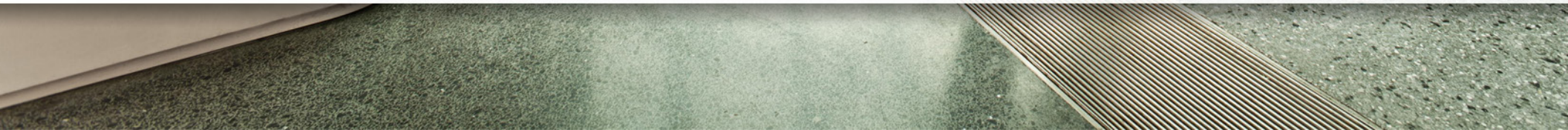
Internet Edge Design Overview

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 Borderless Networks

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 Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

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

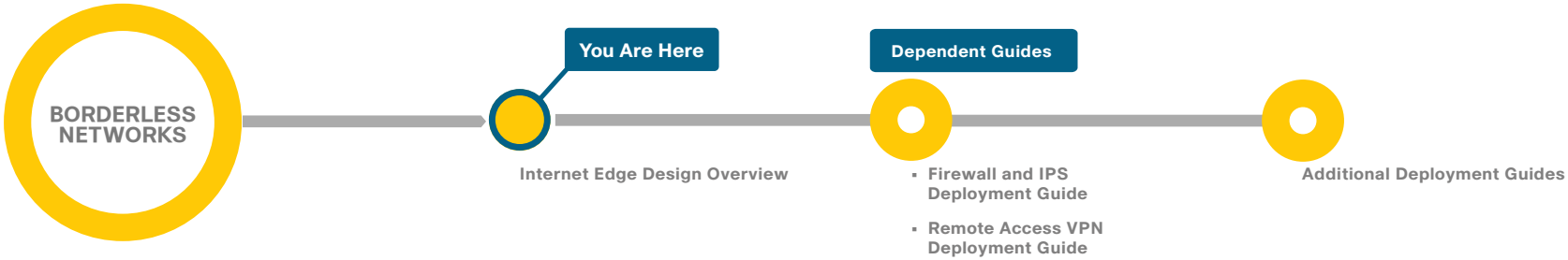
This *design overview* provides the following information:

- 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

Cisco Smart Business Architecture (SBA) is a series of network design and deployment best practice guides for organizations with up to 10,000 connected users. An important segment of Cisco SBA is the Internet edge, where the corporate network meets the public Internet. As employees reach out to websites and use email for business-to-business communication, the resources of the corporate network must remain both accessible and secure.

Cisco SBA provides employees with the secure network access they require, from a wide variety of locations and devices. Cisco SBA for the Internet edge includes the following functional solutions:

- **Firewall and intrusion prevention**—Protects the network infrastructure and data resources from Internet-based threats such as worms, viruses, and targeted attacks.
- **Remote access (RA) VPN**—Provides secure, consistent access to network resources from remote locations.
- **Secure mobile access**—Provides network access through the public infrastructure for users with mobile devices.
- **Email security**—Provides spam and malware filtering services that help protect against lost data and reduced employee productivity.
- **Web security**—Provides acceptable-use control and monitoring while managing the increasing risk associated with clients browsing the Internet.
- **IPv6 DMZ web service**—Supports secure, seamless IPv6 and IPv4 co-existence in order to provide ongoing connectivity as customers and markets migrate to IPv6.

Notes

Firewall and Intrusion Prevention

Firewalls and intrusion prevention systems (IPS) provide vital security at the Internet edge. Firewalls control access into and out of the different segments of the Internet edge to filter unwanted and malicious traffic. Many firewalls also provide a suite of additional services such as Network Address Translation (NAT) and multiple security zones. Support for policy-based operation can enhance firewall effectiveness by providing security without interfering with access to Internet-based applications or hindering connectivity to business partners' data via extranet VPN connections.

Intrusion prevention systems complement firewalls by inspecting the traffic traversing the Internet edge to identify malicious behaviors.

Cisco SBA addresses firewall and IPS needs at the Internet edge with the Cisco Adaptive Security Appliance (ASA) firewall family. Cisco ASA firewalls provide affordable, enterprise-class performance and security in a scalable design that can readily adapt to changing needs. They are situated between the organization's internal network and the Internet to minimize the impact of network intrusions while maintaining worker productivity and data security.

