Cloud Web Security with Cisco Integrated Services Router

Design Guide

September, 2014

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Contents

Introduction **3**

Supported Cisco ISR Cloud Web Security Topologies **3**

Integrated Features Supported with Cisco CWS Connector on ISR **7**

Scaling **8**

User Experience **8**

Additional Design Considerations **11**

Cisco CWS and Shared Assets 11
Cisco CWS on LAN Interfaces 11
Cisco CWS with Dual WAN Interfaces 11
Cisco CWS with ACL-Based Crypto Maps 11
Cisco CWS with GETVPN 12
Cisco CWS with WAAS or WAAS Express 12

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Introduction

The Cisco[®] Integrated Services Router (ISR) with Cisco Cloud Web Security (CWS) offers a web security and web filtering solution that requires no additional hardware or client software. Cisco CWS can help branch offices to intelligently redirect web traffic to the cloud to enforce detailed security and acceptable-use policies for user web traffic.

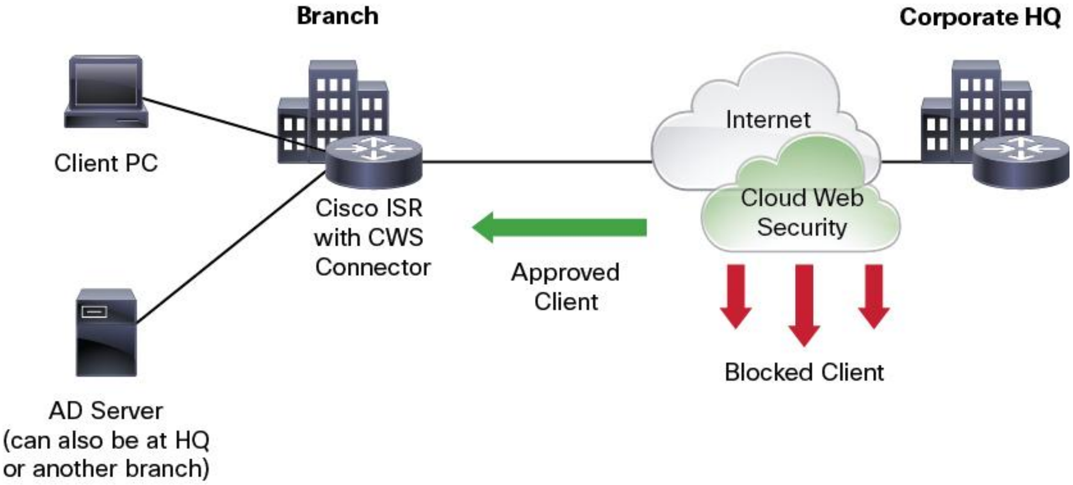
This guide provides a high-level overview of supported topologies with the Cisco ISR and the Cisco CWS Connector. (See Figures 1 through 4.) Several options are available for deploying Cisco CWS; this guide focuses specifically on the Cisco ISR with Cisco CWS Connector solution. Although not an exhaustive list, the topologies and integrated features in this guide represent the most commonly deployed and tested scenarios. Your network may include variations that are also compatible with the Cisco ISR and Cisco CWS Connector solution. Contact your Cisco sales representative for more information on specific deployment scenarios.

For additional information about Cisco ISR and the Cisco CWS solution, please visit the links below:

