The Cisco SD-WAN Solution

The Cisco SD-WAN SEN

The Need for the Cisco SD-WAN SEN

Legacy networking technology has become increasingly expensive and complex, and it cannot scale to meet the needs of today’s multisite enterprises. The Cisco SD-WAN Secure Extensible Network (SEN), which is based on time-tested and proven elements of networking, offers an elegant, software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large and complex networks that are distributed across multiple locations and geographies. Built in to the Cisco SD-WAN SEN are inherent authentication and security processes that ensure the safety and privacy of the network and its data traffic.

The Cisco SD-WAN SEN represents an evolution of networking from an older, hardware-based model to a secure, software-based, virtual IP fabric. The Cisco SD-WAN fabric, also called an overlay network, forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and broadband. The overlay network also supports next-generation software services, thereby accelerating your shift to cloud networking.

Challenges in Legacy Network Design

The traditional approach to network design cannot scale to meet today’s needs for four fundamental reasons:

• Cost—Legacy networks run on expensive hardware such as routers and switches, which require time-consuming configuration and maintenance. In addition, these networks require expensive transport connections or carrier circuits to secure and segment the network.

• Complexity—Legacy networks operate on the old model of a distributed control plane, which means that every node in the network must be configured with routing and security rules. Remote site management, change control, and network maintenance represent major logistical challenges.
The Need for the Cisco SD-WAN SEN

- Lengthy installation times—Legacy networks that run on dedicated carrier circuits depend on the carrier to install new circuits, which can take several months. This can dramatically delay the launch of new branch locations.

- Control—Legacy networks that run on carrier circuits sacrifice control to the ISP, from network design to configuration to monitoring. Requesting changes from the ISP also requires extra time and is prone to communication errors.

Cost and complexity become even more prohibitive for legacy networks in the face of today’s requirements, including:

- Rigorous end-to-end security
- Disparate transport networks
- High-bandwidth cloud applications that are hosted in multiple data centers
- Ongoing increase in the number of mobile end users
- Any-to-any connectivity over fluid topologies
- Unique needs of particular businesses

The Cisco SD-WAN Solution

The Cisco SD-WAN SEN is a Software-Defined WAN (SD-WAN). As with all SD-WANs, it is based on the same routing principles that allowed the Internet to scale during the 1990s and 2000s. What separates the Cisco SD-WAN SEN from other SD-WANs is that it re-imagines the WAN for a new generation of enterprise networks, separating the data plane from the control plane and virtualizing much of the routing that used to require dedicated hardware.

The virtualized network runs as an overlay on cost-effective hardware, whether physical routers, called vEdge routers, or virtual machines in the cloud, called vEdge Cloud routers. Centralized controllers, called vSmart controllers, oversee the control plane of the Cisco SD-WAN fabric, efficiently managing provisioning, maintenance, and security for the entire SEN overlay network. Another device, called the vBond orchestrator, automatically authenticates all other Cisco vEdge devices when they join the SEN overlay network.
This division of labor allows each networking layer to focus on what it does best. The control plane manages the rules for the routing traffic through the overlay network, and the data plane passes the actual data packets among the network devices. The control plane and data plane form the warp and weft of a flexible, robust fabric that you weave according to your needs, on your schedule, over existing circuits.

The Cisco SD-WAN vManage NMS provides a simple, yet powerful, set of graphical dashboards for monitoring network performance on all devices in the overlay network, from a centralized monitoring station. In addition, the vManage NMS provides centralized software installation, upgrade, and provisioning, whether for a single device or as a bulk operation for many devices simultaneously.

The Cisco SD-WAN SEN is ideally suited to the needs of cloud networking. Cisco SD-WAN virtual IP fabric supports software services that streamline and optimize cloud networking, allowing you to take full advantage of the power of the overlay network for individual cloud applications.

The Virtual IP Fabric

The complexity in legacy enterprise networks stems from three main sources:

• There is no clear separation between entities that exchange data traffic and the transport network that binds these entities together. That is, there is no clear separation between hosts, devices, and servers on the service side of the network and the interconnects between routers on the transport side of the network.

• Policy and control decisions are embedded at every hop across the enterprise network.

• Security is a time-intensive, manual process, and security management must be implemented either at every node in the network or by using centralized security servers to manage group keys.

The Cisco SD-WAN Secure Extensible Network (SEN) uses time-tested and proven elements of networking in innovative ways to build the secure, virtual IP fabric. These networking elements include:

• Using routing and routing advertisements to establish and maintain the flow of traffic throughout the network.
• Layer 3 segmentation, sometimes called virtual routing and forwarding (VRF), to isolate different flows of traffic. This is useful to separate traffic from different customers or different business organizations within an enterprise.

• Peer-to-peer concepts to set up and maintain bidirectional connections between pairs of protocol entities

• Authentication and encryptions.

• Policies for routing and data traffic.

With five simple steps, the Cisco SD-WAN virtual IP fabric transforms a complex legacy network into an easy-to-manage, scalable network:

• Step 1: Separate transport from the service side of the network.

• Step 2: Centralize routing intelligence and enable segmentation.

• Step 3: Secure the network automatically.

• Step 4: Influence reachability through centralized policy.

• Step 5: Simplify orchestration and provisioning.

