Cisco SD-WAN for Critical Networks Infrastructure

SRv6 and Multitransport

Contents

Introduction

Cisco® Software-Defined WAN (SD-WAN) is an overlay architecture that helps to overcome the biggest drawbacks of the traditional WAN. It builds secure, unified connectivity over any transport technology: Segment Routing (SR), Multiprotocol Label Switching (MPLS), internet, mobile and satellite networks, and others. It also provides simplified operations with centralized management, policy control, and application visibility across the enterprise. Cisco SD-WAN helps ensure security by leveraging the highest encryption standards for data confidentiality. In scenarios where (national) requirements mandate the use of a dedicated cryptographic device, SD-WAN employs Generic Routing Encapsulation (GRE) tunnels for data transport, while the crypto device handles encryption to maintain confidentiality and compliance with stringent security policies. With this architecture, you can provide secure connectivity everywhere, deploy new services and applications faster, and reduce operational complexity in the WAN.

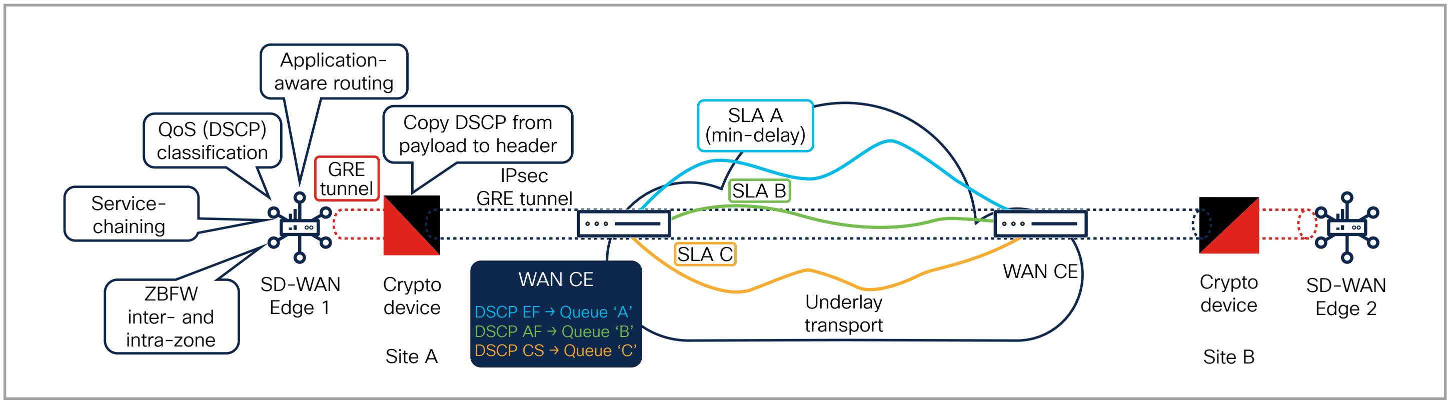

Figure 1. SD-WAN overlay secured by cryptography devices

This solution brings together the best of Cisco SD-WAN for branch management simplicity, overlay fabric virtualization that is carrier- and transport-agnostic, and the best of crypto agility by adding dedicated crypto devices. Features like Zone-Based Firewall (ZBFW), Quality-of-Service (QoS) classification using Differentiated Services Code Point (DSCP), and application-aware routing are used to assign traffic to respective Service-Level Agreement (SLA) classes in the underlay transport. This allows networkwide segmentation for lines of business, compliance, and business partners. It also offers optimized performance for public clouds and the internet.

SD-WAN benefits

Zero-trust security model

Cisco SD-WAN is based on the zero-trust model. All the components mutually authenticate each other, and all the edge devices are authorized before they are allowed onto the network. Every packet that flows through the network across data plane, control plane, and management plane is encrypted using SSL and IP Security (IPsec) or the crypto device technologies. The Cisco SD-WAN solution has unique differentiated capabilities to build a large-scale encrypted network across tens of thousands of sites.

Quality of service

Cisco SD-WAN's QoS feature is designed to optimize network performance by managing bandwidth and includes the use of DSCP for traffic classification and prioritization. It includes several key components: classification, scheduling, queueing, shaping, and policing. These components work together to minimize delay, jitter, and packet loss for critical application flows.

