Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

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

Open the latest version of this guide

Access the latest series of CVD Guides

Continue reading this archived version

Internet Edge

Design Summary

January 2014

CISCO VALIDATED DESIGN

Table of Contents

Preface 1
Introduction 2
Firewall and Intrusion Prevention 3
Remote Access VPN 5
Email Security Using ESA 6
Web Security 8
Cisco Web Security Appliance 9
Cisco Cloud Web Security 10
Cisco CWS Using the Connector for Cisco ASA 10
Cisco CWS Using Cisco AnyConnect 12
Secure Mobile Access 14

Preface

Cisco Validated Designs (CVDs) provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

This design summary provides information about the use cases covered in a series or set of related CVD guides and summarizes the Cisco products and technologies that solve the challenges presented by the use cases.

Comments and Questions

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

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd/edge

Introduction

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

CVDs for the Internet edge provide users with the secure network access they require, from a wide variety of locations and devices. CVDs for the Internet edge include 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 network-user productivity.
- **Web security**—Provides acceptable-use control and monitoring while managing the increasing risk associated with clients browsing the Internet.

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.

CVDs for the Internet edge address firewall and IPS needs 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.

CVDs for the Internet edge use Cisco ASA 5500-X Series Adaptive Security Appliances, 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

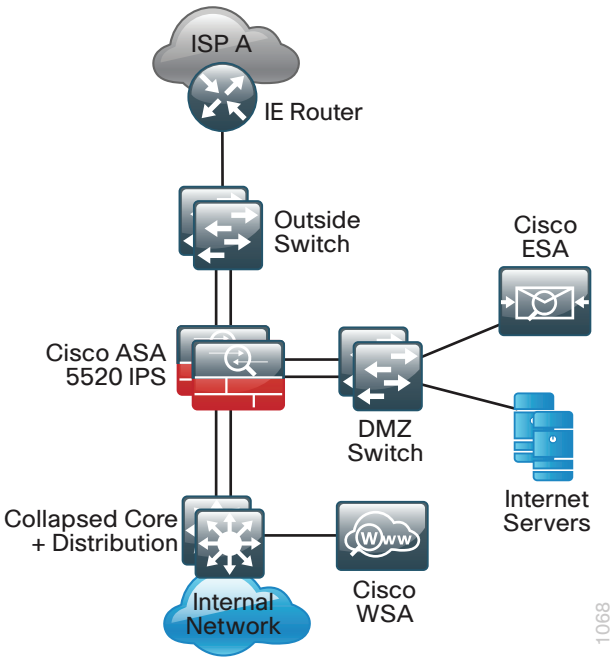
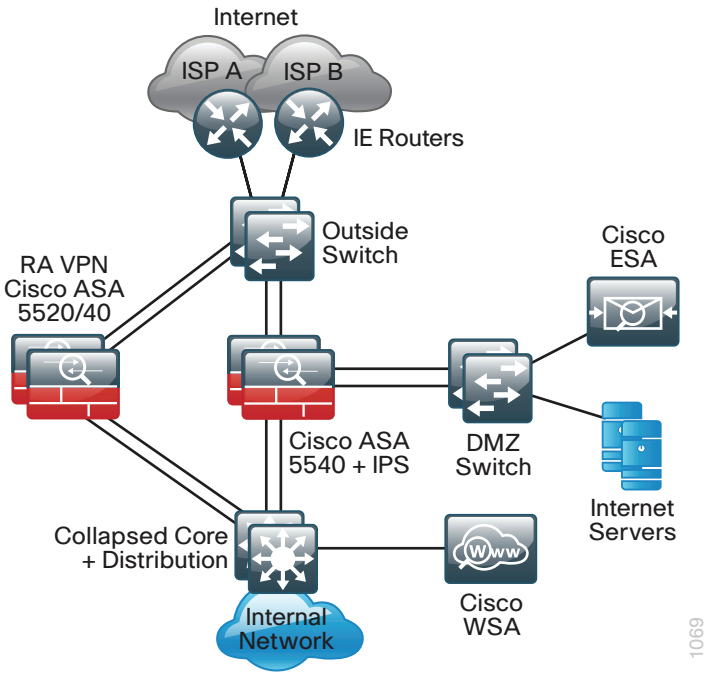


Figure 2 shows a dual ISP design that provides highly resilient Internet access. This design uses a separate pair of appliances in order to provide a remote access VPN, which offers additional scalability and operational flexibility.