The Cisco SBA Internet edge architecture uses Cisco ASA 5500-X Series firewalls, configured in routing mode in active/standby pairs for high availability. They apply NAT and firewall policy and support intrusion prevention modules that detect and mitigate malicious or harmful traffic.

Two deployment options are available to address Internet access requirements for high availability and to meet operational requirements for device-level separation between the remote access VPN and the firewall. The design shown in the following figure uses a single Internet connection and integrates the remote-access VPN function in the same Cisco ASA pair that provides the firewall functionality.

Figure 1 - Single ISP topology

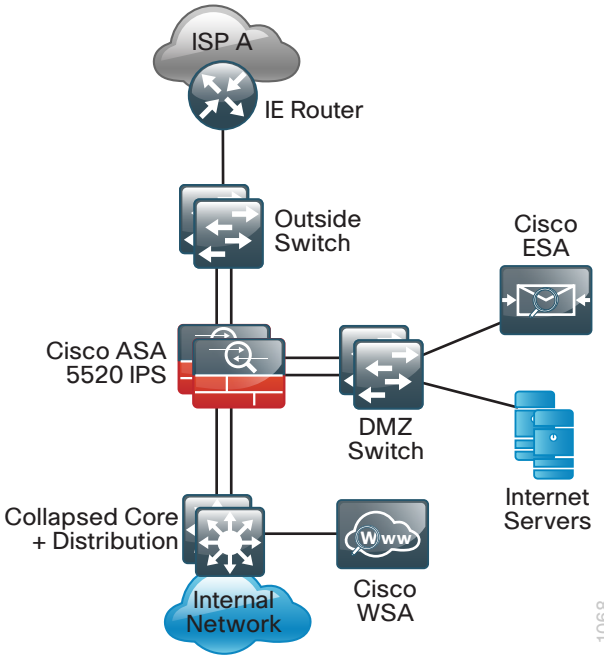
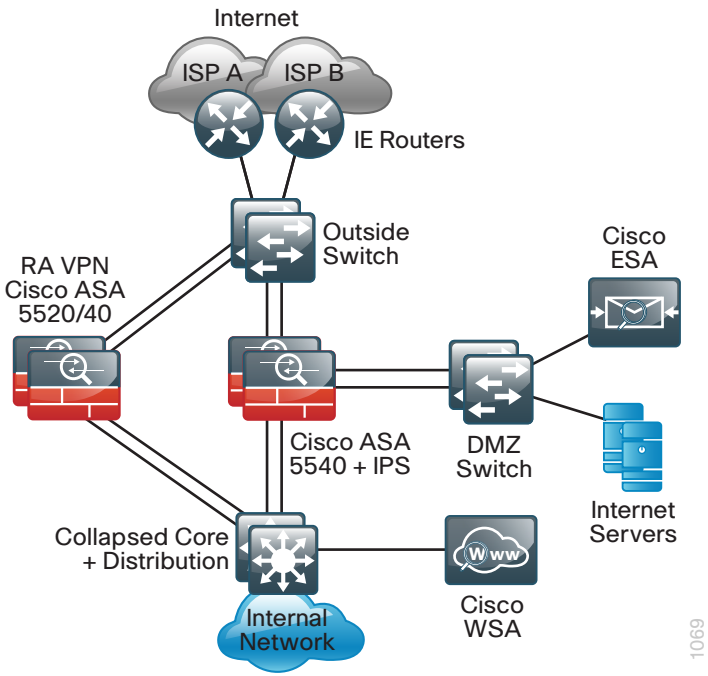


Figure 2 shows a dual ISP design that provides highly resilient Internet access. This design uses a separate pair of appliances in order to provide a remote access VPN, which offers additional scalability and operational flexibility.

Figure 2 - Dual ISP topology



For more information about Cisco SBA firewall and IPS solution deployment, see the *Cisco SBA—Borderless Networks Firewall and IPS Deployment Guide*, at the following location:
http://www.cisco.com/go/sba

This guide focuses on the Internet edge firewall and IPS security services that protect your organization's gateway to the Internet. It covers the creation and use of demilitarized zone (DMZ) segments for Internet-facing services such as a web presence. The IPS content covers Internet edge inline deployments and internal distribution layer intrusion detection system (IDS) (promiscuous) deployments.