- **Classification:** Classification involves categorizing incoming data packets into different forwarding classes based on their importance. DSCP values are used to classify packets into different forwarding classes, which determine the priority and handling of the packets as they traverse the network. Each class is then assigned to specific output queues, which are serviced according to configured policies.
- **Scheduling:** Scheduling determines the order and rate at which packets are transmitted from the queues. It can be configured using methods like weighted round robin or low-latency queueing to ensure timely delivery of high-priority traffic.
- **Queueing:** Queueing involves managing the storage of packets in different queues based on their classification. This helps in controlling the flow of traffic and ensuring that high-priority packets are transmitted first.
- **Shaping:** Traffic shaping controls the rate of outgoing traffic to prevent congestion. It uses buffers to hold packets temporarily and releases them at a controlled rate, ensuring that the network does not become overloaded.
- **Policing:** Policing monitors the rate of traffic and enforces limits by dropping or marking packets that exceed predefined thresholds. This helps in maintaining network performance and preventing abuse of bandwidth.

Note: Best practice for operators of critical networks infrastructure is to reclassify DSCP values to ensure that mission-critical traffic is treated consistently across overlay and underlay.

Application-aware dynamic routing based on real-time network telemetry

Application-aware routing is a feature that optimizes the path for data traffic based on real-time network conditions and predefined SLAs. Here are the key components and benefits of application-aware routing:

- **Identification:** Applications are identified and mapped to specific SLA requirements using centralized data policies. These policies are configured on a Cisco Catalyst™ SD-WAN controller and passed to the appropriate devices.
- **Monitoring and measuring:** Enhanced application-aware routing uses inline data and Bidirectional Forwarding Detection (BFD) packets for more accurate, faster, and more detailed measurements.
- **Routing policy:** Application-aware routing allows network administrators to set preferred paths for business-critical applications, helping ensure that they meet SLA requirements. If the preferred path does not meet the SLA, a backup path can be used.

This routing method helps minimize performance degradation during network brownouts or soft failures by redirecting traffic to optimal paths. It also reduces network costs through efficient load sharing and improves application performance.

Zone-based firewall

Cisco SD-WAN ZBFW is an additional security feature that allows for the inspection and control of traffic between different zones within a network. It uses a flexible zone-based model for traffic inspection that is more intuitive compared to the older interface-based model. The ZBFW enables the creation of security policies that define how traffic flows between source and destination zones, allowing for stateful inspection of TCP, UDP, and ICMP data traffic flows. The ZBFW policy can be configured to allow or deny traffic between different VPNs based on predefined rules, providing secure and efficient traffic management. Firewall High Availability (HA) can be deployed in active-active or active-standby mode to maintain service continuity during failover by synchronizing the stateful firewall state.

Service chaining

The service-chain feature in Cisco SD-WAN, also known as service insertion, allows for the integration of network and security services into the data traffic path within the SD-WAN overlay fabric. This feature is highly flexible and automated, enabling service chains to be deployed on a per-VPN basis and across various topologies. Key capabilities include automatic traffic forwarding through all services in a chain, built-in load balancing, high availability, and advanced service tracking. Service chaining can be used for various traffic types, such as inter-VPN, branch-to-cloud, and cloud-to-cloud traffic, and supports multiple attachment methods like IPv4, IPv6, and tunneling. The services can be local at the edge or centralized.

- **Local service hosting:** Service chains can be hosted locally on devices, allowing traffic to be processed by services such as firewalls or load balancers within the same site. This setup is beneficial for ensuring security and compliance without routing traffic to a central location.

- **Centralized service processing:** Traffic can be routed through centralized service hubs where services like firewalls and intrusion detection systems are deployed. This is useful for regulatory compliance, such as meeting national standards, by routing traffic through firewalls in a centralized data center or regional hub.

Solution components

The primary components for the Cisco SD-WAN solution consist of the manager as the network management system (management plane), the controller (control plane), the validator (orchestration plane), and the WAN edge router (data plane).

- **Manager:** This centralized software-based network management system is virtualized and provides a GUI interface to easily monitor, configure, and maintain all SD-WAN devices and their connected links in the underlay and overlay network. It provides a single pane of glass for day-0, day-1, and day-2 operations to the enterprise.
- **Controller:** This software-based component is virtualized and responsible for the centralized control plane of the SD-WAN network. It maintains a secure connection to each edge router and distributes routes and policy information via the Overlay Management Protocol (OMP), acting as a route reflector.
- **Validator:** This software-based component is virtualized and performs the initial authentication of edge devices and orchestrates controller, manager, and edge router connectivity. It also has an important role in enabling communication between the devices that sit behind Network Address Translation.
- **Edge router:** This device, available as either a hardware appliance or a virtualized router, sits at a physical site or in the cloud and provides secure data plane connectivity among the sites over one or more underlay WAN transports. It is responsible for traffic forwarding, security, QoS, routing protocols such as Border Gateway Protocol and Open Shortest Path First, and more.
- **Crypto device (third party):** A cryptographic device optimized for network encryption is typically designed with both hardware and software tailored for secure communication. It features, for example, Field-Programmable Gate Array (FPGA)-based hardware capable of achieving high throughput rates per direction, for high-speed encryption across Layer 2 and Layer 3 WAN technologies. Security is a cornerstone, with, for example, Advanced Encryption Standard - Galois/Counter Mode (AES-GCM) encryption implemented in hardware for both data and control planes, providing integrity and replay protection against active attacks. The devices are typically hardened against Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks and side-channel vulnerabilities, maintaining strict separation between cryptographic security and network functions. This design minimizes the attack surface and provides robust protection against zero-day vulnerabilities.

