Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

Teleworking—Design Overview

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide 1
Route to Success 1
About This Guide 1
Introduction 2
Cisco SBA Teleworker Solutions 3
VPN Phone 3
Cisco ASA 5505 3
Cisco OfficeExtend 4
Cisco Virtual Office 6
For More Information 8

What's In This SBA Guide

Cisco SBA Solutions

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

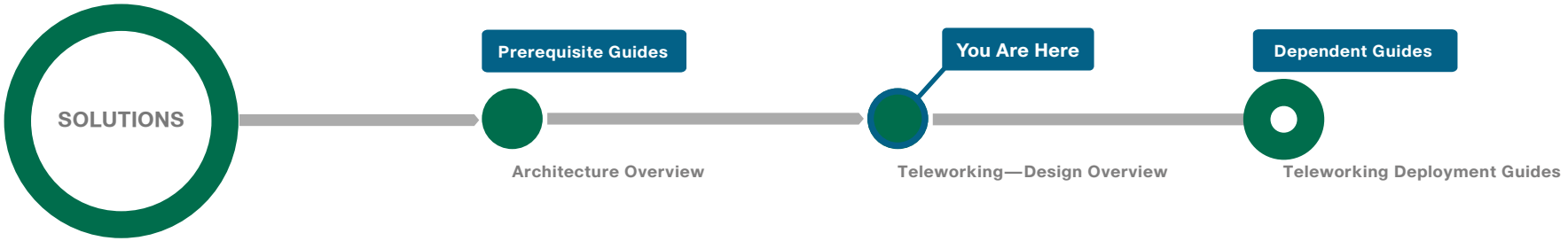
This *design overview* provides the following information:

- An introduction to a Cisco SBA design
- An explanation of the requirements that shaped the design
- A description of the benefits that the design will provide your organization

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

In 2010, International Data Corporation (IDC) estimated that there were over 30-million teleworkers *(also known as telecommuters)* worldwide. Teleworkers differ from mobile workers in that they require a more office-like environment and typically work from a single semi-permanent location, in most cases their houses. These workers may have an informal arrangement with their supervisors, or the work arrangement may be more formalized with a written policy and enrollment.

Today, teleworkers are becoming more productive and connected, enabling companies to recruit the best talent, regardless of their location. At the same time, teleworking allows the workers to find the optimal life-work balance and job satisfaction while maintaining productivity and business continuity.

Providing employees access to networked business services from a residential environment poses challenges for both the end-user and IT operations. For the home-based teleworker, it is critical that access to business services is reliable and consistent, providing an experience that is as similar to sitting in a cubicle or office in the organization's facility. Additionally, solutions must support a wide range of teleworking employees with varying skill sets, making it critical to have a streamlined and simplified way to implement devices that allow for access to the corporate environment.

IT operations have a different set of challenges when it comes to implementing a teleworking solution, including properly securing, maintaining, and managing the teleworker environment from a centralized location. The introduction of cloud-based services requires IT to help ensure that employees have access to these services while minimizing the risk of viruses or attacks by providing secure Internet access. Because operational expenses are a constant consideration, IT must implement a cost-effective solution that provides investment protection without sacrificing quality or functionality.

The needs of teleworkers vary depending on the frequency and type of information they use to perform their jobs. There is no "one size fits all" technology solution for telework. To optimize teleworker solutions, organizations must understand the unique requirements of individual end-users while providing a consistent, secure operating environment for all users, regardless of location.

Cisco offers a suite of teleworking solutions that provides options for all types of teleworkers. The Cisco SBA teleworking solution includes:

- Cisco AnyConnect PC and Phone.
- Cisco Adaptive Security Appliances (ASA) Series 5505.
- Cisco OfficeExtend.
- Cisco Virtual Office (CVO).

This document has been divided into multiple sections, each covering one of the teleworking solutions. To help decide which teleworking solution is the best fit for your organization, use the following table to identify your requirements and the solutions that support them.

Table 1 - Teleworking requirements and the solutions that support them

Your requirement	AnyConnect PC + Phone	ASA 5505	OfficeExtend	CVO
Wireless	X[1]		X	X
Wired	X[1]	X	X[2]	X
Efficient Intrasite Communication[3]		X		X
Advanced Technology Support (Multicast, Medianet)				X
Provisioning Complexity	Medium	High	Low	Low
Resiliency	Medium	Medium	Low	High
Recommended Scale in this Deployment	500	50	500	900

Notes:

1. Every device must support Cisco AnyConnect natively.
2. The Cisco OfficeExtend 600 Series AP supports one physical LAN connection and up to four MAC addresses.
3. Defined as traffic not having to leave the site to communicate between devices.

