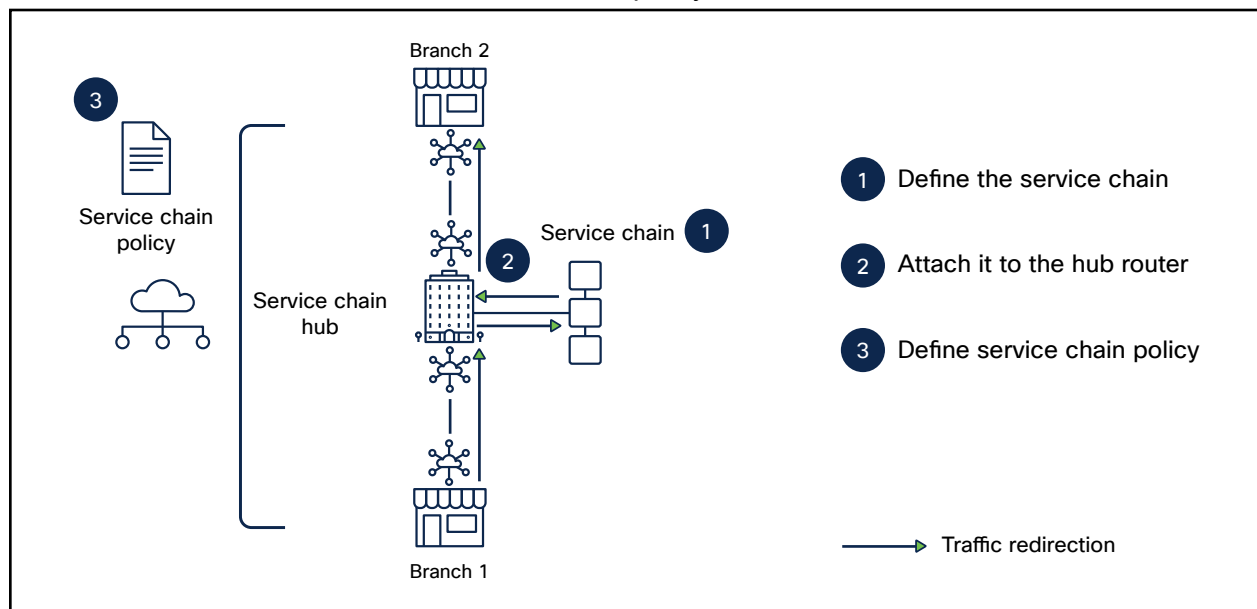

Figure 1.   Steps for service insertion

Licensing and onboarding

Q: What type of license is needed for Cisco Catalyst SD-WAN Service Insertion?

A: All devices in the SD-WAN fabric must be licensed with Cisco DNA Advantage for SD-WAN. For more information on license types, please refer to the Cisco DNA Software for SD-WAN Feature Matrix.

Additional resources

Q: Where can I find more information about Cisco Catalyst SD-WAN Service Insertion?

A: Read the Cisco Catalyst SD-WAN Service Insertion At-a-Glance.