cisco.



Web Security Using Cisco WSA TECHNOLOGY DESIGN GUIDE

August 2013



Table of Contents

Preface	.1
CVD Navigator	.2
Use Cases	2
Scope	2
Proficiency	2
Introduction	.3
Technology Use Case	3
Use Case: Manage the Safe Use of Web-based and Social Networking	
Applications with an On-premise Security Appliance	3
Design Overview	4
Deployment Details	.7
Configuring Cisco WSA	8
High Availability and Resilience	27
Additional Information	38
Monitoring	38
Troubleshooting	38
Summary	38
Appendix A: Product List	39

Preface

Cisco Validated Designs (CVDs) provide the framework 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

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 with an On-premise Security Appliance–All web traffic from the primary-site and remote-site networks accesses the Internet through a centralized Cisco Adaptive Security Appliance (ASA) firewall. Cisco Web Security Appliance (WSA) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security using a dedicated on-premises appliance.

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 for Internet edge firewall security
- Cisco Web Security Appliance for granular control over all web content that is accessed
- · Integration of the above with the LAN switching infrastructure

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** Cloud Web Security Using cisco. Cisco ASA Technology ALIDATED **Design Guide** Remote Mobile Access cisco. VALIDATED **Technology Design Guide**

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

Introduction

Technology Use Case

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 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, is that of 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" to gather in 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.





Use Case: Manage the Safe Use of Web-based and Social Networking Applications with an On-premise Security Appliance

All web traffic from the primary site and remote-site networks accesses the Internet through a centralized Cisco ASA firewall. Cisco Web Security Appliance (WSA) complements the deep packet inspection and stateful filtering capabilities of the firewall by providing additional web security using a dedicated on-premises appliance.

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 Cisco WSA service. No configuration changes are required on user devices.
- Web filtering—Cisco WSA supports filters based on predefined content categories, as well as custom categories. The filtering rules can be configured to block, monitor or warn based on the specific web usage policies of an organization.
- Malware protection—Cisco WSA analyzes every web request to determine if content is malicious. Cisco Cloud Web Security (CWS) updates its malware protection policies by using the Cisco Security Intelligence Operations (SIO), which is designed to help organizations secure business applications and processes through identification, prevention, and remediation of threats.
- **Differentiated policies**—Policies for Cisco WSA are applied on a per-group basis. Group membership is determined by identity, which can include authenticated user information or the source IP address of the web request.

Design Overview

Cisco Web Security Appliance (WSA) addresses the need for a corporate web security policy by offering a combination of web usage controls with category and reputation-based control, malware filtering, and data protection.





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.

The Cisco WSA family is a web proxy that works with other Cisco network components such as firewalls, routers, or switches in order to monitor and control web content requests from within the organization. It also scrubs the return traffic for malicious content.

Figure 3 - Logical traffic flow using Cisco WSA



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

Cisco WSA uses several mechanisms to apply web security and content control. Cisco WSA begins with basic URL-filtering with predefined, category-based web usage controls. These controls are based on an active database that includes analysis of sites in 190 countries and over 50 languages. Content is filtered by the reputation database. The Cisco Security Intelligence Operations updates the reputation database every five minutes. These updates contain threat information gleaned from multiple Internet-based resources, as well as content reputation information obtained from customers with Cisco security appliances that choose to participate in the Cisco SenderBase network. If no details of the website or its content are known, Cisco WSA applies dynamic content analysis to determine the nature of the content in real time, and findings are fed back to the SenderBase repository if the customer has elected to participate.

Cisco WSA uses an on-premise appliance for web security that is similar in function to Cisco Cloud Web Security (CWS), which is a cloud-based method of implementing web security. This guide is focused on the deployment of Cisco WSA.

5

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

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

Table 1 - Cisco Web Security solution comparison

Cisco WSA inspects the content for remote-access VPN connected users in both the integrated and standalone deployment models as described in the Remote Access VPN Design Guide.





6

Deployment Details

The first step to planning the Cisco WSA deployment is to determine how to redirect web traffic to the appliance. There are two possible methods to accomplish the redirection of traffic to Cisco WSA: transparent proxy mode and explicit proxy mode.

In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design, and the Cisco ASA firewall is used to redirect traffic to the appliance because all of the outbound web traffic passes through the device and is generally managed by the same operations staff who manage Cisco WSA.

In an explicit proxy deployment, a client application, such as a web browser, is configured to use an HTTP proxy, such as Cisco WSA. From an application support standpoint, this method introduces the least amount of complications, as the proxy-aware applications know about and work with Cisco WSA directly to provide the requested content. However, from a deployment standpoint, the explicit proxy method presents challenges as to how the administrator configures every client in the organization with the Cisco WSA proxy settings and how they configure devices not under the organization's control. Web Proxy Auto-Discovery and proxy automatic configuration scripts, along with other tools, such as Microsoft Group and System policy controls within Microsoft Active Directory, make deploying this method simpler, but a discussion of those tools is beyond the scope of this guide.

It is possible to use both options—explicit proxy and transparent proxy—at the same time on a single Cisco WSA appliance. Explicit proxy is also a good way to test the Cisco WSA configuration, as explicit proxy mode does not depend on anything else in the network to function.

The next step in planning a Cisco WSA deployment is to determine what type of physical topology you are going to use. Cisco WSA has multiple interfaces and can be configured in different ways. In the Internet edge designs, Cisco WSA is deployed using a single interface for both proxy and management traffic.

A single Cisco WSA appliance was deployed in the Internet edge design to support up to 5,000 users. For those who need either additional performance or resilience, a simple upgrade solution is possible by adding an additional appliance. When deployed in high availability mode, the two appliances load-share the outgoing connections. If one device fails, the load is moved to the other appliance. It is possible that network performance could be degraded if one device is handling the load that was designed for two, but Internet web access remains available and protected.



Procedure 1 Configure the distribution switch

The LAN distribution switch is the path to the organization's internal network. As configured in the Firewall and IPS Design Guide, a unique VLAN supports the Internet edge devices and the routing protocol peers with the appliances across this network.

CO Reader Tip

Before you continue, ensure that the distribution switch has been configured following the guidance in the Campus Wired LAN Design Guide.

Step 1: Configure the interfaces that are connected to the distribution switch.

```
interface GigabitEthernet1/0/22
description WSAs370 M1 Management interface
switchport access vlan 300
switchport host
macro apply EgressQoS
logging event link-status
no shutdown
```

8

Step 1: Connect a standard null modem cable, with the terminal emulator settings of 8-1-none-9600 baud, to the appliance's serial console port.

```
Tech Tip
The default username is admin, and the default password is ironport.
    ironport.example.com> interfaceconfig
    Currently configured interfaces:
    1. Management (192.168.42.42/24 on Management: ironport.example.com)
    Choose the operation you want to perform:
    - NEW - Create a new interface.
    - EDIT - Modify an interface.
    - DELETE - Remove an interface.
    []>EDIT
    Enter the number of the interface you wish to edit.
    []> 1
    IP Address (Ex: 192.168.1.2):
    [192.168.42.42]> 10.4.24.15
    Netmask (Ex: "255.255.255.0" or "0xfffff00"):
    [255.255.255.0]> 255.255.255.224
    Hostname:
    [ironport.example.com] > WSAs370.cisco.local
    Do you want to enable FTP on this interface? [Y]> y
    Which port do you want to use for FTP?
    [21]> 21
    Do you want to enable SSH on this interface? [Y] > y
    Which port do you want to use for SSH?
    [22]> 22
    Do you want to enable HTTP on this interface? [Y]> {\boldsymbol{y}}
    Which port do you want to use for HTTP?
    [8080]> 8080
```