Step 1: Separate Transport from the Service Side of the Network

The job of the transport network is to carry packets from one transport router to another. The transport network need only know about the routes to follow to reach the next-hop or destination router. It need not know about the prefixes for non-transport routers, the routers that sit behind the transport routers in their local service networks.

Separating network transport from the service side of the network allows the network administrator to influence router-to-router communication independently of the communication between users or between hosts.

This approach has many benefits:

• The network administrator can choose transport circuits based on SLA and cost.

• The routing system can assign attributes to transport links for optimal routing, load balancing, and policy-based routing.
Step 2: Centralize Routing Intelligence and Enable Segmentation

Every router at the edge of a network has two sides for routing: one to the transport network and one to the service side of the network. To have any-to-any communication among all routers, all routers need to learn all prefixes. Traditionally, routers learn these prefixes using full-mesh IGP/BGP or by enabling routing on an overlay tunnel (for example, BGP or IGP over MPLS or GRE). Various techniques allow the scaling issues associated with full-mesh routing adjacencies to be mitigated or eliminated, such as employing a route reflector for BGP.

The Cisco SD-WAN fabric builds on the route reflector model by centralizing routing intelligence. Essentially, all prefixes learned from the service side on a router are advertised to a centralized controller, which then reflects the information to other routers over the network’s control plane. The controllers do not handle any of the data traffic; they are involved only in control plane communication.

This approach has many benefits:

- The centralized controller can use inexpensive or commodity servers for control plane processing.
- The routers can use off-the-shelf silicon, allowing cost benefits from economies of scale.
- Scale challenges associated with full-mesh routing on the transport side of the network are eliminated.
- The network administrator can create multiple segments without the need for complex signaling protocols. For example, in the figure here, all P<sub>x</sub> prefixes can be part of one VPN, while all S<sub>x</sub> prefixes can be part of a different VPN.

---

**Note**

The centralized controller only “influences” routing on the routers. The controller does not participate in every flow going through the network, nor does it participate in routing on the service side. This design allows the routers to have local intelligence—enough intelligence to make local site decisions quickly.
**Step 3: Secure the Network and Links Automatically**

The Cisco SD-WAN fabric identifies transport side links and automatically encrypts traffic between sites. The associated encryption keys are exchanged over a secure session with the centralized controller. Secure sessions with the controller are set up automatically using RSA and certificate infrastructure.

This approach has many benefits:

- The Cisco SD-WAN fabric itself authenticates all devices participating in the network, which is an important step to secure the infrastructure.
- The fabric automatically exchanges encryption keys associated with the transport links, eliminating the hassle of configuring thousands of pair-wise keys.
- The fabric ensures that the network is not prone to attacks from the transport side.

**Step 4: Influence Reachability through Centralized Policy**

Policy configured on a centralized controller strongly influences how prefixes are advertised among the routers. For example, if all traffic between routers P3 and P4 in the figure here has to make a U-turn at router vEdge-1, the network administrator can apply a simple route policy on the centralized controller. The controller then passes the policy to the affected edge routers. The network administrator does not need to provision the policy on each individual router.

This approach has many benefits:

- The controller centrally influences access control, that is, which prefixes are allowed to talk to each other inside a VPN.
- The controller optimizes user experience by influencing transport link choice based on SLA or other attributes. The network administrator can color transport links (such as gold and bronze), and allow applications to map the colors to appropriate transport links.
- The network administrator can map business logic from a single centralized point.
• The network can react faster to planned and unexpected situations, such as routing all traffic from high-risk countries through an intermediate point.

• The network can centralize services such as firewalls, IDPs, and IDSs. Instead of distributing these services throughout the network at every branch and campus, the network administrator can centralize these functions, achieving efficiencies of scale and minimizing the number of touch points for provisioning.

**Step 5: Simplify Provisioning and Management**

Legacy network devices are provisioned and monitored manually through a CLI. Network administrators must type configurations line by line, and enter operational commands one at a time on individual devices in order to retrieve and read status information. This method is error prone and time consuming when provisioning and troubleshooting a network, and it can present serious difficulties when devices are in remote locations or when management ports are inaccessible.

The Cisco SD-WAN SEN centralizes and significantly simplifies provisioning and management through the vManage Network Management System (NMS). The vManage NMS provides an easy-to-use, graphical dashboard from which you can monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. For example, the dashboard's GUI provides a templated view of various configurations to ease provisioning a service, so all common elements, such as AAA and company-specific servers, can be pushed to multiple devices with a single click, from a single point.

This approach has many benefits:

• The network administrator provisions and manages the network as a whole, efficiently and easily, as opposed to a piece-meal approach that deals with individual devices one at a time.

• The network administrator has improved network visibility (for example, viewing network-wide VPN statistics) from a single point.

• Troubleshooting tasks are simplified and presented visually, instead of requiring network administrators to read lengthy configurations and output from individual devices.
Components of the Cisco SD-WAN SEN

Primary SEN Components

The secure, virtual IP fabric of the Cisco SD-WAN Secure Extensible Network (SEN) is made up of four fundamental components:

- **vManage Network Management System (NMS)**—The vManage NMS is a centralized network management system that lets you configure and manage the entire overlay network from a simple graphical dashboard.

- **vSmart Controller**—The vSmart controller is the centralized brain of the Cisco SD-WAN solution, controlling the flow of data traffic throughout the network. The vSmart controller works with the vBond orchestrator to authenticate Cisco vEdge devices as they join the network and to orchestrate connectivity among the vEdge routers.