Figure 2 - Dual ISP topology



For more information about firewall and IPS solution deployment, see the Firewall and IPS Technology Design Guide.

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.

CVDs for the Internet edge address 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.

CVDs for the Internet edge offer two 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 Remote Access VPN Technology Design Guide.

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.

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 network users 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 network users 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 network-user productivity.

Cisco Email Security Appliance (ESA) protects the email infrastructure and network users 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 3 and Figure 4.

Figure 3 - Inbound email message flow

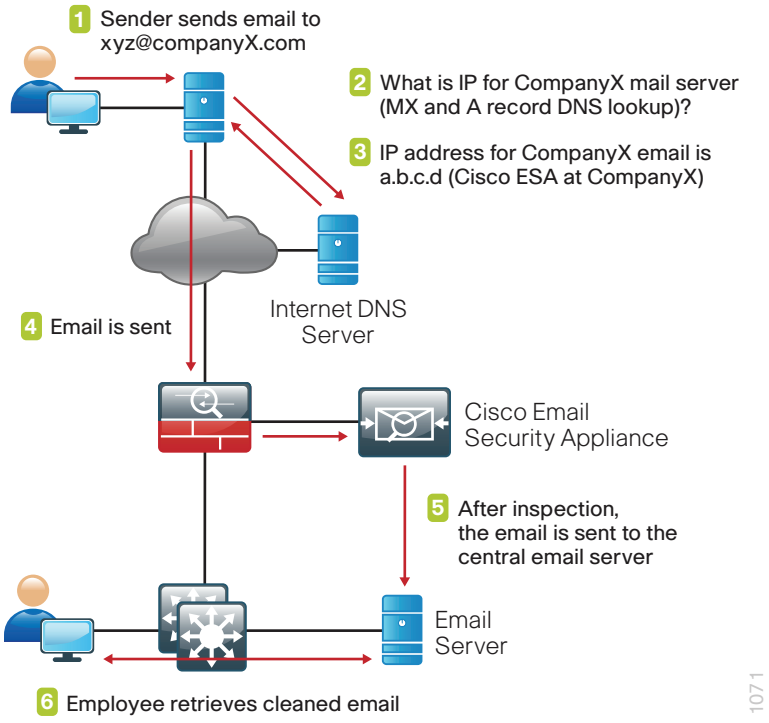
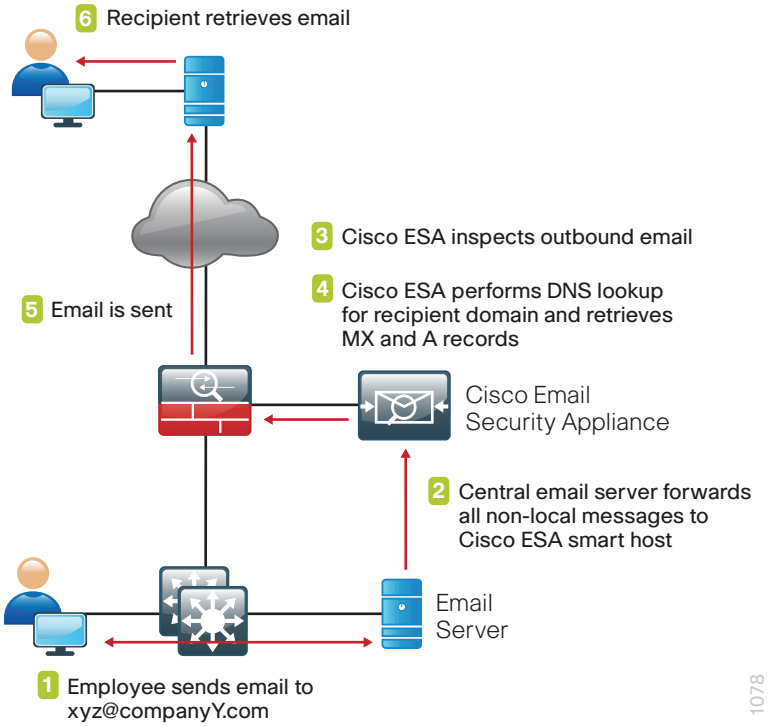


Figure 4 - Outbound email message flow



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 Email Security Using ESA Technology Design Guide.

