Solution Use Cases

For Releases 16.1R2 and later.

Versa Networks solutions are extremely flexible and provide a rich set of features. As such, you can deploy them in many different scenarios to address your specific business needs—from a basic virtual CPE (vCPE) or software-defined router or stateful firewall to a full-featured SD-WAN. This section describes some of the common use cases for Versa Networks solutions:

SD-Branch

The Versa enterprise SD-Branch solution provides a full set of integrated networking and security functions that run on a low-cost appliance with a single management screen. Instead of requiring multiple hardware appliances and software packages, the Versa SD-Branch solution allows enterprises to simplify their WAN and branch architectures by consolidating networking and security functions into a single Versa Operating System™ (VOS™) software instance that has a broad set of IP services, as shown in Figure 1. With the SD-Branch solution, enterprises can reduce their capital and operational expenses and minimize the time needed to manage the network, while significantly strengthening branch security and control.

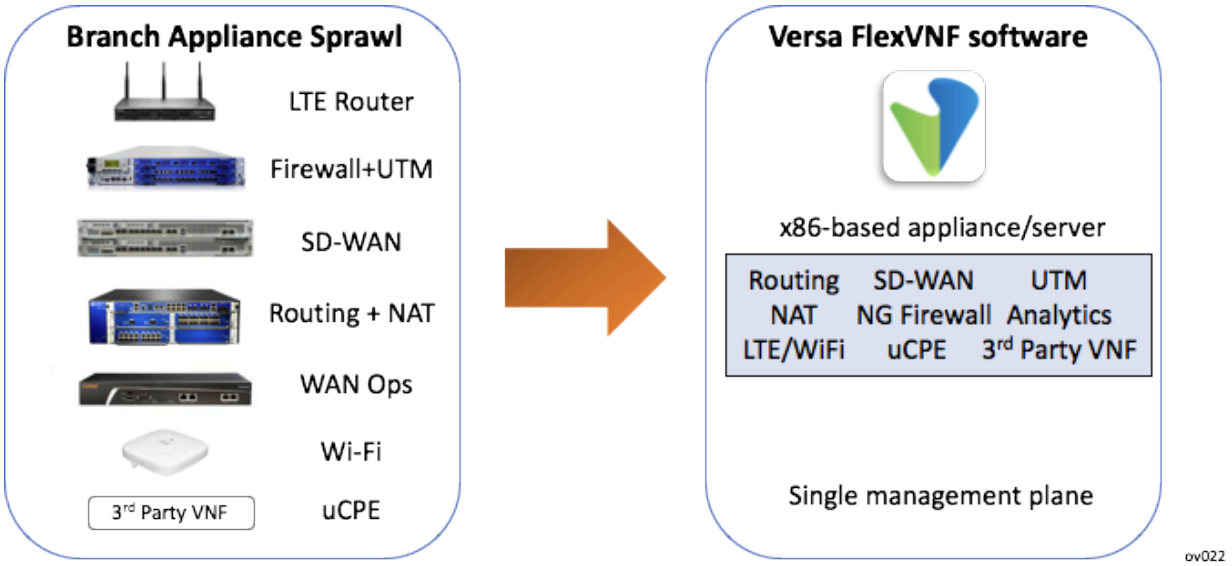

Figure 1: Eliminating Branch Sprawl with Versa SD-Branch Solution

Updated: Wed, 16 Dec 2020 23:56:20 GMT

The Versa SD-Branch solution allows service providers to deliver cost-effective and operationally efficient managed services that include traditional local-area and wide-area networking, SD-WAN, layered security functions, and new IP services. The solution includes full multitenancy from the data center or cloud to the branch office, Versa Networks and third-party service chaining, service elasticity, and ZTP for all networking and security functions.

SD-WAN

The Versa Networks SD-WAN solution provides a unified, secure VPN across multiple public and private WANs. This solution fully integrates Versa VOS services to allow enterprises and service providers to deploy a centrally managed SD-WAN solution.

Versa SD-WAN features and functions include:

- Application identification and policy-based management
- Secure overlays
- Continuous measurement of network conditions
- Traffic engineering based on policies and network conditions
- CODEC and mean opinion score (MOS)-based traffic engineering
- Direct internet access (DIA) and direct cloud access (DCA) SaaS site traffic engineering

Figure 2 shows a sample SD-WAN topology.