- **vBond Orchestrator**—The vBond orchestrator automatically orchestrates connectivity between vEdge routers and vSmart controllers. If any vEdge router or vSmart controller is behind a NAT, the vBond orchestrator also serves as an initial NAT-traversal orchestrator.

- **vEdge Routers**—The vEdge routers sit at the perimeter of a site (such as remote offices, branches, campuses, data centers) and provide connectivity among the sites. They are either hardware devices or software, called a vEdge Cloud router, that runs as a virtual machine. vEdge routers handle the transmission of data traffic.

Of these four components, the vEdge router can be a Cisco SD-WAN hardware device or software that runs as a virtual machine, and the remaining three are software-only components. The software vEdge router, vManage NMS, and vSmart controller software runs on servers, and the vBond orchestrator software runs as a process (daemon) on a vEdge router.

The figure below illustrates the components of the Cisco SD-WAN SEN. The sections below describe each component in detail.
vManage NMS

The vManage NMS is a centralized network management system. The vManage NMS dashboard provides a visual window into the network, and it allows you to configure and manage Cisco vEdge network devices. The vManage NMS software runs on a server in the network. This server is typically situated in a centralized location, such as a data center. It is possible for the vManage NMS software to run on the same physical server as vSmart controller software.

You can use vManage NMS to store certificate credentials, and to create and store configurations for all Cisco vEdge network components. As these components come online in the network, they request their certificates and configurations from the vManage NMS. When the vManage NMS receives these requests, it pushes the certificates and configurations to the Cisco vEdge network devices.

For vEdge Cloud routers, vManage NMS can also sign certificates and generate bootstrap configurations, and it can decommission the devices.

vSmart Controller

The vSmart controller oversees the control plane of the Cisco SD-WAN overlay network, establishing, adjusting, and maintaining the connections that form the Cisco SD-WAN fabric.

The major components of the vSmart controller are:

- Control plane connections—Each vSmart controller establishes and maintains a control plane connection with each vEdge router in the overlay network. (In a network with multiple vSmart controllers, a single vSmart controller may have connections only to a subset of the vEdge routers, for load-balancing purposes.) Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the vSmart controller and the vEdge router. This payload consists of route information necessary for the vSmart controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the vEdge routers. The DTLS connection between a vSmart controller and a vEdge router is a permanent connection. The vSmart controller has no direct peering relationships with any devices that a vEdge router is connected to on the service side.

- OMP (Overlay Management Protocol)—The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the vSmart controller and the vEdge routers and carries only control plane information. The vSmart controller processes the routes and advertises reachability information learned from these routes to other vEdge routers in the overlay network.

- Authentication—The vSmart controller has pre-installed credentials that allow it to authenticate every new vEdge router that comes online. These credentials ensure that only authenticated devices are allowed access to the network.

- Key reflection and rekeying—The vSmart controller receives data plane keys from a vEdge router and reflects them to other relevant vEdge routers that need to send data plane traffic.

- Policy engine—The vSmart controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets, and other network needs.

- Netconf and CLI—Netconf is a standards-based protocol used by the vManage NMS to provision a vSmart controller. In addition, each vSmart controller provides local CLI access and AAA.

The vSmart controller maintains a centralized route table that stores the route information, called OMP routes, that it learns from the vEdge routers and from any other vSmart controllers in the Cisco SD-WAN overlay network.
network. Based on the configured policy, the vSmart controller shares this route information with the Cisco vEdge network devices in the network so that they can communicate with each other.

The vSmart controller is software that runs as a virtual machine on a server configured with ESXi or VMware hypervisor software. The vSmart software image is a signed image that is downloadable from the Cisco SD-WAN website. A single Cisco SD-WAN root-of-trust public certificate is embedded into all vSmart software images.

During the initial startup of a vSmart controller, you enter minimal configuration information, such as the IP addresses of the controller and the vBond orchestrator. With this information and the root-of-trust public certificate, the vSmart controller authenticates itself on the network, establishes a DTLS control connection with the vBond orchestrator, and receives and activates its full configuration from the vManage NMS if one is present in the domain. (Otherwise, you can manually download a configuration file or create a configuration directly on the vSmart controller through a console connection.) The vSmart controller is now also ready to accept connections from the vEdge routers in its domain.

To provide redundancy and high availability, a typical overlay network includes multiple vSmart controllers in each domain. A domain can have up to 20 vSmart controllers. To ensure that the OMP network routes remain synchronized, all the vSmart controllers must have the same configuration for policy and OMP. However, the configuration for device-specific information, such as interface locations and addresses, system IDs, and host names, can be different. In a network with redundant vSmart controllers, the vBond orchestrator tells the vSmart controllers about each other and tells each vSmart controller which vEdge routers in the domain it should accept control connections from. (Different vEdge routers in the same domain connect to different vSmart controllers, to provide load balancing.) If one vSmart controller becomes unavailable, the other controllers automatically and immediately sustain the functioning of the overlay network.

**vBond Orchestrator**

The vBond orchestrator automatically coordinates the initial bringup of vSmart controllers and vEdge routers, and it facilities connectivity between vSmart controllers and vEdge routers. During the bringup processes, the vBond orchestrator authenticates and validates the devices wishing to join the overlay network. This automatic orchestration process prevents tedious and error-prone manual bringup.

