Cisco Cloud VPN Service-Level Packages

Cisco® Virtual Managed Services (VMS) is an open software platform. This platform together with the innovative Cisco Cloud VPN Service-Level Packages can help you serve your customers better by offering them a flexible selection of VPN connectivity and security applications that are easily customized through a self-service portal. The packages greatly reduce your costs for service creation, customer acquisition, service fulfillment, repair time, and maintenance. You can accelerate your revenue growth by at least 15 percent while reducing your current operating expenses (OpEx) by up to 76 percent*.

With Virtual Managed Services, you can offer your customers cloud-based managed services, and they can use a self-service portal to obtain cloud VPN and security services in minutes instead of waiting for weeks or months. Your customers can easily scale the services up or down as needed, avoid capital costs by consuming these software capabilities as a service, reduce their IT capital expenditures (CapEx) and OpEx, and always have access to the latest security technologies and services that you offer from your catalog.

Product Overview

Cloud VPN Service-Level Packages are a suite of prepackaged software capabilities that fully automate cloud VPN service creation, including ordering, service chaining, orchestration, service assurance, and all the necessary virtual network functions (VNFs) on the Virtual Managed Services platform. With these fully validated service-level packages, your customers can quickly turn on, control, and assure cloud VPN services.

Two Cloud VPN Service-Level Packages are currently available with Virtual Managed Services:

- **Cloud VPN Foundation**: This entry-level service package enables business customers to connect multiple enterprise sites securely while managing Internet access locally on their premises. An enterprise can unify its corporate network by interconnecting sites through this hosted cloud VPN service. All customer premises equipment (CPE)–based sites can securely communicate with each other over the Internet through a hosted virtual router in a hub-and-spoke topology with encrypted IPsec tunnels.
- **Cloud VPN Advanced**: In addition to enabling business customers to connect multiple sites securely, this package provides a firewall service for secure access to the Internet. All traffic traversing the hub-and-spoke cloud VPN topology is secured through encrypted IPsec tunnels. Two optional services also can be offered through the Cloud VPN Advanced package: remote-access SSL VPN for mobile users, and web content security with advanced malware protection and real-time malware scanning capabilities.

Features and Benefits

Feature	Benefit
Customer self-service portal	• Reduces service acquisition costs for business customers • Increases business agility, enabling customers to order what they need when they need it, providing an excellent tool for new branch offices, businesses entering new markets, and businesses that need to make seasonal changes • Reduces business IT operation costs, enabling services to be ordered with just a few mouse clicks

Feature	Benefit
Zero-touch configuration of CPE	• Eliminates the need for service calls, which results in lower service costs for business customers. • Reduces business IT operating costs associated with CPE configuration
Automated service creation	• Enables services to be deployed more quickly by reducing service lead time from weeks to minutes
Enterprise-class security	• Enables business customers to comply with regulatory requirements with strong encryption of data in motion, advanced firewalls, web content security, real-time malware scanning, and advanced malware protection (AMP) • Provides constant security intelligence updates from one of largest security intelligence networks, Cisco Talos Security Intelligence and Research Group, to protect businesses across the attack continuum • Uses the security expertise of managed service providers to meet cybersecurity needs