- Cisco ISR with CWS Connector
- Cisco Cloud Web Security
- Cisco ISR G2

Supported Cisco ISR Cloud Web Security Topologies

Figure 1. Topology 1: Branch over the Internet

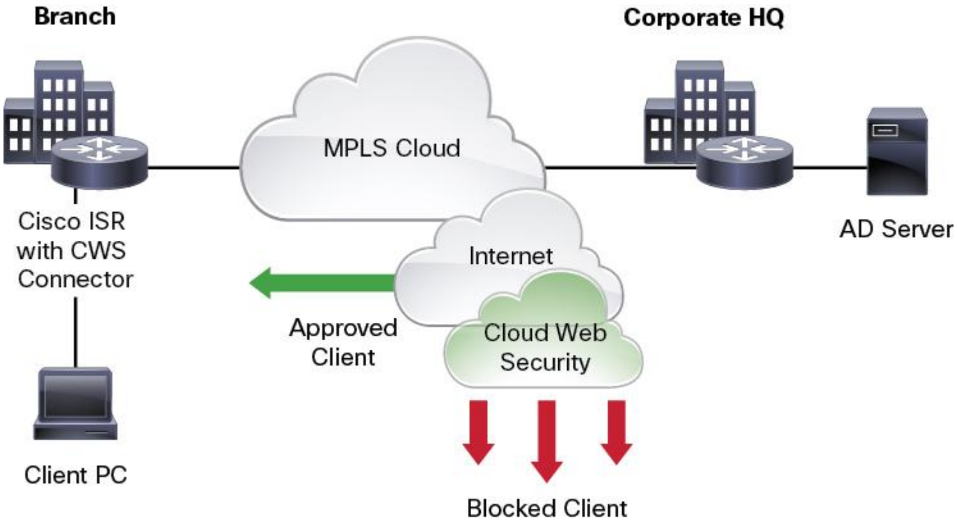


Primary highlights of topology 1 include the following:

- Split tunneling is made possible with direct Internet access from the branch.
- Cisco CWS is deployed at the branch ISR.
- Active Directory (AD) server is deployed at the branch *or* at the headquarters. The time for authentication may differ for different branches depending on where the AD server is located in relation to the client and the number of hops in between.
- After successful authentication, the Cisco CWS Connector on ISR requests the HTTP/HTTPS session and passes user information to the Cisco CWS Connector server.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Figure 2. Topology 2: Branch over Multiprotocol Label Switching

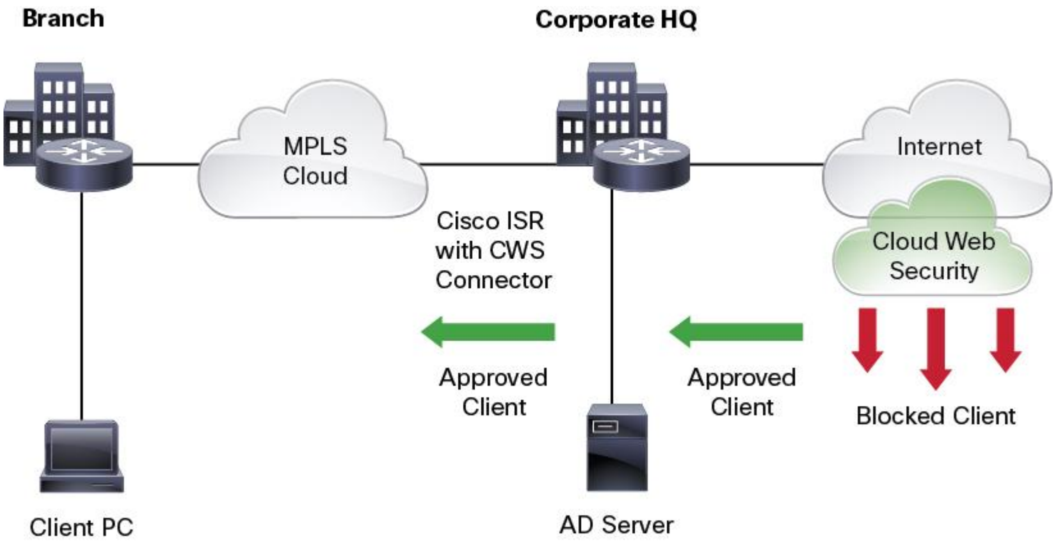


Primary highlights of topology 2 include the following:

- No direct Internet access is possible from the branch.
- Cisco CWS is deployed at each branch ISR.
- Internet access is typically from the MPLS cloud, but traffic must first travel to the MPLS cloud before reaching the Internet.
- AD is typically deployed at headquarters but can also be deployed at the branch. The time for authentication may differ for different branches depending on where the AD server is located in relation to the client and the number of hops in between.
- After successful authentication, Cisco CWS Connector on ISR requests the HTTP/HTTPS session and passes user information to the Cisco CWS Connector server.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Figure 3. Topology 3: AD and the Internet from Headquarters