The vBond orchestrator is the only Cisco vEdge device that is located in a public address space. This design allows the vBond orchestrator to communicate with vSmart controllers and vEdge routers that are located behind NAT devices, and it allows the vBond orchestrator to solve any NAT-traversal issues of these Cisco vEdge devices.

The major components of the vBond orchestrator are:

- **Control plane connection**—Each vBond orchestrator has a persistent control plane connection in the form of a DTLS tunnel with each vSmart controller in its domain. In addition, the vBond orchestrator uses DTLS connections to communicate with vEdge routers when they come online, to authenticate the router, and to facilitate the router’s ability to join the network. Basic authentication of a vEdge router is done using certificates and RSA cryptography.

- **NAT traversal**—The vBond orchestrator facilitates the initial orchestration between vEdge routers and vSmart controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration.

- **Load balancing**—In a domain with multiple vSmart controllers, the vBond orchestrator automatically performs load balancing of vEdge routers across the vSmart controllers when routers come online.

The vBond orchestrator is a software module that authenticates the vSmart controllers and the vEdge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that
all Cisco vEdge devices in the network can connect to it. (It is the only Cisco vEdge device that must have a public address.)

The vBond orchestrator orchestrates the initial control connection between vSmart controllers and vEdge routers. It creates DTLS tunnels to the vSmart controllers and vEdge routers to authenticate each node that is requesting control plane connectivity. This authentication behavior assures that only valid customer nodes can participate in the Cisco SD-WAN overlay network. The DTLS connections with vSmart controllers are permanent so that the vBond controller can inform the vSmart controllers as vEdge routers join the network. The DTLS connections with vEdge routers are temporary; once the vBond orchestrator has matched a vEdge router with a vSmart controller, there is no need for the vBond orchestrator and the vEdge router to communicate with each other. The vBond orchestrator shares only the information that is required for control plane connectivity, and it instructs the proper vEdge routers and vSmart controllers to initiate secure connectivity with each other. The vBond orchestrator maintains no state.

To provide redundancy for the vBond orchestrator, you can create multiple vBond entities in the network and point all vEdge routers to those vBond orchestrators. Each vBond orchestrator maintains a permanent DTLS connection with each vSmart controller in the network. If one vBond orchestrator becomes unavailable, the others are automatically and immediately able to sustain the functioning of the overlay network. In a domain with multiple vSmart controllers, the vBond orchestrator pairs a vEdge router with one of the vSmart controllers to provide load balancing.

vEdge Routers

The vEdge router, whether a hardware or software device, is responsible for the data traffic sent across the network. When you place a vEdge router into an existing network, it appears as a standard router.

To illustrate this, the figure here shows a vEdge router and an existing router that are connected by a standard Ethernet interface. These two routers appear to each other to be Layer 3 end points, and if routing is needed between the two devices, OSPF or BGP can be enabled over the interface. Standard router functions, such as VLAN tagging, QoS, ACLs, and route policies, are also available on this interface.

The vEdge router's components are:

- DTLS control plane connection—Each vEdge router has one permanent DTLS connection to each vSmart controller it talks to. This permanent connection is established after device authentication succeeds, and it carries encrypted payload between the vEdge router and the vSmart controller. This payload consists of route information necessary for the vSmart controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the vEdge routers.

- OMP (Overlay Management Protocol)—As described for the vSmart controller, OMP runs inside the DTLS connection and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the vEdge router and the vSmart controller and carries only control information.
• Protocols—The vEdge router supports standard protocols, including OSPF, BGP, VRRP, and BFD.

• RIB (Routing Information Base)—Each vEdge router has multiple route tables that are populated automatically with direct interface routes, static routes, and dynamic routes learned via BGP and OSPF. Route policies can affect which routes are stored in the RIB.

• FIB (Forwarding Information Base)—This is a distilled version of the RIB that the CPU on the vEdge router uses to forward packets.

• Netconf and CLI—Netconf is a standards-based protocol used by the vManage NMS to provision a vEdge router. In addition, each vEdge router provides local CLI access and AAA.

• Key management—vEdge routers generate symmetric keys that are used for secure communication with other vEdge routers, using the standard IPsec protocol.

• Data plane—The vEdge router provides a rich set of data plane functions, including IP forwarding, IPsec, BFD, QoS, ACLs, mirroring, and policy-based forwarding.

The vEdge router has local intelligence to make site-local decisions regarding routing, high availability (HA), interfaces, ARP management, ACLs, and so forth. The OMP session with the vSmart controller influences the RIB in the vEdge router, providing non-site-local routes and the reachability information necessary to build the overlay network.

The hardware vEdge router includes a Trusted Board ID chip, which is a secure cryptoprocessor that contains the private key and public key for the router, along with a signed certificate. All this information is used for device authentication. When you initially start up a vEdge router, you enter minimal configuration information, such as the IP addresses of the vEdge router and the vBond orchestrator. With this information and the information on the Trusted Board ID chip, the vEdge router authenticates itself on the network, establishes a DTLS connection with the vSmart controller in its domain, and receives and activates its full configuration from the vManage NMS if one is present in the domain. Otherwise, you can manually download a configuration file or create a configuration directly on the vEdge router through a console connection.

**SEN Software Services**

To streamline and optimize cloud networking, Cisco SD-WAN offers next generation software services that run on the secure, virtual IP fabric:

• **CloudExpress service**—CloudExpress service optimizes the performance of Software as a Service (SaaS) cloud applications. It provides clear visibility of the performance of individual applications and automatically chooses the best path for each one. CloudExpress service calculates metrics about loss and latency using a formula customized for each application.

