Cisco Virtual Office Overview

Contents

Scope of Document

This document provides an overview of the Cisco® Virtual Office solution components and capabilities, along with links to deployment guides containing configurations and image platform recommendations.

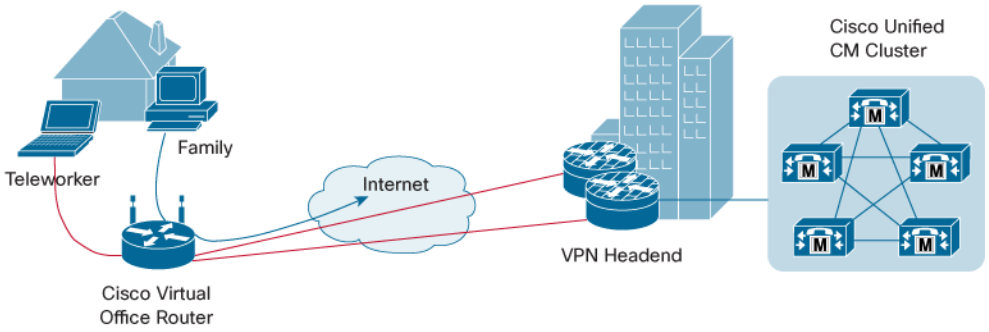
Introduction

Cisco® Virtual Office is a highly scalable solution for midsize and large organizations looking to provide teleworkers, small offices, and mobile users with office-like experiences combining voice, video, wireless, and real-time data applications in a secure environment.

Cisco Virtual Office features zero-touch deployment, allowing enterprise IT staff to provision and manage large-scale deployments with improved efficiency. Multiple access methods for workers at home, workers at remote offices, or mobile workers can be aggregated into a converged VPN without the need for separate aggregation and management models. The solution integrates layered identity services that provide control over the devices

and users that use the network, as well as the extent to which various users have access to resources in trusted and untrusted domains. Figure 1 shows a graphic of a simplified Cisco Virtual Office deployment.

Figure 1. Simplified Cisco Virtual Office Deployment



Cisco Virtual Office allows IT staff to extract full value out of the powerful technology integration within Cisco IOS® Software-based customer-premises-equipment (CPE) routers. The solution facilitates the deployment of voice, video, wireless, and security technologies as services that can be incrementally enabled on the CPE in response to changing business requirements. In addition, the solution achieves high scalability through addition of aggregation devices in a virtual farm in the data center. These devices help avoid additional expensive network upgrades and redesigns, reducing the total cost of ownership (TCO).

Cisco Virtual Office includes “cookie-cutter” design and implementation guides that render the solution fully deployable by customers. These best practices have been proven useful and have been refined over the years within Cisco’s own successful teleworker deployment. In addition, advanced services from Cisco and our partners provide lifecycle services for planning, design, implementation, remote management, and optimization.

For more information about the Cisco Virtual Office solution, visit http://www.cisco.com/go/cvo/.

Requirements Addressed

Cisco Virtual Office is designed to meet the following challenges that midsize to large organizations typically face:

- Scalability: As a business grows to new locations (national and international), the IP network services available to employees in various locations need to be consistent—allowing consistent secure access for users at corporate headquarters, remote sites, home offices, and public hotspots.
- A secure zero-touch deployment model is required to quickly proliferate CPE deployments to remote sites with no IT staff. Automation of ongoing operations through central network management, using push technology, is needed to simplify administration and keep costs low.
- Ability to deliver application performance required for latency and bandwidth-sensitive voice, video, and real-time data applications: This capability calls for advanced integration of VPN technologies with quality of service (QoS), IP Multicast, voice, and video services. The VPN architecture also needs to cater for CPE-based access as well as software-only access whether using IP Security (IPsec) or Secure Sockets Layer (SSL) VPN.
- The advanced threat defense solution covers proactive security, including firewalling and intrusion prevention system (IPS), as well as adaptive security to address new and unknown threats.
- Complete control over the entities attempting to access the network at remote, off-campus locations where ascertaining physical identity is not possible: This control includes being able to limit access to certain

devices or users, separate domains for employees and guests and families, and the ability to allow employees to use resources in untrusted domains without compromising security.

