BYOD—Design Overview

SMART BUSINESS ARCHITECTURE

February 2013 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 February 2013 is the "February 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

Comments and Questions

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

Table of Contents

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

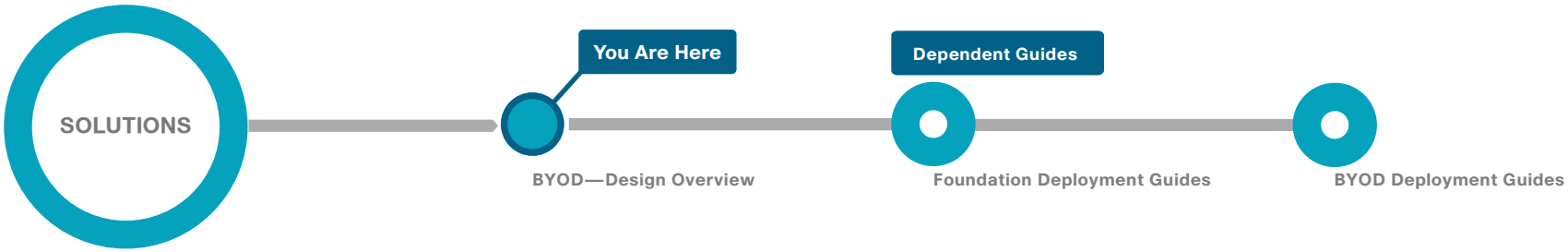
This *design overview* provides the following information:

- 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

Organizations are experiencing an unprecedented transformation in the network landscape. In the past, IT typically provided network resources only to corporate-managed PCs, such as laptops and desktops. Today, employees are requiring access from both corporate managed and unmanaged devices, including mobile devices like smart phones and tablets. This rapid proliferation of mobile devices capable of supporting applications drastically increases workforce mobility and productivity, but it also presents an enormous challenge to IT organizations seeking to enforce security policies across a growing population of devices, operating systems, and connectivity profiles.

The distinction between a work device and a personal device has evolved. This evolution of mobile device usage and the introduction of mobile devices into the workplace have caused a paradigm shift in how IT views what qualifies as a network "end point device" and also what it means to "be at work."

An organization needs to know not only who is accessing their wired and wireless networks, but also when the networks are accessed and from where. In addition, with the wide adoption of mobile devices, such as smart phones and tablets, and people bringing their own devices to access the network, organizations need to know how many of these devices are connecting. With this information, the organization can create policy to prevent connection by these devices, limit connection to approved devices, or make access to network resources easier for these nontraditional devices. This presents a challenge for IT organizations that seek to provide end-users with a consistent network access experience and the freedom to use any device, while still enforcing stringent security policies to protect corporate intellectual property. Further complicating the situation is delivering both consistent access and enforcing proper security policy based on the specific user-access scenario (wired, wireless, guest, local, branch, and remote users).

This trend is often referred to as Bring Your Own Device (BYOD). BYOD is a spectrum of business problems that can be solved in various ways. These range from allowing access to guest wireless networks to providing device authentication and identification. The goal is to provide a common work environment, regardless of the type of device being used. This could be accomplished by providing a virtualized desktop or by allowing users to self-register devices for use on the network.

To balance the productivity gains versus the security risks, IT needs to implement a solution that allows for seamless on-boarding of users and devices, simplicity of on-going operations, and the ability to extend end user applications to any user or any device at any time.

Cisco SBA BYOD supports a spectrum of five reference designs that can be combined to meet specific requirements. The solution lays a foundation for more advanced mobile access security infrastructures that end customers can deploy at any time. The currently available Cisco SBA deployment options are these:

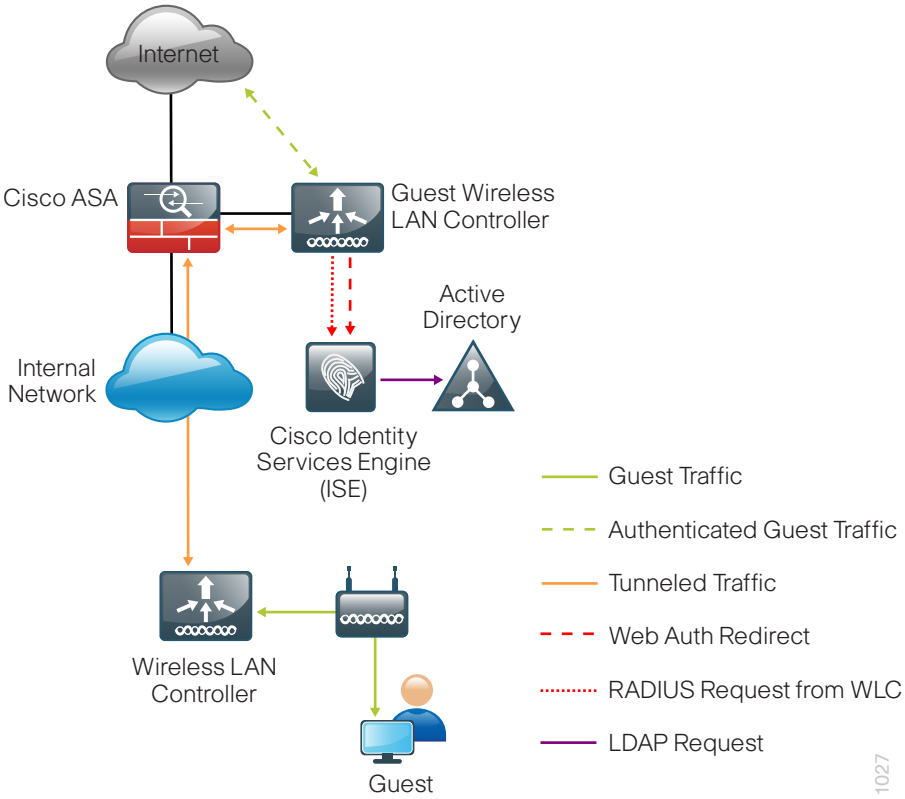
- **Guest wireless access**—Provides basic Internet access to mobile devices.
- **Identification and authentication**—Allows mobile devices to connect to the Internet and use internal network services while monitoring their activities.
- **Internal corporate access**—Overlays policy controls on what mobile devices are allowed to do inside the corporate wireless network and allows users to provision their personal devices.
- **Virtual desktops access**—Provides users with personal devices access to a virtualized desktop for internal network access.
- **Remote mobile device access**—Enables secure connections with corporate IT applications and services from outside locations.

Guest Wireless Access

Most organizations host *guest user* access services for customers, partners, contractors, and vendors, providing guest users the ability to check their email and other services over the Internet.

This design provides Internet access for guest users and denies access to corporate resources. In the broadest sense, a guest user can be any mobile device including those belonging to or used by employees, making this architecture a logical first phase of mobile device access.

Figure 1 - BYOD guest wireless access



Cisco Identity Services Engine (ISE) includes a complete provisioning and reporting system that provides temporary network access for guests. To enable guest access, a *sponsor* within the organization logs into the Cisco ISE sponsor portal and sets up a guest-level account for known individuals. Cisco ISE acts as a RADIUS server for authentication and accounting. ISE queries Active Directory to authenticate the sponsor and then allows creation of a guest account and registers it with the Cisco wireless LAN controller (WLC) designated for guest access. The sponsor can specify start and end dates and times in order to coincide with a contract period or a specific visit.

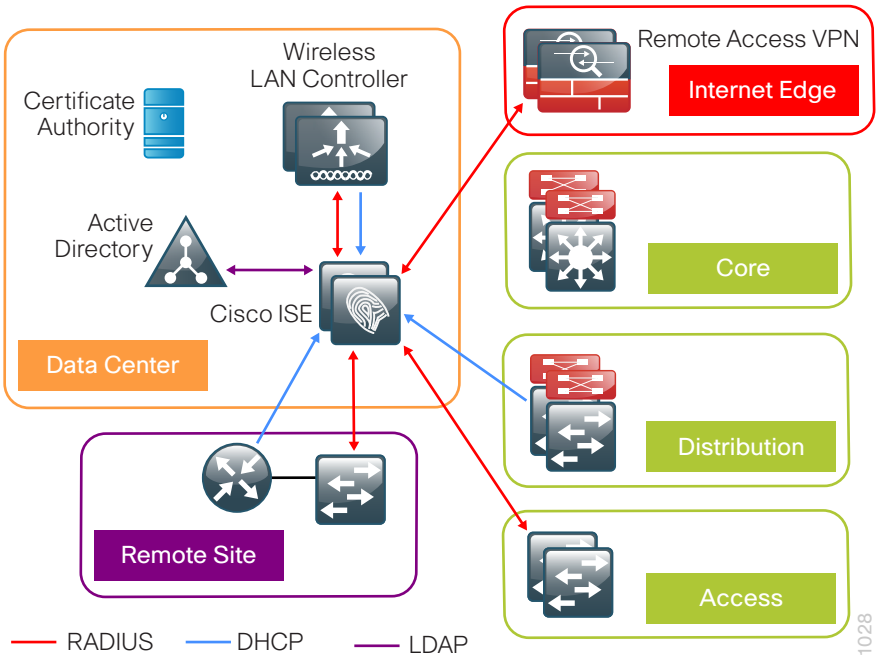
For example, suppose a sponsor has a visitor coming the following day for a meeting. She sets up a guest account, and the system sends a Short Message Service (SMS) text message to the visitor's smartphone or tablet with login details. The guest can log in as soon as he arrives for the meeting and check his email and calendar. After the meeting is over, Cisco ISE notifies the network that the account has expired, and the guest can no longer log into the guest network.