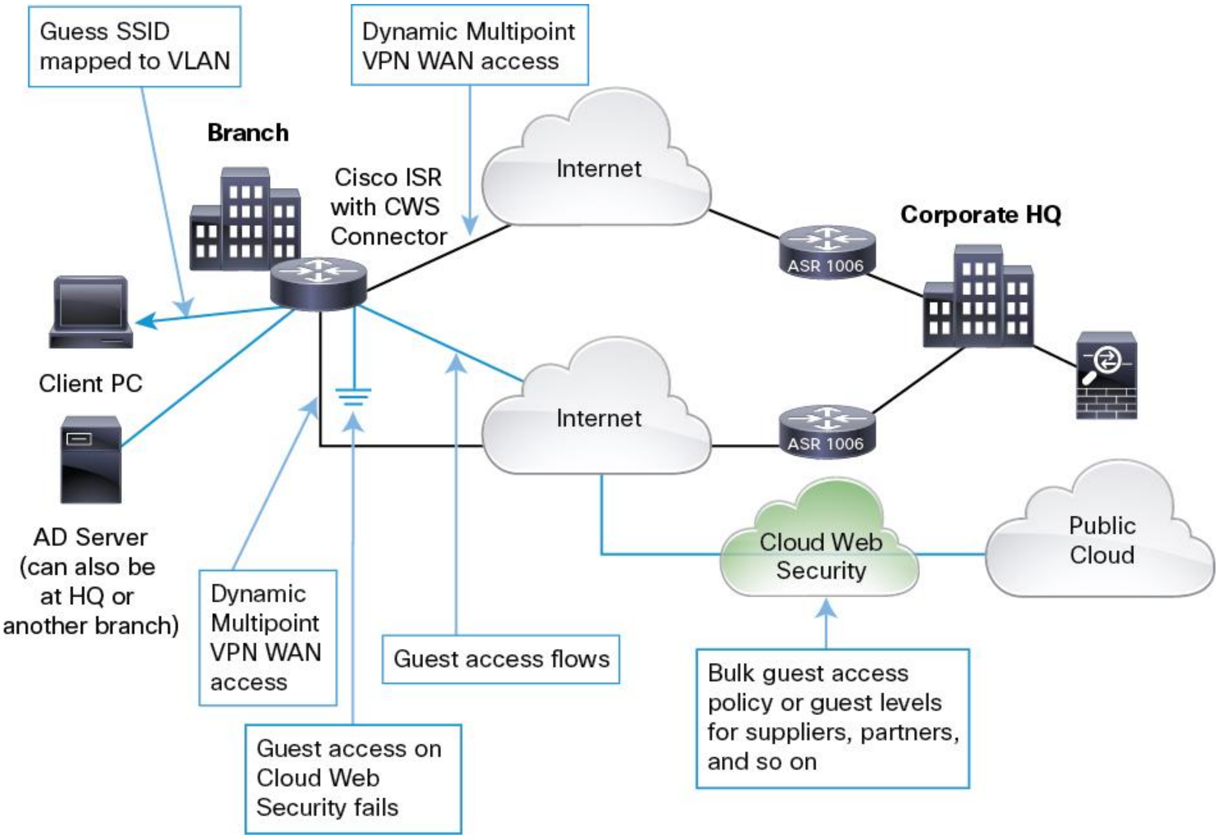


Primary highlights of topology 3 include the following:

- All traffic from the branch goes over the MPLS tunnel, terminating at the headend.
- There is no direct Internet access from the branch. Branch traffic must travel to headquarters before backhauling to the Internet.
- Cisco CWS is deployed at the headend ISR.
- AD is typically deployed at headquarters but can also be deployed at the branch. The time for authentication may differ for different branches depending on where the AD server is located in relation to the client and the number of hops in between.
- After successful authentication, Cisco CWS Connector on ISR requests the HTTP/HTTPS session and passes user information to the Cisco CWS Connector server.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Figure 4. Topology 4: Cisco Intelligent WAN AD at Headquarters with DMVPN, and Split Tunneling at the Branch


Guess SSID mapped to VLAN
Dynamic Multipoint VPN WAN access
Branch
Cisco ISR with CWS Connector
Internet
Corporate HQ
ASR 1006
Client PC
Internet
ASR 1006
AD Server (can also be at HQ or another branch)
Cloud Web Security
Public Cloud
Dynamic Multipoint VPN WAN access
Guest access flows
Bulk guest access policy or guest levels for suppliers, partners, and so on
Guest access on Cloud Web Security fails

Cisco Intelligent WAN (IWAN) helps businesses deliver an uncompromised experience over any connection. Now IT professionals can use less expensive WAN transport options for branch-office connections without affecting performance, security, or reliability. With Cisco IWAN, traffic is dynamically routed to deliver an excellent user experience regardless of application, endpoint, and network conditions. The savings realized from IWAN not only pays for the infrastructure upgrades but also frees resources for business innovation. With IWAN, your IT staff can simplify VPN connections across all sites to deliver high performance with high security using Dynamic Multipoint VPN (DMVPN). You can also provide direct Internet access with Cisco CWS for better software-as-a-service (SaaS) application performance while protecting branch-office endpoints and centralizing the management of your information security policy.