Remote Access VPN

Employees, contractors, and partners often need to access the network when traveling or working from home or from other off-site locations. Many organizations therefore need to provide users in remote locations with network connectivity to data resources.

A secure connectivity solution for the Internet edge should support:

- A wide variety of endpoint devices.
- Seamless access to networked data resources.
- Authentication and policy control that integrates with the authentication resources used by the organization.
- Cryptographic security to prevent sensitive data from exposure to unauthorized parties who accidentally or intentionally intercept the data.

Cisco SBA addresses these needs with the Cisco ASA Family and Cisco AnyConnect Secure Mobility Client.

The Cisco ASA Family of security devices provides a full complement of security services, including intrusion prevention, VPN, content security, unified communications, and remote access. All Cisco ASA devices support IP Security (IPsec), web portal, full-tunnel Secure Sockets Layer (SSL) VPNs for client-based remote access, and IPsec for site-to-site VPN.

The Cisco AnyConnect Secure Mobility Client is recommended for remote users who require full network connectivity. The Cisco AnyConnect client uses SSL and is designed for automated download and installation. SSL access can be more flexible and is likely to be accessible from more locations than IPsec, as few companies block HTTPS access out of their networks.

Cisco SBA offers two different remote-access VPN design models:

- **Remote access VPN integrated with Cisco ASA Series firewall (integrated design module)**—This option is available with a lower capital investment and reduces the number of devices the network engineering staff must manage.
- **Remote access VPN deployed on a pair of standalone Cisco ASA appliances (standalone design module)**—This design offers greater operational flexibility and scalability while providing a simple migration path from an existing RA VPN installation.

For detailed configuration information about implementing a remote access VPN via Cisco AnyConnect for SSL connections, see the *Cisco SBA—Borderless Networks Remote Access VPN Deployment Guide*, here:
http://www.cisco.com/go/sba

This guide includes sections for configuring a variety of access methods, beginning with a configuration that is common to all of the access methods. Configurations for both the integrated and standalone design modules offer identical functionality and capability, so the user experience is unchanged regardless of the design chosen. Unless specifically noted, the configuration described in this document is common to both the integrated and standalone designs.

Secure Mobile Access

One of the most profound advances in modern networks is the degree of mobility those networks support. Users can move around wirelessly inside the campus and enjoy the same degree of connectivity as if they were plugged in using cables in their offices. Users can leave their primary networks completely and work from a home-office environment that offers the same connectivity and user experience as they would get in their offices. Users also have the option of being truly mobile and connecting from any place that offers Internet access. With smartphones and tablets, this mobility now commonly includes connecting while travelling down the highway or on a train.

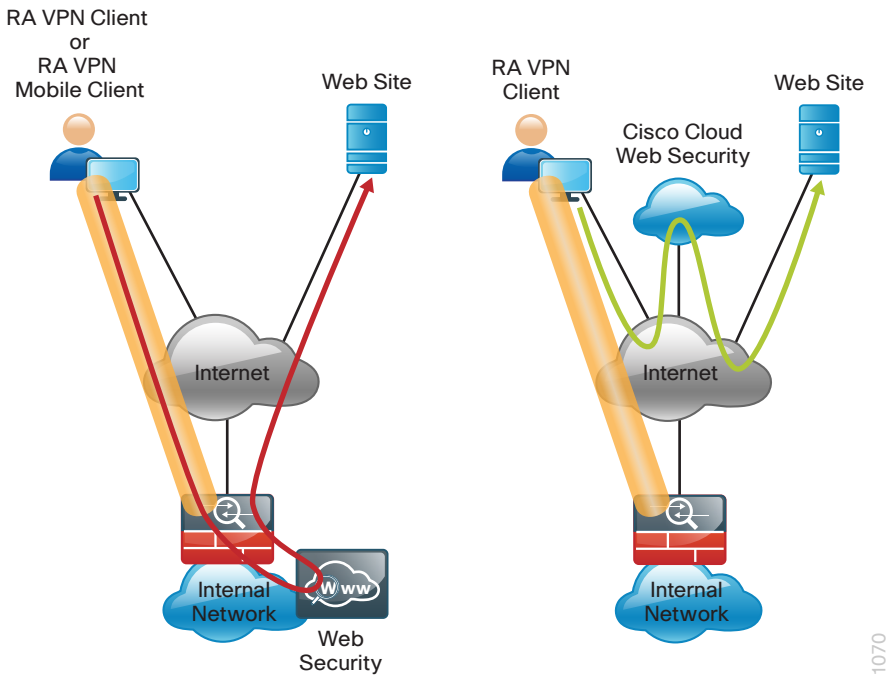
Because these mobile users are outside the traditional perimeter (or physical border) of the network, their devices are exposed to potentially more malicious activity than a device that is located inside the protection of the network. Businesses must provide connectivity solutions that are not only secure, but offer seamless operation that facilitates productivity.

