

Cloud Web Security Using Cisco ASA

Technology Design Guide

December 2013



Table of Contents

Preface	1
CVD Navigator	2 2 2 2
Introduction	3 3
Internal Users and Guests	3 4
Deployment Details 10 Configuring Cisco CWS Policies for Internal Users 10 Configuring Policy Exceptions for Apple Wireless Devices 12 Configuring Cisco ASA for Cisco Cloud Web Security 18 Configuring Cisco CWS Policies for Guest Users 29) 1 3 9
Appendix A: Product List	5
Appendix B: Changes	3
Appendix C: Configuration Files	7 7
Appendix D: Provisioning Email Example	9

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.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

class-map [highest class name]

Commands at a CLI or script prompt appear as follows:

Router# enable

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

police rate 10000 pps burst 10000 packets conform-action set-discard-classtransmit 48 exceed-action transmit

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

interface Vlan64

ip address 10.5.204.5 255.255.255.0

Comments and Questions

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

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

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

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

 Manage the Safe Use of Web-Based and Social Networking Applications for Internal Users and Guests—All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco Cloud Web Security (CWS) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security though a cloud-based service.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Cisco ASA 5500-X Series Adaptive Security Appliances
 provide Internet edge firewall security and intrusion prevention.
- Cisco Cloud Web Security provides granular control over all web content that is accessed.

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- CCNA Routing and Switching–1 to 3 years installing, configuring, and maintaining routed and switched networks
- CCNA Security–1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

Related CVD Guides Firewall and IPS Technology cisco. VALIDATED **Design Guide** Remote Access VPN cisco. ALIDATED DESIGN Technology Design Guide **Cloud Web Security** cisco. Using Cisco AnyConnect ALIDATED **Technology Design Guide**

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd/wan

Introduction

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 employees 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. As the monetary gain for malicious activities on the Internet has grown and developed, the methods used to affect these malicious and or illegal activities has grown and become more sophisticated. *Botnets*, one of the greatest threats that exists in the Internet today, are malicious Internet servers (mostly web) being used to host content that then attacks innocent user's browsers as they view the content. These types of attacks have been used very successfully by *bot herders* (originators of the attack) in order to gather millions of infected members that are subject to the whims of the people who now control their machines. 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. Examples of these attacks are the Internet worms that gathered so much attention in the early to mid-2000s. These types of risks are depicted in the figure below.





Technology Use Cases

Cisco Cloud Web Security (CWS) 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.

Browsing websites can be risky, and many websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or lax security configurations. The websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the Internet in search of additional web servers that they can infect in order to continue propagating. This dynamic environment introduces significant challenges to maintain up-to-date Internet threat profiles.

Use Case: Manage the Safe Use of Web-Based and Social Networking Applications for Internal Users and Guests

All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco CWS complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security though a cloud-based service.

3

This design guide 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, 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.

Design Overview

The Cisco Validated Design (CVD) Internet edge design provides the basic framework for the enhancements and additions that are discussed in this guide. A prerequisite for using this design guide is that you must have already followed the guidance in the Firewall and IPS Technology Design Guide.

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.

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. This integration uses the Cloud Web Security Cloud Connector for Cisco ASA and requires no additional hardware.

Cloud Connectors are software components embedded in, hosted on, or integrated with platforms in order to enable or enhance a cloud service. The native integration of the CWS Cloud Connector for Cisco ASA provides users with transparent access to a cloud service and is classified as an embedded cloud connector application.





Mobile remote users connect to their organization's network by using devices that generally fall into two categories: laptops and mobile devices such as smartphones and tablets. Because the devices operate and are used differently, the capabilities currently available for each group differ. Laptops and other devices that support the Cisco AnyConnect Secure Mobility Client with Cisco CWS are not required to send web traffic to the primary site. This solution is covered in detail in the Cloud Web Security Using Cisco AnyConnect Technology Design Guide. If you have an existing CWS deployment for remote-access users, the procedures are similar.

Cisco CWS using Cisco ASA also protects mobile users who are using a non-CWS-enabled Cisco AnyConnect Secure Mobility Client that connects through remote-access VPN, as detailed in both the Remote Access VPN Technology Design Guide and the Remote Mobile Access Technology Design Guide.

Cisco CWS is a cloud-based method of implementing web security that is similar in function to the Cisco Web Security Appliance (WSA), which uses an on-premise appliance for web security. This guide is focused on the deployment of Cisco CWS on Cisco ASA. For more information about using Cisco WSA, see the Web Security Using Cisco WSA Technology Design Guide.

5

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

Table $T = CISCO Web Security Solution Comparison$	Table 1	-	Cisco	Web	Security	solution	comparisor
--	---------	---	-------	-----	----------	----------	------------

	Cisco CWS	Cisco WSA
Web/URL filtering	Yes	Yes
Supported protocols	HTTP and HTTPS	HTTP and 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-premises redirect
Policy and reporting	Web portal (cloud)	On premises

Many organizations provide guest access by using wireless LAN and enforce an acceptable use policy and provide additional security for guest users by using Cisco CWS. This guide includes a section on how to deploy CWS for wireless guest users without requiring any configuration changes to Cisco ASA.

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 by using a cloud connector. This method is considered a transparent proxy, and no configuration changes are required to web browsers on user devices.

6

Figure 3 - Cisco Cloud Web Security detailed traffic flow



The easiest way to apply the service policy is to modify the existing global service policy to add Cisco CWS inspection. The global policy applies to traffic received on any interface, so the same service policy applies to the following:

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

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



Figure 4 - Cisco Cloud Web Security with internal and guest users





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 DMZ networks. The creation of these exemptions is shown in the "Deployment Details" chapter of this guide.

8

The Cisco CWS cloud is accessed through a network of proxy servers, which have a broad geographic distribution in order to support a globally diverse set of customers. Cisco ASA is configured with a primary and secondary proxy server in order to provide high availability. Specific details for which proxy servers to use are provided by Cisco and based on the location and size of the deployment.

Cisco CWS is administered by using the CWS ScanCenter web portal. This includes creating filters and rules for policies, creating groups, activating keys, and viewing reports. All required CWS administration tasks are covered in this guide.

9

Deployment Details

The first part of this chapter describes how to configure the components in order to enable Cisco CWS service for internal users who access the Internet through the Internet-edge Cisco ASA, including users at the primary site and remote sites. Additionally, if internal users are using remote-access VPN from mobile devices, they are also protected with Cisco CWS. The second part of this chapter describes how to configure CWS for guest users, who may require a different policy than internal users.



Procedure 1 Enable Cisco CWS security configuration

This guide assumes you have purchased a Cisco CWS license and created an administrative CWS account that allows a user to log in and manage the account.

Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to Admin > Management > Groups.

Tech Tip
Policy can differ based on group assignment. The simplest method for assigning group membership is to generate a unique key for a group and use that key during deployment to group members. If more granular policies are required, other methods for group assignment include IP address range or mapping to an Active Directory group.
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
CISCO Cloud Web Security logged into: Cisco Validated Design Group Helo Guides Loggut
Home Dashboard Web Virus Spyware Web Filtering Email Admin Reports

Your Account Auther	ntication (Managen	Home Dashboard	Web Virus Spyware	Web Filtering Email on (Downloads (Admin Reports
Manage Groups	Manage Groups				
	Search:	Search Nothing fi Add Custom Group	ound to display	<u>Reload list</u> 🐓	

Step 3: Click Add Custom Group.

Step 4: In the Add New Custom Group pane, enter the group name (Example: CWS IE-ASA5545X), and then click **Save**.

A group-specific authentication license key is generated for use in the Cisco ASA VPN configuration.

Step 5: Navigate to Admin > Authentication > Group Keys.

