Solution Architecture

For supported software information, click here.

The Versa Networks SD-WAN deployment architecture consists of two basic components: headends and branch (edge) nodes. A Versa headend node consists of the Versa Controller, Versa Director, and Versa Analytics. A branch node is a Versa Operating System™ (VOS™) device. instance.

Headend Node

A Versa headend node consists of the Versa Controller, Versa Director, and Versa Analytics. The headend can be deployed in a data center or in a colocated, public, or private cloud. In most deployments, redundant headends are used for high availability. They are typically located in two geographically separate data centers or other centralized locations, or in the cloud in separate zones or regions.

The headend components communicate across a secure, IP-based control channel and work in conjunction with each other to manage a network of VOS devices that are located at branches. The VOS branch devices are connected to each other and to the headend through a public network (such as the internet) or through a private network (such as an MPLS network), or through both.

Figure 1 shows the headend components.

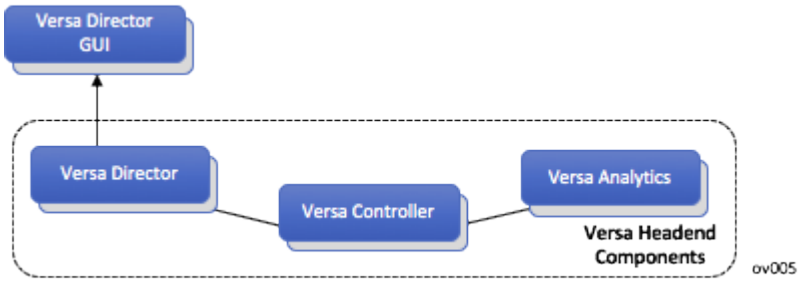

Figure 1: Headend Components

Versa Controller

The Versa Controller is a VOS instance that provides the control plane element for all VOS instances in the network,

including branches, hubs, and gateways (nodes). It is typically located in a centralized location (data center, central office, or public cloud) from which it connects to all the nodes in the network. Control overlay tunnels from each node to Versa Controllers form the control plane of the Versa SD-WAN solution. These tunnels carry both IPsec and MP-BGP traffic. Failure detection on the control plane is governed by the IKE keepalive mechanism, called dead peer detection, and by the MP-BGP hold-on timer.

The Versa Controller is responsible for the following functions:

- Onboard SD-WAN VOS branches into the network—Versa Controller uses IKE and PKI certificates to authenticate branch VOS instances, and in conjunction with Versa Director, it uses two-factor authentication to authenticate branch routers.
- Maintain a secure control channel with each node—The secure IKE channel carries all control traffic between branch nodes and the Versa Controller, which then communicates with Versa Director and Versa Analytics nodes. Using the secure IKE channel, Versa Controller handles all management activities between the remote and headend nodes, such as using Netconf over SSH to push configuration templates and activate services, and distributing control plane information using MP-BGP.
- Distribute reachability information for all the nodes—Versa Controller distributes BGP routes toward VPNs and tenants. It uses a custom multi-instance MP-BGP route reflector to distribute route and security association (SA) information to branch nodes in the network group, based on the tenant or VPN. When a branch node advertises its overlay route information, it includes an inbound SA. The Versa Controller redistributes the BGP route updates, labels (in the case of multitenant VPN), and SAs so that destination branches can establish secure data channels toward all branch node CPEs in the same VPN. Based on how you configure the redistribution policy, the appropriate topology (hub and spoke, full mesh, or partial mesh) is created.
- Enable IPsec connectivity between branches without the overhead of maintaining a full mesh of IKE keys among all branches—This optimization avoids the overhead of managing N2 links and keys, instead having Versa Controller distribute the SA information. The IPsec link between the branch node and the Versa SD-WAN Controller distributes IPsec keys to other branch nodes. The result is that branch nodes have to maintain N+1 keys instead of N2 keys.

You can deploy one Versa Controller for each SD-WAN network, or you can deploy multiple Versa Controllers to provide high availability. A single Versa Controller can support up to 256 tenants.

