

Web Security Using Cisco WSA

Technology Design Guide

August 2014 Series



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 6**
 - Configuring Cisco WSA..... 8
 - High Availability and Resilience 27
 - Additional Information..... 38
 - Monitoring 38
 - Troubleshooting 38
 - Summary 38
- Appendix A: Product List 39**
- Appendix B: Changes 41**

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

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 Design Guide



Cloud Web Security Using Cisco ASA Technology Design Guide



Remote Mobile Access Technology Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

Technology Use Case

Web access is a requirement for the day-to-day functions of most organizations. The challenge is maintaining 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 confirm that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.

One 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 exist 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" 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.

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 any remote-site networks access 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.

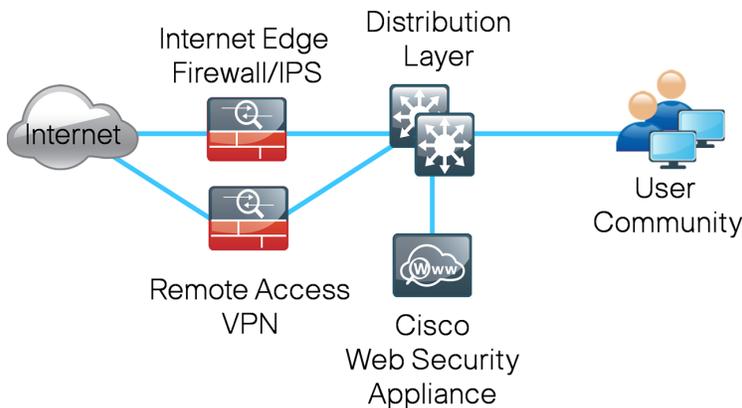
This design guide enables the following security capabilities:

- **Transparent redirection of user web traffic**—Through the 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 WSA 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.

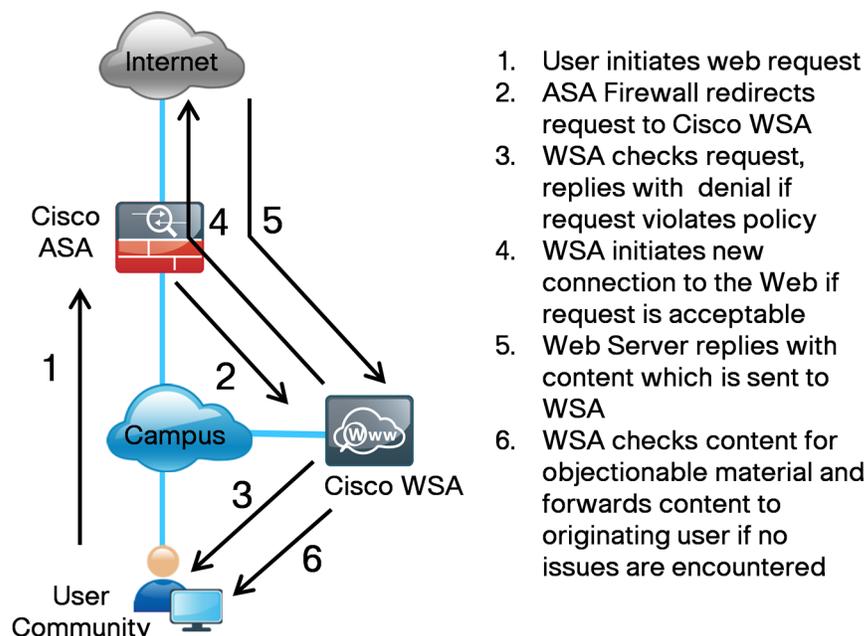
Figure 1 - Web security deployment



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 2 - Logical traffic flow using Cisco WSA