Step 6: For the group created in Step 4, click **Create Key**. ScanCenter generates a key that it sends to an email address of your choosing.

cisco	Cisco Cloud Web Secu	urity	logged into: Cisco Vali	dated Design Group	Hel	p <u>Guides</u> <u>Loqout</u>
Your Account	Authentication Authentication	Home Dashboard agement 4 Audit	Web Virus Sp HTTPS In	yware Web Filtering spection	Email Admin	Reports
Group Autho	Create, activate and deactivate To add or delete a group, go to the "G Search:	a group authentication key groups" link in the "Management" m	nenu or <u>click here</u>		Reload list	
	Group Name	Key Ref	State	Action	Sel.	
	CWS IE-ASA5545X	(E) No key	(1) No key	Create Key		
	1	One	e item found. ted Revoke Selected Se	lect All Deselect All		

Step 7: Store a copy of this key by copying and pasting it into a secure file, because the key cannot be rebuilt and can only be replaced with a new key. After it is displayed the first time (on generation) and sent in email, you can no longer view it in ScanCenter. After this key is generated, the page options change to Deactivate or Revoke.

Step 8: Navigate to Web Filtering > Management > Filters.



Step 9: Click Create Filter.

Step 10: Assign a name to the filter (Example: Filter Blocked Sites), select the categories blocked by your organization's policy (Examples: Pornography and Hate Speech), and then click **Save**. Access to these categories is completely restricted.

Step 11: Click Create Filter.

Step 12: Assign a name to the filter (Example: Filter Warned Sites), select the categories that are considered inappropriate by your organization's policy (Example: Gambling), and then click **Save**. Access to these categories is permitted, but only after accepting a warning message.

Cisco Cisco Cic	oud Web Security	logged into: Cisco Validated Design (iroup		Help Guides Logout
Management • Notific	ations (Dashboard Web Virus Spyware W	eb Filtering	Email	Admin Reports
Web Filtering > Management > Filte	r <u>s</u> > Manage Filters	rs 🔛 Edit Filter 🗮 Create Filter			
	List of Filters				
	Filter Name	Created on	Edit	Delete	
	Filter Blocked Sites	01 May 13 17:15 UTC	D/	畲	
	Filter Warned Sites	01 May 13 17:16 UTC	E/	1 1 1	
	default	15 Feb 11 10:18 UTC	E/		

Step 13: Navigate to Web Filtering > Management > Policy.

Step 14: Select the Rule name Default, change the rule action to Allow, and then click Save.

Step 15: Click Create Rule.

Step 16: Assign a name to the rule (Example: Block_Blocked_Sites), and then select Active.

Step 17: In the Rule Action list, choose Block.

Step 18: In the Define Group pane, click Add group.

Step 19: On the dialog box, in the Search box, enter the name of the group created in Step 4, and then click Go.

1 Groups of 5	Search IE-ASA5545X	Go	¢
# A B C D E F G	H I J K L M N O F	P Q R S T U V W X Y Z	
CWS IE-ASA5545X		Select	

Step 20: Click Select, and then click Confirm Selection.

Step 21: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 10 (Example: Filter Blocked Sites), and then click **Add**.

Step 22: Click Create rule. The policy rule has now been created.

Cisco Cloud	d Web Security	logged into: Cisco Validated Design Group	,	Не	elp <u>Guides</u> <u>Loqout</u>
	Home	Dashboard Web Virus Spyware Web F	iltering Email	Admir	Reports
Management	ens (<u> </u>	710111	i inceptires
Web Filtering > Management > Policy > (Create Rule				
inconnecting (indiagement (indiagement)	(-				
	Manage P	olicy III Edit Rule III Create Rule			
Name	Block_Blocked_Sites			Active 🔽	
Description	Apply Rule Action "Block" to filter "F	ilter Blocked Sites" for group "CWS IE-ASA5545X"			
Rule Action 🗢	Block 💌				
C Define Group (("WHO")				
Search for a grou	up by clicking on "Add Group". To set a g	roup as an exception to the rule, select the corresponding	Set as Exception" box	(action of	
If no group is sele	ected, this rule will apply to anyone. Ad	ding multiple groups has the action of "OR", so users will nee	d to be in any of the g	roups listed	
for the rule to tak	ke effect. If a user is a member of both	a regular group and an exception group the rule will not be r	matched.		
Group		5	Set as Exception	Delete	
CWS IE-ASA554	45X				
Hod Group (2)					
Define Filters (("WHAT")				
Choose a Hiter fr	rom the list and click "Add". To set a Hiti	er as an exception to the rule, select the corresponding "Set	as Exception ⁻ box (ac	tion of NOT).	
Add Filter Filt	ter Blocked Sites Add CP				
Filter	taa	2	et as Exception	Delete	
Title blocked sit	tes			ш	
Define Schedu	le ("WHEN")	Schadula as an avcention to the rule, relact the correspond	ing "Cat as Everation"	hav (action	
of NOT).	ile indiri die list and dick. Add 1 to set a	Schedule as an exception to the rule, select the correspond	ing Secas Exception	box (acuon	
Adding multiple so	chedule is not recommended unless one	is going to be "Set as Exception" (action of "AND NOT")			
Add Schedule	e Choose a schedule from the list 💌	Add⊕			
Schedule		5	Set as Exception	Delete	
anytime				Ξ	
Reset			1	Create Rule	

Next, create a new rule.

Step 23: Click Create Rule.

Step 24: Assign a name to the rule (Example: Warn_Warned_Sites), and then select Active.

- Step 25: In the Rule Action list, choose Warn.
- Step 26: In the Define Group pane, click Add group.

Step 27: On the dialog box, in the search box, enter the name of the group created in Step 4, and then click Go.

Step 28: Click Select, and then click Confirm Selection.

Step 29: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 12 (Example: Filter Warned Sites), and then click **Add**. Click **Create rule**. The policy rule has now been created.Because all rules are evaluated on a first-hit rule, the following is the correct order for the rules in this example:

- 1. Block Blocked Sites (which blocks access to restricted categories)
- 2. Warn Warned Sites (which allows access to sites but with a warning)
- 3. Default (which permits all other sites)