This solution lets customers offer limited Internet access privileges to guests and track when and where specific guests log in and log off, providing visibility into guest activities that help the organization protect itself.

Identification and Authentication

This reference design grants all mobile devices unrestricted access to both the Internet and to internal services and applications. This architecture supports phased deployment of identity services without affecting existing connectivity. Cisco ISE can profile device types and track their usage and also track device activity such as when the device logged in, from which port, and when it logged off. This setup is valuable for organizations that wish to monitor mobile device activity for regulatory compliance or to gather real-time, contextual information about mobile device usage for developing advanced wireless security policies.

Figure 2 - BYOD identification and authentication

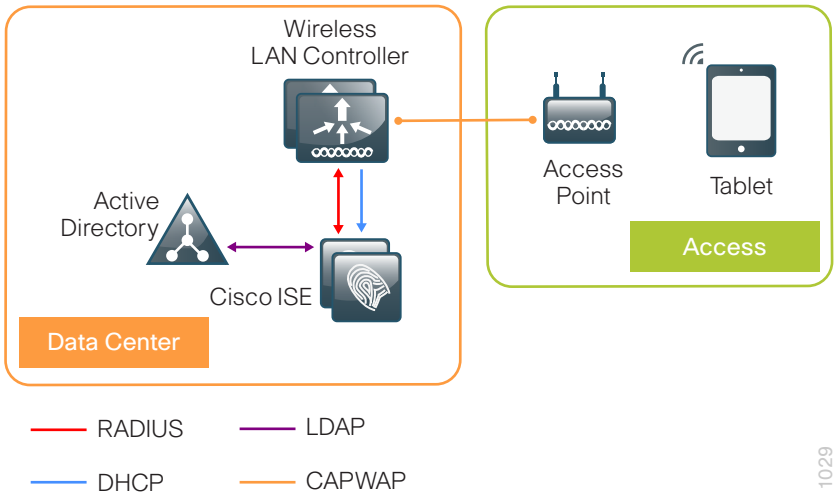


As with guest access, Cisco ISE acts as a RADIUS server for 802.1X authentication and accounting. Cisco ISE configures Cisco switches and WLCs to accept login requests from mobile devices at both headquarters and remote sites. (A dedicated Cisco WLC manages wireless guest access as described in the previous section.) Using data from the switches and WLCs, Cisco ISE determines the type of device connecting and applies access policy based on this information. Access policy is also applied based on whether the user has been provisioned with a digital certificate and what Active Directory group they are a member of. This access policy is enforced by pushing an access list to the switch or the WLC for each connection. Additional policy is enforced using the Security Group Access (SGA) features of Security Group Tags (SGT) and Security Group Exchange Protocol (SXP).

Internal Corporate Access

This reference design allows onsite users and teleworkers to access the internal network with personal mobile devices by using their existing Active Directory network credentials. This allows Cisco ISE to enforce policies on mobile devices not owned by the organization, allowing or restricting access to protect confidential and sensitive information and assets. The design alsoallows users to onboard their devices. Onboarding registers the device with Cisco ISE and then provisions a digital certificate to the device and allows for different policies for devices that have been registered.