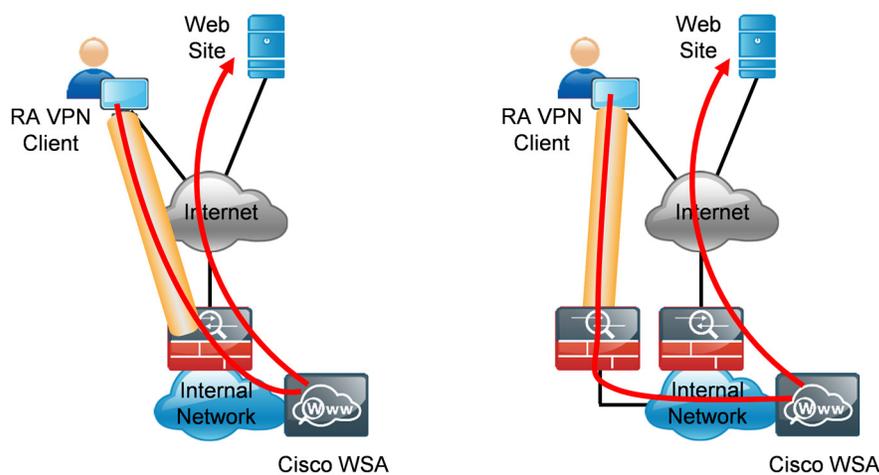
Cisco WSA is connected by one interface to the inside network of the Cisco Adaptive Security Appliance (ASA). In the Internet edge design, Cisco WSA connects to the same LAN switch as the Cisco ASA appliance and on the same VLAN as the inside interface of the appliance. Cisco ASA redirects HTTP and HTTPS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

Cisco WSA inspects the content for remote-access VPN connected users in both the integrated (seen in Figure 3 on the left) and standalone (seen in Figure 3 on the right) deployment models as described in the [Remote Access VPN Technology Design Guide](#).

Figure 3 - Web security for remote-access VPN



Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

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.

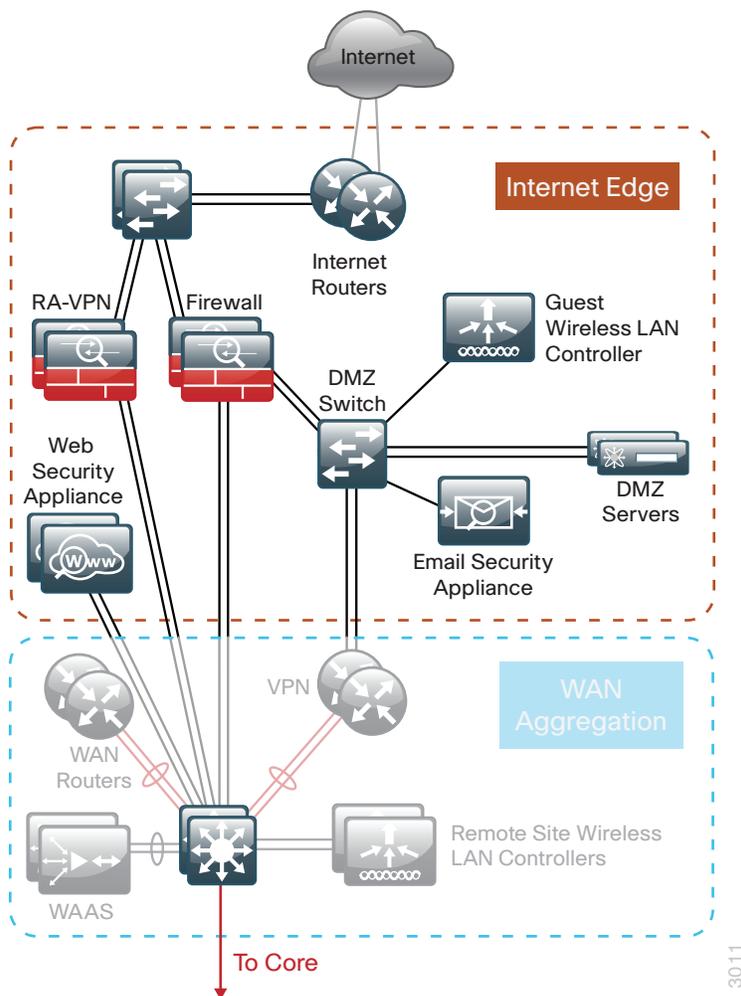
In a transparent proxy deployment, a WCCP v2-capable network device redirects all TCP traffic with a destination of port 80 or 443 to Cisco WSA, without any configuration on the client. The transparent proxy deployment is used in this design guide, and the Cisco ASA firewall is used to redirect traffic 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 the 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.

Figure 4 - Internet Edge Topology for Cisco Validated Designs



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.