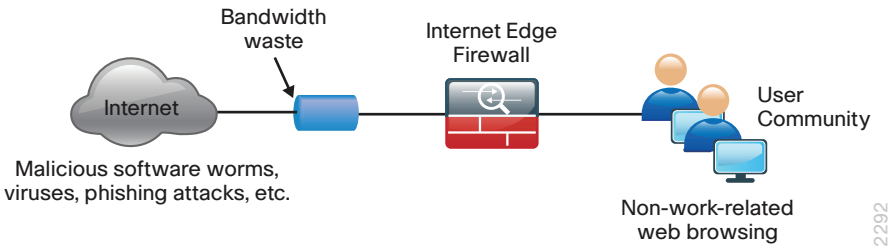
This guide focuses on protecting the email infrastructure and its users. It describes how SPAM and malicious email can threaten data and reduce productivity, and how Cisco ESA uses a multilayer approach that combines reputation-based and context-based filtering with the use of antivirus signatures to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

Web Security

Web access is a requirement for the day-to-day functions of most organizations, but a challenge exists to maintain appropriate web access for everyone in the organization, while minimizing unacceptable or risky use. A solution is needed to control policy-based web access in order to ensure users work effectively and ensure that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

Another risk associated with Internet access for the organization is the pervasive threat that exists from accessing sites and content. Other threats include the still popular and very broad threats of viruses and *Trojans*, in which a user receives a file in some manner and is tricked into running it, and the file then executes malicious code. The third variant uses directed attacks over the network. These types of risks are depicted in the figure below.

Figure 5 - Business reasons for deploying Cisco Cloud Web Security



Two options address 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 Web Security Appliance (WSA), which is deployed on premise
- Cisco Cloud Web Security (CWS), which is accessed by using the Cloud Web Security Connector for Cisco ASA or by using Cisco AnyConnect Secure Mobility Client.

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

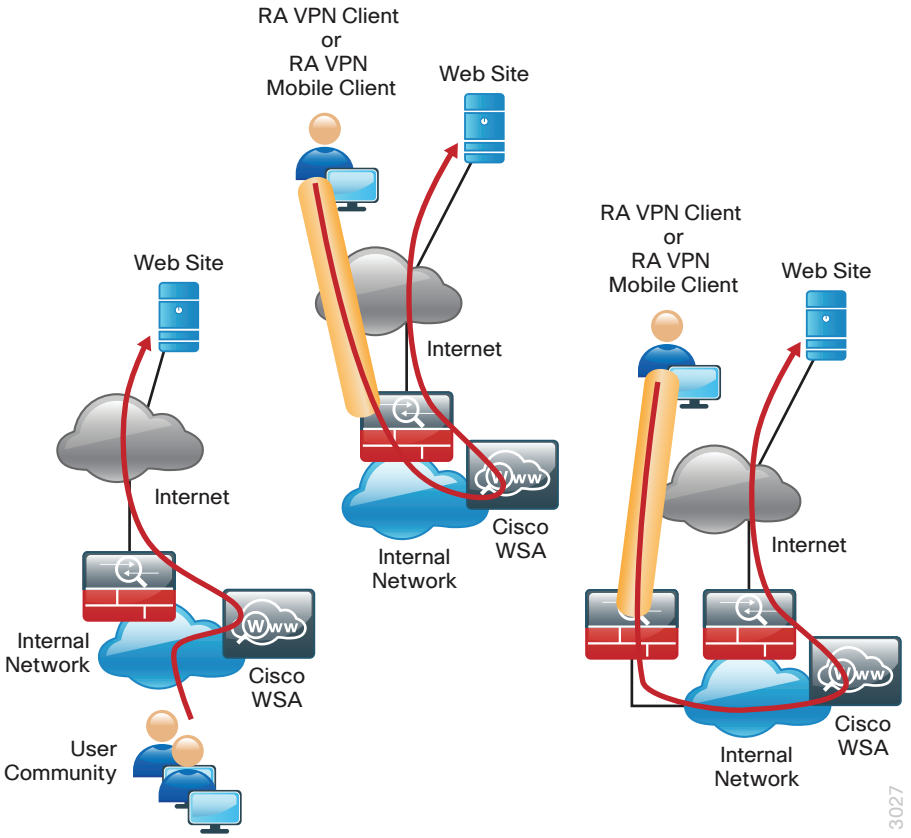
Table 1 - Cisco Web Security solution comparison