Primary highlights of topology 4 include:

- Branch-to-branch and branch-to-HQ traffic goes over the DMVPN tunnel.
- Direct Internet access from the branch with Cisco CWS is provided at the headend ISR.
- AD is typically deployed at headquarters but can also be deployed at the branch. The time for authentication may differ for different branches depending on where the AD server is located in relation to the client and the number of hops in between.
- After successful authentication, Cisco CWS Connector on ISR requests the HTTP/HTTPS session and passes user information to the Cisco CWS Connector server.

- Application visibility is provided through performance monitoring
- Dynamic application “best path” is based on policy. Load balancing optimizes bandwidth use. Network availability is improved.
- Certified strong encryption and comprehensive threat defense help protect your assets.

Integrated Features Supported with Cisco CWS Connector on ISR

The following features are supported by Cisco ISRs:

- Quality of service (QoS) with traffic shaping
- IP Security site-to-site VPN versions 1 and 2
- Easy VPN
- Dynamic Multipoint VPN (DMVPN)
- Cisco IOS® Performance Agent, IP SLA, Embedded Event Manager (EEM), and Measurement, Aggregation, and Correlation Engine (MACE)
- Cisco IOS Zone-Based Policy Firewall
- Cisco IOS Intrusion Prevention System (IPS) (supported only on ISR Generation 2)
- Object group access control lists (ACLs)
- Management integration with Cisco Security Manager and Cisco Prime™ Network Control System 1.2
- Windows NT LAN Manager (NTLM) active and passive, Web Authentication Proxy, or HTTP Basic authentication

This is not an exhaustive list of all supported and integrated features. Please contact your Cisco Sales representative for specific inquiries on integrated features.

The following point needs to be considered before deploying Cisco CWS Connector on the ISR G2:

- Web Cache Communication Protocol (WCCP) for Cisco Wide Area Application Services and WAAS Express: Internet-bound CWS traffic should not be subjected to WAAS.

Please refer to the Cisco ISR G2 with Cisco Cloud Web Security Solution Guide for additional details and workarounds.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Scaling

The scaling numbers for features described in this document pertain to the ISR G2 for Cisco CWS only. These numbers do not reflect the number of seats purchased for the Cisco CWS service or to the number of users or sessions that the Cisco CWS Connector server can handle. For more information on scaling for the Cisco CWS Connector server, please refer to Cisco's official Web Security page.

The scaling on the ISR G2 for Cisco CWS is determined by the number of sessions originating from the platform and sent to the Cisco CWS Connector server. Calculations were done to translate the number of sessions into the estimated number of supported users, factoring in appropriate CPU usage. For a detailed explanation of how these calculations were made, refer to the Scaling and Sizing Guide in the Appendix.

Table 1 shows the estimated number of users supported by various ISR G2 platforms for Cisco CWS. Note that these numbers are determined for the ISR G2 running the Cisco CWS Connector only (that is, no other features are enabled); the actual number of users may vary depending on other features deployed on the ISR G2.

Table 1. Number of Users Supported on the ISR G2, by Model Number

	3945E	3945	3925E	3925	2951	2911	2901	1941	1921	891
With authentication*	1200	1200	1,200	900	600	500	350	350	300	120
No authentication	5000	1200	5,000	900	600	500	350	350	300	120

*HTTP Basic authentication, Web Authentication Proxy, or NTLM authentication

User Experience

The ISR G2 acts as a transparent proxy, forwarding relevant Internet-bound traffic to the nearest Cisco CWS Connector server. Without authentication, end users should not notice anything out of the ordinary (that is, that their traffic is not going directly to the Internet) unless they try to access a page that issues a warning or is blocked per the Cisco CWS policy. With authentication, end user experience could vary.