Figure 3 - BYOD internal corporate access

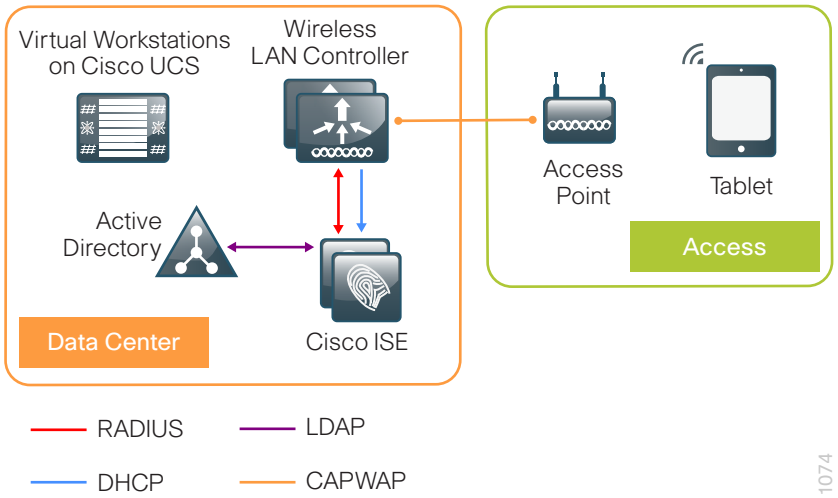


As with the guest access option, this architecture uses Cisco ISE to authenticate mobile devices by using Active Directory services. It also allows the devices to register with Cisco ISE. The architecture then permits or denies access to the internal network using access lists and Security Group Tags (SGTs), making proactive policy decisions by correlating device identity with network elements such as access switches and Cisco WLCs.

Virtual Desktop Access

Many customers want to provide a common work environment regardless of the type of device used to access the network. This is done by using a Virtualized Desktop Infrastructure (VDI) in the data center and by providing users a client to access this virtual desktop from various devices and provide a consistent interface. Similar to the internal corporate access option, onsite users and teleworkers who are using their existing Active Directory network credentials with their personal mobile devices are given access to the network. Cisco ISE enforces policies, allowing the device access only to the VDI services and the Internet. Users are able to register their device with Cisco ISE, which provisions a digital certificate for the device. Once registered, the device is given access to the network based on the user's Active Directory group membership, and the policy is enforced with access lists and Security Group Tags (SGTs.)

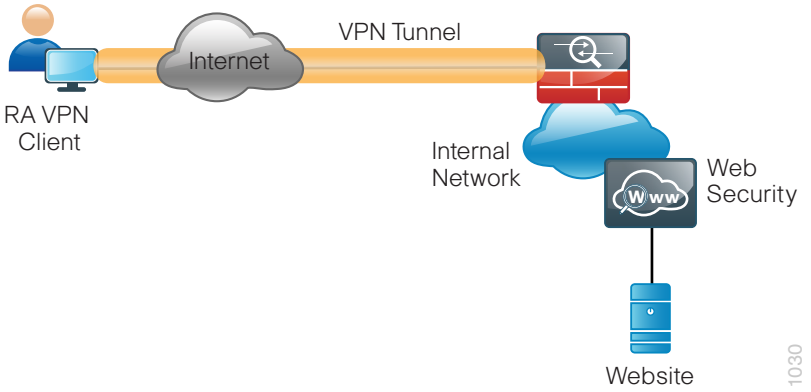
Figure 4 - BYOD virtual desktop access



Remote Mobile Device Access

True mobility fulfills its greatest potential when users can securely access corporate applications and services, with the device of their choice, from anywhere. The device must support a secure VPN with automatic roaming capabilities. For example, a sales representative depends upon a smartphone to maintain constant access to email, voicemail, and a customer relationship management (CRM) application as she travels from meeting to meeting throughout her region. The phone roams between wireless and cellular networks, even from carrier to carrier, without the user noticing.

Figure 5 - BYOD remote mobile device access



Remote mobile device access uses Cisco AnyConnect Secure Mobile Client software to establish a roaming Secure Sockets Layer (SSL)-encrypted VPN connection with Cisco Adaptive Security Appliance (ASA) at the Internet edge of the corporate network. Behind the firewall, Cisco ISE manages authentication and authorization as described in previous sections. The device accesses the Internet through the VPN tunnel at the Internet edge, allowing the corporation to apply firewall, intrusion prevention, and other Web security capabilities in order to protect both the mobile device and the internal network from malware and other security risks.

For More Information

For more information about Cisco SBA, please see *How to Get Started with Cisco SBA*, here:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_GetStarted_Feb2013.pdf

For more information about the Cisco SBA BYOD design solutions described in this paper, please see:

BYOD—Advanced Guest Wireless Access Deployment Guide:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_SLN_BYOD_AdvancedGuestWirelessAccessDeploymentGuide-Feb2013.pdf

BYOD—Internal Corporate Access Deployment Guide:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_SLN_BYOD_InternalCorporateAccessDeploymentGuide-Feb2013.pdf

BYOD—Identity and Authentication Deployment Guide:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_SLN_BYOD_IdentityAndAuthenticationDeploymentGuide-Feb2013.pdf

BYOD—Virtual Desktop Access Deployment Guide:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_SLN_BYOD_VirtualDesktopAccessDeploymentGuide-Feb2013.pdf

BYOD—Remote Mobile Access Deployment Guide:
http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_SLN_BYOD_RemoteMobileAccessDeploymentGuide-Feb2013.pdf

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

SMART BUSINESS ARCHITECTURE

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.

B-0000135-1 4/13