• **vAnalytics platform (available in beta)**—vAnalytics platform is a SaaS service hosted by Cisco SD-WAN as part of the SEN solution. vAnalytics platform provides graphical representations of the performance of your entire overlay network over time and lets you drill down to the characteristics of a single carrier, tunnel, or application at a particular time.

**CloudExpress Service**

Enterprises have been adopting business critical SaaS applications including Microsoft Office365, Salesforce, Dropbox, and others. Enterprises use three primary methods to offer connectivity to SaaS applications for their users:

• Direct Internet Access (DIA) from a branch office.
Internet access through gateways in regional facilities.
Cloud exchange or direct connection through gateways in a Carrier Neutral Facility (CNF).

Latency and packet loss have a direct impact on the performance of applications and on end-user experience, but in many cases network administrators have limited or no visibility into the network performance characteristics between the end-user and SaaS applications. When path impairment occurs and application performance suffers, shifting traffic from a primary to an alternate path usually requires the network administrator to perform a set of complex, manual, time-consuming, and error-prone steps.

Cisco SD-WAN CloudExpress service provides visibility and continuous monitoring of network performance characteristics. It makes real-time decisions by choosing the best performing path between the end-user and SaaS application for an optimal user experience. It automatically reacts to changes in network performance by intelligently re-routing application traffic away from any degraded network paths.

CloudExpress service supports all access methods for cloud-based SaaS applications, including DIA, internet access through a regional facility, and access through a CNF.

CloudExpress service calculates an application performance value called the Viptela Quality of Experience (vQoE) for enterprise cloud applications. The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best.

You enable CloudExpress service in vManage NMS with a few clicks of the mouse, and then you access the CloudExpress dashboard in vManage NMS for continuous visibility into the performance of individual applications.

vAnalytics Platform (Available in Beta)

Now available in a beta release, vAnalytics platform offers visibility into the performance of applications and the network over time. vAnalytics platform is a SaaS service hosted by Cisco SD-WAN as part of the SEN solution. vAnalytics platform provides graphical representations of your entire overlay network and lets you drill down to display the characteristics of a single carrier, tunnel, or application at a particular time.

The vAnalytics dashboard serves as an interactive overview of your network and an entrance point for more details. The dashboard display information for the last 24 hours. When you drill down, you can select different time periods for different data sets to display. The dashboard displays data for network availability, WAN performance by carrier, and applications.

vAnalytics platform calculates application performance with the vQoE value, which is customized for individual applications. This value ranges from zero to ten, with zero being the worst performance and ten being the best. vAnalytics platform calculates vQoE based on latency, loss, and jitter, customizing the calculation for each application.

vAnalytics platform offers insight into planning the WAN and into its operational aspects, from historical performance, to forecasting, to providing recommendations for optimizing the WAN. vAnalytics platform stores months of data, applies machine learning algorithms, and provides unique insights and recommendations.

vAnalytics platform offers:

- Visibility—vAnalytics platform provides visibility into application and network performance based on information collected from your overlay as well as correlated information from other networks. This gives you insight into top to bottom performing applications as well as anomalous applications over a period of time.
• Forecasting—vAnalytics platform can help you plan for sites that may need additional bandwidth in the next three to six months.

• What-If Scenarios—What-if scenarios help you identify opportunities for balancing cost, performance, and availability of networks and applications.

• Recommendations—vAnalytics platform runs machine learning algorithms to identify opportunities to fine-tune the WAN. For example, vAnalytics platform can recommend application-aware routing policies based on historical information from your environment. In addition, vAnalytics platform can mine data across a variety of network service providers and recommend network service providers for a specific location.

Application visibility features include:

• Best and worst performing applications—Display the best and worst performing applications and drill down to details at the site level.

• Most bandwidth consuming applications—Display applications consuming the most bandwidth and drill down to sites and users.

• Anomalous applications families—Display changes in bandwidth consumption over a period of time.

Network visibility features include:

• Network availability and circuit availability—Display network availability and correlate network and circuit availability.

• Carrier health views—Display providers and their network characteristics.

• Best and worst performing tunnels—Display the worst performing tunnels and circuits and the providers on which they run.

You enable vAnalytics platform in vManage NMS with a few clicks of the mouse. You log in with a username and password provided by Cisco SD-WAN, and then you access the vAnalytics dashboard from vManage NMS.

Working with the Cisco SD-WAN SEN

Build a Basic Overlay Network

Let’s use a simple network design, one that has two vEdge routers and one vSmart controller, to illustrate how to form a functioning overlay network from Cisco vEdge components. In this topology, the vBond orchestrator software has been enabled on one of the vEdge routers. Once you understand a simple network, you can start designing and building more complex topologies.

A Simple Network Topology

The figure below illustrates our simple topology. Here, we have two sites, Site-100 and Site-200. vEdge-1 is the edge device in Site-100, and vEdge-2 is the edge device at Site-200. At each local site, the vEdge router connects to an existing traditional router via a standard Ethernet interface. vEdge-2 is connected to the transport network through a NAT device that also has firewall functionality.
The goal of our design is to create a private network so that Router-1 and Router-2 can be adjacent to each other from a Layer 3 perspective and so that hosts connected to each of these routers can communicate through the private network.