CI	sco	2	Cisco Cloud V	Neb Security	logged into: C	Sisco Validated Design Group			Help	Guides Log
				Home	Dashboard Web Virus	Spyware Web F	iltering Er	nail	Admin	Repor
Man	agen	nent	Notifications	•						
eb Fil	terino	1 > 1	lanagement > Policy > Man	age Policy						
				E Marrier Dal	ten (III retabula) (III our	to Dula				
				= Manage Po		ste Kule				
ules	highe	r in t	he list will take priority over	the lower ones. Use the arrows to ch	nange the priority of each rule b	y moving them up or down i	n the list.			
ules	highe	r in t	he list will take priority over	the lower ones. Use the arrows to ch	hange the priority of each rule b	by moving them up or down i	n the list.	in the same w	w as the re	et of the rul
ules lease nd a	highe note	r in t thai nizat	he list will take priority over t anonymization rules are tre ion will always take preceder	the lower ones. Use the arrows to ch eated separately from the main policy nce.	nange the priority of each rule b r. Hence these appear in a sepa	by moving them up or down i arate part of the table. Thes	n the list. e can be ordered	in the same wa	ay as the re	st of the rul
ules lease nd ar	highe note nonyr	r in t tha nizat	he list will take priority over t anonymization rules are tre ion will always take preceder	the lower ones. Use the arrows to ch eated separately from the main policy nce.	nange the priority of each rule b r. Hence these appear in a sepa	ay moving them up or down i arate part of the table. Thes	n the list. e can be ordered	in the same wa	ay as the re	st of the rule
ules lease nd ar	highe note nonyn e is a	r in t tha nizat ma	he list will take priority over t anonymization rules are tre ion will always take preceder ximum of 100 enabled r	the lower ones. Use the arrows to ch eated separately from the main policy nce. ules allowed for the policy.	nange the priority of each rule b r. Hence these appear in a sepa	y moving them up or down i arate part of the table. Thes	n the list. e can be ordered	in the same wa	ay as the re	st of the rul
ules lease nd ar her Com	highe note nonyn e is a pany i	r in t thai nizat ma Polic	the list will take priority over t anonymization rules are tre ion will always take preceder ximum of 100 enabled r	the lower ones. Use the arrows to ch eated separately from the main policy nce. ules allowed for the policy.	nange the priority of each rule b	by moving them up or down i arate part of the table. Thes	n the list. e can be ordered	in the same wa	ay as the re	st of the rul
lease nd ar her Com	highe note nonyn e is a pany i Mo	r in t thai nizat ma Polic	he list will take priority over t anonymization rules are tre ion wil always take preceder ximum of 100 enabled r Rules	the lower ones. Use the arrows to ch eated separately from the main policy nce. ules allowed for the policy. Groups/Users/IPs	nange the priority of each rule b , Hence these appear in a sepa Filter	by moving them up or down i arate part of the table. Thes © Schedule	n the list. e can be ordered Action	in the same wa	ay as the re	st of the rul
lease nd ai her Com #	highe note nonyn e is a pany i Mo	r in t thai nizat ma Polic ove	he list will take priority over t anonymization rules are tra ion will always take preceden ximum of 100 enabled r Rules Block Blocked Sites	the lower ones. Use the arrows to ch aated separately from the main policy nce. ules allowed for the policy. Groups/Users/IPs "CWS IE-ASA5545X"	Ange the priority of each rule b . Hence these appear in a sepa Filter Filter Telter Blocked Sites"	oy moving them up or down is rrate part of the table. Thes © Schedule "anytime"	an the list. e can be ordered Action Block	in the same wa	ey as the re	est of the rul Delete
tules Iease Ind ar There Com #	highe note nonyn e is a pany i Mo	r in t thai nizat ma Polic ove	he list will take priority over t anonymization rules are tre ion will always take preceder ximum of 100 enabled r Rules Block Blocked Sites Warn Warned Sites	the lower ones. Use the arrows to ch eated separately from the main policy nce. ules allowed for the policy. Groups/Users/IPs "CWS IE-ASA5545x" "CWS IE-ASA5545x"	nange the priority of each rule b Hence these appear in a sepa Filter Filter Blocked Sites" Filter Warned Sites"	or moving them up or down is arrate part of the table. Thes	Action	in the same wa	Edit	st of the ruk Delete 습 습



Procedure 1 Create exceptions to bypass Captive Network Assistant

When an Apple iDevice (such as an iPad, iPod, or iPhone) or an Apple Mac OS X machine connects to a wireless network, it sends an HTTP request to one of a variety of destinations to help determine if a captive portal is blocking access to the Internet.

If the success page is returned, the device assumes it has network connectivity and no action is taken.

If the success page is not returned, an Apple feature called the Captive Network Assistant (CNA) assumes there is a captive portal present. CNA then launches a browser to prompt the user with the login page from the captive portal. The CNA browser is limited in function and is used only to authenticate with a captive portal.

December 2013

Table 2 - Known sites used to trigger Apple Captive Network Assistant

Website	CWS category
.apple.com	Computers and Internet
.apple.com.edgekey.net	Computers and Internet
.akamaiedge.net	currently unclassified
.akamaitechnologies.com	SaaS and B2B
www.airport.us	Computers and Internet
www.appleiphonecell.com	Mobile Phones
www.ibook.info	Science and Technology
www.itools.info	Computers and Internet
www.thinkdifferent.us	Business and Industry

If you have implemented a CWS block or Warn policy that blocks access to the known sites listed in the previous table, then the CNA may be invoked.

Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to Web Filtering > Management > Filters.

Step 3: Click Create Filter.

Step 4: Assign a name to the filter (Example: Filter Domain Whitelist), and then in the Inbound Filters pane, click **Domains**.

Step 5: In the domain pane, enter the full list of websites listed in Table 2, and then click Save all Settings.



	logged into: Cisco Validated Design Group
	Home Dashboard Web Virus Spyware Web Filtering Email Admin Re
Management 🔹	Notifications (
eb Filtering > Management	t> <u>Filters</u> > Edit Filter
	III Manage Filters IIIY Edit Filter III Create Filter
	Filter Name: Filter Domain Whitelist
	Enter the Domains / Natworks / TDs to be included in the filter
Inbound Filters	anle.com
Categories	apple.com.edgekey.net
Domains	.akamaiedge.net .akamaitechnologies.com
Content Types	www.airport.us www.angleinbonecell.com
File Types	www.ibook.info
	www.tkinkdifferent.us
♥!♥ Bi-directional Filter	/5
Applications	Domains can be entered as an explicit URL or as domain names (without the "/" suffix). You must omit the "http://". You may specify sub-domains and
Exceptions	paths.
User Agents	
	Sort Alphabetically
	- Networks/IPs
	Networks/IPs can be entered as a specific network address or a single IP address(without the "/" suffix, the default netmask would be 32).

When you save the list, the ScanCenter portal automatically alphabetizes it.

Step 6: Navigate to Web Filtering > Management > Policy.

Step 7: Click Create Rule.

Step 8: Assign a name to the rule (Example: Permit_Domain_Whitelist), and then select Active.

Step 9: In the Rule Action list, choose Allow.

Step 10: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 3 (Example: Filter Domain Whitelist), and then click **Add**.

Step 11: Click Create rule. The policy rule has now been created.

Cisco Cloud	Web Security	logged into: Cisco Validated E	Design Group	Hel	p <u>Guides</u> <u>Loqout</u>
	Home	Dashboard Web Virus Spyware	Web Filtering Emai	Admin	Reports
Management	ns ()				
Web Filtering > Management > Policy > 0	Create Rule				
	III Manage	e Policy 🛛 🙀 Edit Rule			
Name	Permit_Domain_Whitelist			Active 🗸	
Description	Apply Rule Action "Permit" to filt	er "Filter Domain Whitelist" for any group			
Rule Action 🎧	Allow				
Define Group ("	'WHO")				
Search for a group NOT).	p by clicking on "Add Group". To set	t a group as an exception to the rule, select the cor	responding "Set as Exception" b	ox (action of	
If no group is sele listed for the rule t	ected, this rule will apply to anyone. to take effect. If a user is a membe	Adding multiple groups has the action of "OR", so r of both a regular group and an exception group th	users will need to be in any of the rule will not be matched.	ne groups	
Group			Set as Exception	Delete	
No Group Selecte	Add Group+			the second secon	
Define Filters ("	'WHAT")				
Choose a Filter fro NOT).	om the list and click "Add". To set a	Filter as an exception to the rule, select the corresp	ponding "Set as Exception" box (action of	
Add Filter Filte	er Domain Whitelist 💌 Add 🕄				
Filter			Set as Exception	Delete	
Filter Domain Wh	nitelist			畲	
⊂ Define Schedule	e ("WHEN")				
Choose a Schedule of NOT). Adding multiple sc	e from the list and click "Add". To s	et a Schedule as an exception to the rule, select the one is going to be "Set as Exception" (action of "Al	e corresponding "Set as Exceptio ND NOT")	n" box (action	
Add Schedule	Choose a schedule from the list 💌	Add 🕀			
Schedule			Set as Exception	Delete	
anytime				童	
Reset				Create Rule	

Because all rules are evaluated on a first-hit rule, the Permit Domain Whitelist rule must be listed first.

Step 12: Click the Up arrow next to the Permit_Domain_Whitelist rule until it is listed first.