Configuring Cisco WSA

1. Configure DNS entries
2. Configure the distribution switch
3. Connect to the Cisco WSA
4. Configure management access to the Cisco WSA
5. Configure DNS entry for WSA
6. Complete the System Setup Wizard
7. Install system updates
8. Install the feature keys
9. Update web usage controls and test
10. Enable logging
11. Create custom URL categories
12. Configure access policies
13. Configure WCCP on Cisco WSA
14. Configure WCCP on the firewall
15. Configure default tunnel gateway
16. Set up HTTPS proxy
17. Configure authentication

Before you begin the Cisco WSA deployment, you need to configure the DNS.

Procedure 1 Configure DNS entries

Prepare for the following configuration procedures by creating the DNS records that are required for communication. The DNS address (A) record provides a Fully Qualified Domain Name (FQDN) to IP addressing mapping and the DNS pointer record (PTR) provides an IP to FQDN mapping, also known as a reverse lookup.

Configure your internal DNS server to advertise the records listed in Table 1.

Table 1 - Example DNS A and PTR records (Internal DNS)

Fully-Qualified Domain Name	IP Address
ie-wsa-s100v.cisco.local	10.4.24.15

Procedure 2 Configure the distribution switch

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



Reader Tip

Before you continue, ensure that the distribution switch has been configured following the guidance in the [Campus Wired LAN Technology Design Guide](#).

Option 1: Switch connection to physical WSA

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

```
interface GigabitEthernet1/0/22
  description WSAs100v M1 Management interface
  switchport access vlan 300
  switchport host
  macro apply EgressQoS
  logging event link-status
  no shutdown
```

Option 2: Switch connection to virtual WSA (vWSA) within a VMware ESXi server

Step 1: Configure the interface(s) connected to the server.

```
interface GigabitEthernet1/4/20
  description IE-C220M3-2 port 2
  switchport
  switchport access vlan 300
  switchport mode access
  logging event link-status
  macro description EgressQoSOneGig
  service-policy type lan-queuing output 1P3Q8T
  no shutdown
```

Procedure 3 Connect to the Cisco WSA

Option 1: Stand-alone, physical Cisco WSA

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.

Option 2: Cisco vWSA on VMware ESXi

Step 1: Using vSphere, right-click on the server name of the vWSA and select **Open Console**.



Tech Tip

The default username is **admin**, and the default password is **ironport**.

