Cisco VMS Service Packs

A central theme behind the VMS solution is reducing the operational cost of deploying and maintaining service provider based managed services. The solution shifts the deployment of managed services away from the manual configuration of the latest network devices to the creation of a software abstraction to represent the service definition. This approach allows the service intent of the user, to be realized through the use of service models to automate the creation and customization of SD-WAN services.

VMS is a next generation managed service solution for service providers who are interested in hosting enterprise connectivity and security features in their cloud infrastructure. The keys to the VMS solution are virtualization, plug-n-play CPE devices, and a flexible orchestration engine capable of centralizing the configurations of all the devices involved in the delivery of a service. With flexibility inherent in the orchestration engine, service providers can offer end customers the ability to order the service that best meets their technical and TCO requirements.

The VMS architecture is based on a service package infrastructure. VMS service packages are bundled Virtual Network Function (VNF) types, the type of services available that are tightly coupled to the VNF types included in a specific service package. The end customer, based on a service provider deployment, has a choice based on services that can be orchestrated given the VNF types, which are included in the service package bundle.

This chapter contains the following sections:

Cisco VMS Cloud VPN Service Pack

VMS Cloud VPN Services evolves traditional Managed Services from a transport offer with excessive operational requirements spread across multiple enterprise sites to a next generation cloud based solution delivering deterministic services based on centralized orchestration of all service components. With the enterprise site domain extended into the Service Provider Cloud, VMS creates a single aggregation point where all off site enterprise traffic is processed by a common set of services. Access to these services is possible from anywhere on the Internet footprint. By using secure tunnels over the Internet, not only does VMS Cloud VPN services offer worldwide access, but removes the need to contract for private VPN service.

At the Customer Facing Service (CFS) level, the VMS Service Interface includes a front-end or OSS level module; a component of the Front-End is a self-service user portal. With this portal, Service Providers have the flexibility to allow their customers or an internal sales group, to order, provision and manage the service. The VMS Service Interface includes a Back-End module to convert the service intent or definition, as determined during Front-End user interaction, into a parameterized set of arguments that represent the service request. The service request is passed to the VMS Solution's Resource Facing Service (RFS) layer, specifically the Network Service Orchestrator (NSO), to initiate service orchestration.

When visualizing VMS Cloud VPN services, the concept of an enterprise boundary defined by a traditional DMZ located at the customer site is replaced with a virtual boundary located in the VMS Cloud VPN Service Cloud. With traditional Managed Services, the site DMZ consists of a series of devices or services located locally to secure the site. The site DMZ must be built out and managed at each site, making management repetitive and costly. The VMS Solution replaces all site DMZ constructs with a single virtualized DMZ implemented within the VMS Cloud VPN Service.

The VMS Cloud VPN Service Pack offer the following Cloud VPN services:

- Cloud VPN Foundation
- Cloud VPN Advanced
- Cloud VPN Advanced w/Web Security

CloudVPN Foundation Service

The Foundation Service is the base level VMS Service, through managed CPE devices; enterprise sites communicate through secure IPSec Tunnels to a vRouter located in the Service Provider's Cloud VPN Service's cloud. The enterprise's CPE devices peer directly to the vRouter using an Over-The-Top model. Both CPE devices and the vRouter have public IP addresses, enabling the use of the Internet as the transport. All site-to-site traffic traverses the vRouter.

Traffic destined to Internet sites, not associated with the SP Cloud VPN service cloud are routed directly to their destination via a "split tunnel" mechanism configured on the CPE device.

CloudVPN Advanced Service

The Advanced Service extends the Foundation Service by providing Internet access in the Cloud VPN Service's cloud. Site-to-site traffic is treated in the same fashion as in the Foundation Service, however traffic destined to general Internet sites utilize a virtual Firewall and NAT located in the Cloud VPN Service's cloud. With this service level, all service access policies are located in a central location, ensuring all users, independent of site location, share a common Firewall service policy and NAT mechanism.