9

```
Do you want to enable HTTPS on this interface? [Y]> y
Which port do you want to use for HTTPS?
[8443]> 8443
```

```
You have not entered an HTTPS certificate. To assure privacy, run "certconfig" first. You may use the demo, but this will not be secure. Do you really wish to use a demo certificate? [Y]> \mathbf{y}
```

```
Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secure service? [Y]> {\bf y}
```

The interface you edited might be the one you are currently logged into. Are you sure you want to change it? [Y]> ${\bf y}$

Currently configured interfaces: 1. Management (10.4.24.15/27 on Management: WSAs370.cisco.local)

Choose the operation you want to perform:

- NEW Create a new interface.
- EDIT Modify an interface.
- DELETE Remove an interface.
- []> <Return>

Tech Tip

The appliance console displays the following message, which corresponds to the default IP address of the Cisco WSA appliance:

```
Please run System Setup Wizard at http://192.168.42.42:8080
```

Do not connect to the GUI at this address.

```
ironport.example.com> setgateway
```

Warning: setting an incorrect default gateway may cause the current connection to be interrupted when the changes are committed. 1. Management Default Gateway 2. Data Default Gateway []> 1 Enter new default gateway: []> 10.4.24.1 ironport.example.com> commit Please enter some comments describing your changes: []> initial setup

Changes committed: Thu Dec 06 23:31:13 2012 GMT

After you configure Cisco WSA, it should be able to ping devices on the network, assuming appropriate network access has been created (on the firewall, if needed). The following output is a capture of Cisco WSA pinging its default gateway:

```
WSA.cisco.local> ping 10.4.24.1

Press Ctrl-C to stop.

PING 10.4.24.1 (10.4.24.1): 56 data bytes

64 bytes from 10.4.24.1: icmp_seq=0 ttl=255 time=0.497 ms

64 bytes from 10.4.24.1: icmp_seq=1 ttl=255 time=9.387 ms

64 bytes from 10.4.24.1: icmp_seq=2 ttl=255 time=0.491 ms

^C
```

Procedure 3 Complete the System Setup Wizard

It is recommended that you configure only the basic network settings, DNS information, time settings, and username/password information through the System Setup Wizard, and you configure the more advanced settings in the respective sections in the UI.

The System Setup Wizard screens and options vary by code version. Depending on the starting code version of the appliance that you are configuring, the screens may differ from those shown below.

Step 1: From a client on the internal network, navigate and log in to the appliance. The GUI uses HTTPS on port 8443. (Example: https://10.4.24.15:8443).



Step 2: Log in, and then navigate to System Administration > System Setup Wizard.

Step 3: On the Start page, read the license, click I accept, and then click Begin Setup.

Step 4: On the System Settings page, in the **Default System Hostname** box, enter the appliance hostname. (Example: WSAs370.cisco.local)

Step 5: Select Use these DNS Servers, and then enter the internal DNS server. (Example: 10.4.48.10).

Step 6: In the NTP Server box, enter the internal NTP server. (Example: 10.4.48.17)

August 2013

Step 7: For the time zone, enter the following information, and then click Next:

- Region-America
- Country–United States
- Time Zone / GMT Offset-Pacific Time (Los_Angeles)

1. Start	2. Network	3. Security	4. Review
System Settings			
Default System Hostname: ?	WSAs370.cisco.local		
	e.g. proxy.company.com		
DNS Server(s):	O Use the Internet's Root DNS Servers		
	Use these DNS Servers:		
	10.4.48.10		
	(optional)		
	(optional)		
NTP Server:	10.4.48.17		
Time Zone:	Region: America 💌		
	Country: United States	•	
	Time Zone / GMT Offset: Pacific Time (Los_/	Ingeles)	
« Prev Cancel			Next »

Step 8: On the Network Context page, click Next.

Step 9: On the Network Interfaces and Wiring page, click **Next**. When you completed Procedure 2, "Configure management access," you completed the necessary configuration for this page.

 ÷	Tech Tin
In this of and is the not use	deployment, for simplicity, M1 is used for both management and proxy services the only interface used. Do not select Use M1 port for Management only . Do the interface P1.

1. Start	2. N	etwork	3. Security	4. Review
Network Interfaces and N	Viring			
Note: If the Management a	Ind Data interfaces are	TI TI PL P2 M1 both configured, they	P1	c on different subnets.
Management		Data		L4 Traffic Monitor
This interface is used to ma Optionally, it may also hand	nage the appliance. le Web Proxy	This interface may t monitoring and L4 T	e used for Web Proxy raffic Monitor blocking.	These interfaces are used for L4 Traffic Monitor data.
Ethernet Port: M1	Shitor blocking.	Ethernet Port: P1		In Duplex mode, T1 receives incoming and
IP Address: 10.4.24.15	;	IP Address:		outgoing traffic and T2 receives incoming
Network Mask: 255,255,2	55.224	Network Mask:		Wiring Type: © Duplex TAP:
Hostname: WSAs370. (e.g. wsa.e	cisco.local example.com)	Hostname: (e.	g. data.example.com)	T1 (In/Out) Simplex TAP: T1 (In) and T2 (Out)
Use M1 port for manag	ement only			
« Prev Cancel				Next »

Step 10: On the Routes for Management and Data Traffic page, click **Next**. When you completed Procedure 2, "Configure management access," you completed the necessary configuration for this page.

Step 11: On the Transparent Connections Settings page, click Next.

Step 12: On the Administrative Settings page, in the **Administrator Password** box, enter and confirm the administrator password.

Step 13: In the **Email system alerts to** box, enter the administrator's email address (Example: admin@cisco. local).

Step 14: In the Send Email via SMTP Relay Host box, enter the internal mail server (Example: internalexchange.cisco.local), and then click Next.



Administrator Password:	Password:
	Confirm Password:
Email system alerts to:	admin@cisco.local e.g. admin@company.com
Send Email via SMTP Relay Host (optional): ?	Internal-exchange.cisco.local Port: (?) <i>i.e., smtp.example.com, 10.0.0.3</i> optional
AutoSupport:	Send system alerts and weekly status reports to Cisco IronPort Customer Support
Network Participation:	Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in orde to identify and stop web-based threats.
	Participation Level: 🛞 Limited - Summary URL information.
	C Standard - Full URL information. (Recommended)
	Learn what information is shared

1. Start	2. Netv	vork	3. Se	curity	4. Review
Security Settings					
Global Poli	cy Default Action: ?	 Monitor all tra 	iffic		
		O Block all traff	ic		
		If block all traffic is protocols (HTTP, H	selected, the Global A TTPS, FTP over HTTP, a	ccess Policy will be initia nd native FTP).	lly configured to block all proxied
	L4 Traffic Monitor:	Action for Suspect	Malware Addresses 🛛 🤅	Monitor only	
			c	Block	
Accepta	able Use Controls: ?	Enable			
		The Global Access	Policy will be initially co	nfigured to monitor all p	pre-defined categories.
	Reputation Filtering:	Enable			
		The Global Access Scanning.	Policy will be intially co	nfigured to use Web Rep	putation Filtering and Adaptive
Malware and	d Spyware Scanning:	Enable Webro	ot 🔽 Enable McAfe	e 🔽 Enable Sophos	
		The Global Access the actions configu	Policy and Outbound Ma red below.	alware Scanning Policy v	vill be initially configured to apply
		Action for Def	ected Malware: 💿 🛛	Monitor only	
			0	Block	
Cisco IronPort Da	ata Security Filtering:	Enable			
		The Global Cisco Ir Web Reputation (if	onPort Data Security Po enabled) and monitor a	olicy will be initially confi all other uploads.	gured to block uploads based on
« Prev Cancel					Next »

Step 15: On the Security Settings page, use the default settings, and then click Next.