Cisco SBA Teleworker Solutions

VPN Phone

The Cisco VPN Client for Cisco Unified IP Phones, working in conjunction with the Cisco AnyConnect Client for PCs and laptops, provides a solution for organizations with remote telecommuters who require only data and voice access.

The solution builds upon the remote access VPN solution in the *Cisco SBA—Borderless Networks Remote Access VPN Deployment Guide*. That solution can be used both for the mobile user and the teleworker at the same time, without modification.

Because the worker may be teleworking full-time, and to make the solution a more office-like environment, a physical phone is used instead of a soft phone running on the PC. To connect the phone back in to the organization, the solution uses Cisco VPN Client for Cisco Unified IP Phones. The Cisco VPN Client is:

- Easy to Deploy—You configure all settings via Cisco Unified Communications Manager (UCM) administration. Using the existing VPN Group configuration on the Cisco ASA, the phone establishes a VPN connection to the same Cisco ASA pair as the Cisco AnyConnect PC clients.
- Easy to Use—After you configure the phone within the enterprise, the user can take it home and plug it in to a broadband router for instant connectivity without any difficult menus to configure. Also, if you provide a Cisco Unified IP Phone 9971 and a laptop with a wireless card, this solution does not require the home office to be wired.
- Easy to Manage—Phones can receive firmware updates and configuration changes remotely.
- Secure—VPN tunnel only applies to traffic originating from the phone itself. A PC connected to the PC port is responsible for authenticating and establishing its own tunnel with VPN client software. As it is with the Cisco AnyConnect PC clients, authentication for the phone requires the users' Microsoft Active Directory (AD) username and password.

This Cisco VPN Client configuration requires that the phone is pre-provisioned and that it establishes the initial connection inside of the corporate network to retrieve the phone configuration. After that, subsequent connections can be made using VPN, as the configuration is retrieved on the phone.

The following Cisco Unified IP Phones are currently supported: 7942, 7962, 7945, 7965, 7975, 8900 series, and 9900 series.

Cisco ASA 5505

Cisco ASA 5505 offers a low-cost option to provide teleworker connectivity to the organization. Cisco ASA 5505 provides secure connectivity for wired data and collaboration endpoints in a compact, fanless form factor, minimizing noise and space requirements.

The Cisco ASA 5505 teleworker solution integrates with the Internet edge portion of the Cisco SBA design. The teleworker's connection terminates at resilient Cisco ASA firewalls at the organization's Internet edge. This solution is configured on the same Cisco ASA firewalls as the remote-access virtual private network (RAVPN) solution. This configuration applies to dedicated and shared-mode RAVPN deployments. Some of the configuration re-uses portions of the RAVPN configuration, although it may be configured to be completely independent of the RAVPN resources. The addition of the head-end's support for Cisco ASA 5505 teleworker termination does not affect RAVPN connectivity, and the configuration can be applied without the imposition of a service outage.

The Cisco ASA 5505 teleworker solution provides access for endpoint devices, such as laptop and desktop computers, IP phones, printers, and other devices that connect to the network via wired Ethernet connections. Two of the Cisco ASA 5505's ports provide Power over Ethernet (PoE) to support IP phones, IP video surveillance, and other endpoints without cluttering the teleworker's office with additional cables and wall-wart power supplies.

The Cisco ASA 5505 teleworker solution offers:

- **Low cost**—With this solution, you get a Cisco ASA 5505, a Cisco IP phone, and the necessary license on the organization's Internet edge Cisco ASAs.
- **Flexible connectivity**—The Cisco ASA 5505's integrated Ethernet switch can accommodate multiple endpoint devices, including two interfaces that can provide PoE.
- **Simple deployment**—The Cisco ASA 5505 can be configured quickly with a brief text-file configuration.
- **Security**—Deactivation of the teleworker site's credentials on the Internet edge appliance can terminate the teleworker's connectivity.

Ideally, the Cisco ASA 5505 teleworker device is preconfigured and sent home with the teleworker user. A newly-provisioned or existing desktop IP-phone can be taken home, as well, and registers to the Cisco Call Manager server over the VPN.