Multitenancy

Cisco SD-WAN provides logical separation of customers through its multitenancy feature. This allows service providers to manage multiple customers, known as tenants, using shared controllers. Each tenant's data is logically isolated on these shared controllers, helping ensure secure and independent management of their network environments.

The key features of Cisco SD-WAN multitenancy are as follows:

- **Full enterprise multitenancy:** Supports segregated roles for service providers and tenants, allowing service providers to offer SD-WAN services to multiple customers.
- **Tenant-specific WAN edge devices:** Each tenant can have specific configurations and monitoring environments, with overlapping VPN numbers possible among different tenants.
- **Multitenant edge devices:** Enables hosting of multiple enterprise customers securely on a single physical or virtual SD-WAN platform.

One secure fabric across multitransport and multicarrier

Critical networks infrastructure often relies on a diverse underlay topology to ensure resilience and reach, commonly incorporating three distinct site types: public WAN sites, private sites using fiber and Carrier Ethernet links for dedicated high-bandwidth connectivity, and internet-connected sites, encompassing wired, mobile, and satellite access for ubiquitous coverage. The challenge lies in seamlessly integrating these disparate networks into a cohesive and manageable whole.

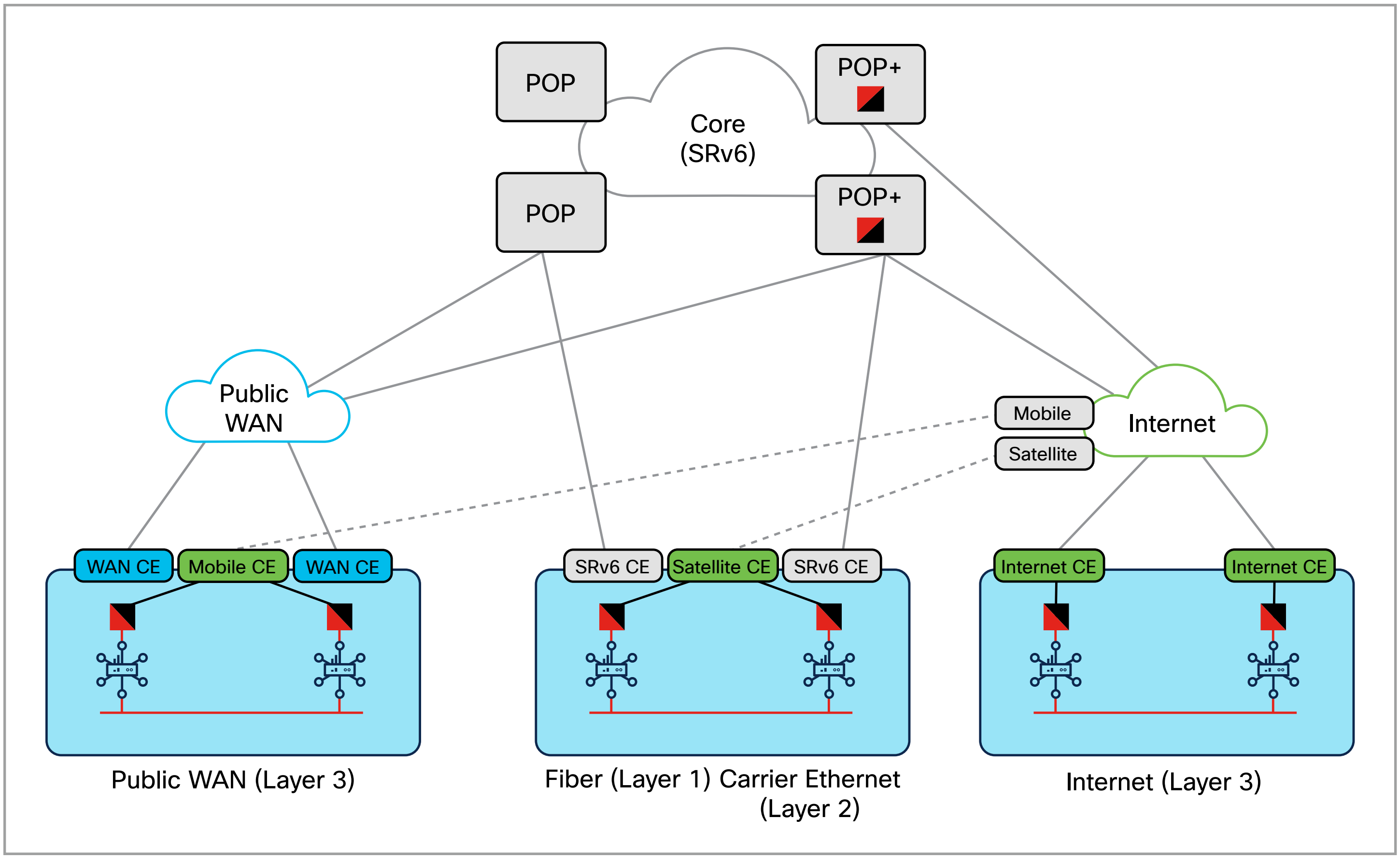

Figure 2. Multitransport and multicarrier site connectivity

Cisco SD-WAN addresses this challenge by creating one unified overlay fabric that abstracts the complexities of the underlay, allowing these diverse site types to operate as a single, logical network. This transport-agnostic approach, shown by the different Customer Edge (CE) types in the figure above, enables consistent policy enforcement, centralized management, and optimized application performance across the entire infrastructure, regardless of the underlying connectivity method, delivering a unified and agile network solution for critical operations.

Secure SD-WAN overlay topology