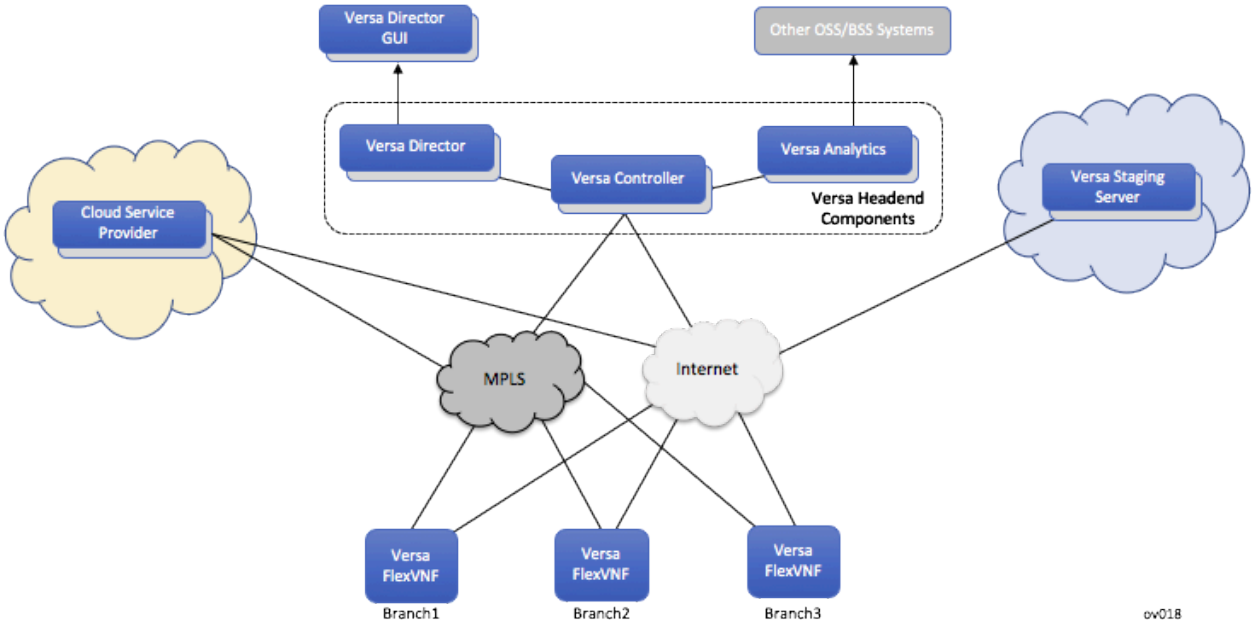

Figure 2: Sample SD-WAN Topology

The Versa SD-WAN Controller, a specially configured VOS instance, deploys and integrates SD-WAN nodes. Versa

Director communicates with each VOS instance through encrypted tunnels that terminate at the Versa Controller, and configuration templates are deployed dynamically that enable zero-touch provisioning (ZTP) of the Versa SD-WAN nodes.

Versa Networks SD-WAN architecture relies on secure IPsec-over-VXLAN overlay tunnels to transmit control-plane and data-plane traffic. Using overlay technologies provides traffic segregation, isolation, and privacy.

The Versa VOS software decouples control-plane functionality from data-plane functionality. The Versa Controller creates IPsec tunnels that carry control-plane information to branches and hubs using either the MPLS or the internet transport network, as shown in Figure 3.