Cisco Virtual Office Solution Components

The Cisco Virtual Office solution consists of the following technology and services components:

- Zero-touch deployment (ZTD) and management: ZTD for IT and end users, the Cisco IOS Secure Device Provisioning (SDP) server, and ArcanaNetworks' ManageExpress Virtual Office (MEVO) tool to accelerate network operations by managing remote spokes and infrastructure devices from a single user interface
- Converged VPN: Dynamic Multipoint VPN (DMVPN) hub-and-spoke and spoke-to-spoke, spouse and kids, Easy VPN (IPsec VPN client and adaptive-security-appliance [ASA] interoperability), Enhanced Easy VPN with per-tunnel quality of service (QoS), and SSL VPN full-tunnel with Cisco Secure Desktop
- Layered identity: 802.1x, Authentication Proxy (Auth-Proxy), and public key infrastructure (PKI); Router, phone, and PC certificates; eTokens; stolen device and hacker lockout; Cisco Secure Access Control Server (ACS) (authentication, authorization, and accounting [AAA]); and Cisco IOS Certificate Authority Server
- Voice and video: IP phones, softphones, dual-mode cell phones with Session Initiation Protocol (SIP) or Skinny Client Control Protocol (SCCP) clients, Cisco Unified Video Advantage (UVA), Cisco Unified IP Phone 7985, Cisco IP/TV, SCCP video, H.323, QoS, and IP Multicast
- Wireless: Wireless access point; 802.11a/b/g; Wireless Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 for enterprise and personal; and Cisco Secure Services Client with 802.1x
- Threat control: Advanced firewall, IPS, content filtering, Cisco IOS Flexible Packet Matching (FPM), Adaptive Control Technology (ACT), Transitory Messaging Services (TMS), and mitigation rules
- Advanced Services: Planning, design, and implementation services; remote management services; and security optimization service

These components are described in the following sections.

Zero-Touch Deployment and Management

The Cisco Virtual Office management solution is used for achieving zero-touch deployment, ongoing management, and "virtualization" for efficient use of server resources.

ManageExpress Virtual Office from ArcanaNetworks

For medium-sized and large deployments, you can accelerate and simplify the management of the Cisco Virtual Office solution using MEVO, a tool developed in partnership with Cisco and Arcana Networks. This enterprise tool centrally provisions all aspects of device configurations and security policies for Cisco firewalls, VPNs, IPSs, and virtually any Cisco IOS Software feature through the use of flexible configuration templates.

MEVO allows the provisioning of thousands of devices with minimal overhead from the IT administrator. It includes a workflow process for employees to sign up and then provides a portal for self-management of the solution. It has a flexible and automated way to push predefined configuration files (or updates) to remote devices or even automatically upgrade images for groups of devices.

For more information about deploying CVO with MEVO, please refer to Cisco Virtual Office Deployment Guide.

Secure Device Provisioning

Secure Device Provisioning is a critical component for achieving zero-touch deployment in the Cisco Virtual Office solution. It permits the end user to initiate the device provisioning from a remote site, without any Cisco Virtual Office administrator's touching the spoke, just starting with factory default configuration in the router.

You can use Secure Device Provisioning to securely push the full CVO configuration to the remote-site router, install a new certificate, configure PKI trustpoint enrollment and IPsec VPN connectivity, and provision system attributes and other desired information to a new spoke router.

Secure Device Provisioning reduces the time and cost of deploying a secure network infrastructure by using a simple web-based enrollment and configuration interface. It involves less user intervention, thereby shortening provision time and lowering TCO.

Converged VPN

The Converged VPN solution standardizes and scales the network by facilitating transparent integration of VPN technologies. You can integrate DMVPN, Easy VPN, and SSL VPN to provide a single, consolidated hub for the VPN deployment. This integration provides standardized and scalable support for all types of end users, including telecommuters, mobile workers, and workers at branch-office sites.

The baseline solution for teleworkers and small-office workers is based on Cisco DMVPN, which optimizes performance, reduces latency for real-time applications, and facilitates dynamic configuration. It reduces the maintenance and configuration on the hubs and uses QoS to provide the priority to the marked network and real-time sensitive applications.

Additional VPN designs that you can combine follow:

- DMVPN high-scalability hub using Application Control Engine (ACE) for load balancing
- Cisco Easy VPN for IPsec-based access for mobile users
- Cisco IOS SSL VPN for SSL-based access for mobile users
- Layer 2 Tunneling Protocol (L2TP) and IPsec for mobile phones capable of data VPN
- DMVPN dial backup

More information about the deployment of a converged VPN solution is available in the Cisco Virtual Office Converged VPN Guide at http://www.cisco.com/go/cvo.