The ISR G2 with Cisco CWS Connector currently supports three methods of authentication: HTTP Basic, Web Authentication Proxy, and NTLM. With HTTP Basic and Web Authentication Proxy, a user will see a dialogue prompt or webpage, respectively, asking for credentials. The user will see only this prompt once until the session expires on the route (the session timer is configurable by the administrator on the ISR G2). For NTLM authentication, the user experience with respect to credential prompts vary depending on the operating system and browser of the client (only Internet Explorer has domain integration with NTLM).

Tables 2 and 3 show whether the end user will see a dialogue pop-up or a credential prompt in various browsers, depending on operating system and authentication type. The tables also show the browser behavior based on whether the user is a corporate or guest user and what domain they are logging in to. For example, a corporate user logging in to the corporate domain may see different browser behavior than a corporate user logging in to a local machine (not on the corporate domain).

Definitions of terms used in Tables 2 and 3 are explained below.

Auth Type: Authentication type; either NTLM, HTTP Basic, Web Authentication Proxy (Web Auth), or no authentication

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Corporate User: A user, typically an employee, with complete access rights to the corporate intranet. This user's credentials are stored in the corporate active directory. Corporate users do not include vendors, consultants, or others who may have restricted access to the corporate intranet.

Domain: The corporate domain. Users must authenticate with the corporate active directory before accessing the domain.

Guest User: A user who is allowed into the company network for Internet browsing only. This user's credentials are not stored in the corporate active directory. This user may have limited access to the Internet and intranet. This category can include vendors, consultants, and others who may have limited access to the corporate intranet.

Nondomain: The public Internet, a separate guest network, or a local machine. The user does not authenticate with the corporate active directory in order to log on or gain access.

Transparent: The user does not see any credential prompts, and no user input is required.

Pop-up: Users see one pop-up asking them to enter their credentials. This pop-up will not appear again until a user's session has expired on the ISR G2. (The session timer can be set by the administrator.) Once a user enters correct credentials, the pop-up will disappear. User input is required.

User must log in: On the first webpage the users try to access, they will be presented with a login screen asking for their credentials. This webpage will not appear again until a user's session has expired on the ISR G2. (The session timer can be set by the administrator.) Once users enter their correct credentials, they will be able to access their original site. User input is required.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Table 2. Browser Behavior for Various Authentication Methods: One Network

		Windows OS				Mac and iOS		Other OS (Android, RIM, Linux, etc.)	
		Corporate User		**Guest User**		**Corporate User**	**Guest User**	**Corporate User**	**Guest User**
Auth Type	Browser	Domain	Nondomain	Domain	Nondomain	—			
NTLM	IE8	Transparent	Pop-up	Transparent	Pop-up				
	IE9	Transparent	Pop-up	Transparent	Pop-up				
	Firefox	Transparent	Pop-up	Transparent	Pop-up	Pop-up	Pop-up	Pop-up	Pop-up
	Chrome	Transparent	Pop-up	Transparent	Pop-up	Pop-up	Pop-up	Pop-up	Pop-up
	Safari	Pop-up							
	Other	Pop-up							
HTTP Basic	All browsers	Pop-up							
Web Auth	All browsers	User must log in							
No auth	All browsers	—							

Note: Guest users are not segregated on a separate VLAN or network from corporate users.

Table 2 shows the experience for guest users when both guests and corporate users are on the same network and cannot be distinguished by different IP ranges. Typically, however, companies separate the guest network from the corporate network so that the guest network has access only to the public Internet and no access to internal corporate resources. If the guest network is on a different subnet or VLAN from the corporate network, the guest user experience will be as shown in Table 3.

Table 3. User Experience for Various Authentication Methods: Segregated Networks

		Windows OS				Mac and iOS		Other OS (Android, RIM, Linux, etc.)	
		Corporate User		**Guest User**		**Corporate User**	**Guest User**	**Corporate User**	**Guest User**
Auth Type	Browser	Domain	Nondomain	Domain	Nondomain				
NTLM	IE8	Transparent	Pop-up	No Auth / No Pop-Up		—	—	—	—
	IE9								
	Firefox (1.0 and later)	Transparent with browser change	Pop-up			Pop-up	No Auth / No Pop-Up	Pop-up	No auth, no pop-up
	Chrome	Transparent	Pop-up			Pop-up		Pop-up	
	Safari	Pop-up	Pop-up			Pop-up		Pop-up	
	Other	Pop-up	Pop-up			Pop-up		Pop-up	
HTTP Basic	All browsers	Pop-up	Pop-up			Pop-up		Pop-up	
Web Auth	All browsers	User must log in	User must log in			User must log in		User must log in	
No auth	All browsers	—							

Note: Guest users are segregated from corporate users and use a separate VLAN or network.