The Advance Service also includes remote user access for mobile or remote workers. Using Cisco AnyConnect, the remote user can access enterprise resources globally through the public Internet.

The end-customer can add an optional Intrusion Prevention Service based on the Service Packages offered by the Service Provider

CloudVPN Advanced w/Web Security Service

The Advanced w/Web Security Service extends the Advanced Service by additional filter granularity through the insertion of Web Security functionality, allowing enterprise greater control over HTTP based traffic destined or received from the Internet.

The end-customer can add an option Intrusion Prevention Service based on the Service Packages offered by the Service Provider.

Cisco VMS Virtual Converged Edge (vCE) Service Pack

As a service provider, you may have customers with remote branches that utilize different WAN access methods (such as Cloud VPN and MPLS). The Virtual Converged Edge (VCE) attachment circuit interface, which is available as an add-on transport option when ordering a Cloud VPN service-level package, enables those branches to communicate and share a common service chain. The VCE service targets the Cisco Cloud Services Router (CSR) 1000V associated with a service chain.

The following list summarizes the benefits that the VCE attachment circuit provides:

- Integration with Cloud VPN service-level packages
- Extension of secure Internet and other NFV services to customers on MPLS networks
- Integration of remote branches and datacenters across Cloud VPN and MPLS networks
- eBGP routing support
- VLAN manual handoff

- VCE data collection
- Graphical user interface for VCE ordering, peering configuration, and metrics

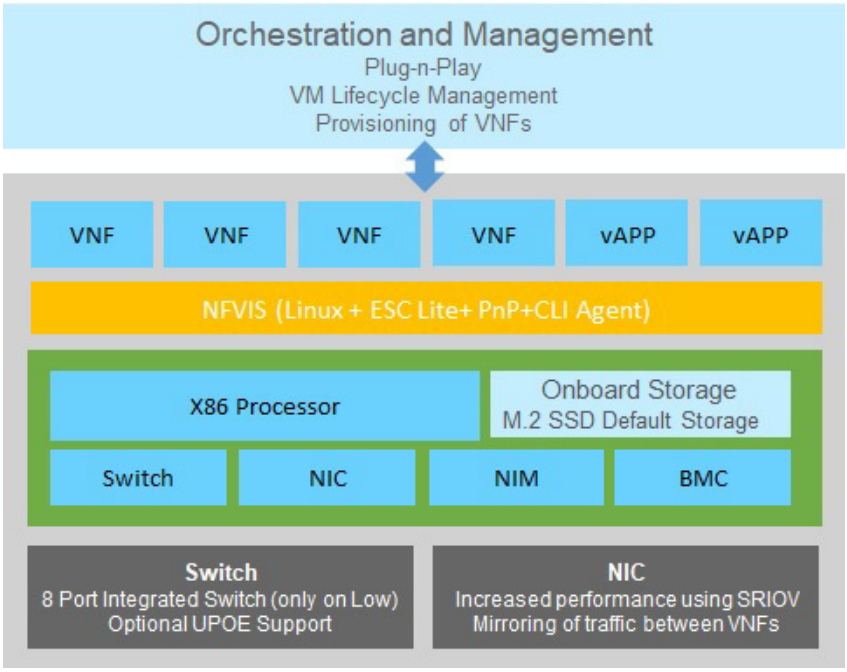
Cisco VMS vBranch Service Pack

Cisco VMS vBranch service pack enables unified routing, switching, storage, processing, and a host of other computing and networking activities into a into a single box. The vBranch service pack provides a way to collapse the services that a branch requires into a single box, which results in easier management of services, and smaller device footprint on a branch site.

The VMS vBranch service pack includes the following:

- An orchestration environment to allow automation of virtualized network service deployment, consisting of multiple Virtualized Network Functions (VNF).
- VNFs, which provide the desired network functionality, or even non-networking software applications, required at a deployment location.
- The NFV Infrastructure Software platform to facilitate the deployment and operation of VNFs and hardware components.