The purpose of these design recommendations is to provide guidance on Cisco's preferred deployment option for implementing SD-WAN when dedicated Cryptography Devices (CDs) are required for the purpose of network encryption. These recommendations target dual-homed edge router designs and highlight key features to gain the most benefit from SD-WAN capabilities, specifically regarding intelligent application-aware routing and the ability to constantly monitor the available transports to assure that the path meets those application requirements beyond achieving the shortest routing costs. There are also several key assumptions that are fundamental to this design, including:

- Red network (inner side of CD): Via the crypto device
- Underlay as black network (outer side of CD):
  Via available WAN transport (fiber, Ethernet, public/private WAN, internet, mobile, satellite) Red network (inner side of CD): Via the crypto device
- Underlay as black network (outer side of CD):
  Via available WAN transport (fiber, Ethernet, public/private WAN, internet, mobile, satellite)
- Allowing SD-WAN DSCP markings unchanged through the CD
  - SD-WAN on inner side of CD (red network)
  - Underlay transport on outer side of CD (black network)
- Alignment of overlay SD-WAN DSCP to underlay transport queues or slices

Finally, Cisco understands that there are multiple designs and requirements that could require different design features and topologies, but we feel that the recommendations proposed in this paper target the most common topologies for critical networks requiring dedicated CDs.

Red network (inner side of CD)

While the internal and external network CD design offer two distinct topologies for the internal (red network) design, there are several key differences from the topology of a commercial SD-WAN deployment. First, the management and controller cluster (manager, controller, validator) must be located and restricted to connectivity within the secure network space, specifically behind the CD routing and security infrastructure. Second, the encapsulation for SD-WAN will not require IPsec encryption of the GRE tunnels between SD-WAN edge devices, as the CDs handle the encryption requirements between locations (see Figure 1).