	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 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.

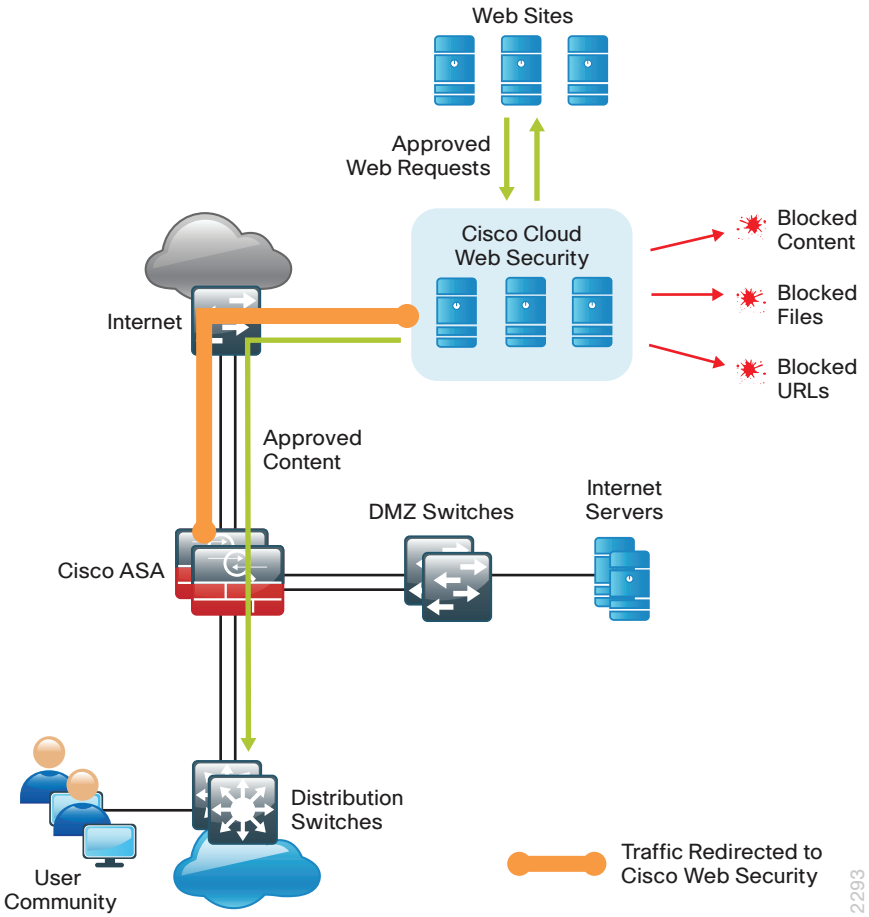
For more information about how to deploy this solution, see the Web Security Using Cisco WSA Technology Design Guide.

This guide focuses on using Cisco WSA in an Internet edge solution. It covers the mechanisms used to apply web security and content control, as well as the use of transparent -proxy mode and explicit-proxy mode deployments for redirecting web traffic to Cisco WSA.

Cisco Cloud Web Security

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

Figure 7 - Cisco CWS Internet edge design



Cisco CWS Using the Connector for Cisco ASA

Internal users at both the primary site and remote sites access the Internet by using the primary site's Internet-edge Cisco 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. This integration uses the Cloud Web Security Connector for Cisco ASA and requires no additional hardware.