The figure below illustrates the functional architecture of a vBranch site.



Some of the advantages of the VMS vBranch service pack are:

- Zero touch provisioning for initial device connectivity through PnP server processes.
- Service provisioning of on-premise CPEs through orchestration.
- User interface portal for ordering service, network visualization, and performance or fault monitoring.
- Lifecycle Management.

In the VMS vBranch 3.1, VMS vBranch supports the branch site on Cisco 5000 Enterprise Network Compute System (ENCS) platform.

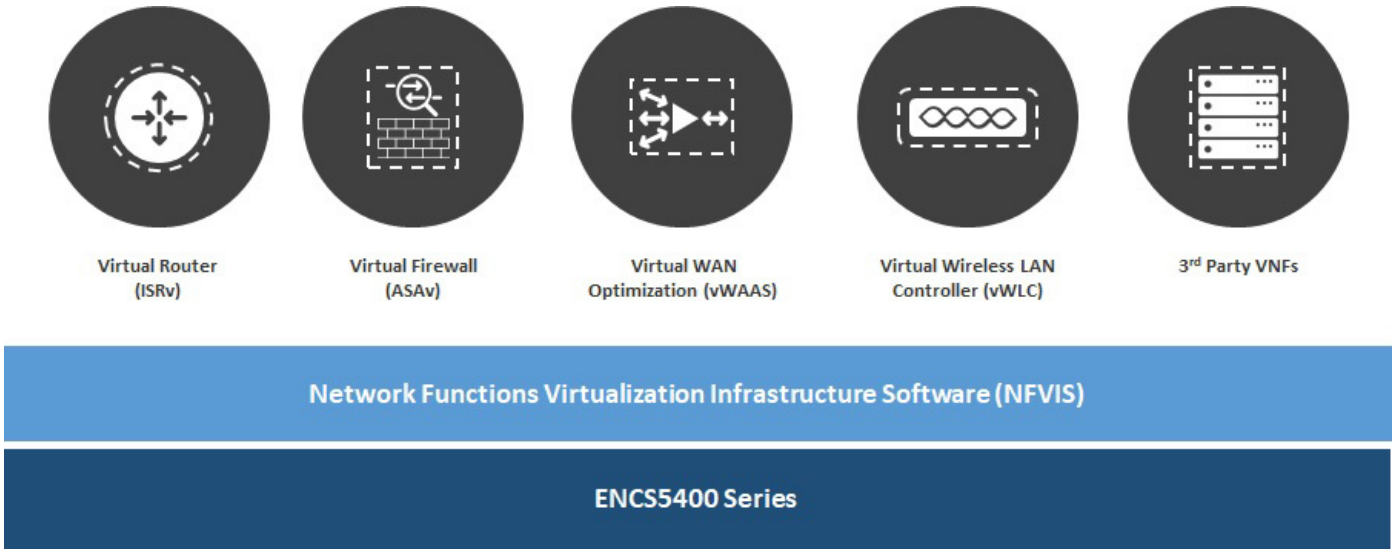
Cisco Enterprise Network Compute System

The Cisco 5000 Enterprise Network Compute System (ENCS) is a line of compute appliances designed for the Cisco Enterprise Network Functions Virtualization (ENFV) solution. It delivers a new standard of software-defined flexibility and performance, and offers a low Total Cost of Ownership (TCO). The 5000 ENCS is a hybrid platform that combines the best attributes of a traditional router and a traditional server, and offers the same functionality with a smaller infrastructure footprint. Offered with the Cisco Integrated Services Virtual Router (ISRv) and NFV Infrastructure Software (NFVIS) as the hosting layer, the platform offers a complete solution for a simplified deployment.