Step 16: On the Review page, review the configuration, and then click Install This Configuration.

Procedure 4 Install system updates

It is important to look at system upgrades for Cisco WSA before going any further. HTTP or HTTPS Internet access for the appliance is required in order to proceed.

		Tech Tip
lt is	not	possible to downgrade software versions, so be certain that an upgrade
is d	esir	ed before proceeding. It is possible that an appliance can receive different
upg	iradi	e options if it is on an early release list.

Step 1: Navigate to System Administration > System Upgrade. The display shows the current software version.

Step 2: Click Available Upgrades.

If newer versions are available, they should be selected and installed. In general, all upgrades should be installed. Each upgrade usually requires a reboot of the appliance. The entire process can take some time.

Procedure 5 Install the feature keys

It is important to install the feature keys for Cisco WSA before going any further. HTTP or HTTPS Internet access for the appliance is required in order to proceed. When installing feature keys, Cisco WSA makes a connection to the license service and submits a query to see if it has all the features it is allowed to run. It is very likely that after upgrading code, especially if many upgrades were applied, there will be missing feature keys.

Step 1: Navigate to System Administration > Feature Keys.

Step 2: Click Check for New Keys.

The figure below shows what an appliance feature key display may look like after being upgraded to the latest version of code and then checking for updated feature keys.

Feature Keys for Serial Number: A4BADB1069	8E-DVY43M1		
Description	Status	Time Remaining	Expiration Date
Cisco IronPort L4 Traffic Monitor	Active	Perpetual	N/A
Cisco IronPort HTTPS Proxy	Active	Perpetual	N/A
Cisco IronPort Web Usage Controls	Active	94 days	Mon Mar 11 02:00:07 2013
Cisco IronPort URL Filtering	Active	94 days	Dormant
McAfee	Active	94 days	Mon Mar 11 02:00:07 2013
Webroot	Active	94 days	Mon Mar 11 02:00:07 2013
Cisco IronPort Web Proxy & DVS Engine	Active	Perpetual	N/A
Cisco AnyConnect Secure Mobility	Active	Perpetual	N/A
Cisco Web Reputation Filters	Active	94 days	Mon Mar 11 02:00:07 2013
Pending Activation			

Tech Tip

1

If the appliance is missing keys or the duration of the keys is not correct, contact a trusted partner or Cisco reseller to resolve the issue. Have the appliance serial number available. You can find the serial number at the top of the Feature Key page.

Procedure 6 Update web usage controls and test

Step 1: Navigate to Security Services > Acceptable Use Controls.

Step 2: Click Update Now, and then wait until the page reports back success.

August 2013

Step 3: Ensure that at least some of the controls have an update that is current or very nearly so.

Tech Tip

i

Due to randomness of update schedules, it is impossible to know when updates will come out for each component. The Web Categories Prefix Filters and the Web Categories List are updated fairly often and show recent update histories.

Acceptable Use Controls				
Acceptable Use Controls Settings				
Acceptable Use Controls Service Status:	Enabled			
Active Acceptable Use Controls Engine:	Cisco IronPort Web Usage C	Controls		
Application Visibility and Control:	Enabled			
Dynamic Content Analysis Engine:	Enabled			
Default action for Unreachable Service:	Monitor			
			Edit Glob	al Settings
Acceptable Use Controls Engine Updates				
File Type		Last Update	Current Version	New Update
Cisco IronPort URL Filtering Engine		Never Updated	5.2.2	Not Available
Cisco IronPort URL Categories Database		Never Updated	1656	Not Available
Cisco IronPort URL Categories Database Increme	ental Updates	Never Updated	1657	Not Available
Cisco IronPort Web Usage Controls - Web Catego	orization Engine	Success - Thu Oct 11 09:36:53 2012	3.0.0.036	Not Available
Cisco IronPort Web Usage Controls - Web Catego	prization URL Keyword Filters	Success - Thu Oct 11 09:36:53 2012	1312487822	Not Available
Cisco IronPort Web Usage Controls - Web Catego	prization Prefix Filters	Success - Thu Dec 6 19:37:06 2012	1354851340	Not Available
Cisco IronPort Web Usage Controls - Web Catego	orization Categories List	Success - Thu Oct 11 09:36:54 2012	1337979188	Not Available
Cisco IronPort Web Usage Controls - Dynamic Co	ontent Analysis Engine	Success - Tue Nov 13 10:37:59 2012	2.1.0.016	Not Available
Cisco IronPort Web Usage Controls - Dynamic Co	ontent Analysis Engine Data	Success - Thu Oct 11 09:12:06 2012	3.1.0.003	Not Available
Cisco IronPort Web Usage Controls - Application	Visibility and Control Engine	Success - Thu Oct 18 14:31:45 2012	1.1.0-076	Not Available
Cisco IronPort Web Usage Controls - Application	Visibility and Control Data	Success - Wed Nov 14 11:41:07 2012	1.1.0.6-003	Not Available
No updates in progress.				Update Now

Step 4: Set up a client on the inside of the network with Cisco WSA as the explicit proxy in the web browser of their choice. Use the IP address of the appliance as the proxy, and then set the port to 3128.

- Step 5: Test two different addresses, as follows:
 - One address should be resolvable externally, for instance www.cisco.com, which should return without issue. This proves the client has Internet access but does not prove the connection is going through Cisco WSA.
 - The other address should be something not resolvable externally. This request should return an error from Cisco WSA, not the browser; proving that Cisco WSA is serving the content.

Cisco WSA returns an error like that shown below:

This Page Cannot Be D	Displayed
The host name resolution (DNS The Internet address may be m temporarily unavailable, or the I	b lookup) for this host name (www.not-a-site.com) has failed. hisspelled or obsolete, the host (www.not-a-site.com) may be DNS server may be unresponsive.
Please check the spelling of the	e Internet address entered. If it is correct, try this request later.
If you have questions, please co	ontact your corporate network administrator and provide the
codes snown below.	

If the web request is not directed to Cisco WSA, your web browser returns an error. An example with the Firefox browser returns an error like that shown below:

Fir	refox can't find the server at www.not-a-site.com.
•	Check the address for typing errors such as ww .example.com instead of www .example.com
-	If you are unable to load any pages, check your computer's network connection
•	If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Procedure 7 Enable logging

To monitor web usage, the appliance stores client access data for a relatively short duration and it rotates logs for space reasons. For users looking for long-term compliance reporting, they should look into the Cisco solution that comes as part of the Cisco Content Security Management Appliance. This guide does not cover the installation or use of the Cisco Content Security Management Appliance.