**Construct a Basic Network**

The following steps allow you to create the simple overlay network depicted in the topology above.

- Step 1: Perform initial bringup and basic configuration.
- Step 2: Enable host or service-side interfaces and routing.
- Step 3: Enable overlay routing over OMP.
- Step 4: Check the automatic setup of the IPsec data plane.
- Step 5: Enforce policies.

Let's look at the steps in a bit more detail.

**Step 1: Perform Initial Bringup and Basic Configuration**

From the perspective of a network administrator, the initial bringup of the Cisco vEdge network components is a straightforward and simple process, involving creating the configurations for each of the network components and ensuring that a few key authentication-related files are in place. From the perspective of user, bringup entails simply powering up the vEdge router and plugging in a cable to connect the router to the network. The remainder of the bringup occurs automatically via a zero-touch-provisioning process.

The network administrator performs the following tasks as part of the initial bringup:

1. Configure the vBond orchestrator function on one of the vEdge routers in the network. In our example, this is vEdge-1.
2. Optionally, configure a top-level vBond orchestrator to act as a ZTP server. In this situation, a DNS server must be present in the enterprise network.
3. Ensure that a DHCP server is present in the enterprise network.
4. Install the signed certificate on the vManage NMS, and download that certificate to the vBond orchestrator.
5. Install the vEdge router authorized serial number file on the vManage NMS, and then download it to the vSmart controllers.
6. From the vManage CLI, create a configuration for each vSmart controller and vEdge router in the overlay network:

   a. Configure a system IP address, which is similar to the router ID address on a traditional router, identifying the Cisco vEdge device with an address that is independent of any of the interfaces on the device. System IP addresses must be pre-allocated and must be unique across each vEdge router and vSmart controller. These addresses need not be routable through the network.

   b. Configure site IDs for the various sites in the overlay network. In our example, vEdge-1 is at site-100 and vEdge-2 is at site-200. The vSmart controller can be collocated at a site, or it can be in its own site.

   c. Configure domain IDs. This is an optional step to create clusters. For our example, configure the domain-ID as 1.

   d. Configure the IP address or DNS name for the vBond server and the vSmart controller.

   e. Configure WAN interfaces on vEdge-1 and vEdge-2. VPN 0 is the VPN reserved for WAN transport interfaces. IP addresses can be automatically obtained through DHCP. Alternatively, you can configure a default gateway and DNS explicitly.

   f. By default, DTLS and IPsec are enabled on the WAN interfaces.

   g. Save the configuration.

When the vSmart controllers join the network, they are authenticated by the vBond orchestrator, and when vEdge routers join the network, they are authenticated by both the vBond orchestrator and the vSmart controllers. These devices then connect to the vManage NMS, which downloads the configuration to them.

**Example Configuration on vEdge-1:**

```plaintext
system
  host-name vEdge-1
  system-ip 1.0.0.1
  domain-id 1
  site-id 100
  vbond 75.1.1.1 local

vpn 0
  interface ge 0/0
    ip address 75.1.1.1/24
    tunnel-interface
    color default
    no shutdown
  ip route 0.0.0.0/0 75.1.1.254
```

The remaining sections in this article describe how to configure additional common functionality on vEdge routers and vSmart controllers. Typically, you configure all functionality at one time, in the configuration that you create on the vManage NMS and that is downloaded to the device when it joins the overlay network. However, to highlight the different functionalities, this article describes the various portions of the configuration separately.

**Step 2: Enable Host or Service-Side Interfaces and Routing**

From the vManage NMS, you can also configure service-side interfaces and regular routing:

1. Configure interfaces on vEdge-1 towards the existing traditional router. Assign IP address and put the interface in a non-default VPN. In our example, this is VPN 1. Do the same on vEdge-2.
2. Configure OSPF or BGP on the vEdge routers towards the existing routers.

3. Commit.

To check for standard IP reachability, routes, and next hops at the local site, use the standard `ping`, `traceroute`, and various `show` commands on the vManage NMS or from the CLI of the device (if you have a direct connection to the device):

**Example Configuration for the Host or Service-side VPN:**

```plaintext
vpn 1
    router
        ospf
            redistribute omp
            area 0
                interface ge 0/1
                exit
            exit
    !
    interface ge 0/1
        ip address 10.1.2.12/24
        no shutdown
```

**Step 3: Enable Overlay Routing over OMP**

All site-local routes are populated on the vEdge routers. Distributed these routes to the other vEdge routers this is done through the vSmart controller, via OMP.

1. If you are using BGP or if there are OSPF external LSAs, allow OMP to redistribute the BGP routes.

2. Re-advertise OMP routes into BGP or OSPF.

3. Commit.

**Example Configuration of Overlay Routing over OMP:**

```plaintext
omp
    advertise ospf external
```

At this point, vEdge-1 is able to learn about the prefixes from site-200, and vEdge-2 is able to learn about prefixes from site-100. Because all the prefixes are part of VPN 1, the hosts in site-100 and site-200 have reachability with one another. From a Cisco SD-WAN overlay network point of view, this reachability is possible because vEdge-1 advertises a vRoute consisting of the address 10.100.0.0/24 and the TLOC color of default, which we write as \{75.1.1.1, default \}, to the vSmart controller. In turn, the vSmart controller advertises this vRoute to vEdge-2. The same process happens with prefix 10.200.0.0/24 on vEdge-2.