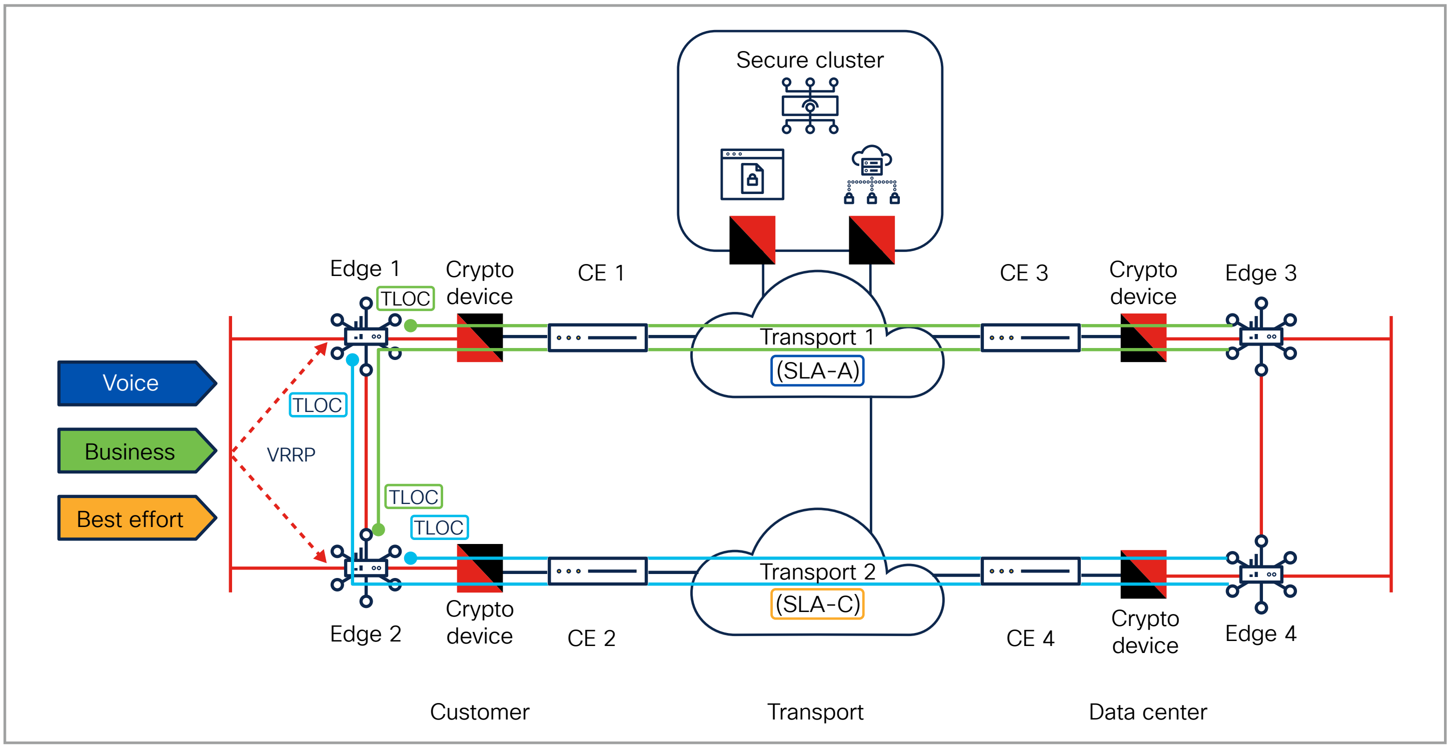

Figure 3. Dual-edge-router dual-homed connectivity

Figure 3 depicts the typical topology for a dual-router dual-homed CD design. Edges 1 and 2 establish a connection over separate physical transports, for example, fiber as Transport 1 with QoS and minimum delay, and internet as Transport 2 without QoS. Note that these have different SLAs. Aside from the caveats above, the Cisco SD-WAN solution fits perfectly into this (national) crypto design topology. The proposed dual-router dual-CD design targets a high level of availability, offering a fail-safe redundant design for critical network customers needing a higher level of uptime. Key benefits are:

- The two transport locators (TLOCs), “green” and “blue,” on the router will be able to measure the link quality over each path, and the application-aware forwarding decision can be made locally regardless of which router the packet landed on, via the Virtual Router Redundancy Protocol (VRRP).
- VRRP is used for load balancing of incoming host traffic from the branch campus network. Cisco recommends the use of a feature called TLOC extensions. TLOC extensions allow TLOCs to be configured in a redundant mode, allowing a partial mesh of TLOC topologies that offers connectivity redundancy as well as SLA transport liveliness from more sources and destination routers.

The TLOC provides the transport attachment point for the overlay tunnel and is also the attachment point for supporting the liveliness probes that are sent to measure various QoS attributes (latency, packet loss, jitter) for link quality. In the CD design, each TLOC will need to route to the destination TLOC within the secure routing space of the CD and, like any other CD network, will perform routing of specific IP addresses. In this case, these will be the source/destination TLOC address endpoints.

As shown in Figure 3, the use of TLOC extensions gives the network designer the ability to originate indirectly connected TLOCs through its backup router. In the example shown in the figure, Edge 2 would establish a directly connected TLOC to Edge 4 but would add a second TLOC to Edge 3 as well (via the Edge 1 path), offering path redundancy to the remote site, even in the event that a CD or the router/transport fails between Edge 2 and Edge 4. The TLOC extension extends a backup TLOC (GRE) across Edge 1 to Edge 3, with Edge 1 acting as a transit path for that TLOC to Edge 3. This TLOC extension design offers two key enhancements to the design:

- It provides another level of redundancy in the event of a CD, link, node, or transport failure.
- Regardless of which router the destination packet lands on from the branch campus network, the application-aware routing policy forwarding can be applied, in this case, to Edge 1 or Edge 2.