Cisco OfficeExtend

The Cisco OfficeExtend solution is specifically designed for the teleworker who primarily uses wireless devices. The solution consists of the following components:

- Cisco Aironet 600 Series OfficeExtend Access Point
- Cisco 2500 Series or Cisco 5500 Series wireless LAN controller

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers (WLCs) are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco OfficeExtend Access Points to support business-critical wireless applications for teleworkers. Cisco WLCs provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

Although a standalone controller can support up to 500 Cisco OfficeExtend sites, Cisco recommends deploying controllers in pairs for resiliency. There are many different ways to configure controller resiliency; the simplest is to use a primary/secondary model where all the access points at the site prefer to join the primary controller and only join the secondary controller during a failure event. However, even when configured as a pair, WLCs do not share configuration information. Each WLC must be configured separately.

The following controllers are included in this release of Cisco SBA:

- **Cisco 2500 Series Wireless LAN Controller**—The 2504 controller supports up to 50 Cisco OfficeExtend Access Points and 500 clients. Cisco 2500 Series WLCsare ideal for small OfficeExtend deployments.
- **Cisco 5500 Series Wireless LAN Controller**—The 5508 controller supports up to 500 Cisco OfficeExtend Access Points and 7000 clients, making it ideal for large OfficeExtend deployments.

Because software license flexibility allows you to add additional access points as business requirements change, you can choose the controller that will support your needs long-term, but only pay for what you need, when you need it.

To allow users to connect their endpoint devices to either the organization's on-site wireless network or their at-home teleworking wireless networks without reconfiguration, the Cisco OfficeExtend teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at teleworkers' homes as those that support data and voice inside the organization.

Cisco OfficeExtend Access Points

Cisco Aironet 600 Series OfficeExtend Access Points are lightweight. This means they cannot act independently of a WLC. As the access point communicates with the WLC resources, it downloads its configuration and synchronizes its software/firmware image, if required. Cisco Aironet 600 Series establishes a secure Datagram Transport Layer Security (DTLS) connection between the access point and the controller to offer remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

Cisco OfficeExtend delivers full 802.11n wireless performance and avoids congestion caused by residential devices because it operates simultaneously in the 2.4-GHz and the 5-GHz radio frequency bands. The access point also provides wired Ethernet connectivity in addition to wireless. The Cisco OfficeExtend Access Point provides wired and wireless segmentation of home and corporate traffic, which allows for home device connectivity without introducing security risks to corporate policy.

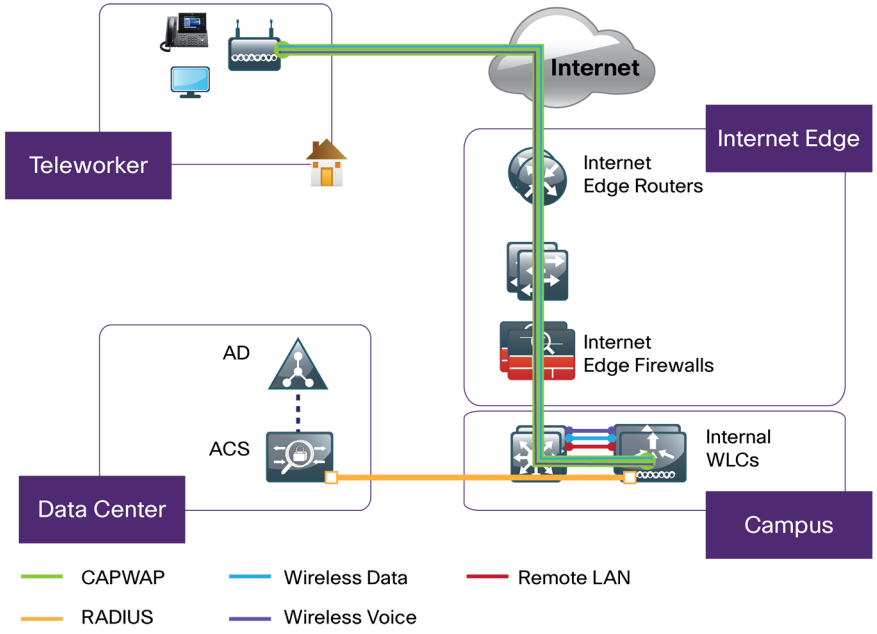
Design Models

You can deploy Cisco OfficeExtend using either a shared controller pair inside the organization or a dedicated controller pair in the Internet edge DMZ.