The Cisco SBA Internet edge design addresses mobile device security with the AnyConnect Secure Mobility client and the Cisco Cloud Web Security (CWS) service.

Mobile remote users generally connect to the network by using either laptop computers or the newer group of mobile devices that includes smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ.

The Cisco SBA Internet edge design covers remote access VPN for laptops running the Cisco AnyConnect Secure Mobility client (for SSL VPN or IP Security [IPsec] connections). A module available for the Cisco AnyConnect 3.1 client adds the ability to interface with the Cisco CWS Security service. This module gives the Cisco AnyConnect client the ability to let Internet web traffic go out through a Cisco CWS proxy directly to the destination without forcing it through the organization's headend. Without Cisco CWS, the traffic must be routed down the VPN tunnel, inspected at the campus Internet edge, and then redirected to the original destination. This process consumes bandwidth and potentially increases latency. With Cisco CWS, the connection can be proxied through the Cisco ScanSafe cloud and never has to traverse the VPN tunnel, as shown in the following figure.

Figure 3 - Web security traffic flow for remote access VPN



For more information about providing your employees with secure mobile access through the Internet edge, see the *Cisco SBA—Borderless Networks Remote Mobile Access Deployment Guide*, here: http://www.cisco.com/go/sba

This guide describes business-use cases related to the truly mobile users who use a laptop, smartphone, or tablet device to connect through infrastructure that is not provided by their organizations. It covers the additional configuration for remote access VPN for the Cisco AnyConnect 3.1 client that is required to activate Cisco CWS, Always On, and other features. It also covers interaction with the Cisco CWS management tool, ScanCenter. Last, the document covers configuration of Cisco ASA to support mobile devices such as smartphones and tablets, and also the configuration of the Cisco AnyConnect client that is required for those devices to connect to Cisco ASA.

Email Security Using ESA

Email is a critical business service used by virtually everyone, every day, which makes it an attractive target for hackers. The two major threats to email systems are spam and malicious email.

If spam is not properly filtered, its sheer volume can consume valuable resources such as bandwidth and storage, and require employees to waste time manually filtering through messages. Or, legitimate messages may be discarded, potentially disrupting business operations.

Malicious email most often consists of embedded or phishing attacks. Embedded attacks contain viruses and malware that perform actions on the end device when clicked. Phishing attacks attempt to mislead employees into releasing sensitive information such as credit card numbers, social security numbers, or intellectual property.

Failing to protect an email service against spam and malicious attacks can result in a loss of data and employee productivity.

Cisco Email Security Appliance (ESA) protects the email infrastructure and employees who use email at work by filtering unsolicited and malicious email before it reaches the user. The goal of the solution is to filter out positively identified spam and quarantine or discard email sent from untrusted or potentially hostile locations. Antivirus scanning is applied to emails and attachments from all servers to remove known malware.

Cisco ESA easily integrates into existing email infrastructures by acting as a Mail Transfer Agent (MTA), or mail relay, within the email-delivery chain. A normal email exchange, in which an organization is using an MTA, might look like the message flows shown in Figure 4 and Figure 5.