The sub-components are described in the following sections.

High Scalability

CVO can scale to support many thousands of devices simultaneously. To achieve this high level of scalability, a load balancer must be deployed at the headend that distributes the incoming connections from the different spokes to a group of servers (server farm) connected behind it. VPN termination and routing are all configured on the servers in the server farm.

There are multiple high-scale headend designs possible, differentiated by the level of redundancy that they provide. Please refer to the Cisco Virtual Office High Scalability Design Guide at http://www.cisco.com/go/cvo for a detailed discussion.

The Cisco Application Control Engine (ACE) module plays the role of the load balancer. It can deliver up to 16-Gbps throughput (4 Gbps is the minimum) and is supported on a Cisco Catalyst® 6500 or Catalyst 7600 chassis

with a Supervisor Engine 720. For more information about the ACE module, please check the ACE module datasheet.

If the CVO network does not have high-throughput requirements, a standalone Cisco ACE 4710 Application Control Engine appliance can be used as the load balancer instead of a module. The appliance provides the same functions as an ACE module, with a maximum throughput of 4 Gbps (0.5 Gbps is the minimum). For more information about the ACE appliance, please check the ACE 4710 appliance datasheet.

Easy VPN

Easy VPN provides access to both software and hardware clients, complementing the other VPN deployments. You can combine Easy VPN with DMVPN for the deployment of the Cisco Virtual Office solution. Easy VPN provides access to both software and hardware clients, complementing the regular DMVPN deployment.

When an existing Easy VPN deployment is based on Cisco IOS Software and you want to add DMVPN to the same hub, you can add DMVPN configuration to the same hub without affecting the existing Easy VPN setup. The converse is also true.

A converged Easy VPN and DMVPN Cisco Virtual Office solution is beneficial when you want to provide full-scale integrated access to both small office or home office (SOHO) teleworkers and mobile users using the same end-to-end secure solution setup. For SOHO users, Easy VPN or DMVPN can run on a home router, providing corporate access to the computers and IP phones connected to the home network. For mobile users, the Easy VPN client (software VPN client) installed on a laptop provides the desired connectivity, because that client can work from any location and will integrate well with the same solution.

With the addition of IPsec Dynamic Virtual Tunnel Interface (DVTI), Enhanced Easy VPN now supports IP Multicast and QoS as well.

More information about Easy VPN or the CVO Express solution is available in the Cisco Virtual Office Express Deployment Guide at http://www.cisco.com/go/cvo.

Layered Identity

The layered identity concept provides various CPE-, device-, and user-level security mechanisms that, in conjunction with perimeter security at the CPE, helps define the securely integrated Cisco Virtual Office Solution framework.

- PKI facilitates CPE-level authentication as part of VPN tunnel establishment. RSA keys and digital certificates are used to authenticate and authorize each CPE before it becomes part of the trusted network.
- Standard 802.1x and its Layer 2 and Layer 3 extensions provide IP device-level security for both the switch- and routed-port CPE.
- Authentication Proxy (Auth-Proxy) provides end-user security by authenticating users with Cisco Secure ACS before they are allowed to access corporate networks.
- USB-based eTokens provide CPE security by providing a location to store critical information such as digital certificates, RSA keys, and secondary configurations. You can enable this information on the CPE by the eToken login, safeguarding against the “stolen-box” scenario and preventing unauthorized users from setting up VPN access back to corporate headquarters.

- Cisco Secure ACS supports RADIUS and TACACS+ and provides the AAA capabilities that a secure network requires. Cisco Secure ACS maintains a central database to validate the user and device authentication and authorization required by PKI, 802.1x, 802.11 wireless authentication, and Auth-Proxy.

More information about layered identity is available in the Cisco Virtual Office—Advanced Layered Security Deployment Guide located at http://www.cisco.com/go/cvo.

The sub-components are described in the following sections.

PKI

Cisco IOS PKI provides certificate management to support security protocols such as IPsec, Secure Shell (SSH) Protocol, and SSL. As defined in the IPsec protocol, the peers must be authenticated during IKE phase 1 to identify the validity before establishing the secure communication.