CI	sco	Cisco Cloud We	eb Security	logged into: Cisco	Validated Design Group			Help	Guides Log
			Home	ashboard Web Virus	Spyware Web Filter	ing Emai	A	dmin	Report
Man	agemen	Notifications	•			_			
/eb Fi	iltering >	Management > Policy > Manag	e Policy						
			Manage Policy	Edit Rule	ule				
None	n noto the	t anonymization rules are treate	d concretely from the main policy. I	Jongo theory panagr in a congrate	nort of the table. There a	in he ordered in	the entry we	w as the r	act of the
Pleas rules, Ther Com	e note tha and anor e is a ma	t anonymization rules are treate nymization will always take prece ximum of 100 enabled rules	d separately from the main policy. H idence. allowed for the policy.	ience these appear in a separate	part of the table. These ca	in be ordered in	the same wa	iy as the r	est of the
Please rules, Ther Com #	e note tha and anor e is a ma pany Polic Move	t anonymization rules are treate nymization will always take prece ximum of 100 enabled rules Rules	d separately from the main policy. H idence. allowed for the policy. Groups/Users/IPs	ience these appear in a separate	© Schedule	Action	the same wa	y as the n	est of the Delete
Pleas rules, Then Com #	e note tha and anor e is a ma pany Polic Move	t anonymization rules are treate iymization will always take prece ximum of 100 enabled rules Rules Permit Domain Whitelist	d separately from the main policy. E dence. allowed for the policy. Groups/Users/IPs Anyone	Filter	© Schedule "anytime"	Action	the same wa	etit	est of the Delete 급
Pleas rules, Then # 1 2	e note tha and anor e is a ma pany Polic Move	t anonymization rules are treate ymization will always take prece ximum of 100 enabled rules Rules Permit. Domain Whitelist Block. Blocked Sites	d separately from the main policy. H dence. allowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASA5545X"	Filter "Filter Domain Whitelist" "Filter Blocked Sites"	© Schedule "anytime"	Action Action Allow Block	Active	Edit	est of the Delete 급
Please rules, Then # 1 2 3	e note tha and anor e is a ma pany Polic Move	t anonymization rules are treate ymization vill always take prece ximum of 100 enabled rules Rules Parmit. Domain Whitelist Block Blocked Sites Warn Warned Sites	d separately from the main policy. H dence. allowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASA5545X" "CWS IE-ASA5545X"	Filter Fi	© Schedule "anytime" "anytime"	Action Action Allow Block Warn	Active	Edit	est of the Delete 습 급

Step 13: Click Apply Changes.



Procedure 1 Configure Cisco CWS servers

Cisco ASA is configured with a primary and backup server. You will receive a provisioning email after purchasing your Cisco CWS license. This email includes the primary and backup server address that you use for configuring Cisco ASA. An example email is included in "Appendix D" in this guide.

Table 3 - Example of Cisco CWS primary and secondary proxy servers from a provisioning email

Primary web services proxy address	proxyXXXX.scansafe.net	
Web services proxy port	8080	
Secondary web services proxy address	proxyXXXX.scansafe.net	
Web services proxy port	8080	

Tech Tip

Domain Name Service (DNS) is required to resolve the Fully Qualified Domain Name (FQDN) of a Cisco CWS web services proxy server.

Step 1: From a client on the internal network, navigate to the Internet-edge firewall's inside IP address, and then launch Cisco ASA Security Device Manager. (Example: https://10.4.24.30)

Step 2: If the firewall is not configured to use DNS resolution, navigate to Configuration > Device Management > DNS > DNS Client, and then configure it as follows:

- Primary DNS Server-10.4.48.10
- Domain Name-cisco.local

Step 3: In the DNS Lookup pane, scroll to view the **Interface** list, click in the **DNS Enabled** column for the interface that is used to reach the DNS server (Example: inside), choose **True**, and then click **Apply**.

Configuration > Device	Management > DNS > DNS Client	
Specify how to resolve DNS	i requests.	
DNS Setup		
Configure one DNS ser	ver group 💿 Configure multiple DNS server groups	
Primary DNS Server:	10.4.48.10	
Secondary Servers:		
Domain Name:	cisco.local	
DNS Lookup	NS lookup on at least one interface.	
Interface	DNS Enabled	
dmz-auests	false	
dmz-management	false	
dmz-tmg	false	
dmz-web	false	
dmz-wlc	false	=
inside	true	
outside-16	false	
outside-17	false	T
DNS Guard This function enforces one Enable DNS Guard on a	DNS response per query. If DNS inspection is configured, Il interfaces.	this option is ignored on that interface.
		Apply Reset

Step 4: In **Configuration > Device Management > Cloud Web Security**, configure the following values from Table 3, and then click **Apply**.

- Primary Server IP Address/Domain Name-[FQDN of primary web services proxy from provisioning email]
- Backup Server IP Address/Domain Name–[FQDN of secondary web services proxy from provisioning email]
- · License Key-[Group key from Step 6 of Procedure 1, "Enable Cisco CWS security configuration"]

Configuration > Device Mar	nagement > Cloud Web Security				
Configure Cloud Web Security servers and license parameters					
Launch <u>Cloud Web Security Por</u>	tal to configure Web content scanning, filtering, malware protection services and retrieving reports.				
Primary Server					
IP Address/Domain Name:	tower1764 scansafe net				
HTTP Ports					
HTTP Port:	0000				
Backup Server					
IP Address/Domain Name:	tower1482.scansafe.net				
HTTP Port:	8080				
Other					
Retry Counter:	5				
License Key:	•••••••••••••••••••••••••••				
Confirm License Key:	••••••				
	Apply Reset				

Step 5: In **Monitoring > Properties > Cloud Web Security**, verify the Cisco CWS server status. Your primary server should show a status of REACHABLE.

loud W	eb Security Status and Statistics			
Server !	Status:			
Server	IP Address/FQDN	Status	Active	
Primary	tower1764.scansafe.net(72.37.248.27)	REACHABLE	Active	
Backup	tower1482.scansafe.net	69.174.58.187	Standby	
Server	Connection Statistics:	Value		
Server (Connection Statistics:	Value		
Server (Server (Current	Connection Statistics: Connection HTTP sessions	Value 0		
Server Server Current Current	Connection Statistics: Connection HTTP sessions HTTPS sessions	Value 0 0		
Server (Server (Current Current Total HT	Connection Statistics: Connection HTTP sessions HTTPS sessions TP Sessions	Value 0 0 32717		
Server (Server (Current Current Total HT Total HT	Connection Statistics: Connection HTTP sessions HTTPS sessions TP Sessions TPS Sessions	Value 0 0 32717 0		
Server (Current Current Total HT Total HT Total Fa	Connection Statistics: Connection HTTP sessions HTTPS sessions TP Sessions TPS Sessions II HTTP sessions	Value 0 0 32717 0 0		
Server Current Current Total HT Total HT Total Fa Total Fa	Connection Statistics: Connection HTTP sessions HTTPS sessions TP Sessions TPS Sessions II HTTP sessions II HTTPS sessions	Value 0 0 32717 0 0 0 0		
Server (Current Current Total HT Total HT Total Fa Total Fa Total By	Connection Statistics: Connection HTTP sessions HTTP5 sessions TP Sessions TP5 Sessions II HTTP sessions II HTTP5 sessions II HTTP5 sessions II HTTP5 sessions	Value 0 0 32717 0 0 0 0 9157153720		
Server (Current Current Total HT Total HT Total Fa Total Fa Total By Total By	Connection Statistics: Connection HTTP sessions HTTP5 sessions TP Sessions IP5 Sessions II HTTP sessions II HTTP5 sessions II HTTP5 sessions tes In tes Out	Value 0 0 32717 0 0 0 9157153720 13998272		
Server (Current Current Total HT Total HT Total Fa Total Fa Total By Total By HTTP se	Connection Statistics: Connection HTTP sessions HTTP5 sessions TP Sessions I PS Sessions I HTTP sessions I HTTP5 sessions Ites In tes Out ssion Connect Latency in ms(min/max/avg)	Value 0 0 32717 0 0 0 9157153720 13998272 53/261/56		

Procedure 2 Co

Configure Cisco ASA firewall objects

In this procedure, you create the network objects listed in the following table.