For the reporting product to work, Cisco WSA needs to send its logs to an FTP server where the reporting device can access them. For this deployment, it is assumed that an FTP server is already deployed and configured. The following configuration moves the access logs off of Cisco WSA and onto an FTP server.

Step 1: Navigate to System Administration > Log Subscriptions, and then click Add Log Subscription.

Step 2: On the New Log Subscription page, add the new logging information, click Submit, and then click Commit Changes.

New Log Subscription				
Log Subscription				
Log Type:	Access Logs			
Log Name:	WSA-AccessLogs (will be used to name the log directory)			
Rollover by File Size:	100M Maximum (Add a trailing K or M to indicate size units)			
Rollover by Time:	None			
Log Style:	© Squid C Apache C Squid Details			
Custom Fields (optional):	Custom Fields Reference 🗗			
File Name:	WSA-AccessLogs			
Log Compression:	Enable			
Log Exclusions (Optional):	(Enter the HTTP status codes of transactions that should not be included in the Access Log)			
Retrieval Method:	C FTP on WSAs370.cisco.local			
	Maximum Number of Files: 100			
	FTP on Remote Server			
	FTP Host: 10.4.48.11			
	Directory: WSA-Logs			
	Username: admin			
	Password:			

Step 3: In the Uncommitted Changes pane, enter a comment to describe the change, and then click Commit Changes.

Uncommitted Changes	
Attention — 🔺 In order to process these changes, the proxy process will restart after Co cause a brief interruption in service. Additionally, the authentication cache which might require some users to authenticate again.	mmit. This will will be cleared,
Commit Changes	
You have uncommitted changes. These changes will not go into effect until you commit them.	
Comment (optional): Added new log subscription	
Cancel Abandon Changes Commit Changes	

Procedure 8 Create custom URL categories

Next, you set up standard custom URL categories that most administrators find they need to implement for their desired URL filtering.

Step 1: Navigate to Web Security Manager > Custom URL Categories, and then click Add Custom Category.

You create four placeholder categories for different action exceptions.

Step 2: In the Edit Custom URL Category pane, in the Category Name box, enter Block List.

Step 3: In the Sites box, enter a placeholder URL (Example: block.com), and then click Submit.

i	Tech Tip
A place	eholder URL (block.com) has to be entered because it is not possible to create
a categ	gory and have it be empty. In the future, when a URL is found that needs to be
blocke	d, add it to the list, and then delete the placeholder.

Custom URL Categories: Add	Category	
dit Custom URL Category		
Category Name:	Block List	
List Order:	1	
Sites: 🕐	block.com	Sort URLS Click the Sort URLS button to sort all site URLs in Alpha-numerical order.
✓ Advanced	Regular Expressions: ⑦	
	Enter one regular expression per line.	
Cancel		Submit

Step 4: Create three more lists by repeating Step 1 through Step 3. In the Category Name box, name the new lists **Monitor List**, **Warn List**, and **Allow List**. The List Order value increments with each new category; use the suggested value.

This creates an ordered list of custom categories.

Custom URL Categories					
Custor	Custom URL Categories				
Add (Add Custom Category				
Order	Category				
1	Block List				
2	Monitor List				
3	Warn List				
4	Allow List				

Step 5: Click Commit Changes.

Step 6: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Procedure 9 Configure access policies

Now that you have created the custom URL categories, you need to enable them for use and define actions for each.

Step 1: Navigate to Web Security Manager > Access Policies, and then under URL Filtering, click the link.

Acce	ess Policies						
Polici	Policies						
Add	Policy						
Order	Group	User Agents	URL Filtering	Applications	Objects	Anti-Malware Filtering	Delete
	Global Policy Identity: All	No blocked items	Monitor: 79	Monitor: 160	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Enabled	

Step 2: Click Select Custom Categories. The policies created in the previous procedure appear.

Step 3: For each custom URL category, in the Setting Selection list, choose Include in Policy, and then click Apply.

Select Custom Categories for this Policy				
Category	Setting Selection			
Block List	Include in policy	•		
Monitor List	Include in policy	•		
Warn List	Include in policy	•		
Allow List	Include in policy	•		
Cancel		Apply		

Step 4: On the Access Policies: URL Filtering: Global Policy page, click in the appropriate boxes in order to change the action of the category to correspond with its name. (Example: Block should be the action for the Block List category, and Monitor should be the action for the Monitor List category.)

Monitor	Web Security Manager	Security Services	Networ	k :	ystem Admin	istration		
Access Policies: URL Filtering: Global Policy								
Custom URL Catego	ry Filtering							
These URL Categorie	es are defined as group membe	rship criteria. All other cat	egories are no	applicable fo	r this policy.			
			Blo	ck Redire	ct Allow?	Monitor	Warn ?	Time-Based
Category			Sele	t all Select	all Select all	Select all	Select all	(Unavailable)
😢 Block List			8	1				-
\varTheta Monitor List						1		-
🕕 Warn List							1	_
C Allow List					1			-
Select Custom Cate	gories					·		

Step 5: Click Submit.

Additionally, on the Access Policies page, the organization's web-acceptable use policy can be implemented. This policy can include the category of the URL (adult, sports, or streaming media), the actions desired (monitor, warn, or block), as well as whether a time-based factor is involved.

Step 6: On the Access Policies page, under URL Filtering, click the link.

Step 7: For testing purposes, next to Gambling select **Block**, next to Sports and Recreation select **Warn**, and then click **Submit**. You may need to scroll to see all predefined URL categories.

Predefined URL Category Filtering						
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.						
	Block 3	Monitor	Warn ?	Time-Based		
Category	Select all	Select all	Select all	(Unavailable)		
3 Gambling	v			-	*	
It Sports and Recreation			\checkmark	-		

Step 8: Click Commit Changes.

Step 9: In the Uncommitted Changes pane, enter a comment to describe the change, and then click Commit Changes.

Step 10: Using a browser explicitly pointing to the appliance, browse to a well-known gambling site. Cisco WSA should return the following message:

This Page Cannot Be Displayed Based on your organization's access policies, access to this web site (been blocked because the web category "Gambling" is not allowed. If you have questions, please contact your corporate network administrator and provide the codes shown below.) has
Date: Fri, 07 Dec 2012 09:56:28 PST Username: Source IP: 10.4.2.14 URL: GET Category: Gambling Reason: BLOCK-WEBCAT Notification: WEBCAT	

Procedure 10 Configure WCCP on Cisco WSA

Now that Cisco WSA is working and applying an access policy for HTTP traffic, you can implement WCCP on the appliance and the appliance firewall. Implementing WCCP allows the Cisco WSA appliance to begin to receive traffic *transparently* (redirected from the firewall) instead of having browsers configured to use Cisco WSA as an explicit proxy.

Step 1: Navigate to Network > Transparent Redirection, and then click Edit Device.

Step 2: In the Type list, choose WCCP v2 Router, and then click Submit.

Step 3: In the Transparent Redirection pane, under WCCPv2 Services, click Add Service.

Step 4: In the WCCP v2 Service pane, ensure the Service Profile Name is HTTP_and_HTTPS_WCCP.