Procedure 4 Configure management access to the Cisco WSA

```
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 "0xffffffff"): 
```

```
[255.255.255.0]> 255.255.255.224
```

```
Would you like to configure an IPv6 address for this interface (y/n)? [N]> N
```

```
Hostname:
```

```
[ironport.example.com]> WSAs100v.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]> y
```

```
Which port do you want to use for HTTP?
```

```
[8080]> 8080
```

```
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]> **y**

Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the secure service? [Y]> **y**

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

Currently configured interfaces:

1. Management (10.4.24.15/27 on Management: WSAs100v.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.

Set the default gateway for:

1. IPv4
2. IPv6

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 5 Configure DNS entry for WSA

Step 1: Prepare for the following configuration procedures by creating the DNS record required for communication with the WSA. The DNS address (A) record provides a Fully Qualified Domain Name (FQDN) to IP addressing mapping and the DNS pointer record (PTR) provides an IP to FQDN mapping, also known as a reverse lookup.

Configure your internal DNS server to advertise the record listed in Table 2.

Table 2 - Example DNS A and PTR Records for WSA

FQDN	IP address
IE-WSA-s100v.cisco.local	10.4.24.15

Procedure 6 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>).

Tech Tip

The default username is **admin**, and the default password is **ironport**.

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: IE-WSA-S100V.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)

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)**

Step 8: For the **Appliance Mode of Operation**, select the **Standard radio button**; then click **Next**.

The screenshot shows the Cisco S100V Web Security Virtual Appliance configuration interface. The page is titled "Cisco S100V Web Security Virtual Appliance" and has a progress bar with four steps: 1. Start, 2. Network, 3. Security, and 4. Review. The "System Settings" section is active, showing the following configuration:

- Default System Hostname:** IE-WSA-s100v.cisco.local
- DNS Server(s):** Use these DNS Servers (selected). The first server is 10.4.48.10. There are two optional fields for additional servers.
- NTP Server:** 10.4.48.17
- Time Zone:** Region: America, Country: United States, Time Zone / GMT Offset: Pacific Time (Los_Angeles)

The **Appliance Mode** section is also visible, with the **Standard** radio button selected. Below it, there is a description: "This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation)." The **Cloud Web Security Connector** option is also present but unselected, with a description: "This appliance will be used primarily to direct traffic to Cisco Cloud Web Security for cloud policy enforcement and threat defense (Cloud Web Security Connector installation)." At the bottom of the page, there are "Prev" and "Next" buttons.

Step 9: On the Network Context page, click **Next**.

Step 10: On the Network Interfaces and Wiring page, click **Next**. When you completed Procedure 4, "Configure management access to the Cisco WSA," you completed the necessary configuration for this page.

Tech Tip

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

Figure 5 - Appliance View of Network Interfaces

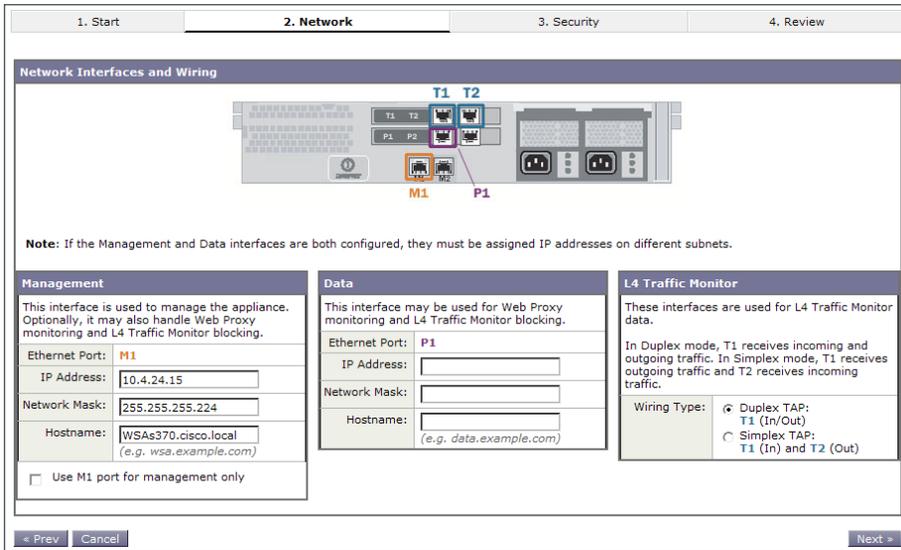
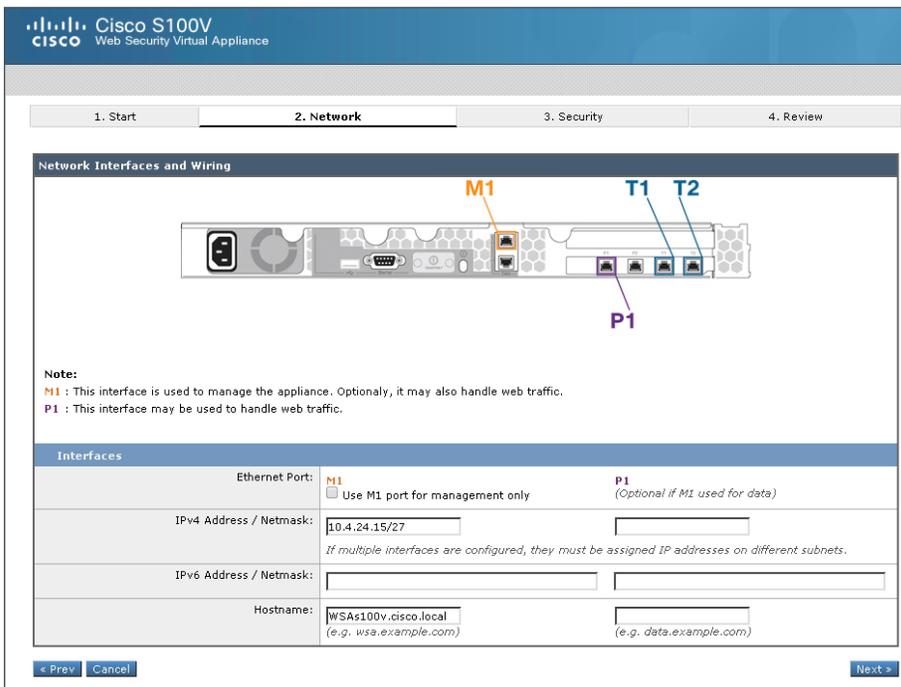


Figure 6 - Virtual WSA View of Network Interfaces



Step 11: On the Routes for Management and Data Traffic page, click **Next**. When you completed Procedure 4, “Configure management access to the Cisco WSA,” you completed the necessary configuration for this page.

Step 12: On the Transparent Connections Settings page, click **Next**.

Step 13: On the Administrative Settings page, in the **Administrator Password** box, enter and confirm the administrator password.

Step 14: In the **Email system alerts to** box, enter the administrator's email address (Example: admin@cisco.local).