Table 4 - Firewall network objects

Network object name	IP address	Netmask	
internal-network	10.4.0.0/15	255.254.0.0	
dmz-networks	192.168.16.0/21	255.255.248.0	

Step 1: Navigate to Configuration > Firewall > Objects > Network Objects/Groups.

Step 2: Click Add > Network Object.

Step 3: On the Add Network Object dialog box, in the **Name** box, enter the Network object name from Table 4. (Example: internal-network)

Step 4: In the Type list, choose Network.

Step 5: In the IP Address box, enter the IP address of the object from Table 4. (Example: 10.4.0.0)

Step 6: In the **Netmask** box, enter the netmask of the object from Table 4, and then click **OK**. (Example: 255.254.0.0)

🔂 Add Networ	rk Object
Name:	internal-network
Type:	Network 👻
IP Version:	IPv4
IP Address:	10.4.0.0
Netmask:	255.254.0.0 👻
Description:	internal network range
NAT	8
	OK Cancel Help

Step 7: Repeat Step 2 through Step 6 for all objects listed in Table 4. If the object already exists, then skip to the next object listed in the table.

Step 8: After adding all of the objects listed in Table 4, in the Network Objects/Groups pane, click Apply.

Procedure 3	Configure	Cisco ASA	service	policy	,
	Connigure			policy	1

The existing global service policy is modified to enable Cisco CWS. The global service policy applies to all interfaces on the firewall, so this procedure enables CWS on all interfaces.

Step 1: In Configuration > Firewall > Service Policy Rules, select Add > Add Service Policy Rule.

Step 2: Skip the Add Service Policy Rule Wizard - Service Policy dialog box by clicking Next.

Step 3: On the Add Service Policy Rule Wizard – Traffic Classification Criteria dialog box, in the Create a new traffic class box, enter **cws-http-class**, for Traffic Match Criteria, select Source and Destination IP Address, and then click Next.

📴 Add Service Policy Rule Wi:	zard - Traffic Classification Criteria
Oreate a new traffic class:	cws-http-class
Description (optional):	Class to match HTTP traffic for Cloud Web Security
Traffic Match Criteria	
Derault Inspection Tra	
Tuppel Group	n IP Address (uses ACL)
TCP or UDP Destinatio	n Port
RIP Range	
IP DiffServ CodePoint:	s (DSCP)
IP Precedence	
Any traffic	
Add rule to existing traffic d	ass: global-class 👻
Rule can be added to an exi	sting class map if that class map uses access control list (ACL) as its traffic match criterion.
Use class-default as the traf	if in class
If traffic does not match a e	vistion traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation
a danc door not match a o	
	Sack Next Cancel Help

Next, create the single global policy for Cisco CWS in order to match traffic on all interfaces. Because this policy may be used by internal users and remote-access VPN users, certain source and destination traffic pairs are exempted from the CWS policy by using **Do not match** as the action, as shown in the following table. The final policy rule matches all other source and destination pairs.

Action	Source object	Destination object	Service	Description
Do not match	any4	internal-network	ip	Do not match any to internal networks
Do not match	any4	dmz-networks	ір	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

The Add Service Policy Rule Wizard allows only a simple policy containing a single match entry, so the following steps are used to configure only the first entry in Table 5. You configure the remaining entries in Table 5 after you complete the first pass of the wizard.

Step 4: On the Add Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in the first row of Table 5. (Example: Do not match)

Step 5: In the Source box, enter the source object listed in the first row of Table 5. (Example: any4)

Step 6: In the **Destination** box, enter the destination object listed in the first row of Table 5. (Example: internal-network)

iource Criteria -		
iource:	any4	
lser:		
iecurity Group:		
estination Crite	eria	
estination:	internal-network -	
iecurity Group:		
iervice:	ip 💮	
escription:	Do not match any to internal networks	
More Options	s	۲

Step 7: In the Service box, enter the service listed in the first row of Table 5. (Example: ip), and then click Next.

Step 8: On the Add Service Policy Rule Wizard – Rule Actions dialog box, click the **Protocol Inspection** tab, select **Cloud Web Security**, and then click **Configure**.

Step 9: On the Select Cloud Web Security Inspect Map dialog box, click Add.

Step 10: On the Add Cloud Web Security Inspect Map dialog box, enter a name (Example: CWS-HTTP-80). On the Parameters tab, in the **Default User** box, enter a username that will be used by default (Example: cvd-default).

Step 11: Select HTTP, and then click OK.

Step 12: On the Select Cloud Web Security Inspect Map dialog box, select the inspect map you created in Step 10, for Cloud Web Security Traffic Action, select **Fail Open**, and then click **OK**.

Tech Tip

ĺ

A *fail open* or *fail closed* condition, in a security context, refers to the default behavior when a service is unavailable. If *fail open* is configured and the Cisco CWS service is unavailable, the firewall allows user web traffic to pass without restriction. Conversely, if *fail closed* is configured and the Cisco CWS service is unavailable, the firewall blocks user web traffic.

CTIQBE			
🔽 Cloud Web Security	Configure	Cloud Web Security Inspect Map: CW5-HTTP-80, fail open	
DCERPC	Configure		
DNS DNS	Configure		
ESMTP	Configure		
FTP	Configure		
C GTP	Configure		
E H.323 H.225	Configure		
H.323 RA5	Configure		
HTTP	Configure		
ICMP			
ICMP Error			
ILS I			
IM	Configure		
IP-Options	Configure		
IPSec-Pass-Thru	Configure		
IPv6	Configure		
MMP	Configure		
- ucco			

Step 13: On the Add Service Policy Rule Wizard - Rule Actions dialog box, click Finish.

Because the Add Service Policy Rule Wizard allowed only a simple policy containing a single match entry, use the following steps in order to configure the remaining entries from Table 5, which are replicated in Table 6.

 Table 6 - Example policy for Cisco Cloud Web Security (remaining entries from Table 5)

Action	Source object	Destination object Service Dest		Description
Do not match	any4	dmz-networks	ір	Do not match any to DMZ networks
Match	any4	any4	tcp/http	Match HTTP to any other networks

Step 14: In **Configuration > Firewall > Service Policy Rules**, select the highest numbered rule for the Cisco CWS policy (Example: cws-http-class). Right-click to Copy, and then right-click to Paste After.

Configuration >	Configuration > Firewall > Service Policy Rules										
🗢 Add - 🕼 Edit 👔 Delete 🛧 🌾 👗 🗞 🔊 - Q. Find 📴 Diagram 🥂 Packet Trace											
Traffic Classificat	on									Dula Antina	Description
Name	#	Enabled	Match	Source	Src Securi	Destination	Dst Security Group	Service	Time	Rule Actions	Description
Global; Policy:	global_	policy									
inspection_d			a Match	🏈 any		🧼 any		Q default-inspec		Q Inspect DNS Map preset Q Inspect ESMTP (14 more inspect actions)	
global-class	1	V	Match	🌍 any4		any4		📧 ip		😂 ips inline, close traffic	
cws-http-class	1	V	ab Do not match	🧇 any4		🏟 any4		💵 ip		Q Inspect Cloud Web Secur	Do not match any to internal networks

Step 15: Skip the Paste Service Policy Rule Wizard - Service Policy dialog box by clicking Next.

Step 16: On the Paste Service Policy Rule Wizard – Traffic Classification Criteria dialog box, select **Add rule to existing traffic class**, and then from list of classes, choose the class created in Step 3 (Example: cws-http-class). Click **Next**.