Main Features

Feature	Description
Self-service portal	All Cloud VPN Service-Level Packages provide access to a self-service portal that customers can use to order and customize the cloud VPN services they use. Customers can select a specific service package based on capabilities (IPsec VPN, firewall, SSL VPN, and web security), the bandwidth of the service, the number of sites and users, and the CPE devices for their specific locations.
Site-to-site VPN	All Cloud VPN Service-Level Packages support hub-and-spoke site-to-site Cisco FlexVPN over any IP transport network based on IPsec Internet Key Exchange Version 2 (IKEv2) encryption.
Dynamic routing	All Cloud VPN Service-Level Packages support Border Gateway Protocol (BGP) dynamic routing protocol through FlexVPN tunnels.
Quality of service (QoS)	All Cloud VPN Service-Level Packages support hierarchical QoS per tunnel and per application, with APIs controlling QoS for upstream and downstream traffic, and traffic-class settings for application priority. Network-based application recognition 2 (NBAR2) is used for application and protocol discovery.
Internet firewall	The Cloud VPN Advanced package supports stateful firewall policies, network address translation (NAT), Layer 3 through Layer 7 (L3-L7) access control lists (ACLs), and application control based on protocols and ports.
Remote-access VPN	The Cloud VPN Advanced package supports browser and client-based remote access SSL VPN as an add-on service. With Cisco AnyConnect® VPN Clients, cloud VPN supports device and user identity management, posture validation, and host scanning.
Web content security	The Cloud VPN Advanced package supports web content security as an add-on service. Web content security base features include web use control, URL filtering covering over 50 million sites, and dynamic content analysis for unknown URLs.
Real-time malware scanning	Real-time malware scanning is available as a web content security service option. Real-time malware scanning finds malware that is embedded in images, JavaScript, text, and flash files. Scanning engine options include Sophos and McAfee.
AMP	AMP uses file reputation and dynamic malware analysis (sandboxing) to identify and block suspicious malware for which no known signature exists. It uses a vast cloud security intelligence network (Cisco Talos Security Intelligence) to provide superior protection across the attack continuum. AMP is available as an option of the web security Cloud VPN Advanced package.

Platform Support

Product Family	Platforms Supported	Cisco IOS® Software Images (Feature Sets) Supported
Cisco Virtual Managed Services platform software	Virtual Managed Services 1.0 and 2.0	
CPE	Cisco Integrated Services Routers Generation 2 (ISR G2) Series	Cisco IOS Software Release 15.5.1T and later

Licensing

Cloud VPN Service-Level Packages	Description	Licensing Term
Cloud VPN Foundation	Supports site-to-site IPsec VPN, including VNF (virtual router and hub) licenses, VNF orchestration, and solution support	Term license based on various bandwidth tiers
Cloud VPN Advanced	Supports site-to-site IPsec VPN and firewall, including VNF (virtual router and hub and firewall) licenses, VNF orchestration, and solution support	Term license based on various bandwidth tiers

Cloud VPN Service-Level Packages	Description	Licensing Term
Web Security Options		
Essential	Provides URL and content filtering	Term license on per-user basis
Malware scanning	Real-time malware scanning add-on based on Sophos scanning engine or McAfee	Term license on per-user basis
AMP	Provides file reputation scanning and sandboxing based on Cisco Sourcefire® AMP technology	Term license on per-user basis
Remote-Access SSL VPN		
Cisco AnyConnect Plus	Provides SSL VPN, FIPS, and endpoint context collection	Term license on per-user basis
Cisco AnyConnect Apex	Includes all features in Cisco AnyConnect Plus as well as additional features such as posture agent next-generation encryption	Term license on per-user basis
Virtual Managed Services platform software	Includes the service interface, orchestration, service assurance, and CPE orchestration that Cloud VPN Service-Level Packages require for deployment	Please refer to the Virtual Managed Services data sheet for detailed licensing terms.

System Requirements

Service-Level Package	Recommended Resource
Cloud VPN Foundation	2 virtual CPUs (vCPUs), 4 GB of memory, and 8 GB of storage per service-chain instance
Cloud VPN Advanced (no web security)	4 vCPUs, 8 GB of memory, and 16 GB of storage per service-chain instance
Cloud VPN Advanced with Web Security	6 vCPUs, 14 GB of memory, and 266 GB of storage per service-chain instance

Cisco and Partner Services

Cisco Services can help your organization implement Virtual Managed Services. Our team provides industry-leading cloud, data center, and systems integration expertise, proven best practices, and a comprehensive integrated approach to help you achieve your business goals and gain greater value from your Virtual Managed Services solution.

Cisco Capital Financing to Help You Achieve Your Objectives

Cisco Capital® Financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx, accelerate your growth, and optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. Cisco Capital financing is available in more than 100 countries. Learn more.

For More Information

For more information about Cisco Virtual Managed Services, please visit the following resources:

- Cisco Virtual Managed Services
- Cisco Powered™ Virtual Managed Services

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-736308-00 12/15