Step 15: In the **Send Email via SMTP Relay Host** box, enter the internal mail server (Example: internal-exchange.cisco.local), and then click **Next**.

i Tech Tip

On this page, you can also elect to participate in the Cisco SenderBase network and select a participation level.

The screenshot shows the '2. Network' configuration page. Under 'Administrative Settings', the 'Email system alerts to' field is set to 'admin@cisco.local'. The 'Send Email via SMTP Relay Host (optional)' field is set to 'internal-exchange.cisco.local'. The 'AutoSupport' checkbox is checked. Under 'SensorBase Network Participation', the 'Network Participation' checkbox is checked, and the 'Participation Level' is set to 'Limited - Summary URL information'.

Step 16: On the Security Settings page, use the default settings, and then click **Next**.

The screenshot shows the '3. Security' configuration page. Under 'Security Settings', the 'Global Policy Default Action' is set to 'Monitor all traffic'. The 'L4 Traffic Monitor' action for suspect malware addresses is set to 'Monitor only'. 'Acceptable Use Controls', 'Reputation Filtering', and 'Cisco Data Security Filtering' are all enabled. Under 'Malware and Spyware Scanning', both 'Enable Webroot' and 'Enable Sophos' are checked, and the action for detected malware is set to 'Monitor only'.

Step 17: On the Review page, review the configuration, and then click **Install This Configuration**.

Step 18: The virtual machine will now try to re-establish the web page using the new machine name you set in this procedure. Check your DNS entries if it cannot connect.

Procedure 7 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

It is not possible to downgrade software versions, so be certain that an upgrade is desired before proceeding. It is possible that an appliance can receive different upgrade 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 8 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.



Tech Tip

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 9 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.

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

i
Tech Tip

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.

The screenshot shows the Cisco S100V Web Security Virtual Appliance interface. The top navigation bar includes Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Acceptable Use Controls" and contains two sections:

Acceptable Use Controls Settings

Acceptable Use Controls Service Status:	Enabled
Application Visibility and Control:	Enabled
Dynamic Content Analysis Engine:	Enabled
Default action for Unreachable Service:	Monitor

[Edit Global Settings...](#)

Acceptable Use Controls Engine Updates

File Type	Last Update	Current Version	New Update
Cisco Web Usage Controls - Web Categorization Engine	Success - Wed Jun 11 15:48:53 2014	3.0.0.044	Not Available
Cisco Web Usage Controls - Web Categorization URL Keyword Filters	Success - Wed Jun 11 15:48:53 2014	1312487822	Not Available
Cisco Web Usage Controls - Web Categorization Prefix Filters	Success - Wed Jun 11 16:57:56 2014	1402530766	Not Available
Cisco Web Usage Controls - Web Categorization Categories List	Success - Wed Jun 11 15:48:53 2014	1387088878	Not Available
Cisco Web Usage Controls - Dynamic Content Analysis Engine	Never Updated	2.1.0-016	Not Available
Cisco Web Usage Controls - Dynamic Content Analysis Engine Data	Success - Mon May 5 11:42:56 2014	3.1.0.003	Not Available
Cisco Web Usage Controls - Application Visibility and Control Engine	Never Updated	1.1.0-076	Not Available
Cisco Web Usage Controls - Application Visibility and Control Data	Success - Wed Jun 11 15:48:10 2014	1.1.0.21-001	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 Displayed

The host name resolution (DNS lookup) for this host name (www.not-a-site.com) has failed. The Internet address may be misspelled or obsolete, the host (www.not-a-site.com) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

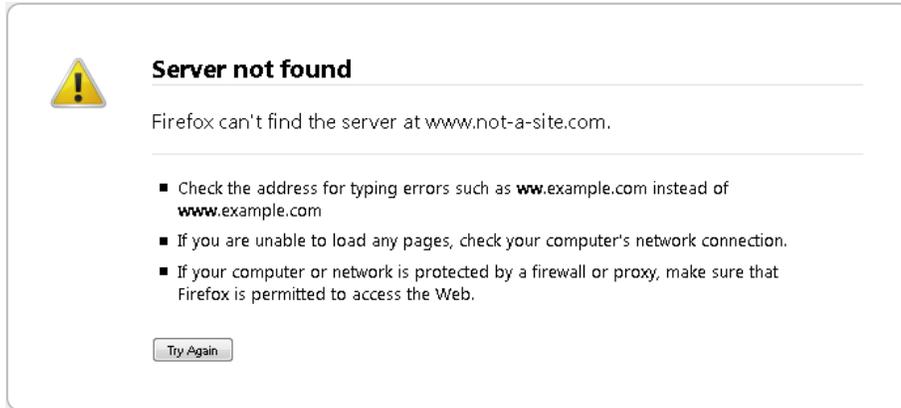
If you have questions, please contact your corporate network administrator and provide the codes shown below.