📴 Paste Service Policy Rule W	izard - Traffic Classification Criteria	×
Create a new traffic class:	global-class1	
Description (optional): Traffic Match Criteria	ffic n IP Address (uses ACL)	
TCP or UDP Destinatio RTP Range IP DiffServ CodePoints IP Precedence	n Port ; (DSCP)	
Any traffic Add rule to existing traffic cl Rule can be added to an exis	ass: cws-http-class 🔹 sting class map if that class map uses access control list (ACL) as its traffic match criterion.	
Use class-default as the traf If traffic does not match a e	fic class. kisting traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.	
	< <u>Back</u> <u>Next</u> > <u>Cancel</u>	Help

Step 17: On the Paste Service Policy Rule Wizard – Traffic Match – Source and Destination Address dialog box, for **Action**, select the action listed in Table 6. (Example: Do not match)

Step 18: In the Source box, enter the source object listed in Table 6. (Example: any4)

Step 19: In the Destination box, enter the destination object listed in Table 6. (Example: dmz-networks)

anna Callanda					
ource Criteria -					
ource:	any4				
iser:			····		
ecurity Group:					
estination Crite	ria				
estination:	dmz-networks				
ecurity Group:					
ervice:	ip				
	Do not match any to DMZ netw	orks			
escription:					
More Options	5				*

Step 20: In the Service box, enter the service listed in Table 6 (Example: ip), and then click Next.

Step 21: On the Paste Service Policy Rule Wizard – Rule Actions dialog box, click Finish.

Step 22: Repeat Step 14 through Step 21 for all of the entries in Table 6.

Step 23: Verify that your service policy rules match the following figure, and then click Apply.

cws-http-class	1	1	a Do not match	🍅 any4	🏟 any4	📧 ip	🔍 Inspect Cloud Web Security .	Do not match any to internal networks
	2	1	Do not match	🏟 any4	🌍 any4	📧 ip		Do not match any to DMZ networks
	3	1	🐚 Match	🏟 any4	any4	🚥 http		Match HTTP to any other networks

Procedure 4 Test Cisco Cloud Web Security

Step 1: From a client machine on the internal network, open a web browser to the following website: http://whoami.scansafe.net This website returns diagnostic information from the Cisco CWS service.

← ⊕ Ø http://whoami.scansafe.net/	P - ⊠¢	🥖 🖉 whoami.scansafe.net	×	6 🛧 🔅
<pre>www.example.com/seconds/s</pre>	0 2 ÷ Q	Se whoami.scansafe.net	x	

If the service is not active, the following information is returned.

C S http://whoami.scansafe.net/	P-⊠¢×	🥔 scansafe.net	×	☆ 🕸
User is not currently using the service				*
oser is not currently using the service				
				*



Configuring Cisco CWS Policies for Guest Users

- 1. Enable Cisco CWS security configuration
- 2. Test Cisco Cloud Web Security

This is an optional process that is only required if you want to apply a different Cisco CWS policy for guest users. Otherwise, the same policy created for internal users is applied.



Procedure 1 Enable Cisco CWS security configuration

Step 1: Access the Cisco CWS ScanCenter Portal at the following location, and then log in with administrator rights:

https://scancenter.scansafe.com

Step 2: Navigate to Admin > Management > Groups.

Cisco Cloud Web Se	BCUrity logged into: Cisco V	'alidated Design Group	Help Guides Logout
Your Account Authentication I	Home Dashboard Web Virus Management 4 Audit 4 HTTPS	Spyware Web Filtering Email Inspection I Downloads I	Admin Reports
Manage Groups			
Manage Group: Search:	Search	Reload list 🚱	
Group Name CWS IE-ASA5545	×	Delete	
1	One item found.		
	Delete Selected	_	
	Add Custom Group Add Directory Grou	up.	

Step 3: Click Add Custom Group.

Step 4: On the Add New Custom Group pane, enter the group name (Example: CWS Wireless Guest), and then click **Save**.

Step 5: On the Admin > Management > Groups page, click the link for the group created in Step 4.

Step 6: In the IP Expressions pane, add the IP subnet range that corresponds to the wireless guest DMZ configuration in the Campus Wireless LAN Technology Design Guide, click **Save**, and then click **Done**.

Cisco Cloud Web Security	Cisco Validated Design Group	Help Guides Logout
Home Dashboard Web Viru	s Spyware Web Filtering Email	Admin Reports
Your Account 4 Authentication 4 Management 4 Audit 4	TIPS Inspection Downloads	
Edit Custom Group		
Please enter the new Custom Group name: Custom Groups can be any alphanumeric combination up to 256 characte [CWS Wireless Guest Please add / edit your user group IP expressions and click Save'. [192.168.28.0/22	rs. Save	
Users The syntax for adding users from active directory is as follows : WinNT://[domain-name]\User-name] (Please note that 'WinNT' is case as	insitive.)	

Step 7: Navigate to Web Filtering > Management > Filters.

The filtering policy in this guide is an example only. The actual policy implemented should align with the organization's security policy and business requirements. This example uses a whitelist policy and uses filters that initially select all categories for blocking or warning. Only specifically selected categories are exempt.

If you make the whitelist too limited, web browsing to many common websites may be restricted.

If your policy uses both a block list and a warn list as suggested in this example, all permitted categories must be contained in both lists.

Step 8: Click Create Filter.

i

Tech Tip

Step 9: Assign a name to the filter (Example: Filter Warned Sites – Guest), click **Select All**, clear the categories that are considered appropriate by your organization's policy that do not require a warning (Example: News, Shopping, Entertainment and Social Networking), and then click **Save**. Access to all other categories is permitted, but only after accepting a warning message.

Step 10: Click Create Filter.

Step 11: Assign a name to the filter (Example: Filter Blocked Sites – Guest), click **Select All**, clear all of the categories that were selected in Step 9. Then clear additional categories that require a warning according to your organization's policy (Examples: Tobacco), and then click **Save**. Access to all other categories is completely restricted.

Cisco Cloud Web Securi	Help Guides Logout								
Home Dashboard Web Virus Spyware Web Filtering Admin Reports Web Filtering > Management > Elters > Manage Filters Management > Elters > Manage Filters Management > Elters > Manage Filters									
List of Filters	Manage Filters	Create Filter							
Filter	lame	Created on Ec	lit Delete						
Filter Blocked Sites	01 May 13 1	7:15 UTC	/ [†]						
Filter Blocked Sites - Guest	07 May 13 2	1:47 UTC	Û						
Filter Warned Sites	01 May 13 1	7:16 UTC	¢ 🛱						
Filter Warned Sites - Guest	07 May 13 2	1:46 UTC	1						
default	15 Feb 11 1	:18 UTC	1						

Step 12: Navigate to Web Filtering > Management > Policy.

Step 13: Click Create Rule.

Step 14: Assign a name to the rule (Example: Block_Blocked_Sites_Guest), and then select Active.

Step 15: In the Rule Action list, choose Block.

Step 16: In the Define Group pane, click Add group.

Step 17: On the dialog box, in the Search box, enter the name of the group created in Step 4, and then click Go.

1 Groups of 6	Search Guest	Go	×
# A B C D E F G	H I J K L M	N 0 P Q R 5 T U	V W X Y Z
CWS Wireless Guest			Select

Step 18: Click Select, and then click Confirm Selection.

Step 19: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 8 (Example: Filter Blocked Sites – Guest), and then click **Add**.

Step 20: Click Create rule. The policy rule has now been created.