For a small number of Cisco IOS Software routers configured as IPsec peers,you can use Pre-Shared Keys (PSKs) to allow them to authenticate each other. However, for medium- to large-sized networks, PSK configuration increases in complexity and becomes difficult to manage; PKI offers a much more secure and scalable method, whether it is a full mesh of security connections for DMVPN or newly supported xVPN technology.

PKI is also better for spoke-to-spoke communication, or for enterprises deploying site-to-site VPN for hundreds of remote branch offices needing to communicate with each other. PKI reduces management overhead and simplifies the deployment of the network infrastructure by using digital-certificates exchange in place of Pre-Shared Keys for device authentication.

More information about the PKI solution is available at: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805249e3_ns855_Networking_Solutions_White_Paper.html.

802.1x Authentication

Standard 802.1x and its Layer 2 and Layer 3 extensions provide IP device-level security for both the switch- and routed-port CPE.

Using this feature, all the IP devices are classified as trusted or nontrusted, based on the 802.1x authentication status. When a new device becomes active on the network, the router initiates an 802.1x exchange. Depending on the 802.1x client running on the user device, the user is prompted for credentials. The credentials are then passed on to the router, which uses them to get authentication from a RADIUS server. Once the authentication is passed, the access device is considered a trusted device and is given more privileges, such as access to the corporate network.

If the device fails the authentication or is a clientless device, it is considered a nontrusted device. This device can be given fewer privileges, such as IP addresses from a separate Dynamic Host Configuration Protocol (DHCP) pool with access only to the Internet.

More information about the 802.1x solution is available in the Cisco Virtual Office Advanced Layered Security Guide at http://www.cisco.com/go/cvo.

Cisco Secure ACS

A RADIUS server is required for different components of the Cisco Virtual Office solution, namely 802.1x, Auth-Proxy, 802.11 wireless authentication, and PKI-AAA authentication of routers. The 802.1x standard was discussed in the preceding section.

The Auth-Proxy feature is used for end-user authentication. You are allowed access to the corporate site only if you provide valid credentials. The credentials need to be verified by a RADIUS server. Upon verification of the credentials, appropriate permit access control entries are downloaded and applied on the remote spoke, granting the appropriate level of access. You can use PKI-AAA authentication for device authentication to check the validity of Cisco Virtual Office routers as part of secure session setup.

You can configure the Cisco Secure ACS to support all these applications. More information about the Cisco Secure ACS solution is available in the Cisco Virtual Office—AAA Deployment Guide at http://www.cisco.com/go/cvo.

Voice and Video

Voice and video capabilities are extended to remote sites through a secure network. This network supports wired and wireless voice-over-IP (VoIP) phones as well as Cisco IP Communicator softphones and the Cisco VT Camera.

Support is provided for SCCP and SIP based on Cisco Unified IP Phones, which are ready to be plugged in behind the CPE. Support is also provided for Cisco IP Communicator, a PC-based Cisco IP softphone solution that supports only SCCP. Cisco wireless IP phones can connect directly to the integrated wireless access point in the Cisco Virtual Office CPE.

Critical aspects of the Cisco Virtual Office solution include:

- Voice VLAN providing secure identity and domain isolation for voice
- SCCP firewall inspection: Integrated security in the form of SCCP firewall support for Cisco wired, wireless, and video phones; for example, the Cisco Unified IP Phones 9900 Series models and the Cisco Unified Wireless IP Phone 7925G
- ALG and AIC: Extended security in the form of SIP application layer gateway (ALG) and application inspection and control (AIC) for Cisco SIP phones
- Mobile phones: Transparent, secure support for Apple iPhone and dual-mode phones for mobile users

More information about secure voice solutions is available in the Cisco Virtual Office Secure Voice and Video Guide at http://www.cisco.com/go/cvo.

Cisco IOS Software Security and IP Services

Cisco IOS Software services such as QoS, IP Multicast, Network Address Translation (NAT), Optimized Edge Routing (OER), and Cisco IOS IP Service-Level Agreement (IP SLA) combine with security services to enable support for voice and video applications behind a CPE (such as a remote router) within a secured network.

- QoS offers prioritization of real-time and latency-sensitive traffic (such as voice). QoS must be initially enabled for voice traffic, based on uplink bandwidth available from the ISP. The bandwidth usage depends on the codec; the most popular codecs are G.729 and G.711.
- IP Multicast services provide solutions for the secure support of IP Multicast applications over VPN technologies. Initial support for securing multicast combines generic routing encapsulation (GRE) over site-to-site IPsec VPNs; however, scalability is a concern when additional devices are included within a domain.