**Step 4: Check the Automatic Setup of the IPsec Data Plane**

For every TLOC on a vEdge router, the vEdge router advertises a symmetric key for encryption. The vSmart controller reflects this key automatically and advertises the TLOC with the symmetric key. A two-way IPsec SA is set up as a result (that is, there is a different key in each direction), and data traffic automatically starts to use this IPsec tunnel. Once a tunnel is up, BFD automatically starts on the tunnel. This is done to ensure fast data plane convergence in the event of a failure in the transport network.

Note that the setup of the IPsec data plane happens automatically. No configuration is necessary. Multiple show commands are available to check the SAs and the state of the IPsec tunnel.
Step 5: Enforce Policies

As an optional step, you can create control and data plane policies on the vSmart controller and push them to the vEdge routers. As an example, if the network administrator wants to enforce a policy to divert traffic destined to \{ vEdge-2, prefix 10.200.0.0/24 \} to go to another site say vEdge-3, a control plane policy can be created on the vSmart controller and pushed to the respective vEdge routers. Note that the results of the policy are pushed to the vEdge routers, not the configuration itself.

Example Configuration of Policies:

```bash
policy
  lists
    site-list site-100
    site-id 100
  !
  prefix-list my-prefixes
    ip-prefix 10.200.0.0/24
  !
  control-policy TE-thru-vedge3
    sequence 10
    match route
      prefix-list my-prefixes
    !
    action accept
    set
      tloc 1.0.0.3 color default
    !
    default action accept
  !
apply-policy
  site-list site-100
  control-policy TE-thru-vedge3 out
  !
```

Advanced Options

Now that we have looked at basic routing, security, and policy, we can start adding various other elements to the network. You are encouraged to look at the Software category to add elements such as High Availability, Convergence, BFD, QoS, ACLs, segmentation, and advanced policy.

Cisco SD-WAN Terminology

The following figure summarizes the terminology used to describe a Cisco SD-WAN overlay network.
Domain ID

A domain is a logical grouping of vEdge routers and vSmart controllers that demarcates the span of control for the vSmart controllers. Each domain is identified by a unique integer, called the domain ID. Currently, you can configure only one domain in a Cisco SD-WAN overlay network.

Within a domain, vEdge routers can connect only with the vSmart controllers in their own domain. The vBond orchestrator is aware of which vSmart controllers are in which domain, so that when new vEdge routers come up, the vBond orchestrator can point those routers to the vSmart controllers in the proper domain. However, the vBond orchestrator is never a member of a domain.

Within a domain there is full synchronization of routing information among the vSmart controllers and vEdge routers, and there is scope for route aggregation and summarization. An organization can divide up its network into domains to serve desired business purposes. For example, domains can correspond to a large geographic area or to data centers so that each data center and the branches for which it is responsible are contained within a single domain.

OMP Routes

On vSmart controllers and vEdge routers, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs. These routes are called OMP routes, to distinguish them from standard IP routes. It is through OMP routes that the vSmart controllers learn the network topology and the available services.

The Cisco SD-WAN control plane architecture uses three types of OMP routes:

- OMP routes—Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.

- Transport locations (TLOCs)—Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.
• Service routes—Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers.

Site ID

A site is a particular physical location within the Cisco SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each Cisco vEdge device at a site is identified by the same site ID. So within a data center, all the vSmart controllers and any vEdge routers are configured with the same site ID. A branch office or local site typically has a single vEdge router, but if a second one is present for redundancy, both routers are configured with the same site ID.

System IP Address

Each vEdge router and vSmart controller is assigned a system IP address, which identifies the physical system independently of any interface addresses. This address is similar to the router ID on a regular router. The system IP address provides permanent network overlay addresses for vEdge routers and vSmart controllers, and allows the physical interfaces to be renumbered as needed without affecting the reachability of the Cisco vEdge device. You write the system IP address as you would an IPv4 address, in decimal four-part dotted notation.

TLOC

A TLOC, or transport location, identifies the physical interface where a vEdge router connects to the WAN transport network or to a NAT gateway. A TLOC is identified by a number of properties, the primary of which is an IP address–color pair, which can be written as the tuple {IP-address, color}. In this tuple, IP address is the system IP address and color is a fixed text string that identifies a VPN or traffic flow within a VPN. OMP advertised TLOCs using TLOC routes.

Additional Information

For a description of the elements in a Cisco SD-WAN overlay network, see Components of the Cisco SD-WAN Solution. For an understanding of how you put together an overlay network using Cisco SD-WAN software and hardware, see Constructing a Basic Network Using Cisco SD-WAN Components. For examples of how the components of the overlay network work, see the Validated Examples.

Licensing on Cisco SD-WAN

A massive transformation is happening in wide-area networks with the second wave of software-defined networking moving from the data center to the WAN. Cisco is reinventing the enterprise network with a new era of intent-based networking solutions that include policy-based orchestration, automation, and assurance. Customers have access to the latest innovations through simple subscription tiers and management flexibility, in the cloud or on premises (on-prem), across the routing stack. For customers who require enterprise-grade Software Defined WAN (SD-WAN), cloud networking and WAN network-as-a-service functions, the Cisco SD-WAN offer is the optimal solution. To use Cisco SD-WAN, you can choose from several Cisco Digital Network Architecture (Cisco DNA) software subscriptions.
Overview of Licensing on Cisco SD-WAN

Cisco DNA Software subscription for SD-WAN gives the flexibility to consume the latest technology, either on the Cloud or On-Premises across the entire routing stack. Cisco DNA Software subscriptions provide customers with four key benefits:

- Investment protection of software purchases through software-services-enabled license portability
- Software suites that address typical customer use-case scenarios at an attractive price
- Flexible licensing models to smoothly distribute your software spending over time
- Access to new technology from Cisco

Cisco DNA licenses offer both portability and flexibility to move from cloud management (Cisco vManage) to on-premises management (Cisco DNA Center) and across hardware platforms.