Figure 4 - Inbound email message flow

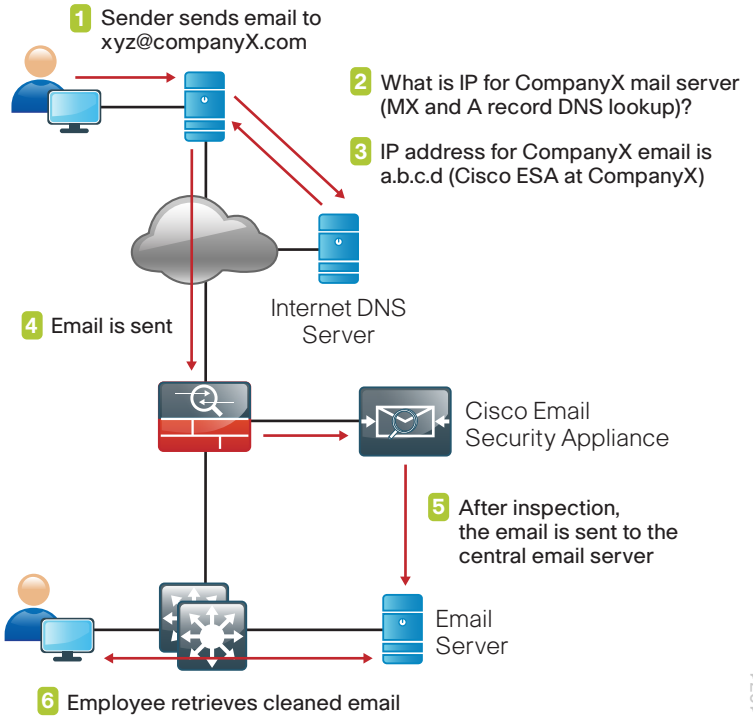
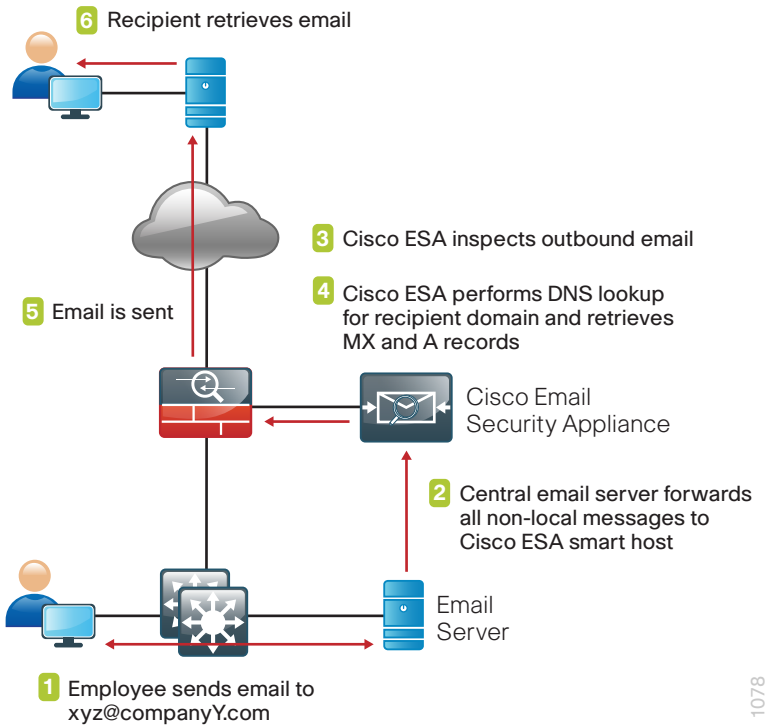


Figure 5 - Outbound email message flow



Cisco ESA can be deployed with a single physical interface to filter email to and from an organization's mail server. A second, two-interface configuration option transfers email to and from the Internet using one interface, and to and from internal servers using the second interface. The Internet Edge design uses the single-interface model for simplicity.

For more information about email security and Cisco ESA, see the *Cisco SBA—Borderless Networks Email Security Using ESA Deployment Guide*, at the following location:
http://www.cisco.com/go/sba

This guide focuses on protecting the email infrastructure and employees who use email at work. It describes how SPAM and malicious email can threaten data and reduce productivity, and how Cisco ESA uses a multilayer approach that combines reputation-based and context-based filtering with the use of antivirus signatures to prevent unsolicited and malicious email from reaching users.

Web Security

Web access is critical for the day-to-day functions of most organizations, but its benefits come with associated risks. Policy-based web access can help ensure that employee web use is aligned with company goals, and that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk. Two different options are available: the Cisco Web Security Appliance (WSA), which is deployed on premise, and Cisco CWS, which is accessed by using the Cloud Web Security Connector for Cisco ASA.

Some key differences between Cisco CWS and Cisco WSA include the items listed in the following table.