```

Date: Thu, 06 Dec 2012 19:54:22 PST
Username:
Source IP: 10.4.2.14
URL: GET http://www.not-a-site.com/
Category: Uncategorized URLs
Reason: UNKNOWN
Notification: DNS_FAIL

```

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:



Procedure 10 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 <small>(will be used to name the log directory)</small>
Rollover by File Size:	100M Maximum <small>(Add a trailing K or M to indicate size units)</small>
Rollover by Time:	None
Log Style:	<input checked="" type="radio"/> Squid <input type="radio"/> Apache <input type="radio"/> Squid Details
Custom Fields (optional):	<input type="text"/> Custom Fields Reference
File Name:	WSA-AccessLogs
Log Compression:	<input type="checkbox"/> Enable
Log Exclusions (Optional):	<input type="text"/> <small>(Enter the HTTP status codes of transactions that should not be included in the Access Log)</small>
Retrieval Method:	<input type="radio"/> FTP on WSAs370.cisco.local Maximum Number of Files: 100
	<input checked="" type="radio"/> 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 Commit. This will cause a brief interruption in service. Additionally, the authentication cache will be cleared, which might require some users to authenticate again.

Commit Changes

You have uncommitted changes. These changes will not go into effect until you commit them.

Comment (optional):

Procedure 11 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**.

Tech Tip

A placeholder URL (block.com) has to be entered because it is not possible to create a category and have it be empty. In the future, when a URL is found that needs to be blocked, add it to the list, and then delete the placeholder.

Custom URL Categories: Add Category

Edit Custom URL Category

Category Name:

List Order:

Sites:

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. example.com, .example.com, 10.1.1.1, 10.1.1.0/24)

Advanced

Regular Expressions:

Enter one regular expression per line.

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	
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 12 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.

Access Policies							
Policies							
Add Policy...							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Web Reputation and 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						
Network						
System Administration						
No Changes Pending						
Access Policies: URL Filtering: Global Policy						
Custom URL Category Filtering						
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>						
Category	Block ⊗	Redirect ↪	Allow (?) ⊕	Monitor ⊕	Warn (?) ⚠	Time-Based ⏰
	Select all	Select all	Select all	Select all	Select all	(Unavailable)
⊗ Block List	✓					—