If you have one controller pair for the entire organization, and that controller pair is connected to the same distribution switch as the Internet edge firewall, you can use a *shared deployment*. In a shared deployment, the traffic from the Cisco OfficeExtend Access Point is tunneled through the Internet edge firewall and terminated on the internal WLC. The Cisco OfficeExtend wireless clients are in the same network as the internal wireless clients, but you must deploy a new network for the wired Cisco OfficeExtend users.

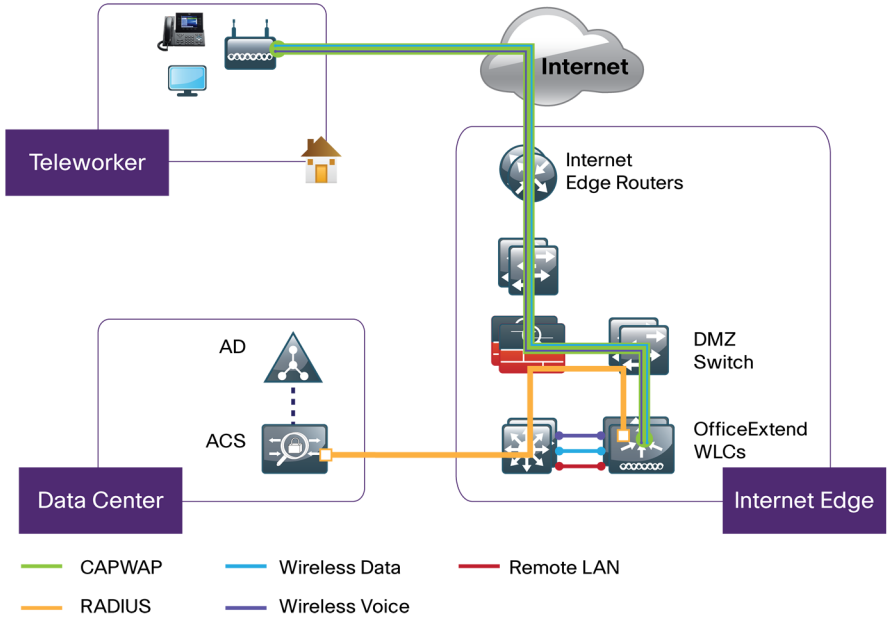
A shared deployment is typically used for small deployments or proof-of-concepts where the existing wireless controller has enough existing license to support the additional access points.

Figure 1 - Cisco OfficeExtend shared design model



If you don't meet the requirements for a shared deployment, or if you want a more secure Cisco OfficeExtend environment, you can deploy a dedicated controller pair using the Cisco 5500 or 2500 Series WLCs. In a dedicated deployment such as this, the controller is directly connected to the Internet edge DMZ and traffic from the Internet is terminated in the DMZ versus on the internal network, while client traffic is still directly connected to the internal network.

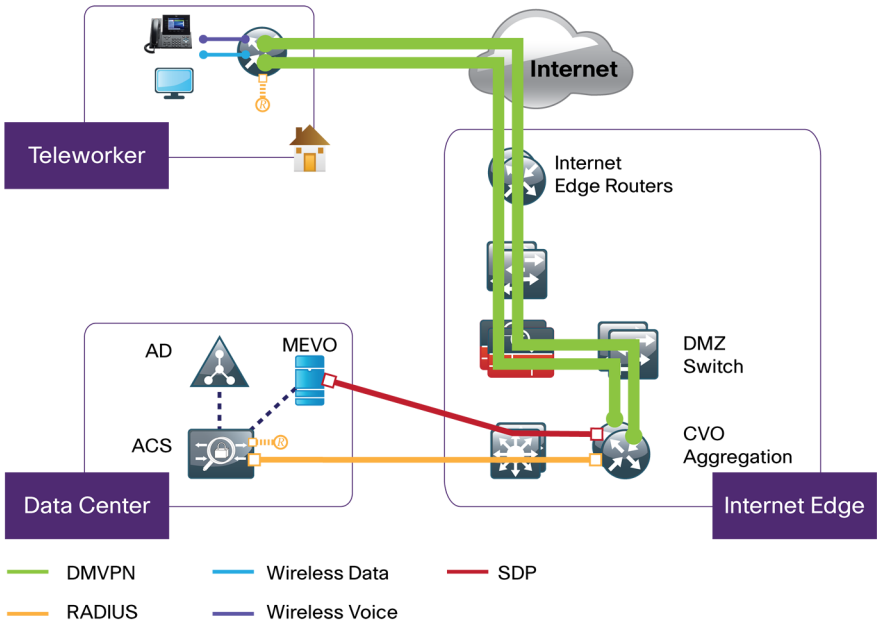
Figure 2 - Cisco OfficeExtend dedicated design model