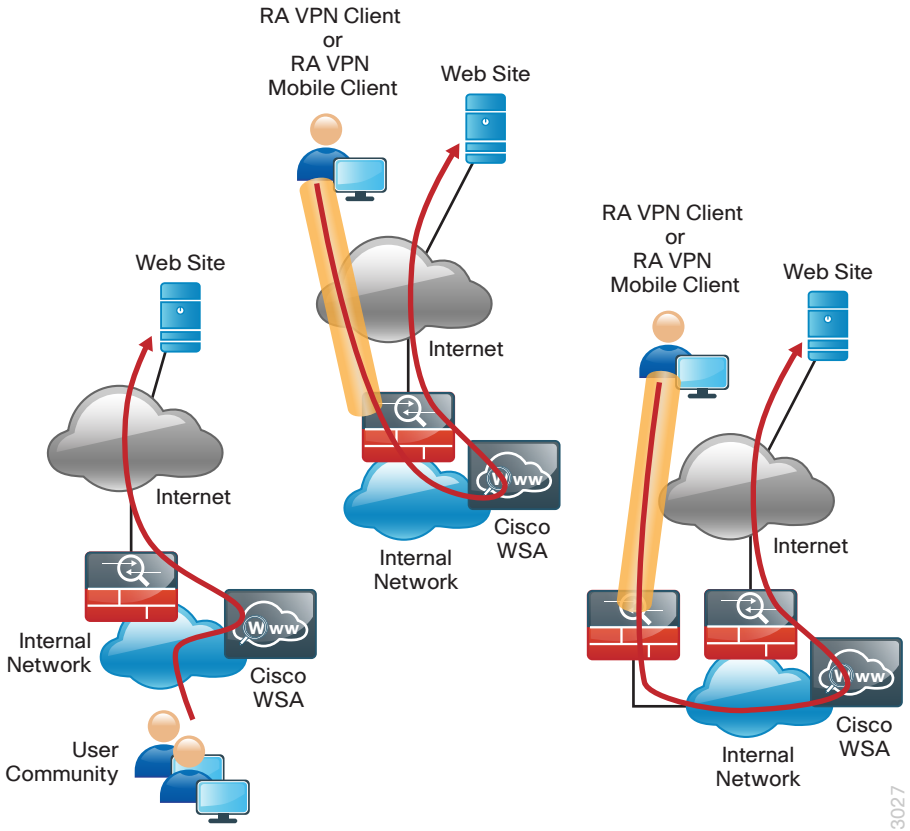
Table 1 - Cisco Web Security solution comparison

	Cisco CWS	Cisco WSA
Web/URL filtering	Yes	Yes
Supported protocols	HTTP/HTTPS	HTTP/HTTPS, FTP
Outbreak Intelligence (Zero Day Malware)	Yes (Multiple scanners for malware)	Yes (URL/IP reputation filtering, multiple scanners for malware)
Remote user security	Direct to cloud using Cisco AnyConnect	VPN backhaul
Remote user security (mobile devices)	VPN backhaul	VPN backhaul
Deployment	Redirect to cloud service	On Premise Redirect
Policy and reporting	Web portal (cloud)	On Premise

Cisco Web Security Appliance

Cisco WSA addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection. Cisco WSA is a web proxy that works with other Cisco network components such as firewalls, routers, or switches in order to monitor and control web content requests from within the organization. It also scrubs the return traffic for malicious content, as shown in the following figure.

Figure 6 - Cisco WSA traffic flows



Cisco WSA is connected by one interface to the inside network of Cisco ASA. In the Internet edge design, Cisco WSA connects to the same LAN switch as the appliance and on the same VLAN as the inside interface of the appliance. Cisco ASA redirects HTTP and HTTPS connections using the Web Cache Communication Protocol (WCCP) to Cisco WSA.

Cisco Cloud Web Security

Using multiple techniques, Cisco CWS provides granular control over all the web content that is accessed by the user community. These techniques include real-time dynamic web content classification, a URL filtering database, and also file type and content filters. The policies enforced by Cisco CWS provide an organization strong web security and control that apply to all users, regardless of their location and device type.

Internal users at both the primary site and at remote sites access the Internet by using the primary site's Internet-edge Cisco Adaptive Security Appliance (ASA), which provides stateful firewall and intrusion prevention capabilities. It is simple and straightforward to add Cisco CWS to a Cisco ASA appliance that is already configured and operational.