Cloud Web Security using Cisco ASA enables the following security capabilities:

- **Transparent redirection of user web traffic**—Through seamless integration with the Cisco ASA firewall, web traffic is transparently redirected to the Cisco CWS service. No additional hardware or software is required, and no configuration changes are required on user devices.
- **Web filtering**—Cisco CWS supports filters based on predefined content categories and it also supports more detailed custom filters that can specify application, domain, and content type or file type. The filtering rules can be configured to block or warn based on the specific web-usage policies of an organization.

- **Malware protection**–Cisco CWS analyzes every web request in order to determine if content is malicious. CWS is powered by the Cisco Security Intelligence Operations (SIO) whose primary role is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- **Differentiated policies**–The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key of the forwarding firewall, source IP address of the web request, or the Microsoft Active Directory user and domain information of the requestor.

The Cisco ASA firewall family sits between the organization's internal network and the Internet and is a fundamental infrastructural component that minimizes the impact of network intrusions while maintaining worker productivity and data security. The design uses Cisco ASA to implement a 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.

The various traffic flows for each of these user types are shown in the following figures.

Figure 8 - Cisco CWS with internal and guest users

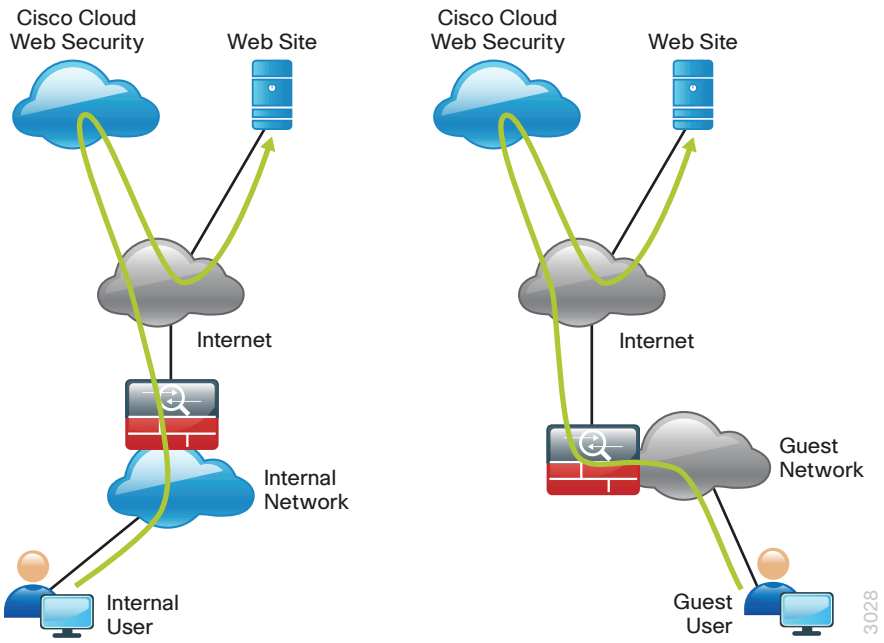
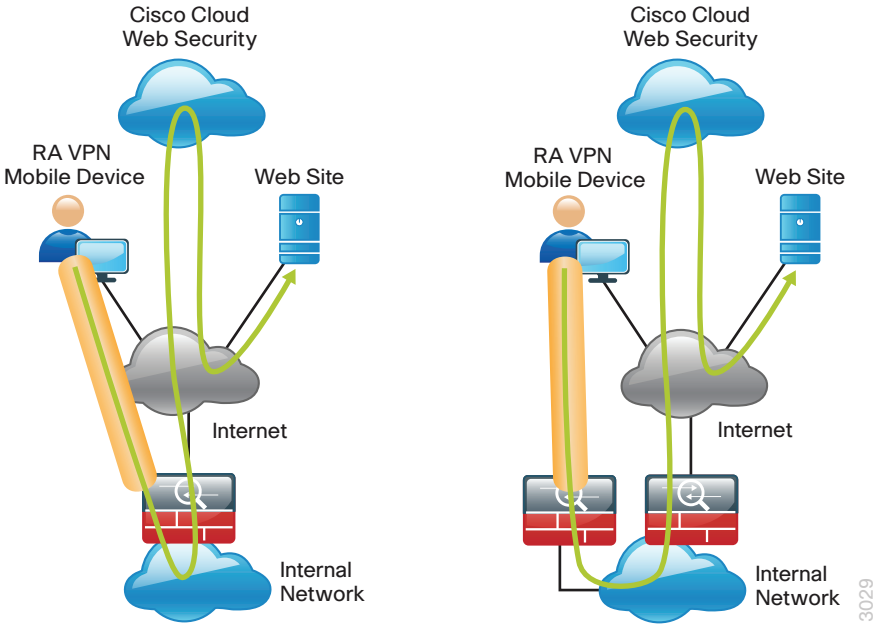