Cisco Virtual Office

The Cisco Virtual Office (CVO) solution is specifically designed for the teleworker who needs the highest level of resiliency and advanced technology support. CVO supports both wired and wireless users at the CVO remote site (home) and allows for direct communication between the devices without their having to traverse the Internet.

Figure 3 - CVO architecture



Components of the CVO solution include:

- Dynamic Multipoint VPN (DMVPN) aggregation router serving as the VPN termination point.
- PKI Certificate authority (CA) server to issue certificates for both remote and aggregation routers.
- Secure device provisioning (SDP) server for provisioning the remote routers.
- Authentication, authorization, and accounting (AAA) server for device and user authentication, typically a Cisco Secure Access Control Server (ACS).
- ArcanaNetworks ManageExpress Virtual Office (MEVO) on a Microsoft Windows 2003 or 2008 server for CVO management and provisioning.
- On the remote-site (the teleworker's home), a Cisco 800 Series router with an optional IP phone, depending on the needs of the customer.

The solution uses two DMVPN aggregation routers for resiliency. The primary VPN aggregation router also hosts the SDP server and the CA server.

Dynamic Multipoint VPN Overview

Dynamic Multipoint VPN (DMVPN) is a solution for building scalable site-to-site VPNs that support a variety of applications. DMVPN is widely used for encrypted site-to-site connectivity over public or private IP networks.

DMVPN was selected as the encryption solution for the CVO solution because it supports on-demand, full-mesh connectivity with a simple hub-and-spoke configuration and a zero-touch hub deployment model for adding remote sites. DMVPN also supports spoke routers that have dynamically assigned IP addresses.

DMVPN makes use of multipoint Generic Route Encapsulation tunnels (mGRE) to interconnect the hub to all of the spoke routers. These mGRE tunnels are also sometimes referred to as *DMVPN clouds* in this context. This technology combination supports unicast, multicast, and broadcast IP, including the ability to run routing protocols within the tunnels.

Public Key Infrastructure Overview

Public key infrastructure (PKI) provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Each device participating in the secure communication is enrolled, a process by which the entity generates a Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key), and a trusted entity (also known as a *CA*) validates its identity.

After each entity enrolls in a PKI, it is granted a digital certificate that has been issued by the CA. When peers must negotiate a secured communication session, they exchange their digital certificates. Using the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

The benefits of PKI integration include:

- PKI integration reduces the need for complex management of preshared keys for CVO routers.
- Security of the CVO router can be increased by the use of RSA keys that are nonexportable and certificate revocation list (CRL) checking to prevent sessions from unauthorized devices.
- PKI integration with AAA protects CVO hubs with even more security.

Cisco Secure ACS Overview

Cisco Secure ACS is required for different components of the CVO solution, namely network device management, end-user authentication through the Cisco IOS Authentication Proxy (AuthProxy), end-user wireless authentication, and PKI-AAA authentication of CVO routers.

MEVO Overview

ArcanaNetworks MEVO, a Microsoft Windows–based management platform, provides the management component of the CVO solution.

Notes

For More Information

For more information about Cisco SBA, please see the How to Get Started with Cisco SBA document.

For more information about the Cisco SBA Teleworking solution described in this paper, see the following guides:

- *Teleworking—VPN Phone Deployment Guide*: http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_SLN_Teleworking_VPNPhoneDeploymentGuide-Aug2012.pdf
- *Teleworking—Cisco ASA 5505 Deployment Guide*: http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_SLN_Teleworking_ASA5505DeploymentGuide-Aug2012.pdf
- *Teleworking—Cisco OfficeExtend Deployment Guide*: http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_SLN_Teleworking_OfficeExtendDeploymentGuide-Aug2012.pdf
- *Teleworking—Cisco Virtual Office Deployment Guide*: http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_SLN_Teleworking_CVODeploymentGuide-Aug2012.pdf

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

B-0000310-1 9/12