Restrictions for Cisco SD-WAN Licensing

- Smart Licensing, a standardized licensing platform that simplifies the Cisco software experience, is supported across ISR Series, ASR series, CSR1000V, and ISRv routers. However, Cisco SD-WAN does not support Smart Licensing. Although you can use the Cisco SD-WAN functionalities through the CSR1000V 17.2.1r image - controller mode, Cisco SD-WAN does not support Smart Licensing.
- You cannot use the management platforms (such as Cisco vManage) to view license consumption information.
- You cannot view license consumption information on Cisco IOS XE SD-WAN devices and Cisco vEdge devices. For information on license consumption, see your purchase order(s).

Cisco SD-WAN Licensing Options

The subscription licensing offers for Cisco SD-WAN are as follows:
• Cisco DNA Essentials: Standard SD-WAN upto 50 devices.
• Cisco DNA Advantage: Cloud-Scale SD-WAN
• Cisco DNA Premier: Advanced Cloud security SD-WAN

These subscriptions are available on a 3-year or 5-year subscription.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco DNA Essentials</th>
<th>Cisco DNA Advantage</th>
<th>Cisco DNA Premier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device limit</td>
<td>Up to 50 devices</td>
<td>Unlimited devices</td>
<td>Unlimited devices</td>
</tr>
<tr>
<td>vManage for Centralized management (cloud or on-premises)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Flexible topology (hub and spoke, partial mesh, full mesh)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application-based policies (including application-aware routing policies)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>L3/L4/App-Aware Firewall</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Snort IPS/IDS with Talos signature updates</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNS monitoring and connector for Cisco Umbrella</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Basic path optimization capabilities including Forward Error Correction (FEC)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dynamic routing protocols (OSPF/BGP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unlimited segmentation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>vAnalytics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud OnRamp for Infrastructure-as-a-Service (IaaS)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud OnRamp for Infrastructure-as-a-Service (IaaS)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Configure Cisco SD-WAN Licensing

Cisco SD-WAN licenses are right-to-use (RTU) licenses. Unlike other Cisco RTU licenses, you need not manually configure the Cisco SD-WAN licenses except in the case of Integrated Services Routers and CSR1000V and ISRv.

To configure Smart Licensing with the above-mentioned routers, perform the following steps:

1. Configure Smart Call Home.
2. Generate the token or authorization ID on Cisco Smart Satellite Manager (CSSM).
3. Register the ISR, CSR1000v, or ISRv device to CSSM.

You can purchase Cisco SD-WAN licenses by placing a sales order. For more information, contact your Cisco sales team.

For Cisco Integrated Services Routers, if you want more than 250 Mbps of throughput, you must have a HSECK9 license. This requirement is due to the US export control regulations. If you ordered the HSECK9 license when you ordered the router, the HSECK9 license is installed by default. If the HSECK9 license was not installed by default, you must get a HSECK9 PAK license file and install the license file on each router.

For virtual routers such as the CSR1000V and ISRv, if you want more than 250 Mbps throughput, you must configure a call-home profile and then perform the other steps to configure a Smart License. To use the controller mode in Cisco IOS XE Release 17.2.1r or later releases on CSR 1000V or ISRv, configure call home profile using CLI Add-on template.

To know how to add and use the CLI Add-on template, see CLI Add-On Feature Templates.

**Configure Call Home Profile For CSR1000V and ISRv**

**Default Configuration**

To configure a call-home profile in a default configuration, execute the following command. This is the minimal configuration and is applicable for direct cloud access either using the Smart Call Home Transport Gateway or using the HTTPS proxy, where the device reaches out to the cloud-hosted CSSM service.

```bash
call-home
  contact-email-addr sch-smart-licensing@cisco.com
  profile "CiscoTAC-1"
  active
  destination transport-method http
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```
Configure a Device With Multiple Interfaces

Perform the following configuration if there are two or more interfaces in the device. In this case, you must configure the `ip http client source interface` CLI so that the device can use that specific interface to reach out to the CSSM portal.

```bash
ip http client source-interface <interface-name>  #==
call-home
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Configure Call Home for DNS Resolution

To configure a call home profile for DNS resolution, instead of `ip http client source-interface`, use the following configuration so that the device uses an IPv4 interface for DNS resolution and to reach out to the CSSM. If there are multiple IPv4 interfaces, one after another is tried for successful DNS resolution, and that specific interface is used to reach out to the CSSM.

```bash
ip http client source-interface <interface-name>  #==
call-home
contact-email-addr sch-smart-licensing@cisco.com
http resolve-hostname ipv4-first  #==
profile "CiscoTAC-1"
active
destination transport-method http
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

**Note**

For detailed information about call-home profile for CSR1000V and ISRv devices, see Configuring Call Home Profile for CSR1000V.