⊕ Monitor List				✓		—
⚠ Warn List					✓	—
⊕ Allow List			✓			—
Select Custom Categories...						

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.

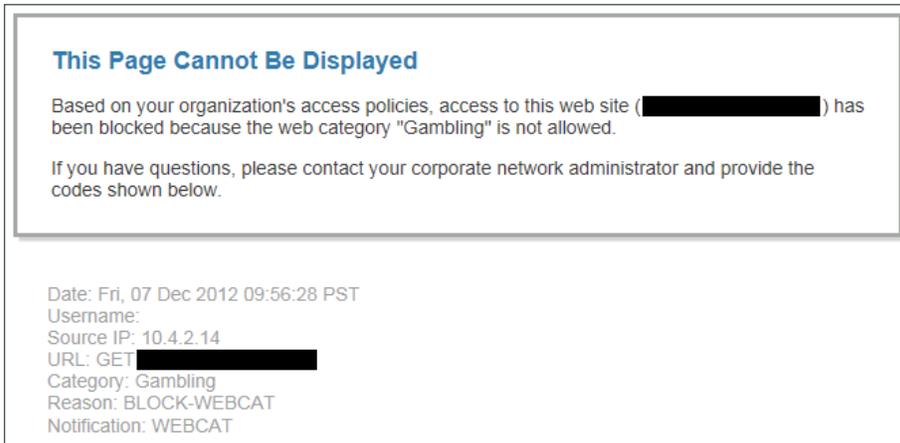
Step 7: For testing purposes, next to Gambling select **Block**, next to Sports and Recreation select **Warn**, and then click **Submit**. You may need to scroll to see all predefined URL categories.

Predefined URL Category Filtering				
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>				
Category	Block ⊗	Monitor ⊕	Warn (?) ⚠	Time-Based ⏰
	Select all	Select all	Select all	(Unavailable)
⊗ Gambling	✓			—
⚠ Sports and Recreation			✓	—

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:



Procedure 13 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**.

WCCP v2 Service

Service Profile Name:

Service:

- Standard service ID: 0 web-cache (destination port 80)
- Dynamic service ID: 0-255
 - Port numbers:
(up to 8 port numbers, separated by commas)
 - Redirect based on destination port
 - Redirect based on source port (return path)
For IP spoofing, define two services, one based on destination port and another based on source port (return path).
 - Load balance based on server address
 - Load balance based on client address
Applies only if more than one Web Security Appliance is in use.

Router IP Addresses:
Separate multiple entries with line breaks or commas.

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**.

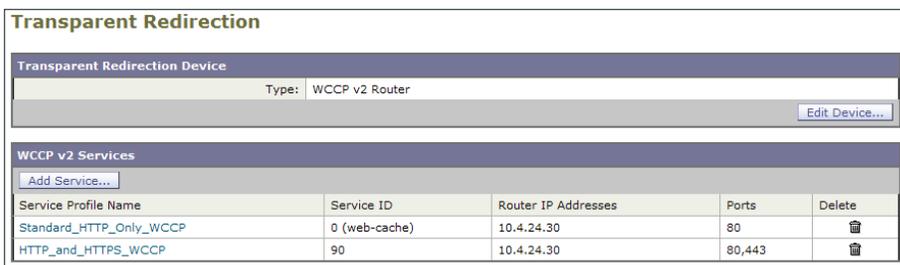
 **Tech Tip**

HTTPS proxy has not yet been set up on Cisco WSA, so if WCCP redirect were to be initiated for HTTPS immediately, those connections would fail. If the Cisco WSA or Cisco ASA deployment is live and operational and cannot have downtime, create an additional policy for just HTTP temporarily. After configuring the HTTPS policy on the Cisco WSA, change the policy used on Cisco ASA to instead reference the HTTP and HTTPS policy.

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.



Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
Standard_HTTP_Only_WCCP	0 (web-cache)	10.4.24.30	80	
HTTP_and_HTTPS_WCCP	90	10.4.24.30	80,443	

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 14 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.

 **Reader Tip**

This procedure assumes that the Internet edge firewall has already been configured following the guidance in [Firewall and IPS Design Guide](#).

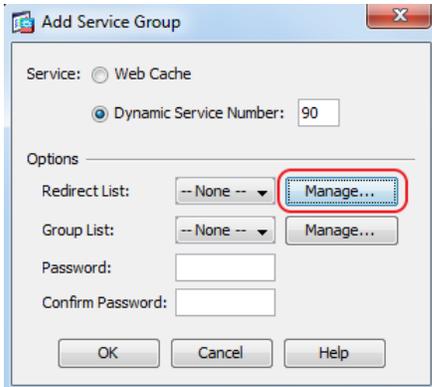
Step 1: From a client on the internal network, navigate to the firewall's inside IP address, and then launch the Cisco ASA Security Device Manager (ASDM). (Example: https://10.4.24.30)