Supported VMs

Currently, the following Cisco supplied VMs and third party VMs are supported on Cisco ENCS:

- **Cisco Integrated Services Virtual Router (ISRv)–**A virtual form-factor of the Cisco IOS XE software router that delivers WAN gateway and network services functions into virtual environments.
- **Cisco Adaptive Security Virtual Appliance (ASAv)–**Enables ASA firewall and VPN capabilities on virtualized environments to safeguard traffic and multitenant architectures. Optimized for data center deployments, it is designed to work in multiple hypervisor environments, reduce administrative overhead, and increase operational efficiency.
- **Cisco Virtual Wide Area Application Services (vWAAS)–**A virtual appliance that accelerates business applications delivered from private and virtual private cloud infrastructure. Cisco vWAAS enables you to rapidly create WAN optimization services with minimal network configuration or disruption.
- **Virtual Wireless LAN Controller (vWLC)–**Virtual form-factor controller for any x86 server with VMware Hypervisor ESXi**.**
- **3rd Party VNFs–**Third party VNFs.



Cisco VMS SDWAN Service Pack

Cisco SDWAN service pack enables service providers to deploy and manage SDWAN service for their customers. The deployment of an SDWAN service in the context of a managed service requires deployment per customer and includes the SDWAN management control plane (vManage, vBond and vSmart), and the corresponding data plane (vEdge).

The SDWAN service pack management control plane and data plane consists of:

- **vManage**—The vManage is a centralized dashboard that enables automatic configuration, management, and monitoring of the overlay network. Users login to vManage to centrally manage all aspects of the network life cycle—from initial deployment, on-going monitoring and troubleshooting, to change control and software upgrades.
- **vBond**—The vBond facilitates the initial bring-up by performing initial authentication and authorization of all elements into the network. vBond provides the information on how each of the components connects to other components. It plays an important role in enabling devices that sit behind the NAT to communicate with the network.
- **vSmart Controller**—The vSmart controllers establish the secure SSL connections to all other components in the network, and run an Overlay Management Protocol (OMP) to exchange routing, security, and policy information. The centralized policy engine in vSmart provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.
- **vEdge Router**—The vEdge router establishes secure connectivity to all of the control components and also establishes IPSec sessions with other vEdge routers in the WAN network. In the VMS SDWAN 3.1.1, you can deploy a customer site on Cisco 5000 Enterprise Network Compute System (ENCS) platform.
  The Cisco 5000 Enterprise Network Compute System (ENCS) is a line of compute appliances designed for the Cisco Enterprise Network Functions Virtualization (ENFV) solution. Cisco 5000 ENCS is a hybrid platform that combines the best attributes of a traditional router and a traditional server, and offers the same functionality with a smaller infrastructure footprint.

Some of the advantages of the VMS SDWAN service pack are:

- Provides the interface to associate the tenant (customer) with the Control Plane and Data Plane.
- User interface portal for ordering service (Control Plane and Data Plane Connectivity) and network visualization.
- Lifecycle management of services.

Cisco VMS Managed Device Service Pack

Cisco VMS Managed Device service pack enables service providers to provide their customers manage devices services through a self-service portal. With Managed Device service pack, IT organizations can bring into its network (on-board) devices located at the customer premise (CPEs) and apply or manage configuration settings remotely from its Network Operations Center (NOC). The service provider can configure parameterized configuration template that need to be deployed on these CPEs.

VMS Managed Device service pack makes device deployment fast and easy. Using this service pack user interface you can configure and deploy a VMS CPEs.

- Some of the advantages are as follows:
- Zero touch provisioning for initial device connectivity through PnP server processes.
- Service provisioning of on-premise routers through NSO orchestration.
- User Interface portal for configuration templates, ordering service, and performance or fault monitoring.

Cisco 4000 Series Integrated Services Routers

Cisco VMS Managed Device, supports ISR 4k series. The Cisco 4000 Series Integrated Services Routers (ISR) revolutionize WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, the routers specifically address the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the Internet.