Cisco Cloud	d Web Security	logged into: Cisco Validated Design G	roup	Help	Guides Logout
	Home	Dashboard Web Virus Spyware W	eb Filtering Email	Admin	Reports
Management 🔹 Notificatio	ons (
Web Filtering > Management > Policy >	Create Rule				
	Manage F	Policy 📑 Edit Rule 🔤 Create Rule			
Name	Block_Blocked_Sites_Guest			Active 🔽	
Description	Apply Rule Action "Block" to filter "F	Filter Blocked Sites - Guest" for group "CWS Wireless Gue	st"		
Rule Action 🗢	Block 💌				
Define Group I Search for a grou NOT). If no group is sel for the rule to ta	("WHO") up by clicking on "Add Group". To set a c lected, this rule will apply to anyone. Ad ke effect. If a user is a member of both	group as an exception to the rule, select the correspond ding multiple groups has the action of "OR", so users will a regular group and an exception group the rule will not	ing "Set as Exception" box need to be in any of the g be matched.	(action of roups listed	
Group			Set as Exception	Delete	
CWS Wireless G	Guest			â	
Add Group 🕂					
Define Filters Choose a Filter fi Add Filter Fi	("WHAT") rom the list and click "Add". To set a Filt	er as an exception to the rule, select the corresponding	"Set as Exception" box (ac	tion of NOT).	
Filter			Set as Exception	Delete	
Filter Blocked Si	ites - Guest			窗	
Define Schedu Choose a Schedu of NOT). Adding multiple s Add Schedul Schedule	Ile ("WHEN") Je from the list and click "Add". To set a ichedule is not recommended unless one le Choose a schedule from the list 💌	Schedule as an exception to the rule, select the corresp is going to be "Set as Exception" (action of "AND NOT") Add:	oonding "Set as Exception" Set as Exception	box (action	
anytime					
Reset			1	Create Rule	

Next, create a new rule.

Step 21: Click Create Rule.

Step 22: Assign a name to the rule (Example: Warn_Warned_Sites_Guest), and then select Active.

Step 23: In the Rule Action list, choose Warn.

Step 24: In the Define Group pane, click Add group.

Step 25: On the dialog box, in the search box, enter the name of the group created in Step 4, and then click Go.

Step 26: Click Select, and then click Confirm Selection.

Step 27: In the Define Filters pane, click the down arrow labeled **Choose a filter from the list**, select the filter created in Step 9 (Example: Filter Warned Sites – Guest), and then click **Add**.

Step 28: Click Create rule. The policy rule has now been created.

CIS	sco	Cisco Cloud We	b Security	logged into: Cisco Valid	dated Design Group			Help G	uides Logo
			Home	ashboard Web Virus Spy	ware Web Filterin	g Email	Ad	min	Report
Mana	igemen	t Notifications	•						
/eb Filt	tering >	Management > Policy > Manage	Policy						
Rules h	higher in	the list will take priority over the	lower ones. Use the arrows to cha	nge the priority of each rule by movir	ig them up or down in the	e list.			
Rules I Please rules, a There Comp	note that and anor is a matany Polic	the list will take priority over the at anonymization rules are treated nymization will always take precect aximum of 100 enabled rules a y	lower ones. Use the arrows to cha I separately from the main policy. H dence. allowed for the policy.	nge the priority of each rule by movir Hence these appear in a separate par	ng them up or down in the	e list. be ordered in t	he same way	r as the re	est of the
Rules P Please rules, a There Comp	note tha and anor is a ma any Polic Move	t the list will take priority over the at anonymization rules are treated nymization will always take precec uximum of 100 enabled rules a y Rules	lower ones. Use the arrows to cha a separately from the main policy. H dence. allowed for the policy. Groups/Users/IPs	nge the priority of each rule by movin Hence these appear in a separate part	ng them up or down in the tof the table. These can be seen to the table of table of the table of	e list. be ordered in t Action	he same way	e as the re	est of the Delete
Rules P Please rules, a There Comp # 1	note that and anor is a mat any Polic Move	the list will take priority over the at anonymization rules are treated nymization will always take precess aximum of 100 enabled rules a y Rules Permit. Domain. Whitelist	lower ones. Use the arrows to cha i separately from the main policy. H dence. allowed for the policy. Groups/Users/IPs Anyone	nge the priority of each rule by movir ience these appear in a separate part Filter "Filter Domain Whitelist"	ing them up or down in the t of the table. These can	e list. be ordered in t Action	Active	Edit	est of the Delete
Rules P Please rules, a There Comp # 1 2	note that and anor is a material any Polic Move	the list will take priority over the at anonymization rules are treated mymization will always take prece- boximum of 100 enabled rules a Rules Permit Domain Whitelist Block Blocked Sites	lower ones. Use the arrows to cha I separately from the main policy. H ence. allowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASA5545X"	nge the priority of each rule by movin ience these appear in a separate part Filter "Filter Domain Whitelist" "Filter Domain Whitelist"	© Schedule "anytime" "anytime"	Action Action Allow Block	Active	Edit	Delete
Rules Please rules, a There Comp # 1 2 3	higher in note that and anor is a mat any Polic Move	the list will take priority over the at anonymization rules are treated mymization will always take preces aximum of 100 enabled rules a Rules Permit Domain Whitelist Block Blocked Sites Warn Warned Sites	lower ones. Use the arrows to cha i separately from the main policy. Hence. Illowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASASS45X" "CWS IE-ASAS545X"	nge the priority of each rule by movin tence these appear in a separate part "Filter Omain Whitelst" "Filter States" "Filter States"	ing them up or down in the t of the table. These can l or schedule "anytime" "anytime" "anytime"	Action Action Allow Block Warn	Active	Edit	Delete
Rules Please rules, a There Comp # 1 2 3 4	higher in note that and ano is a material is a material is a material is a material is a material is a material is a material Move	the list will take priority over the at anonymization will rules are treated myrnization will avery state prece- tor of 100 enabled rules a Rules Permit Domain. Whitelist Block Blocked Sites Warn Warned Sites Block Blocked Sites Guest Block Blocked Sites Guest	lower ones. Use the arrows to cha 4 separately from the main policy. H ercc. allowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASAS545X" "CWS IE-ASAS545X" "CWS Wireless Guest"	Filter Blocked Sites - Guest"	ig them up or down in the t of the table. These can in "anytime" "anytime" "anytime" "anytime"	Action Action Allow Block Warn Block Block	Active	Edit Edit E E E	Delete
Rules F Please rules, a There Comp # 1 2 3 4 5	higher in note that and anor is a material any Polic Move 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	the list will take priority over the at anonymization will always take prece- minimum of 100 enabled rules a Rules Permit. Domain. Whitelist Block. Blocked Sites Warn. Warned Sites Block Blocked Sites Guest Warn Warned Sites Guest	lower ones. Use the arrows to cha i separately from the main policy. I elerce. allowed for the policy. Groups/Users/IPs Anyone "CWS IE-ASA5545X" "CWS Wireless Guest" "CWS Wireless Guest"	Filter Varies Gless - Guest" "Filter Varies Gless - Guest" "Filter Slocked Sites" "Filter Slocked Sites" "Filter Warned Sites - Guest" "Filter Slocked Sites - Guest" "Filter Stars - Guest"	ing them up or down in the t of the table. These can in "anytime" "anytime" "anytime" "anytime" "anytime" "anytime"	Action Action Allow Block Warn Block Warn	Active	Edit Edit E E E E E E E E	est of the Delete

Because the guest user traffic and internal user traffic is all redirected from the same Cisco ASA, the same group key is used. In order to properly match the guest traffic by the source IP address, the guest rules must be evaluated before the internal user rules.

Step 29: Click the Up arrow next to the Block_Blocked_Sites_Guest rule until it is listed second (after the Permit Domain Whitelist).

Step 30: Click the Up arrow next to the Warn_Warned_Sites_Guest rule until it is listed third, and then click **Apply Changes**.