Step 5: In the Service section, in the **Dynamic service ID** box, enter **90**. This is the number used to define this policy and is the ID used by Cisco ASA to request the policy.

Step 6: In the Port numbers box, enter 80, 443. In this policy, redirect ports are HTTP and HTTPS.

Step 7: In the **Router IP Addresses** box, enter the IP address of the inside interface of your firewall (Example: 10.4.24.30) and then click **Submit**.



Step 8: If you want to create an HTTP-only policy, repeat Step 3 through Step 7 using the following information:

- Service Profile Name-Standard_HTTP_Only_WCCP
- Service-Standard Service ID
- Router IP Addresses-10.4.24.30

After completion, the WCCP services panel should look like the following figure.

Transparent Redirection				
Transparent Redirection Device				
Type:	WCCP v2 Router			
				Edit Device
WCCP v2 Services				
Add Service				
Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
Standard_HTTP_Only_WCCP	0 (web-cache)	10.4.24.30	80	Ŵ
HTTP_and_HTTPS_WCCP	90	10.4.24.30	80,443	Ŵ

Step 9: Click Commit Changes.

Step 10: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Procedure 11 Configure WCCP on the firewall

The WCCP policy configured redirects all HTTP and HTTPS traffic to Cisco WSA. This includes any traffic from the inside network to the DMZ web servers and any device management traffic that uses HTTP or HTTPS. It is unnecessary to send any of this traffic to Cisco WSA. To avoid having any of this traffic redirected to Cisco WSA, you must create an access control list (ACL) on the firewall in order to filter out any HTTP or HTTPS traffic destined to RFC 1918 addresses.



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

Step 2: Navigate to Configuration > Device Management > Advanced > WCCP > Service Groups, and the click Add.

Step 3: If you are configuring an HTTP and HTTPS policy, on the Add Service Group dialog box, select **Dynamic Service Number**, and then enter the value of **90** that was configured as a service ID in Procedure 10, Step 5.

If you are configuring a temporary HTTP-only policy, then select Web Cache.

Step 4: On the Add Service Group dialog box, next to Redirect List, click Manage.

🔂 Add Service Group
Service: 🔘 Web Cache
Dynamic Service Number: 90
Options
Redirect List: None Manage
Group List: None 🗸 Manage
Password:
Confirm Password:
OK Cancel Help

Step 5: In the ACL Manager window, click Add.

Step 6: Click Add ACL.

Step 7: On the Add ACL dialog box, in the ACL Name box, enter WCCP_Redirect_List, and then click OK.

Step 8: Repeat Step 9 and Step 10 for all entries in Table 2.

Table 2 - Access control entries for WCCP redirect

Action	Source	Destination	Service	Description
deny	any4	10.0.0/8	ip	Block RFC-1918 10.0.0.0/8
deny	any4	172.16.0.0/12	ip	Block RFC-1918 172.16.0.0/12
deny	any4	192.168.0.0/16	ip	Block RFC-1918 192.168.0.0/16
permit	any4	any4	ip	Permit all others

Step 9: In ACL Manager window, select the WCCP_Redirect_List ACL, click Add, and then click Add ACE.

Step 10: In the Add ACE dialog box, using the fields from Table 2, select the Action and then enter the Source, Destination, Service and Description fields.

Add ACE	
Action: 🔘 Pern	nit o Deny
Source Criteria -	
Source:	any4
User:	
Security Group:	
Destination Crite	ria
Destination:	10.0.0/8
Security Group:	
Service:	ip
Description:	Block RFC-1918 10.0.0.0/8
📝 Enable Loggi	ng
Logging Leve	l: Default 👻
More Options	s 🛞
	OK Cancel Help

Step 11: After completing in the ACL Manager window all entries in Table 2, click OK.

F	Enabled	Source	User	Se	Destination	Sec	Service	Action	Logging	Time	Description	
WCC	P_Redirect_	List										
1		🇳 any4			🚅 10.0.0.0/8		💴 ip	😢 Deny			Block RFC-1918 10.0.0.0/8	
2		🍅 any4			172.16.0.0/12		IP ip	😢 Deny			Block RFC-1918 172.16.0.0/12	
3	\checkmark	🇳 any4			📑 192.168.0.0/16		💶 ip	😢 Deny			Block RFC-1918 192.168.0.0/16	
4	\checkmark	🍪 any4			🌍 any4		IP ip	🖌 Permit			Permit all others	

Step 12: On the Add Service Group dialog box, in the **Redirect List** list, choose the ACL created above (Example: WCCP_Redirect_List), and then click **OK**.

Add Service Group
Service: 🔘 Web Cache
Oynamic Service Number: 90
Options
Redirect List: WCCP_Redirect_List - Manage
Group List: None 👻 Manage
Password:
Confirm Password:
OK Cancel Help

Step 13: On the Service Groups pane, click Apply.

Step 14: Navigate to Configuration > Device Management > Advanced > WCCP > Redirection, and then click Add.

Step 15: If you are configuring an HTTP and HTTPS policy, on the Add WCCP Redirection dialog box, in the **Interface** list, choose **inside**, in the **Service Group** list, choose **90**, and then click **OK**.

If you are configuring an HTTP-only policy, in the **Interface** list, choose **inside**, in the **Service Group** list, choose **web-cache**, and then click **OK**.

Add WCCP I	Redirection	×
Interface:	Inside 🔹	
Service Group:	90 👻	New
ОК	Cancel	Help

Step 16: On the Redirection pane, click Apply.

Step 17: If you want to test the configuration, use a browser that is not already configured to go to the appliance as an explicit proxy (or remove the explicit proxy settings), and test to the following sites:

- A resolvable allowed address, such as www.cisco.com
- A resolvable blocked address (from one of the previously configured Blocked categories)

Next, in Cisco ASDM, you check that WCCP redirection is working.

Step 18: Navigate to Monitoring > Properties > WCCP > Service Groups.

The status window should show a router ID that is the highest IP address of the appliance and the number of cache engines is 1, which is the Cisco WSA appliance. If things are working correctly and redirections are occurring, the Total Packets Redirected counter increases.

onitoring > Pro	perties > WCCP > Service Gro	ups			
Service Group:	All Service Groups				
Display Mode:	None 👻				
	Hash Settings				
	Destination Ip Address:			Destination Port:	
	Source Ip Address:			Source Port:	
Global WCCP Router i	information: nformation:				[
Global WCCP Router i Rout Prot	information: nformation: er Identifier: ocol Version:		192.168	.28.1	
Global WCCP Router i Rout Prot	information: nformation: er Identifier: ocol Version:		192.168 2.0	.28.1	
Global WCCP Router i Rout Prot Service Numb	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines:		192.168 2.0	.28.1	
Global WCCP Router i Rout Prot Service Numb Numb	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers:		192.168 2.0 1	.28.1	
Global WCCP Router i Rout Prot Service Numb Tota	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected:		192.168 2.0 1 1 142	.28.1	
Global WCCP Router i Rout Service Numb Numb Tota Redi	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected: rect access-list:		192.168 2.0 1 142 WCCP Re	.28.1 direct List	
Global WCCP Router i Rout Service Numb Numb Tota Redi Tota	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected: rect access-list: 1 Connections Denied Red	lirect:	192.168 2.0 1 142 WCCP_Re 4	.28.1 direct_List	
Global WCCP Router i Rout Service Numb Numb Tota Redi Tota Tota	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected: rect access-list: 1 Connections Denied Red 1 Packets Unassigned:	lirect:	192.168 2.0 1 1 142 WCCP_Re 4 0	.28.1 direct_List	
Global WCCP Router i Rout Service Numb Numb Tota Redi Tota Tota Crou	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected: rect access-list: 1 Connections Denied Red 1 Packets Unassigned: p access-list:	lirect:	192.168 2.0 1 1 142 WCCP_Re 4 0 -none-	.28.1 direct_List	
Global WCCP Router i Rout Prot Service Numb Numb Tota Redi Tota Tota Grou Tota	information: nformation: er Identifier: ocol Version: Identifier: 90 er of Cache Engines: er of routers: 1 Packets Redirected: rect access-list: 1 Connections Denied Red 1 Packets Unassigned: p access-list: 1 Messages Denied to Gro	lirect:	192.168 2.0 1 142 WCCP_Re 4 0 -none- 0	.28.1 direct_List	