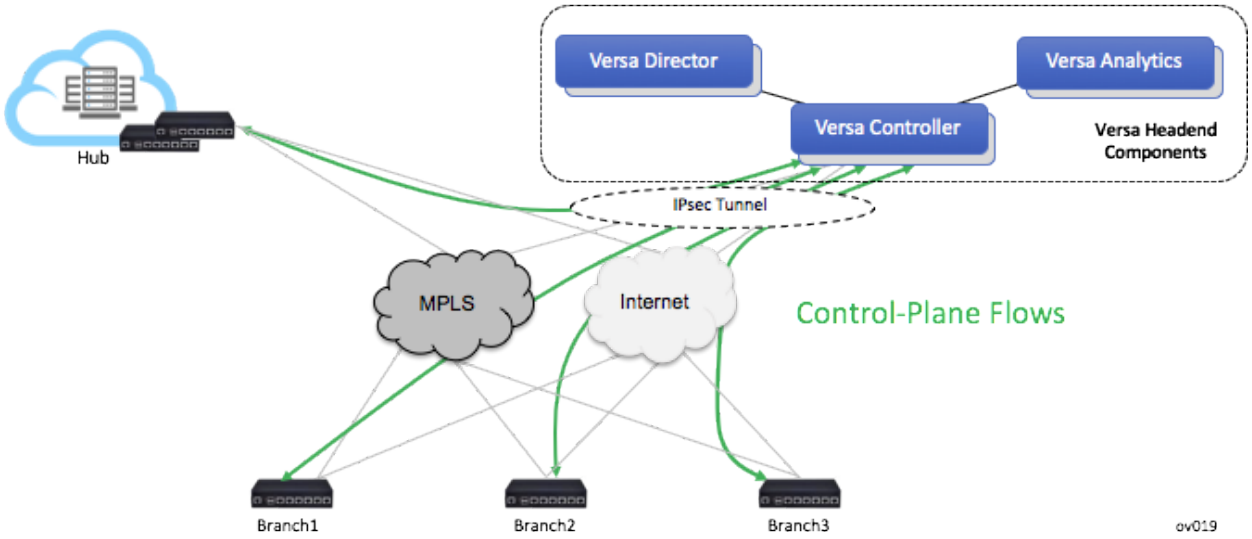

Figure 3: SD-WAN Control-Plane Flows

Similarly, hub and branch devices form IPsec tunnels that carry data-plane traffic, as shown in Figure 4.

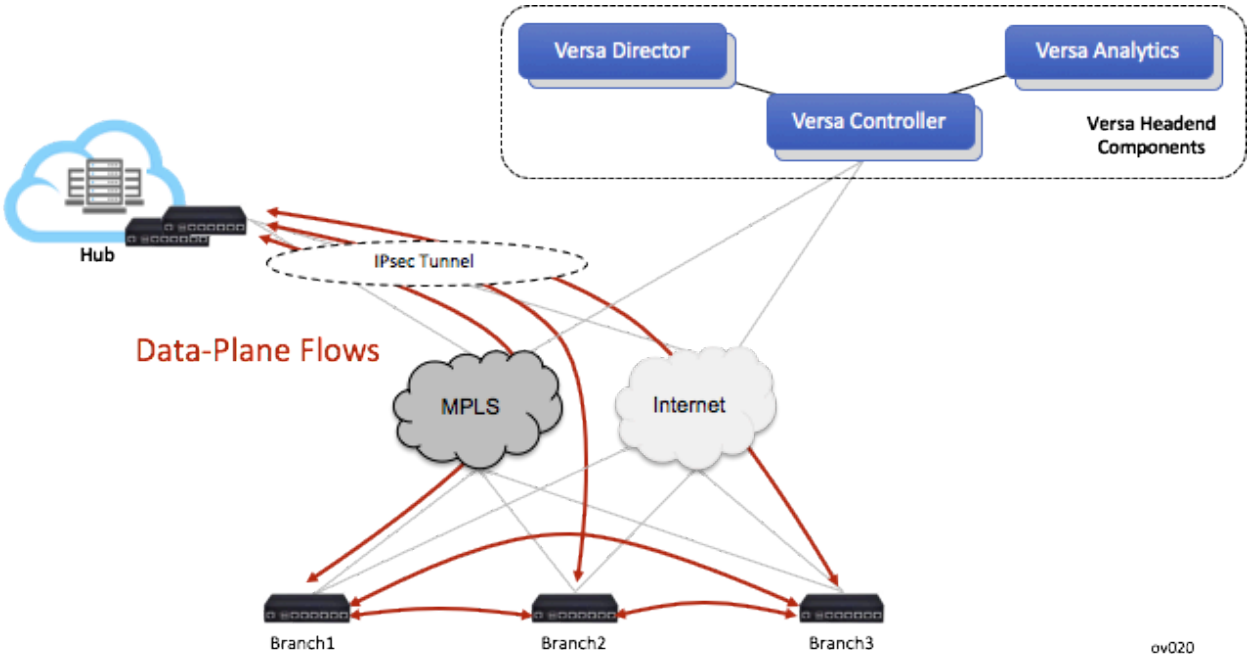

Figure 4: SD-WAN Data-Plane Flows

Figure 5 shows the component parts of the Versa SD-WAN solution. All control-plane and data-plane paths are secured using the Versa SD-Security services (native NGFW and UTM), which are discussed later in this article.