While the Cisco SD-WAN solution can run VRFs over IP (GRE), the SD-WAN solution reserves VPN 0 for control plane traffic. In the case of the CD design, all VPN 0 traffic will be routable via the CD-secured transport, including the secure controller cluster, which must be reachable by all edge devices and secured by the CDs' (national) encryption.

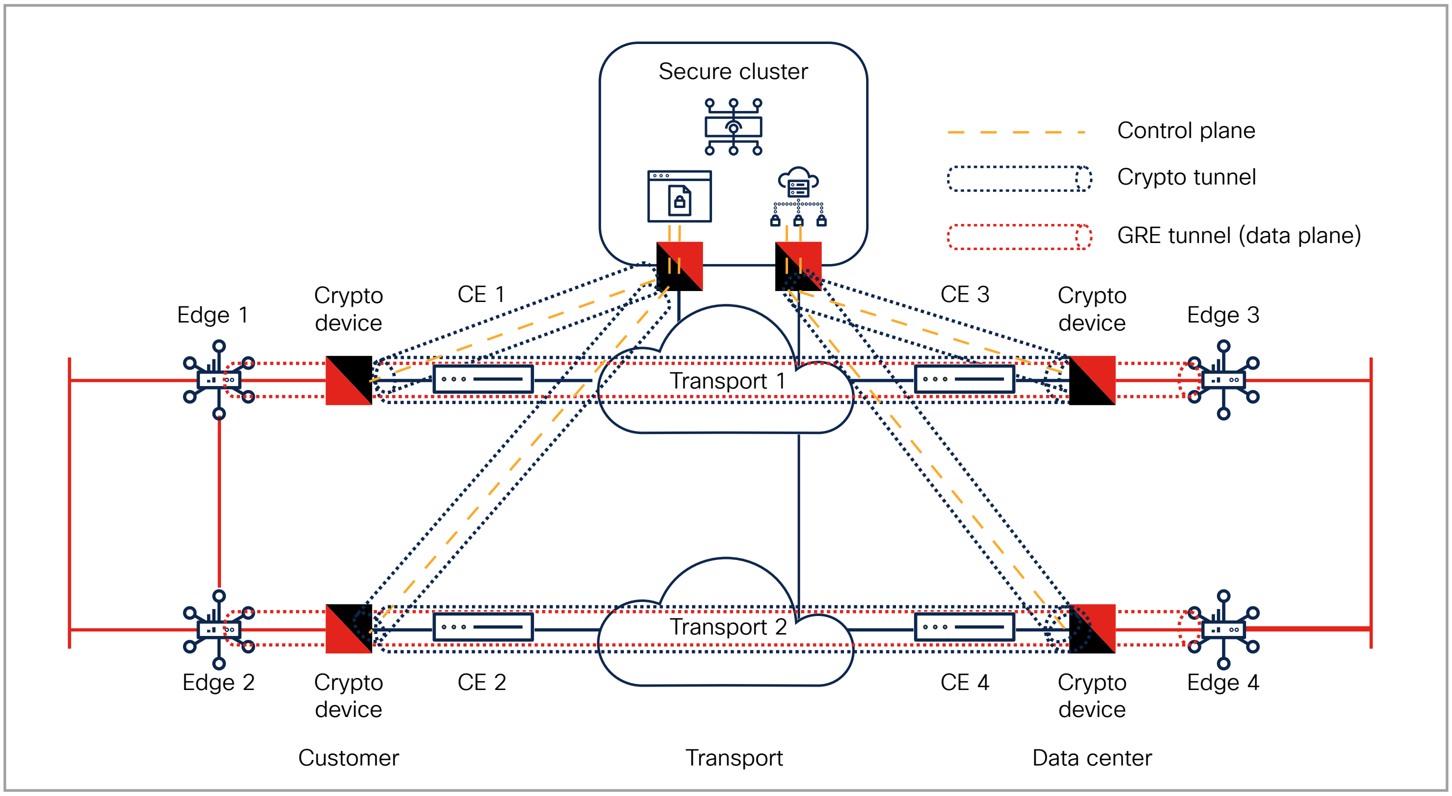

Figure 4. End-to-end secure infrastructure

Note: This allows all control plane traffic (routing updates, BFD probes, key exchange for controller access) in the Cisco SD-WAN solution to be secured by the (national) CDs, as well as the router-to-router data plane traffic, creating an end-to-end secure infrastructure.

The application awareness is what differentiates Cisco SD-WAN from other WAN solutions, and the end-to-end measurement, in the case of Figure 3, from each router via TLOC extensions also takes into account the aggregated latency, loss, and jitter, including those induced by the CDs, as well as the external transport (black network) directly connected to the transport services. The variations of path selection can change based on the agency's operators and how they handle specific applications, especially those in failure scenarios (for example, should low-latency voice take the best effort path if the SLA path fails?), so the options are endless through policy provisioning and the needs of the mission.