Figure 9 - Cisco CWS for mobile devices using remote-access VPN



Certain source and destination pairs should be exempted from the service policy, such as remote-access VPN users accessing internal networks or internal users accessing demilitarized zone (DMZ) networks.

For information about how to deploy this solution, see the Cloud Web Security Using Cisco ASA Technology Design Guide.

This guide focuses on using Cisco 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.

Cisco CWS Using Cisco AnyConnect

Mobile remote users connect to their organization's network by using devices that generally fall into two categories:

- Laptops
- Mobile devices such as smartphones and tablets

Reader Tip

The Cisco CWS using Cisco AnyConnect solution focuses on the Cisco AnyConnect Secure Mobility client for laptops running Microsoft Windows and Apple Mac OS. For mobile device security that includes smart phones and tablets in addition to laptops, see the Secure Mobile Access section.

When provisioned with the Cisco AnyConnect Secure Mobility Client with Cisco CWS, laptops are not required to send web traffic to the primary site.

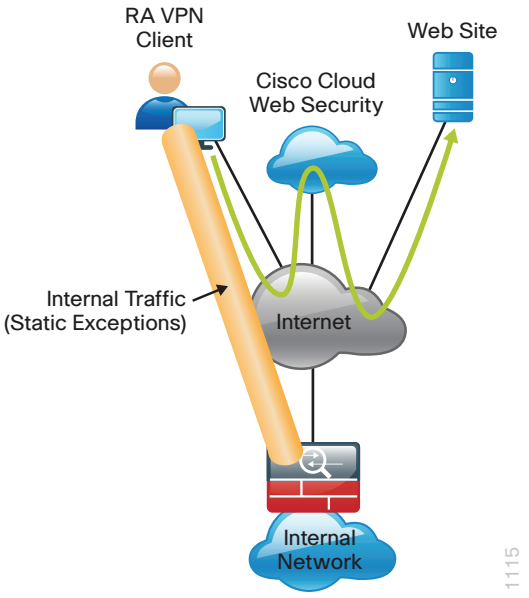
For the web security of Microsoft Windows and Apple Mac OS laptops, Cloud Web Security using Cisco AnyConnect enables the following security capabilities:

- **Redirect web traffic**–The Cisco CWS module can be integrated into the Cisco AnyConnect client, allowing web traffic to be transparently redirected to the Cisco CWS service. The CWS module is administered centrally on the RAVPN firewall and requires no additional hardware. Once installed, the CWS module continues to provide web security even when disconnected from the RAVPN firewall.
- **Filter web content**–Cisco CWS supports filters based on predefined content categories, as well as custom filters that can specify application, domain, content type, or file type. The filtering rules can be configured to block or warn based on the specific web usage policies of an organization.
- **Protect against malware**–Cisco CWS analyzes every web request to determine if the content is malicious. CWS is powered by the Cisco Security Intelligence Operations, the primary role of which is to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- **Apply differentiated policies**–The Cisco CWS web portal applies policies on a per-group basis. Group membership is determined by the group authentication key assigned within the Cisco AnyConnect CWS profile on the RAVPN firewall.