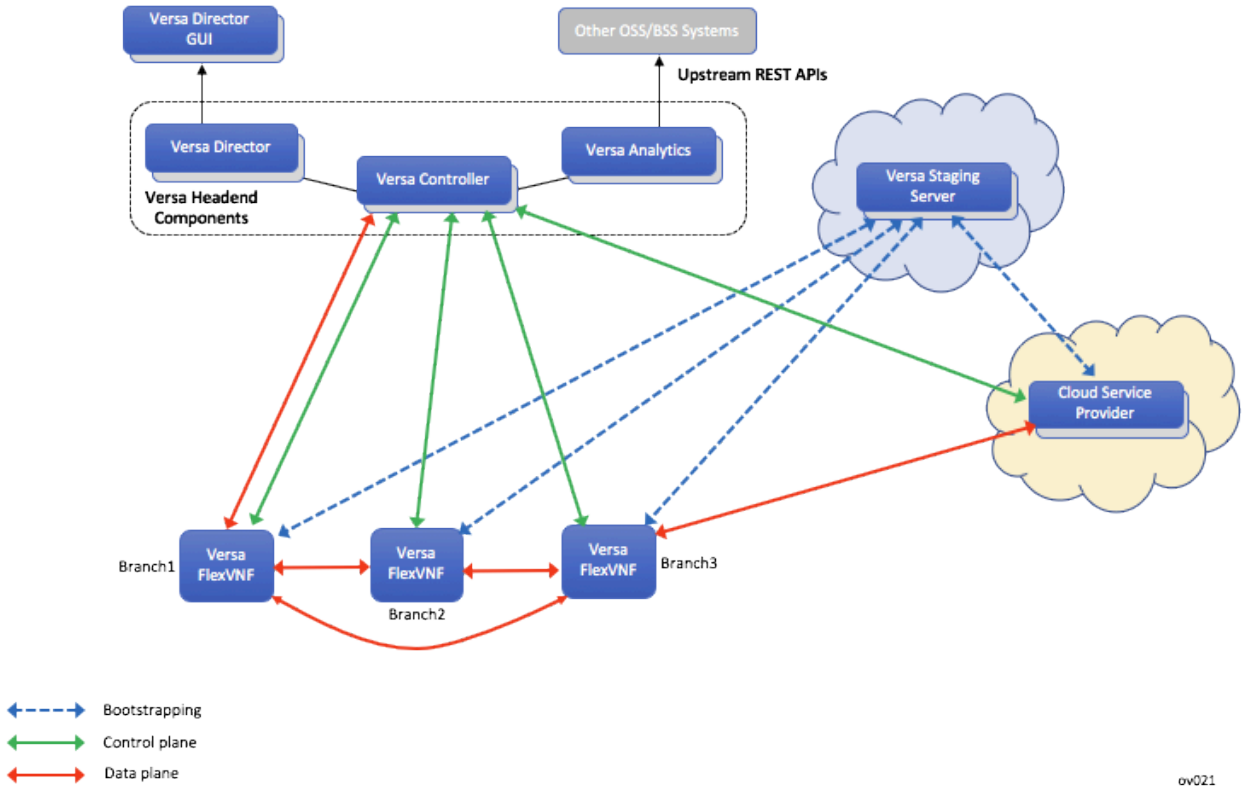

Figure 5: Versa SD-WAN Solution Components

The illustration shows the following SD-WAN components:

- Headend—Headend components can be located at corporate headquarters, a corporate data center, or a colocation data center
- Versa Director—Communicates with cloud management systems (such as VMware vCloud and OpenStack) using upstream RESTful APIs. It is also used by the staging server during the initial bootstrapping of a branch node
- Branch—Branch nodes are connected to the Versa SD-WAN controller in a full mesh topology
- Versa staging server—Responsible for initial bootstrapping and registration in SD-WAN branch deployments
- Cloud service provider (CSP)—Hosts other branch nodes and is connected to the control plane and the data plane

SD-Router

The Versa SD-Router solution enables you to quickly and easily deploy a low-cost, white-box appliance CPE router or a VNF cloud-based service that can be brought up with zero-touch provisioning (ZTP) and that can support multiple tenants. The Versa SD-Router consists of VOS carrier-grade routing features and is centrally managed by Versa Director, which provides a single, integrated dashboard to manage the entire WAN.