High Availability and Resilience

For availability purposes, if Cisco WSA fails, the WCCP reports that fact to the appliance, and it stops redirecting traffic to Cisco WSA by default. If web security resilience is a requirement, two or more Cisco WSAs can be deployed. To deploy multiple devices, define multiple WCCP routers on the appliance, and the WCCP protocol load-balances between them. If one is down, the appliance takes that device out of the list until it comes back online and starts responding to WCCP requests again.

Procedure 12 Configure default tunnel gateway

This procedure is required when using the integrated deployment model for firewall and remote-access VPN. If you are using the standalone deployment model, the default tunnel gateway is already configured, skip to Procedure 13, "Set up HTTPS proxy."

Cisco WSA must inspect traffic from remote-access VPN clients to and from the Internet. To accomplish this, all traffic to and from the VPN clients must be routed toward the LAN distribution switch, regardless of the traffic's destination, so that the Cisco ASA appliance can properly redirect the traffic to the Cisco WSA appliance.

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

Step 2: In Configuration > Device Setup > Routing > Static Routes, click Add.

Step 3: On the Add Static Route dialog box, configure the following values, and then click OK.

- Interface-inside
- Network-any4
- · Gateway IP-10.4.24.1
- Options-Tunneled (Default tunnel gateway for VPN traffic)

付 Add Static Route	2
IP Address Type:	⑧ IPv4
Interface:	inside 👻
Network:	any4
Gateway IP:	10.4.24.1 Metric: 255
Options	
🔘 None	
Tunneled (Def	ault tunnel gateway for VPN traffic)
🔘 Tracked	
Track ID:	Track IP Address:
SLA ID:	Target Interface: inside 🚽
Monitoring C	options
Enabling the tra state of the rou	cked option starts a job for monitoring the ite, by pinging the track address provided.
ОК	Cancel Help

Step 4: Verify the configuration, and then click Apply.

filter: 🧿 B	ioth 🔘 IPv4	i only 💿 IPv6 onl	У			
Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options	Add
inside	0.0.0.0	0.0.0.0	10.4.24.1	255	Tunneled	Edit
outside-16	0.0.0.0	0.0.0.0	172.16.130.126	1	Tracked ID - 1 Address - 172.18.1.1 Interface - outside-16	Delete
outside-16	172.18.1.1	255.255.255.255	172.16.130.126	1	None	
outside-17	0.0.0.0	0.0.0.0	172.17.130.126	50	None	

Procedure 13 Set up HTTPS proxy

To set up Cisco WSA to proxy HTTPS connections, start by enabling the feature.

Step 1: On the Cisco WSA appliance, navigate to Security Services > HTTPS Proxy, and then click Enable and Edit Settings.

Step 2: On the HTTPS Proxy License Agreement page, click Accept.

i	Tech Tip
You ne proxy warn a uploac to the machin author	eed to generate a certificate for Cisco WSA to use on the client side of the connection. Generating a self-signed certificate causes the client browser to about the certificate for each connection to an HTTPS website. To avoid this, d a certificate that was issued from an organization's trusted certificate authority appliance. If the clients already have the trusted root certificate loaded on their nes, the HTTPS proxy does not generate errors related to unknown certificate rity.

Step 3: On the Edit HTTPS Proxy Settings page, in the Root Certificate for Signing section, select Use Generated Certificate and Key, and then click Generate New Certificate and Key.

Step 4: In the Generate Certificate and Key dialog box, enter values relevant to your organization, and then click **Generate**.

Generate Certificate and Key	×
Common Name: WSAs370.cisco.local	
Organization: Cisco Validated Design Group	
Organizational Unit: cisco.local	
Country: US	
Duration before expiration: 36 months	
Basic Constraints: 🔲 Set X509v3 Basic Constraints Extension to Critical	
Cancel Ger	ierate

Step 5: In the Invalid Certificate Handling section, define the action that Cisco WSA should take when it encounters an invalid certificate on the HTTPS server. The choices, depending on the certificate error, can range from dropping the connection, decrypting it, or monitoring it. This example uses the default setting of **Monitor** for all errors.

TPS Proxy Settings				
Enable HTTPS Proxy				
HTTPS Ports to Proxy:	443			
HTTPS Transparent Request: ?	If a user has not been authenticated and surrogate type is IP address			
	 Decrypt the HTTPS request and redirect for authentication 			
	O Deny the HTTPS request			
	Once the user is authenticated, subsequent HTTPS requests are subject to no	rmal Decryption polici	es.	
	Transparent user discovery will not be affected by the above decision.			
Applications that Use HTTPS: (?)	Enable decryption for enhanced application visibility and control			
Root Certificate for Signing:	C Use Uploaded Certificate and Key	Upload Files		
	Certificate: Browse Key: Browse			
	Private key must be unencrypted.			
	No certificate has been uploaded.			
	Use Generated Certificate and Key Generate New	Certificate and Key		
	Common name: WSAs370.cisco.local			
	Organization: Cisco Validated Design Group			
	Organizational Unit: cisco.local			
	Country: US			
	Expiration Date: May 6 14:56:39 2016 GMT			
	Basic Constraints: Not Critical			
	Download Certificate Download Certificate Signing Request			
	Signed Certificate:			
	-			
	To use a signed certificate, first download a certificate signing request u the link above. Submit the request to a certificate authority, and when yu receive the signed certificate, upload it using the field below.	sing ou		
	Certificate: Browse	Upload File		
Invalid Certificate Handling:		Drop	Decrypt	Monitor
	Certificate Error	Select all	Select all	Select a
	Expired			1
	Mismatched Hostname			1
	Unrecognized Root Authority			1
	All other error types			1
	No end-user notification will be provided for dropped HTTPS connections. Use equivalent certificate will be generated.	this setting with cautio	on. If the connection i	not dropped,

Step 6: When you are finished editing, click Submit, and then click Commit Changes.

Step 7: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Reader Tip	
For more information at mechanism, see the <i>Cis</i> products/ps10164/products sales representative.	out using certificates as part of the Cisco WSA HTTPS proxy aco WSA End-User Guides at http://www.cisco.com/en/US/ ucts_user_guide_list.html, or consult a trusted partner or Cisco

Next you configure policies for the HTTPS proxy.