CI	sco	01300 01000 1101	b Security	logged into: Cisco Valio	lated Design Group			Help G	uides Log
			Home D	ashboard Web Virus Spy	ware Web Filtering	g Email	Ad	min	Report
Management									
eb Fi	ltering >	Management > Policy > Manage	Policy						
			Manage Policy	/ Edit Rule 📑 Create Rule					
lease ules,	e note th and and	at anonymization rules are treated nymization will always take preced	separately from the main policy. Hence,	Hence these appear in a separate par	of the table. These can l	be ordered in t	he same way	as the re	st of the
lease ules, here	e note th and and e is a m	at anonymization rules are treated mymization will always take preced aximum of 100 enabled rules a	separately from the main policy. H lence. Illowed for the policy.	Hence these appear in a separate par	of the table. These can l	be ordered in t	he same way	as the re	st of the
ease les, here iom; #	e note th and and e is a ma pany Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a sy Rules	separately from the main policy. Hence. Illowed for the policy. Groups/Users/IPs	Hence these appear in a separate part	© Schedule	be ordered in the ord	he same way	e as the re	st of the Delete
ease les, here Comp	a note th and ano is a m pany Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a www.common.common.common.common.common.common.common.common.common.common.common.common.common.common.common.com Rules Permit. Domain. Whitelist	separately from the main policy. Hence.	Hence these appear in a separate part Filter	© Schedule	Action	Active	Edit	st of the Delete
ease iles, here 20mp #	e note th and and is a ma cany Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a Rules Permit. Domain Whitelist Block Blocked Sites Guest	separately from the main policy. Hence. Illowed for the policy. Groups/Users/IPs Anyone "CWS Wireless Guest"	Hence these appear in a separate part Filter "Filter Domain Whitelist" "Filter Blocked Sites - Guest"	© Schedule "anytime"	Action Allow Block	Active	Edit	St of the Delete
ease iles, here 20mp #	a note th and ano a is a ma cany Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a Permit. Domain Whitelist Block Blocked Sites Guest Warn Warned Sites Guest	separately from the main policy. I ence. Illowed for the policy. Groups/Users/IPs Anyone "CWS Wireless Guest" "CWS Wireless Guest"	Filter Filter "Filter Domain Whitelist" "Filter Blocked Sites - Guest"	© Schedule "anytime" "anytime"	Action Ac	Active	Edit	st of the Delete
lease iles, here #	a note th and ano a is a ma bany Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a Rules Remit. Domain Whitelist Block Blocked Sites Guest Warn Warned Sites Guest Block Blocked Sites	separately from the main policy. I ence. Illowed for the policy. Groups/Users/IPs Anyone "CWS Wireless Guest" "CWS Wireless Guest" "CWS Wireless Guest"	Filter Filter Filter Filter Filter Filter Blocked Sites - Guest" Filter Varned Sites - Guest"	© Schedule anytime" anytime" anytime" anytime"	Action Action Allow Block Warn Block	Active	Edit Edit E E E	st of the Delete 量 量
lease ules, There # L 2 3 4	a note thand and and and and and any Polic Move	at anonymization rules are treated nymization will always take preced aximum of 100 enabled rules a Print Domain Whitelist Block Blocked Sites Guest Warn Warned Sites Block Blocked Sites	separately from the main policy. I ence. Illowed for the policy. Groups/Users/IPs Anyone "CWS Wireless Guest" "CWS Ureless Guest" "CWS UF-ASA5545X" "CWS IE-ASA5545X"	Filter "Filter Domain Whitelist" "Filter Domain Whitelist" "Filter Blocked Sites - Guest" "Filter Warned Sites - Guest" "Filter Warned Sites"	© Schedule "anytime" "anytime" "anytime" "anytime" "anytime"	Action Action Allow Block Warn Block Warn Warn	Active	Edit Edit EV EV EV	st of the Delete

Procedure 2 Test Cisco Cloud Web Security

Step 1: From a client machine on the guest network, open a web browser to the following website: http://whoami.scansafe.net This website returns diagnostic information from the Cisco CWS service.

Attp://whoami.scansafe.net/	Q - ⊠ ¢	🥔 whoami.scansafe.net	×	6 🛠 🛱
<pre>with the provide an and a second second</pre>		whoami.scansafe.net	×	<u>n x u</u>

If the service is not active, the following information is returned.

C Set the private service C Set Set X C Set Set X C Set Set X C Set		
Liser is not currently using the service	← ② Ø http://whoami.scansafe.net P ~ 🗟 C × Ø scansafe.net	6 🛧 🕸
	User is not currently using the service	*
	Osci is not currently using the service	
		-

r

Appendix A: Product List

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1)
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	IPS 7.1(7) E4
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Web Security

Functional Area	Product Description	Part Numbers	Software
Cloud Web Security	Cisco Cloud Web Security (ScanSafe)	Cisco Cloud Web Security	_
	Cisco Cloud Web Security (ScanSafe)	Please Contact your Cisco Cloud Web Security Sales Representative for Part Numbers:scansafe-sales-questions@ cisco.com	

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco CVD series.

- We made changes to improve the readability and technical accuracy of this guide.
- We added a new process to create exceptions to bypass the Captive Network Assistant for Apple wireless devices.

Appendix C: Configuration Files

IE-ASA5545X

The Cisco ASA commands below represent the configuration added to the Cisco ASA appliance, hostname IE-ASA5545X, as configured in the Firewall and IPS Technology Design Guide. The additional configuration below enables the functionality described in this guide.

```
dns domain-lookup inside
dns server-group DefaultDNS
name-server 10.4.48.10
domain-name cisco.local
L
object network internal-network
 subnet 10.4.0.0 255.254.0.0
description The organization's internal network range
object network dmz-networks
 subnet 192.168.16.0 255.255.248.0
description The organization's DMZ network range
!
access-list global mpc 1 remark Do not match any to internal network
access-list global mpc 1 extended deny ip any4 object internal-network
access-list global mpc 1 remark Do not match any to DMZ networks
access-list global mpc 1 extended deny ip any4 object dmz-networks
access-list global mpc 1 remark Match HTTP to any other networks
access-list global mpc 1 extended permit tcp any4 any4 eq www
1
scansafe general-options
server primary ip 72.37.248.27 port 8080
server backup ip 69.174.58.187 port 8080
retry-count 5
license 6B2F23DCD7704A3947F02CBA6A17BCF2
L
class-map cws-http-class
description Class to match HTTP traffic for Cloud Web Security
match access-list global mpc 1
!
policy-map type inspect scansafe CWS-HTTP-80
description Cloud Web Security TCP-80
parameters
 default user cvd-default
 http
```

```
policy-map global_policy
  class cws-http-class
    inspect scansafe CWS-HTTP-80 fail-open
!
service-policy global_policy global
```

Appendix D: Provisioning Email Example

From: ScanSafe Provisioning [mailto:provisioning@scansafe.net] Subject: Provisioning Notification: Customer X / PO Ref:XXXXXXX

On Day-Month-Year we completed the provisioning of the ScanSafe Web Security services for Customer X in accordance with the order details below:

Services:	Subscription Seats and Services
Term:	Subscription Months
Registered IP Addresses:	-None configured yet-
Domains:	-None configured yet-

The service is now available and you should make the necessary configuration changes described below to use the service. Please configure your system so that external Web traffic is sent via ScanSafe, using the explicit proxy setting below:

Primary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080
Secondary Web Services Proxy Address:	proxyXXXX.scansafe.net
Web Services Proxy port:	8080

The exact configuration changes required will vary depending in your specific existing infrastructure.

To log in to the service configuration Web portal and administer the service, please visit https://scancenter. scansafe.com/portal/admin/login.jsp and enter your email and password details below:

Email:	contact@CustomerX.com
Password :	-Not Shown-
Company ID:	XXXXXXXXXX

As part of our ongoing commitment to quality and service, a member of the ScanSafe Customer Services team will be in touch with you to ensure that the service is functioning according to your expectations.

If you require any assistance or experience any problems with the service, please do not hesitate to contact our support team.

We appreciate your choosing ScanSafe to provide Web security and look forward to a successful working partnership with you.

Customer Services EMEA +44 (0) 207 034 9400

US + (1) 877 472 2680

support@scansafe.com

This email and any attachments are strictly confidential and intended for the addressee(s) only. If this email has been sent to you in error, please let us know by forwarding it to us at support@scansafe.com.

Neither ScanSafe nor its directors, officers or employees accepts any liability for the accuracy or completeness of this email. Unless expressly stated to the contrary, no contracts may be concluded on behalf of ScanSafe by means of e-mail communication.

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.

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

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

© 2013 Cisco Systems, Inc. All rights reserved.

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)