The standard SD-Router solution includes all the features needed for WAN router functionality. This solution can be

used to:

- Build SD-WAN overlays for any topology (full mesh, partial mesh, and hub and spoke) across any number of active or standby links
- Perform application identification and application policy-based forwarding
- Dynamically measure network performance and provide traffic engineering

Standard SD-Router standard software includes the following features:

- Application-aware carrier-grade NAT, to provide broadband connectivity
- BGPv4
- DHCP
- External service chaining
- IP geolocation
- IPv4
- LAG
- OSPF
- QoS and HQoS
- Route reflector
- Routing policies and policy-based forwarding (PBF)
- Stateful firewall, DoS protection, and IPsec to protect branch communications
- VLAN
- VRF
- VRRP
- ZTP

Advanced SD-Router advanced software includes the following features:

- IPv6
- MPLS VPNs
- Multicast
- Universal CPE (uCPE)

In SD-WAN deployments, Versa VOS devices provide routing for three main traffic patterns:

- Branch-to-branch routing—A VOS device in a branch node can route application traffic directly to a VOS instance in another branch. Branch-to-branch routing is preferred for application traffic that requires low latency, such as video and multimedia flows.
- Branch-to-cloud routing—A VOS device in a branch node can route traffic to cloud SaaS applications. This traffic might have unique routing policies local to the branch or redundancy and resiliency requirements for MPLS and broadband access links. This traffic might also have unique security policy and encryption requirements. Also, virtual private cloud (VPC) applications might require tight integration with branch or headend sites. In these cases, a VOS device provides complete traffic management to handle per-flow and end point security requirements.
- Branch-to-data center routing—Traffic can be routed from a branch node to mission-critical enterprise applications

located in corporate data centers. These applications typically have the strictest security and availability requirements. A VOS device enables routing policies based on source, destination, application type, latency, and jitter. Optimal paths, such as higher-cost MPLS links, can be preferred when available, but alternate encrypted links, such as broadband and LTE links, can serve as redundant alternatives to ensure business continuity.

Virtual Routers

Versa VOS devices support multitenancy by using multiple virtual routers (VRs) per node. A branch node can use three types of virtual routers:

- Transport virtual router
- Control virtual router
- LAN virtual router

A transport virtual router is responsible for one or more WAN links. It has its own forwarding table and is part of the underlay network, and it can run a routing protocol for split-tunnel gateways or direct internet access (DIA). The transport virtual router can also be used by other virtual routers in the node for connectivity to other SD-WAN nodes.

A control virtual router is tied to an organization (either a tenant or a customer). It typically runs MP-BGP and sends and receives per-tenant IPv4 VPN or IPv6 VPN routes to SD-WAN controllers using route reflectors. The control virtual router uses IPsec or VXLAN tunnels to forward traffic to other control virtual routers. Tunnels to Versa Controllers are static, and the tunnels to branch, hub, and gateway nodes are created dynamically. You can use the service provider control virtual router to send and receive Versa BGP private address family routes that transmit underlay route changes and IPsec key refreshes. You can also use tenant control virtual routers to transmit Versa private address family routes.

The LAN virtual router is also tied to an organization (either a tenant or a customer) and is responsible for the LAN interfaces in the node. The LAN virtual router is a special type of virtual router that performs virtual routing and forwarding (VRF). The LAN virtual router is paired with a control virtual router that is responsible for sending the LAN virtual router's routes to other devices in the VRF. The Versa software uses MP-BGP with IPv4 VPN address families to advertise routes, so route targets and route distinguishers are assigned to the LAN routes.

SD-Security

The Versa SD-Security solution provides fully integrated and layered security services to deepen and simplify branch security. It is a carrier-class, multitenant solution that has built-in and programmable service chaining. SD-Security is a software-only solution, so there is no reliance on proprietary hardware, and you can deploy it anywhere in a Versa SD-WAN at the branch, cloud, or data center. You manage the SD-Security centrally, using control, security, and threat policies, and feeds provided by Versa Networks and third parties, and you can enforce these policies globally for branches, hubs, and data centers, whether on premises, off premises, or in the cloud.

The Versa SD-Security solution has received multiple certifications, including:

- ICSA Labs Firewall Certification for Stateful Firewall and DOS Protection
- NSS Labs NGFW, NG-IPS, SSL-Proxy Certified

- ONUG SD-WAN and SD-Security Working Groups: Top 10 Requirements Verified
- VMware Ready for NFV Certification

uCPE

The Versa Networks universal CPE (uCPE) solution is an open platform that allows VNFs from Versa Networks and third-party vendors to be deployed in customer branches or hub sites. You can deploy a variety of services as they are needed. The Versa uCPE runs in a virtual machine (VM) on x86-based server hardware within a branch node, and it is managed by Versa Director.