Cisco SBA provides deployment guidance for Cisco CWS using Cisco ASA for the following types of users:

- Internal users at the primary site or at remote sites
- Wireless guest users connected to a demilitarized zone (DMZ) network
- Remote-access VPN users who are using a non-CWS enabled AnyConnect client connecting with either the integrated firewall and VPN model or standalone VPN model

The various traffic flows for each of these use cases are shown in the following figures.

Figure 7 - Cloud Web Security with internal and guest users

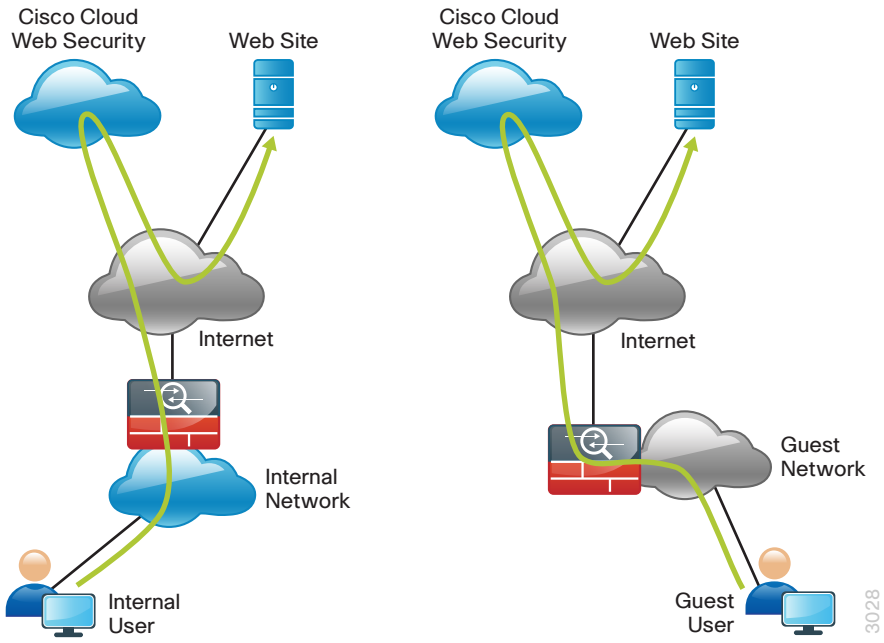
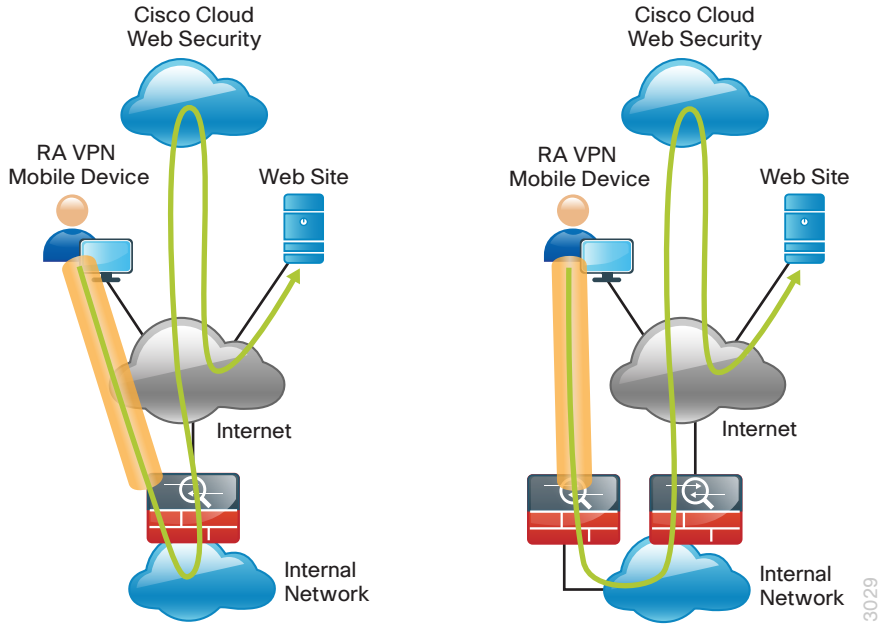


Figure 8 - Cloud Web Security for mobile devices using remote access VPN



For more information about supporting secure, productive, and resource-efficient web access by using Cisco SBA, see the *Cisco SBA—Borderless Networks Web Security Using WSA Deployment Guide* and *Cisco SBA—Borderless Networks Cloud Web Security Using Cisco ASA Deployment Guide*, here:
http://www.cisco.com/go/sba

The *Web Security Using WSA Deployment Guide* focuses on using WSA in an Internet edge solution. It covers the mechanisms used to apply web security and content control, such as URL-filtering with category-based Cisco web usage controls, as well as the use of transparent proxy mode and explicit proxy mode deployments for redirecting web traffic to Cisco WSA.