Underlay as black network (outer side of CD)

A transport-independent underlay is a modern network architecture designed to support a multicarrier and multitransport approach, leveraging diverse technologies such as fiber, Ethernet, public/private WAN services, internet, mobile, and satellite as transport (see Figure 2). It leverages, for example, segment routing over IPv6 (SRv6) for multiplanar routing, enabling deterministic traffic engineering and virtual topology formulation. This approach helps ensure a highly resilient and scalable backbone with 99.999+ percent reliability capable of meeting the demands of modern applications and services in critical network infrastructures.

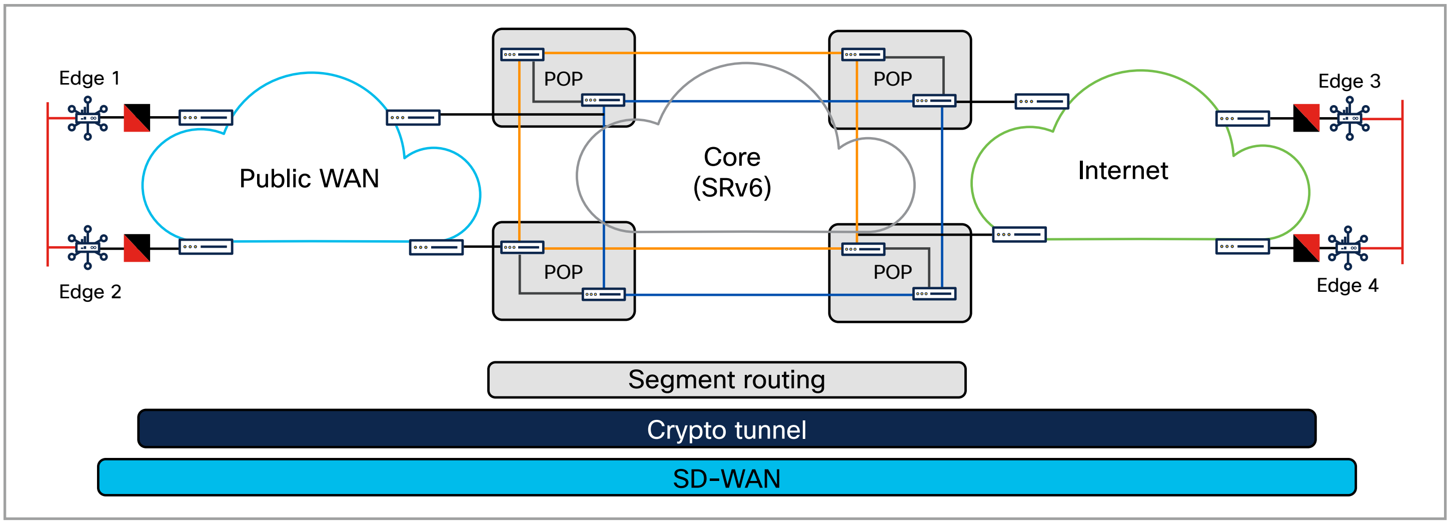

Figure 5. Multiplanar core extended by public WAN and internet transport

SRv6 as a transport protocol simplifies network operations by embedding routing instructions directly into IPv6 headers. This approach eliminates the need for additional protocols, enabling seamless integration across diverse network environments. Key features include advanced traffic engineering capabilities like Flexible Algorithm (Flex Algo), which allows operators to define custom routing paths based on metrics such as latency and bandwidth, and robust security, for example, through MACsec encryption for secure data transmission over both public and private networks. Additionally, SRv6 is designed to support emerging technologies like routed optical networking and 5G slicing.