Additional Design Considerations

Special design considerations and configurations may be required for using Cisco CWS in certain topologies and with specific Cisco IOS features.

Cisco CWS and Shared Assets

Since the ISR G2 router caches only the IP address of the user for authentication, the ISR and Cisco CWS Connector solution may not be appropriate for all types of shared-asset deployment models. Essentially, if another user logs in with the same IP address on the same device, the ISR G2 may not recognize the second user as a different user and will not prompt for authentication.

For example, let's assume User A logs in to a workstation, uses the Internet, and then does not log out (and authentication expiry timers have not run out yet). Now, when User B uses the same workstation, the ISR will treat User B as User A. (The ISR does not get any "log off" notifications from the AD servers.) Therefore, User B will be using the Internet with User A's policies and access privileges.

Although this is not entirely preventable, the occurrence of this situation can be reduced. Simply adjust the authentication absolute timer or inactivity timer, or both, so that authentication challenges will be sent more frequently to the AD.

Cisco CWS on LAN Interfaces

In some deployments, you may not want Cisco CWS on the WAN outbound interface (for example, you may want to apply Cisco CWS only to certain VLANs). In this case, deploy Cisco CWS ("content-scan out") only on the LAN interfaces where you want traffic to be filtered by the Cisco CWS Connector server. In general, remember that Cisco CWS cannot be deployed on any LAN physical interface, but only on virtual interfaces such as the Bridge Group Virtual Interface (BVI) or VLAN interface.

Cisco CWS with Dual WAN Interfaces

Deployments with dual WAN interfaces often use a primary-plus-backup model in which the backup interfaces will come up should the primary interface go down. Because Cisco CWS is configured on the WAN interface, if that interface goes down, Cisco CWS will also be disabled.

In order to prevent Cisco CWS from being disabled when an interface goes down in a dual-WAN scenario, deploy Cisco CWS ("content-scan out") on both interfaces. Then use a loopback interface instead of the physical interface in the parameter map for CWS. Additionally, make sure that this loopback interface has gone through Network Address Translation (NAT) and can be pinged.

Currently, certain active-active interfaces may not be supported. Contact your Cisco sales representative or write ss-isr-connector-sales@cisco.com for more information on your specific deployment.

Cisco CWS with ACL-Based Crypto Maps

In some site-to-site VPN deployments, ACL-based crypto maps are used on the interface with no tunnels, no Easy VPN Dynamic Virtual Tunnel Interface (DVTI), or the like. In this case, all traffic goes through the same WAN interface, including corporate intranet traffic. Normally, if Cisco CWS is deployed with this configuration, even corporate intranet traffic will be sent to the Cisco CWS Connector server for filtering.

To prevent corporate intranet traffic from being subject to Cisco CWS, a specific ACL should be created that includes all corporate networks. Apply this ACL to the Cisco CWS whitelist to bypass all internal corporate networks.

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Cisco CWS with GETVPN

Similar to the ACL-based crypto maps case, deployments using GETVPN will not have a tunnel interface, and all traffic (intranet and Internet) will go through the same physical interface.

To prevent corporate intranet traffic from being subject to Cisco CWS, a specific ACL should be created that includes all corporate networks. Apply this ACL to the Cisco CWS whitelist to bypass all internal corporate networks. Alternatively, use the GETVPN local ACL instead.

Cisco CWS with WAAS or WAAS Express

Additional configuration is required when Cisco CWS is used in conjunction with the Cisco Services-Ready Engine WAAS on the branch ISR G2 router or with a Wide Area Application Engine (WAE) appliance at the branch. When WAAS is configured, the optimization happens first in the flow before Cisco CWS headers are applied. Thus, traffic forwarded to the Cisco CWS Connector server would already be optimized.

To prevent optimizing Internet-bound traffic destined for the Cisco CWS Connector server, use a WCCP ACL list to explicitly deny Internet-bound traffic. This prevents Internet-bound traffic from being optimized, because only internal corporate traffic should be optimized by WAAS.

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)

Printed in USA

C07-732660-00 09/14

© 2014 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.