Branch Nodes

The branch nodes in a Versa Networks solution provide networking and security functions consolidated into a single VOS instance that can be deployed on a bare-metal x86 appliance (such as a Versa Cloud Services Gateway) or as a virtual machine (VM). Branch nodes are located, as the name implies, at branch office sites. They are connected to each other and to the headend through a public network (such as the internet) or through a private network (such as an MPLS network), or through both.

You can deploy branch nodes in one of the following topologies:

- Hub and spoke
- Full mesh
- Partial mesh

In a multitenant environment, you can deploy the desired topology on a per-tenant basis. Versa Director provides workflows to guide you through the configuration of branch nodes in the desired topology.

Hub and Spoke

A hub-and-spoke topology allows you to choose whether and how spoke nodes communicate with each other, depending on your business requirements. Hub-and-spoke topologies are widely deployed because they are easier to set up and manage and are generally less expensive than full-mesh or partial-mesh topologies. In hub-and-spoke branch deployments, at least one node is configured as a hub and one or more nodes are configured as spokes.

Figure 2 shows a hub-and-spoke topology in which three branch nodes are spokes connected to the hub node.

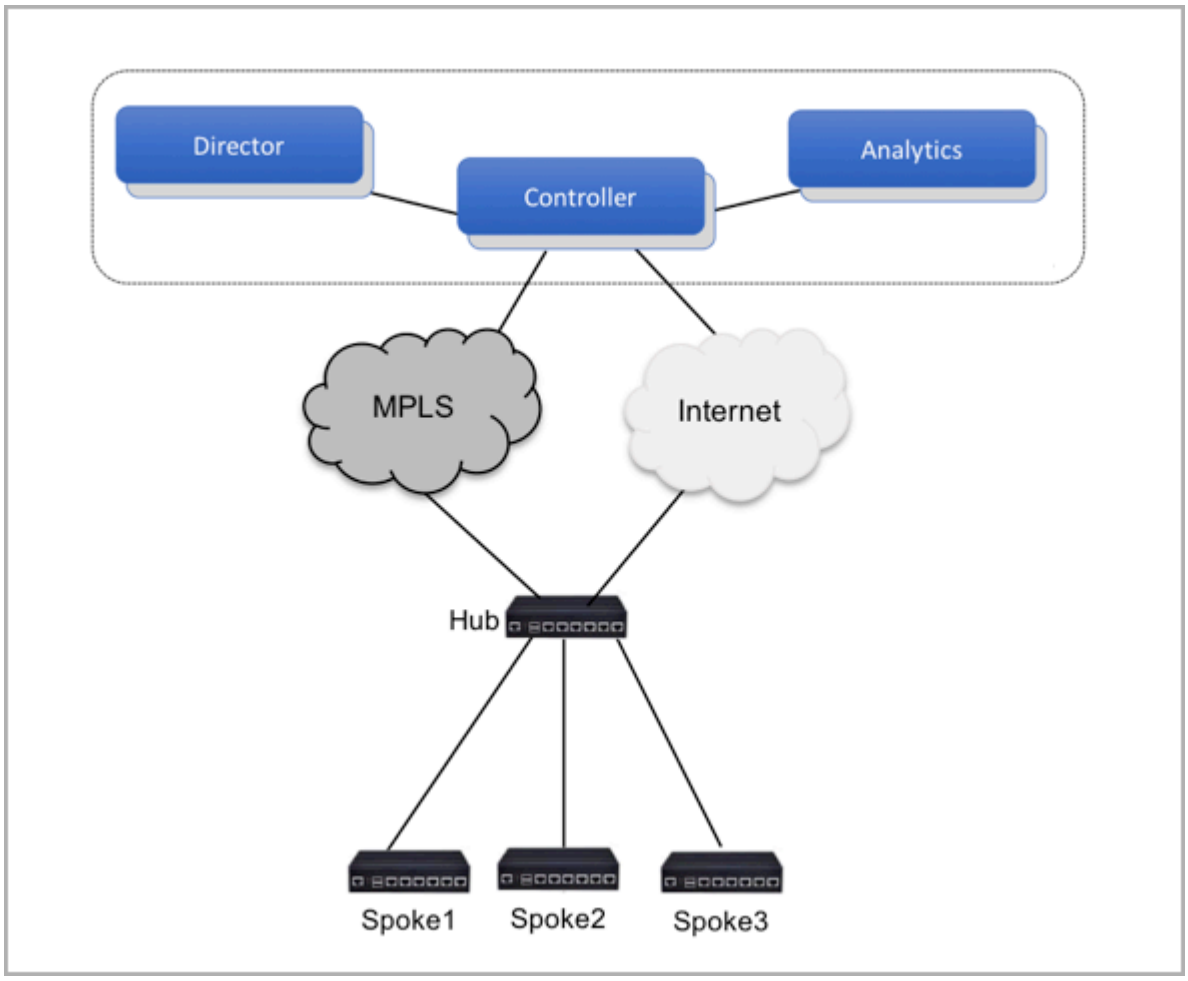

Figure 2: Hub-and-Spoke Deployment

When you configure a hub-and-spoke topology, you can choose whether a spoke can communicate with other spokes that are connected to the same hub by allowing or limiting route advertisements from the hub to the spoke. To do this, you create spoke groups and assign one of three topology types, as follows:

- Spoke to hub only—Branches must route all traffic through the hub. Use this topology when a spoke needs to communicate only outward from the hub (for example, to access central services) and does not need to communicate with other spokes.

- Spoke to spoke through a hub—Branches can route traffic to other branches, but all traffic must pass through the hub. With this topology, the spoke group policy allows routes from one branch to another branch that pass through the hub and it rejects direct routes from one branch to another branch.
- Spoke to spoke direct—Creates groups of branches that are connected in a full-mesh fashion so that they can communicate directly with each other but so that they also have connectivity to other spoke groups through the hub.
- Spoke-hub-hub-spoke—A spoke-hub-hub-spoke (SHHS) topology consists of islands of spoke devices that are interconnected using hubs. You can group hubs and spokes into regions. This topology is useful in large SD-WAN networks that have a large number of geographically dispersed devices. The Versa Director workflow that creates a hub-and-spoke topology automatically generates configurations that control the route advertisements that correspond to the desired topology.

The Versa Director workflow that creates a hub-and-spoke topology automatically generates configurations that control the route advertisements that correspond to the desired topology.

Full Mesh

In a full-mesh branch topology, all branch nodes can communicate directly with all other branch nodes, as shown in Figure 3.