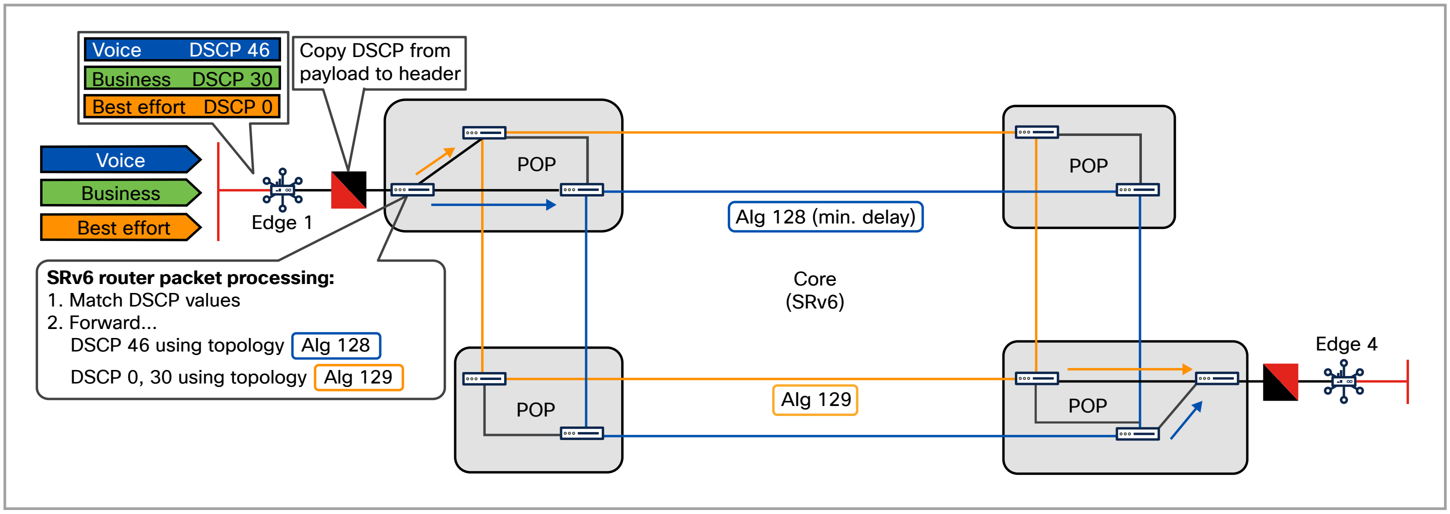

Figure 6. SD-WAN overlay over SRv6 underlay

Figure 6 shows the integration of SD-WAN Edge 1, a CD, and an SRv6 router, which unlocks new possibilities for service differentiation and SLA management. The overlay edge router reclassifies customer traffic with respective DSCP values, which are passed through by the CD. On the underlay SRv6 router, DSCP values are matched and forwarded in the associated Flex Algo (for example, voice traffic with a requirement for minimum delay in Alg. 128).

This integration allows SD-WAN policies to leverage SRv6 paths to meet specific application requirements, such as low latency or high reliability. Unified visibility across SD-WAN overlays and SRv6 underlays simplifies troubleshooting and improves quality of experience.

Advanced automation and analytics

Automation

The Cisco Crosswork® Network Controller enhances network management by providing centralized automation for IP transport networks such as SRv6. It supports dynamic traffic engineering, real-time monitoring, and closed-loop automation, helping ensure high performance and reliability. The controller integrates with external probes and APIs to enable automated issue detection and resolution, reducing operational complexity.

Analytics

Cisco Provider Connectivity Assurance (PCA) offers a unified dashboard for monitoring both underlay and overlay networks. It provides actionable insights by measuring critical metrics like delay, jitter, and packet loss, helping ensure optimal transport network performance. PCA also correlates SD-WAN overlay performance with underlay metrics, enabling resource optimization and SLA compliance.

Summary

Critical networks require uncompromising security and reliability, yet traditional WANs often struggle to deliver. Cisco SD-WAN offers a transformational overlay architecture to overcome these limitations, providing a secure, unified, and intelligent solution, especially when combined with underlay transport solutions like SRv6 and dedicated (national) CDs. Organizations managing critical networks face challenges in maintaining unbreakable security, ensuring high availability, optimizing application performance, simplifying management, and controlling costs. Cisco SD-WAN addresses these challenges by creating a secure, intelligent overlay network independent of the underlying transport, allowing organizations to leverage any transport technology while maintaining consistent security and performance. This solution is built on mutual authentication, offers flexible encryption options including dedicated third-party CDs for compliance, dynamically optimizes traffic paths based on real-time conditions, prioritizes traffic with QoS, provides granular control with a ZBFW, seamlessly integrates network services with service chaining, enables secure multitenancy, and simplifies management through a single pane of glass. Integrating with SRv6 unlocks new levels of performance and scalability, automated by Cisco Crosswork Network Controller and monitored by PCA. Cisco SD-WAN enhances security, optimizes application performance, simplifies management, reduces costs, and enhances reliability, empowering organizations to build a secure, agile, and high-performing WAN that meets the demanding needs of critical networks infrastructure.

Author
Stefan Heidelmann, Delivery Architect, Cisco Customer Experience

Reviewers
Jason Yang (jayang), Principal Technical Marketing Engineer, Cisco Product Management
Marco Lolischkies, Delivery Architect, Cisco Customer Experience
Rene Klose, Systems Architect, Cisco Sales