Step 8: Navigate to Web Security Manager > Custom URL Categories, and then click Add Custom Category.

You create three placeholder categories for different action-exceptions.

Step 9: In the Edit Custom URL Category pane, in the category name box, enter Drop List.

Step 10: In the Sites box, enter a placeholder URL (Example: drop.com), and then click Submit.

Step 11: Repeat Step 9 and Step 10 to create two more custom categories. For the category names, enter **Decrypt List** and **Pass Through List**, and then click **Commit Changes**.

Step 12: In the Uncommitted Changes pane, enter a comment to describe the change, and then click Commit Changes.

Monitor		Web Security Manager	Security Services				
Custom URL Categories							
Succes	ss — The Cu	stom URL Category "Pass Th	rough List" was added				
Custor	n URL Catego	ries					
Add (Custom Catego	ry					
Order	Category						
1	Block List						
2	Monitor List						
3	Warn List						
4	Allow List						
5	Drop List						
6	Decrypt List						

Step 13: Navigate to Web Security Manager > Decryption Policies.

Step 14: Under the URL Filtering box, click the link.

Step 15: On the Decryption Policies: URL Categories: Global Policy page, click Select Custom Categories.

Step 16: In the Select Custom Categories for this Policy window, for each of the three new custom categories, in the **Setting Selection** list, choose **Include in policy**, and then click **Apply**.

Select Custom Categories for this Policy					
Category	Setting Selection				
Block List	Exclude from policy	•			
Monitor List	Exclude from policy	-			
Warn List	Exclude from policy	•			
Allow List	Exclude from policy	-			
Drop List	Include in policy	•			
Decrypt List	Include in policy	•			
Pass Through List	Include in policy	-			
Cancel		Apply			

Step 17: On the Decryption Policies: URL Filtering: Global Policy page, change the action of the category to correspond with its name, (Example: Drop should be the action for the Drop List category) and then click **Submit**.

	Monitor	Web Security Manager	Security Services	Ne	twork	System A	dministratio	n	
I	Decryption Policies: URL Filtering: Global Policy								
	Custom URL Category	y Filtering							
[These URL Categories	are defined as group members	hip criteria. All other cate	gories are	not applicable f	or this polic;	γ.		
					Pass Through	Monitor ()	Decrypt	Drop ?	Time-Based
	Category				Select all	Select all	Select all	Select all	(Unavailable)
	🕴 Drop list							1	-
ĺ	🖰 Decrypt List						V		-
ľ	😳 Pass through list				1				-
I	Select Custom Categories								
Ì	Cancel								Submit

Step 18: Click Commit Changes.

Step 19: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Step 20: Navigate to Web Security Manager > Decryption Policies.

Step 21: Under the URL Filtering box, click the link.

The predefined URL categories at the bottom of the page allow an administrator to create and enforce a policy around how Cisco WSA handles specific types of websites with relation to decryption. Some organizations have strict policies about not decrypting certain sites, such as health care or financial websites. The categories on this page allow an administrator to enforce that policy on the appliance. For example, it is possible to configure Cisco WSA so that financial HTTPS websites are set to Pass Through so they are not proxied, while gambling sites are set to Drop.

Step 22: Change the action for Gambling to Drop, and change the action for Finance to Pass Through, and then click Submit.

Predefined URL Category Filtering							
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.							
Pass Through Monitor Decrypt Drop ? Time-Based							
Category	Select all	Select all	Select all	Select all	(Unavailable)		
Finance	v				-		
\varTheta Freeware and Shareware		1			-		
3 Gambling				\checkmark	-		

Step 23: Click Commit Changes.

Step 24: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

Step 25: If your Cisco ASA is configured to use an HTTP and HTTPS policy, skip to Step 28.

If your Cisco ASA was configured with an HTTP-only policy, you should now change to the HTTP and HTTPS policy. On the Cisco ASA appliance, navigate to **Configuration > Device Management > Advanced > WCCP > Redirection**, and then click **Edit**.

Step 26: In the Edit WCCP Redirection dialog box, in the Service Group list, choose 90, and then click OK.

👩 Edit WCCP F	Redirection	23
Interface:	inside 👻	
Service Group:	90 👻	New
ОК	Cancel	Help

Step 27: On the Redirection pane, click Apply.

Step 28: If you want to test the new configuration, set up categories for webpages that you know are encrypted (HTTPS) and then use those URLs in the testing process. Because the administrator has to know whether the site uses HTTPS, use a custom URL category and put the address in the Drop List. When that site is accessed, Cisco WSA should drop the connection.

Procedure 14 Configure authentication

Authentication is the act of confirming the identity of a user. When authentication is enabled, Cisco WSA authenticates clients on the network before allowing them to connect to a destination server. When using authentication, it is possible to set up different web access policies by user or group membership, using a central user directory. Another primary driver for using authentication is that of user tracking, so that when a user violates an acceptable-use policy, Cisco WSA can match the user with the violation instead of just using an IP address. The last reason for authentication of web sessions is for compliance reporting.

Cisco WSA supports two different authentication protocols: Lightweight Directory Access Protocol (LDAP) and NT LAN Manager (NTLM). Because most organizations have an Active Directory server, they use NTLM. Single Sign-On is also only available when using NTLM.

When Cisco WSA is deployed in transparent mode with authentication enabled and a transaction requires authentication, Cisco WSA asks for authentication credentials from the client application. However, not all client applications support authentication, so they have no way to prompt users to provide their user names and passwords. These applications might have issues when Cisco WSA is deployed in transparent mode because the application tries to run non-HTTP traffic over port 80 and cannot handle an attempt by Cisco WSA to authenticate the connection.

Here is a partial list of applications that do not support authentication (these are subject to change as newer code versions are released):

- Mozilla Thunderbird
- Adobe Acrobat Updates
- Microsoft Windows Update
- Outlook Exchange (when trying to retrieve Internet-based pictures for email messages)

If applications need to access a particular URL, then it is possible to create an identity based on a custom User Agent category that does not require authentication. When this happens, the client application is not asked for authentication. For organizations that require authentication, consult a trusted Cisco Partner or reseller or your Cisco account team. They can assist in setting up an authentication solution that meets the organization's requirements, while minimizing any possible complications.

The first step in setting up authentication is to build an authentication realm. A realm defines how authentication is supposed to occur.

In this deployment, a realm was built for NTLM authentication to the Active Directory server.

Step 1: Navigate to Network > Authentication, and then click on Add Realm.

Step 2: On the Add Realm page, specify the Active Directory Server and the Active Directory Domain, and then click Join Domain.

Add Realm

NTLM Authentication Realm					
Realm Name:	WSA Authentication				
Authentication Protocol and Scheme(s):	NTLM (NTLMSSP or Basic Authentication)				
NTLM Authentication					
Active Directory Server:	Specify up to three Active Directory servers:				
	10.4.48.10				
	hostname or IP address				
Active Directory Account:	Active Directory Domain: ⑦ CISCO.LOCAL				
	Computer Account (?)				
	Location: Computers				
	(Example: Computers/BusinessUnit/Department/Servers)				
	Join Domain				
	Status: Computer account WSAs370\$ not yet created.				
Active Directory Agent: ?	Enable Transparent User Identification using Active Directory Agent				
	Primary Active Directory Agent:				
	Server: Shared Secret:				
	Backup Active Directory Agent (Optional):				
	Server: Shared Secret:				
	(Host names or IP addresses) (specify the shared secret for each server)				
Network Security:	Client Signing Required				

Step 3: In the Computer Account Credentials dialog box, enter the Active Directory domain administrator credentials (or ask an administrator to enter them), and then click **Create Account**.