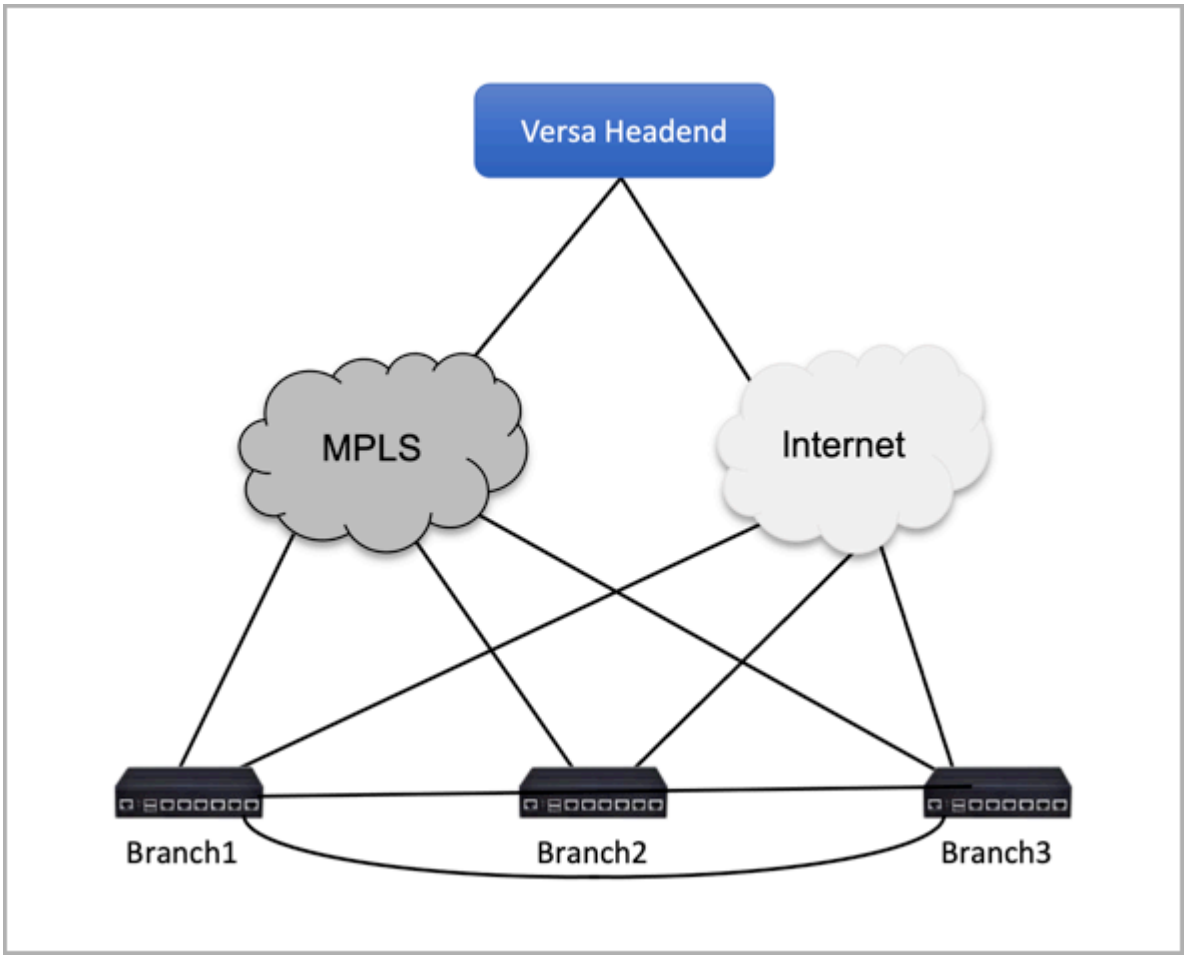

Figure 3: Full-Mesh Deployment

A full-mesh topology uses network resources more efficiently than a hub-and-spoke topology or a partial-mesh topology, offering the least amount of traffic latency. It is also highly redundant and fault tolerant—because all sites can be reached using multiple paths, there is no single point of failure. However, it takes more time and effort to create and maintain a full-mesh topology than a hub-and-spoke or partial-mesh topology.

Partial Mesh

In a partial-mesh deployment, two or more nodes are connected to each other to form a full mesh topology while other nodes communicate through a hub (optional) or connect directly to a Versa Controller. Figure 4 shows a partial mesh in which Branch1, Branch2, and Branch3 form a full mesh while Branch4 is not part of the mesh.