Cloud Web Security using Cisco AnyConnect enables the following network capabilities:

- **User authentication**–The AnyConnect client requires all remote access users to authenticate before negotiating a secure connection. Both centralized authentication and local authentication options are supported.
- **Differentiated access**–The remote access VPN is configured to provide different access policies depending on assigned user roles.
- **Strong encryption for data privacy**–The Advanced Encryption Standard cipher with a key length of 256 bits is used for encrypting user data. Additional ciphers are also supported.
- **Hashing for data integrity**–The Secure Hash Standard 1 cryptographic hash function with a 160-bit message digest is used to ensure that data has not been modified during transit.

Figure 10 - Web traffic flow for CWS with Windows and Mac OS X clients



For more information about how to deploy this solution, see the Cloud Web Security Using Cisco AnyConnect Technology Design Guide.

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.

CVDs for the Internet edge address mobile device security–including smart phones and tablets–with the Cisco AnyConnect Secure Mobility client and the Cisco CWS service.

Reader Tip

For Cisco Cloud Web Security for remote users, see the Cisco CWS Using Cisco AnyConnect section.

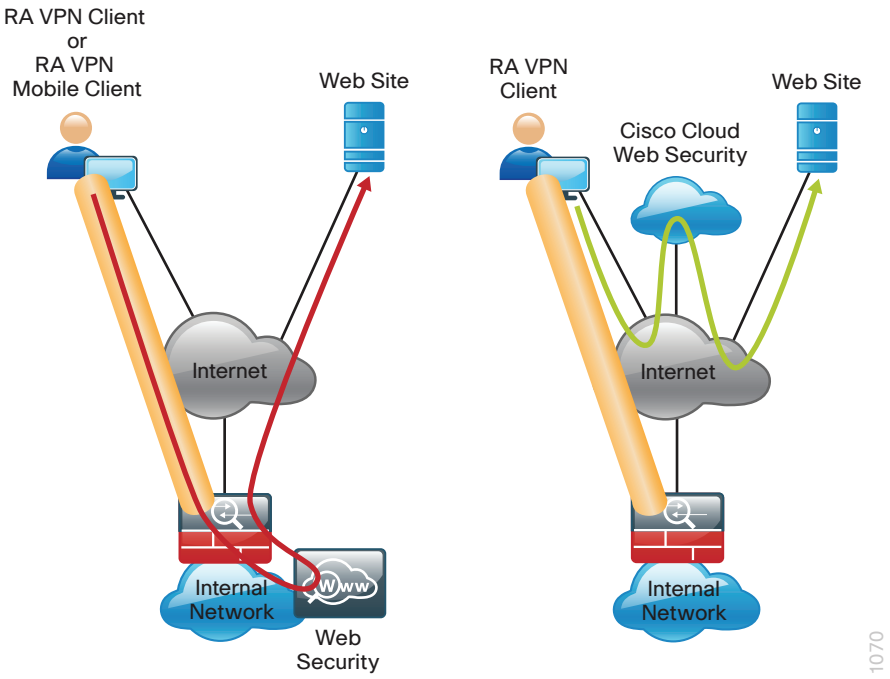
Mobile devices typically use a different deployment model in which basic services, such as mail, calendar, and contacts, are provided over Microsoft ActiveSync, which gives quick access to these commonly used services. For access to other services, including voice, video, internally hosted web servers, file shares, or other network services, a VPN tunnel is required. For secure mobile access, CVDs for Internet edge enable the following additional security features in the Cisco AnyConnect Secure Mobility client with the Cisco CWS service:

- **Always-on VPN**–The Trusted Network Detection capability of the Cisco AnyConnect client determines if a laptop is on a trusted internal network or an untrusted external network. If on an untrusted network, the client automatically tries to establish a VPN connection to the primary site. The user needs to provide authentication, but no other intervention is required. If the user disconnects the connection, no other network access is permitted.
- **Mobile data services using Microsoft ActiveSync**–Cisco ASA Firewall and Microsoft Forefront Threat Management Gateway, when deployed in a DMZ network, provide an integrated solution for securing mobile data services. This solution supports a variety of mobile devices that run on Android, iOS, and Windows Mobile operating systems.

CVDs for the Internet edge cover 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 11 - Web security traffic flow for remote access VPN



For more information about providing secure mobile access through the Internet edge, see the Remote Mobile Access Technology Design Guide.

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.

Feedback

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

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 02/14