Computer Account Credentials						
Enter login credentials to create a computer account on your Active Directory server. These credentials are used once and will not be stored.						
Username: administrator						
Password:						
Cancel	Create Account					

Step 4: On the Add Realm page, click **Start Test**. This tests the NTLM connection to the Active Directory domain.

Step 5: In the Test Authentication Realm Settings box, monitor the results.



Step 6: When the test is completed successfully, click Submit, and then click Commit Changes.

Step 7: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit** Changes.

Next you configure identity groups. Identities are based on the identity of the client or the transaction itself.

Step 8: Navigate to Web Security Manager > Identities, and then click Add Identity.

You create two different sample identities: Exempt Subnets and Exempt User Agents.

Step 9: On the Add Identity page, in the Name box, enter Exempt Subnets.

Identities: Add Identity

Identity Settings	
✓ Enable Identity	
Name: ?	Exempt Subnets (e.g. my IT policy)
Description:	Subnets that are exempt from user authentication.
Insert Above:	1 (Global Policy)
Membership Definition	
Membership is defined by any combination of the	following options. All criteria must be met for the policy to take effect.
Define Members by Subnet:	10.4.0.0/19, 10.4.32.0/20, 10.4.48.1-60, 10.4.48.80-255, 10.4.49.0/24, 10.4.50.0/24, 10.4.51.0/24, 10.4.52.0/22, 10.4.56.0/21, 10.4.64.0/18, 10.4.128.0/17, 10.5.0.0/16 (examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)
Define Members by Protocol:	All protocols HTTP/HTTPS Only ⑦ Native FTP Only
Define Members by Authentication:	No Authentication This option may not be valid if any preceding Identity requires authentication on all subnets.
Advanced	Define additional group membership criteria.

Step 10: In the **Define Members by Subnet** box, enter the subnet(s) that you want to allow to access the Internet without authentication.

Step 11: In the Define Members by Authentication list, choose No Authentication, and then click Submit.

Tech Tip

1

Performing this action defeats the purpose of running authentication for that IP address, and log information from Cisco WSA will never have authentication data from employees using that IP address. Even so, taking this action may be required in certain cases and is given here as an example of how to change the operational policy of Cisco WSA.

Step 12: On the Identities page, click Add Identity.

Step 13: On the Add Identity page, in the Name box, enter Exempt User Agents, and then click Advanced.

Step 14: In the Advanced section, next to User Agents, click None Selected.

Step 15: On the Membership by User Agent page, Under Common User Agents click Others.

Step 16: Under Others, select Microsoft Windows Update and Adobe Acrobat Updater.

 Tech Tip

 Selecting these agents means that when connections over HTTP with those User

 Agents in the HTTP Header are seen, no authentication is requested.

Common User Agents:	▶ Browsers					
	▽ Others					
	Microsoft Windows Update ^Windows-Update-Agent\$					
	Adobe Acrobat Updater Adobe Update Manager Acrobat SOAP					
Custom User Agents:	Enter any regular expression, one regular expression per line, to specify user agents. Use a pound sign (#) to start a comment; comments are any text added after a pound sign up to a newline and can be on the same line as the regular expression.					
	Example User Agent Patterns 🗗					
Match User Agents:	Match the selected user agent definitions					
	C Match all except the selected user agent definitions					
Cancel	Done					

Step 17: In the Custom User Agents box, enter any application that uses HTTP and is failing authentication, and then click **Done**.



Step 18: On the Identities: Add Identity page, click Submit.

Step 19: On the Identities page, at the bottom of the Client/Transaction Identity Definitions section, click **Global Identity Policy**.

This is the identity group for anybody who does not meet one of the preceding two groups you just built. Since those groups were built for the purpose of not authenticating, change the global identity to authenticate everybody else.

Step 20: On the Identity Policies: Global Group page, in the Define Members by Authentication list, choose Require Authentication.

Monitor	Web Security Manager	Security Services	Network	System Administration				
Identity Policies: Global Group								
Settings for Global P	olicy							
	Define Me	mbers by Authentication:	Require Authenticatio	n ▼				
			Select a Realm or Sec	quence:	All Realms 👻			
			Select a Scheme:		Use Basic or NTLMSSP -			
Source satisfy against for TTP/TTP only. If a user fails authentication: Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Meagers - Decrystan Prioles authorization and specific service)					Scheme setting applies to HTIPHTTPS only. Support Cleast privileges ? quent policy layers blices and Access Policies).			
	Authentication Surrogate for	Transparent Proxy Mode:	Surrogate Type: ?	IP Address				
				Persistent Cookie				
				Session Cookie				
Explicit Forward Request: T								
Cancel					Submit			

Step 21: In the Select a Realm or Sequence list, choose All Realms.

Step 22: In the Select a Scheme list, choose Basic or NTLMSSP, and then click Submit.

Step 23: Click Commit Changes.

Step 24: In the Uncommitted Changes pane, enter a comment to describe the change, and then click **Commit Changes**.

It is now possible to test the deployment to ensure that the system is enforcing policy as expected, that all applications and processes work as before, and that the data that the system is logging meets all of your needs or requirements.

August 2013

Additional Information

Monitoring

To monitor the health of Cisco WSA and the actions being taken by the appliance on traffic it is examining, there are a variety of reports available on the Monitor tab. These reports allow an administrator to track statistics for client web activity, malware types, web reputation filters, system status, and more.

Because the appliance itself stores data for only a limited amount of time, you need to use the Cisco Content Security Management Appliance in order to allow for long-term storage and reporting of events from Cisco WSA.

Consult with your Cisco account team or your trusted partner for more information on the Cisco Content Security Management Appliance and long-term reporting.

Troubleshooting

To determine why Cisco WSA took the action it did on a web connection to a specific site from a specific user, an administrator can run the Trace tool by navigating to **System Administration > Policy Trace**.

By filling out the tool, you can test a specific URL to find out what the expected response from the appliance would be if it processed the URL. This information is especially useful if some of the more advanced features are used.

Summary

You have now installed Cisco WSA. A basic configuration has been applied, and the device can be inserted into the network and receive redirects from the appliance firewall. A default policy has been built that allows an organization to set up access controls for HTTP and HTTPS. A policy has been built to configure HTTPS decryption. And authentication has been set up to allow Cisco WSA to authenticate users and tie usernames with the access controls in the logs.

A more detailed discussion about specific implementation of policy should be initiated with a trusted partner or Cisco account representative.

OO Reader Tip

For additional Cisco WSA user documentation, see the documentation here: http://www.cisco.com/web/ironport/index.html

Appendix A: Product List

Web Security

Functional Area	Product Description	Part Numbers	Software
Web Security Appliance	Cisco Web Security Appliance S370	S370-BUN-R-NA	AsyncOS 7.5.0-833

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 ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904- 40G module	CVR-CFP-4SFP10G	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 IP Services license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

Feedback

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

•1|1•1|1• CISCO

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)

B-0000345-1 08/13