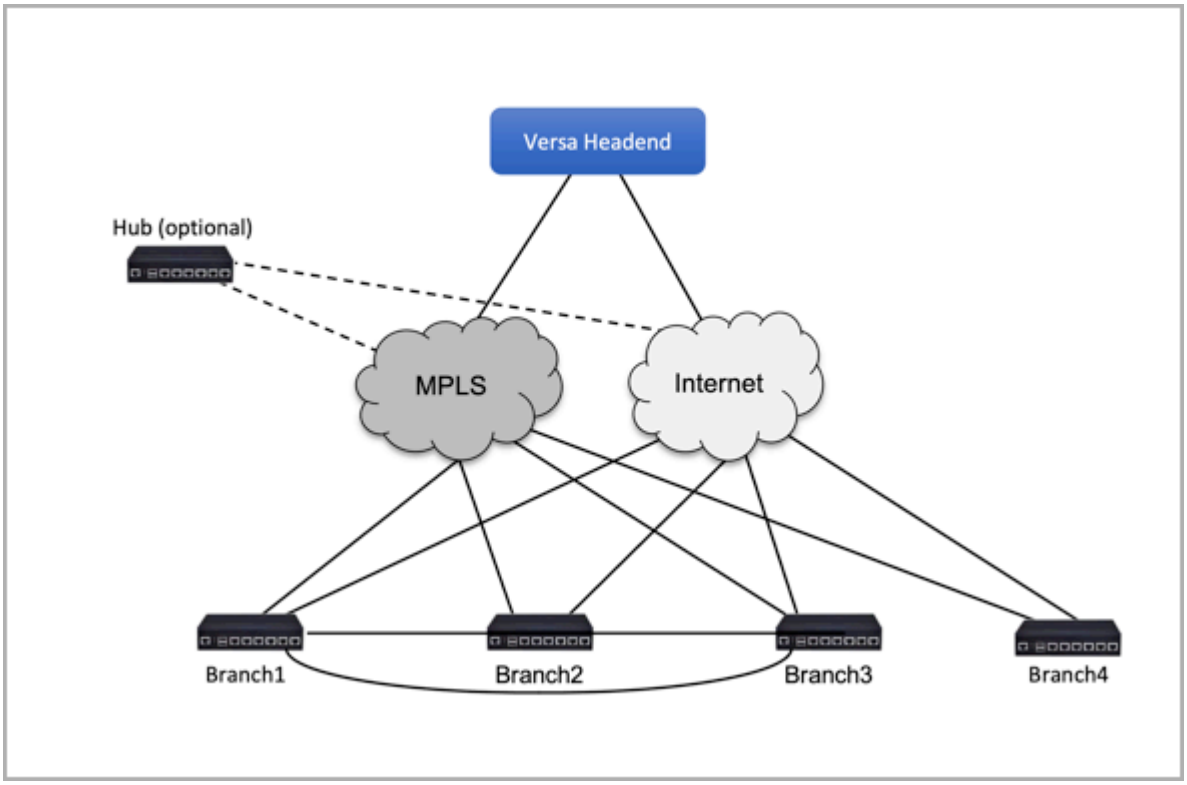

Figure 13. Partial-Mesh Deployment

A partial-mesh topology has most of the same advantages as a full-mesh topology, and it has the additional advantage of allowing for sites that do not, or should not, communicate directly with other sites. The nodes that are part of the full-mesh portion of the topology provide redundancy and fault tolerance, and the non-mesh nodes are easier to set up and manage. A partial-mesh topology takes more time and effort to create and maintain than a hub-and-spoke topology, but less time and effort than a full-mesh topology.

Updated: Wed, 23 Oct 2024 07:32:36 GMT

SD-WAN Gateway

In SD-WAN architectures, a gateway element is deployed to connect the SD-WAN domain to a non-SD-WAN domain (such as an MPLS VPN or an IPsec VPN) or even to a security service for connectivity to cloud or SaaS applications. A primary SD-WAN Gateway function is to distribute routing information between the MPLS VPN and SD-WAN VPN domains so that forwarding paths between the two domains can be established. In the Versa Networks SD-WAN solution, each VOS instance in the network can be configured as a gateway. This means that each node in a Versa SD-WAN provides a connection point between an MPLS VPN domain and an SD-WAN VPN domain for forwarding data traffic from one domain to the other.

Versa Staging Server

The Versa staging server is a cloud-hosted node that is responsible for the initial bootstrapping and registering of branch devices in SD-WAN deployments. The staging server can be hosted by Versa Networks or by a service provider.

New branch hardware devices are preloaded with Versa VOS software and shipped with a Versa signed certificate, which the staging server uses to authenticate the VOS instance. During its initial bootstrapping sequence, a branch device sets up an IPsec tunnel to the staging server, over which it sends a staging request that includes the signed certificate. The staging server verifies the signed certificate and then sends a staging configuration to the branch device. The staging configuration reboots the device, creates an IPsec tunnel from the branch device to the Versa Controller, and redirects the branch device to the Versa Controller to continue the bring-up sequence. After this point, the branch device has no further communication with the staging server.

Note: To ensure that the deployed network elements are completely secured and under the control of the correct network owner, the Versa signed certificate is replaced with the network owner certificate during the bootstrapping process.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Features and Capabilities
Software Licensing
Solution Components
Solution Overview
Solution Use Cases