  With the advent of new technologies, including DMVPN and Enhanced Easy VPN, you can enjoy the benefits of improved IP Multicast performance and scalability—and easy deployment.

In DMVPN, multicast packets are encapsulated within the GRE header and then encrypted when sent over the tunnel. This feature supports routing protocols and multicast data forwarding, and simplifies configuration management and scalability. However, the packets are replicated and then encrypted, limiting the number of multicast receivers in a multipoint GRE (mGRE) interface based on the router platform and stream bandwidth.

Enhanced Easy VPN (DVTI) dynamically creates a virtual interface, similar to a point-to-point GRE tunnel, when the session is established. Multicast forwarding is possible using this virtual interface. All you need to do is enable the configuration for the virtual tunnel interface (VTI) server as multicast in the template configuration.

- Firewall: Although a firewall access control list (ACL) in a Cisco Virtual Office-enabled CPE will block anything needed for these voice services (except the control messages), other security features (such as 802.1x and Auth-Proxy) should also bypass authentication confirmation from VoIP phones. Firewall inspection will open necessary ports to permit voice traffic after a call has been initiated. Zone-based firewall allows the creation of explicit zones; for example, trusted, untrusted, and DMZ, simplifying the policies and rules.
- NAT allows Cisco Virtual Office spokes and hubs to reside behind existing NAT devices and also allows the spokes and hubs to support split tunneling.
- Optimized Edge Routing (OER) chooses the best path when two or more physical or logical paths are available.
- IP SLAs provide support for performing network performance measurements.

More information about IP services is available at http://www.cisco.com/en/US/products/ps6537/products_ios_sub_category_home.html.

Wireless

Integrated secure wireless managed services focus on enabling wireless applications behind the Cisco Virtual Office-enabled CPE within a secure network. Strong security policies, which protect the company from rogue access points, intruders, unauthorized users, and unauthorized viewing of transmitted data, are required for enterprise wireless LANs. Cisco supports IEEE 802.1x authentication and numerous Extensible Authentication Protocol (EAP) types, providing a centrally managed, standards-based, open wireless network security scheme in addition to some of the earlier 802.11 WEP implementations.

Integrated secure wireless managed services provide support for Temporal Key Integrity Protocol (TKIP), which provides enhancements to 128-bit encryption such as per-packet key hashing, digital certificates on every frame, and rotation of broadcast keys in wireless access points to encrypt both unicast and broadcast packets. Several EAP types are supported, including Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), Protected EAP (PEAP), and EAP-Subscriber Identity Module (EAP-SIM). The WPA standards-based solution addresses wireless LAN vulnerabilities and provides enhanced protection from targeted attacks. WPA uses TKIP for encryption.

More information about secure wireless solutions is available in the Cisco Virtual Office Secure Wireless Guide at http://www.cisco.com/go/cvo.

Threat Control

Proactive Security

Proactive security services provide secure LAN and WAN infrastructures for the Cisco Virtual Office solution. These security services help secure the remote CPE, IP devices, IP-based applications, and end users, vendors, and customers. Technologies include:

- Cisco IOS Firewall provides perimeter security by blocking unauthorized access to the end devices sitting behind the spoke router, thereby protecting the internal networks from security attacks. Advanced filtering functions include zone-based firewall, user-group firewall, and object group ACLs.
- Cisco IOS IPS features further strengthen perimeter security by monitoring permitted traffic for any malicious signatures in real time and taking appropriate action.

Advanced Services

Realize the full value of Cisco Virtual Office with support for deployment, operation, and ongoing optimization through services from Cisco and our approved partners.

As part of the Cisco Virtual Office solution, we help you successfully deploy and integrate headend solution components and guide you through automating the deployment and management of remote sites by providing support for planning, design, and implementation. We also help you reduce operating costs; keep devices working efficiently; and continually assess, tune, and evolve your Cisco Virtual Office to keep pace with changes in your business and evolving security threats through ongoing operational support and optimization.

More information about available services for Cisco Virtual Office is available at http://www.cisco.com/en/US/netsol/ns855/index.html#~acc~panel-5.

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 C07-683001-00 08/11