The Versa uCPE solution consists of the following major components:

- x86-based white box uCPE appliance
- VOS host OS with the appropriate virtualization capabilities
- Standard virtualization mechanisms, including KVM and QEMU
- Built-in service-chaining and intelligent traffic-steering capabilities
- Lightweight VM life cycle management (VMLM) capabilities
- Versa Director as the management platform to define, deploy, and manage policies and service chains

Figure 6 shows a high-level view of the Versa uCPE solution.

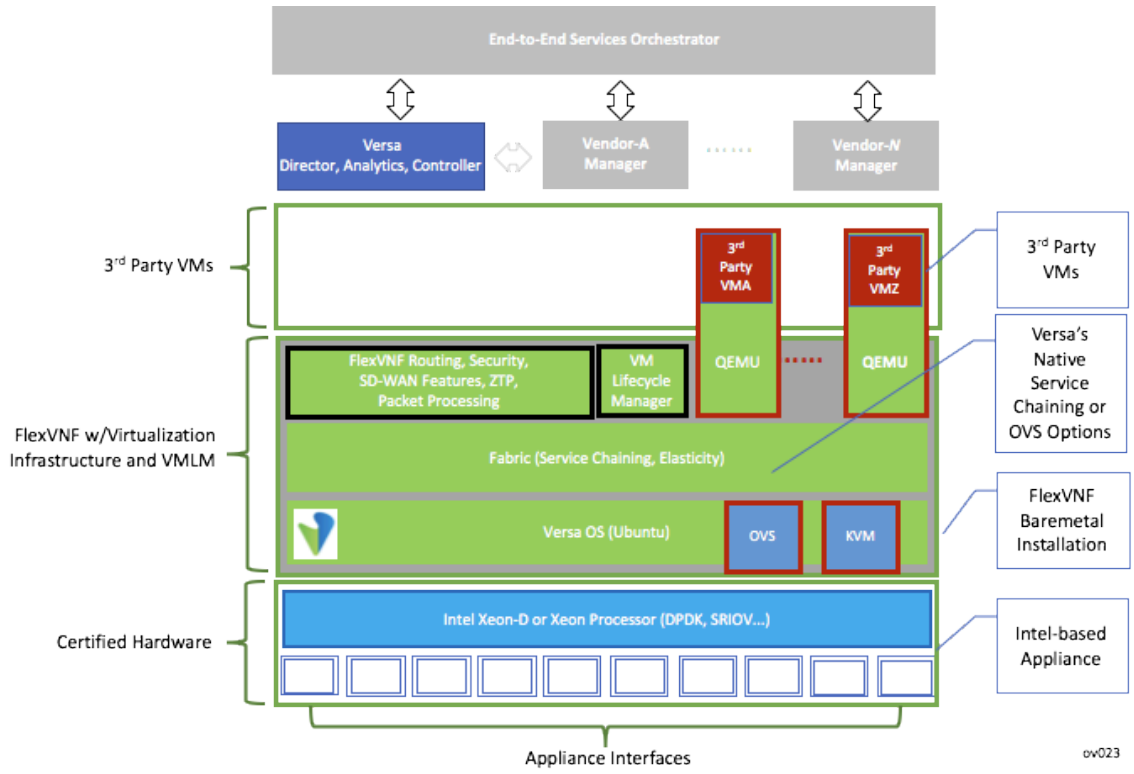

Figure 6: High-Level View of Versa uCPE Solution

The Versa uCPE solution delivers WAN edge functionality, including:

- Single appliance, optimized for uCPE performance
- Single point of integration to enable management, control, and visibility
- Automation of networking stack and security-stack interoperability
- Automation and management of the lifecycle of third-party VNFs

The Versa uCPE solution provides the following third-party VMLM functions and service chaining capabilities:

- Provide the equivalent functions of cloud-init utilities, including booting VMs with IP addresses and providing service tags to steer traffic into and out of each VM
- Provide a basic staging configuration for each VM
- Bring up an out-of-band (OOB) management interface for each VM, and connect the interface to the Versa secure management channel so that each VM can communicate with its EMS or NMS application (which is located in the management cloud) over an encrypted channel
- Provide intelligent service chaining between Versa native services and physical or virtual third-party services
- Steer packets to and from third-party VNFs to VOS instances
- Route third-party management and control plane traffic to and from the VOS uCPE

Software Release Information

Releases 16.1R2 and later support all content described in this article.

Additional Information

Features and Capabilities
Solution Architecture
Solution Components
Solution Overview