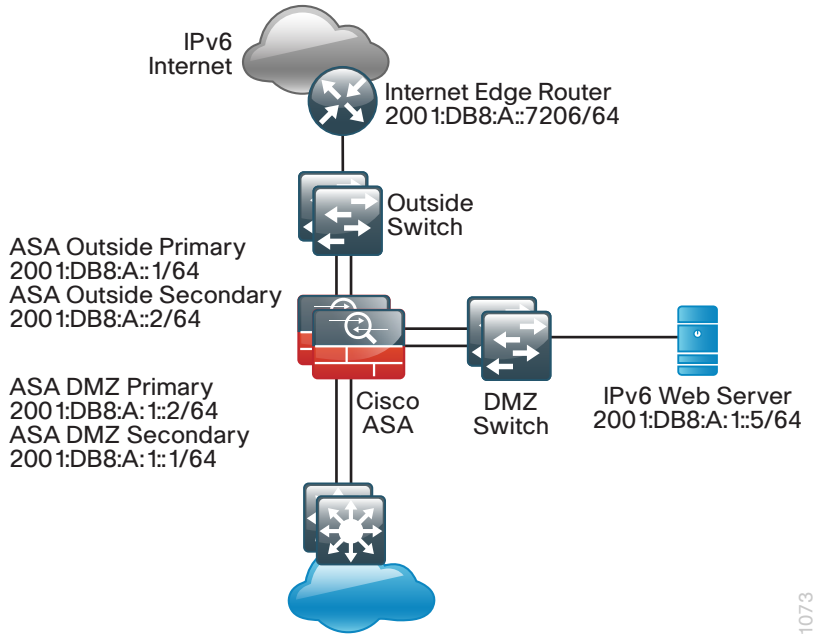
The *Cloud Web Security Using Cisco ASA Deployment Guide* focuses on using CWS with the Cloud Web Security Connector for Cisco ASA. It covers the procedures required to implement a Cisco ASA service policy that matches specified traffic and redirects the traffic to the Cisco CWS cloud for inspection. This method is considered a transparent proxy, and no configuration changes are required to web browsers on user devices. It also covers interaction with the Cisco CWS management tool, ScanCenter.

IPv6 DMZ Web Service

IPv4 addresses are no longer available from the Internet Assigned Numbers Authority (IANA), and the Regional Internet Registries (RIRs) will soon run out as well. Technologies such as NAT and the use of RFC 1918 addressing will allow most organizations to continue operating on IPv4 for the foreseeable future, but the transition to IPv6 is already occurring in some regions and will quickly spread worldwide. To maintain network operations and prepare for a future in which IPv6 will play an increasingly large role, businesses must begin phasing IPv6 connectivity into their IPv4 environments.

Cisco SBA accommodates IPv6 Internet edge servers while continuing to support IPv4 clients by using a dual stack approach. A dual stack architecture allows logically separate IPv4 and IPv6 networks to coexist on the same equipment. IPv6 can be added to Cisco SBA Internet Edge through additional configuration of existing software that is specified for the existing IPv4 Internet Edge (Figure 6). The solution includes reconfiguring Cisco ASA firewalls, which are managed via IPv4. The Cisco ASA firewall for IPv4 provides application inspection and IPS for applications running over IPv6.

Figure 9 - IPv6 Internet Edge deployment architecture



For more information about addressing IPv6 integration by using Cisco SBA, see the *Cisco SBA—Borderless Networks IPv6 DMZ Web Service Deployment Guide*, here:
http://www.cisco.com/go/sba

This guide shows how to use existing hardware in the Internet edge to support native IPv6 access to Internet-facing services. The example solution accommodates IPv6 HTTP and HTTPS web traffic to and from the Internet edge.

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-0000190-1 1/13