Step 2: Navigate to **Configuration > Device Management > Advanced > WCCP > Service Groups**, and then 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 13, Step 5.

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

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



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 16 for all entries in Table 3.

Table 3 - Access control entries for WCCP redirect

Action	Source	Destination	Service	Description	Logging
Deny	any4	10.0.0.0/8	IP	Block RFC-1918 10.0.0.0/8	Enable / Default Level
Deny	any4	172.16.0.0/12	IP	Block RFC-1918 172.16.0.0/12	Enabled / Default Level
Deny	any4	192.168.0.0/16	IP	Block RFC-1918 192.168.0.0/16	Enabled / Default Level
Permit	any4	any4	IP	Permit all others	Enabled / Default Level

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

Step 10: For the **Action** option, select the action. (Example: deny)

Step 11: In the **Source** box, choose the source. (Example: any4)

Step 12: In the **Destination** box, choose the destination. (Example: 10.0.0.0/8)

Step 13: In the **Service** box, enter the service. (Example: ip)

Step 14: In the **Description** box, enter a useful description. (Example: Block RFC-1918 10.0.0.0/8)

Step 15: Select or clear **Enable Logging**. (Example: Selected)

Step 16: In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

Add ACE

Action: Permit Deny

Source Criteria

Source: any4

User:

Security Group:

Destination Criteria

Destination: 10.0.0.0/8

Security Group:

Service: ip

Description: Block RFC-1918 10.0.0.0/8

Enable Logging

Logging Level: Default

More Options

OK Cancel Help

Step 17: After adding all of the ACEs listed in Table 3, click **OK**.

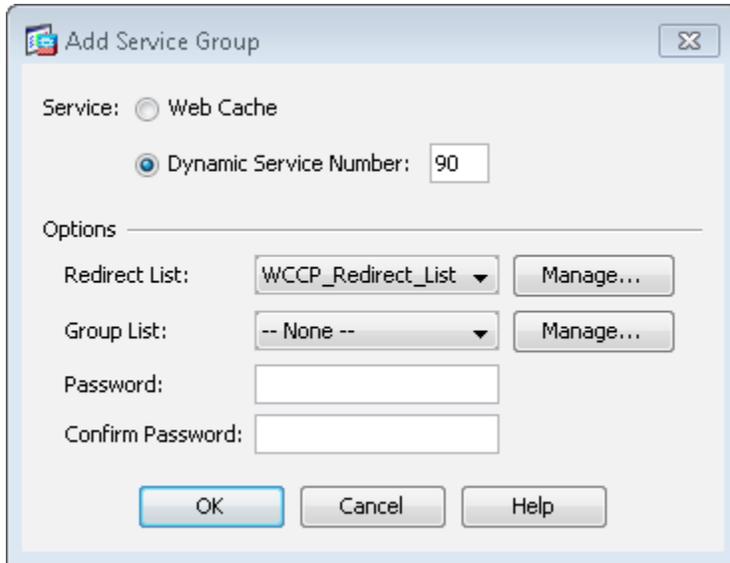
ACL Manager

#	Enabled	Source	User	Se...	Destination	Sec...	Service	Action	Logging	Time	Description
1	<input checked="" type="checkbox"/>	any4			10.0.0.0/8		ip	Deny	<input checked="" type="checkbox"/>		Block RFC-1918 10.0.0.0/8
2	<input checked="" type="checkbox"/>	any4			172.16.0.0/12		ip	Deny	<input checked="" type="checkbox"/>		Block RFC-1918 172.16.0.0/12
3	<input checked="" type="checkbox"/>	any4			192.168.0.0/16		ip	Deny	<input checked="" type="checkbox"/>		Block RFC-1918 192.168.0.0/16
4	<input checked="" type="checkbox"/>	any4			any4		ip	Permit	<input checked="" type="checkbox"/>		Permit all others

Collapse All Expand All

OK Cancel Help

Step 18: 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**.

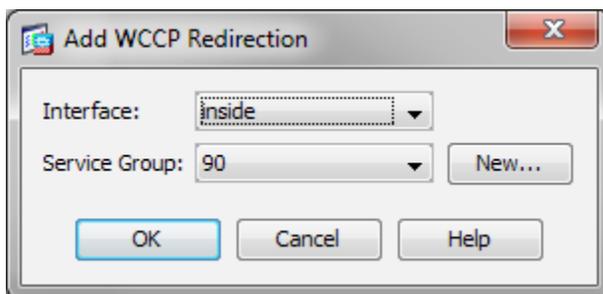


Step 19: On the Service Groups pane, click **Apply**.

Step 20: Navigate to **Configuration > Device Management > Advanced > WCCP > Redirection**, and then click **Add**.

Step 21: 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**.



Step 22: On the Redirection pane, click **Apply**.

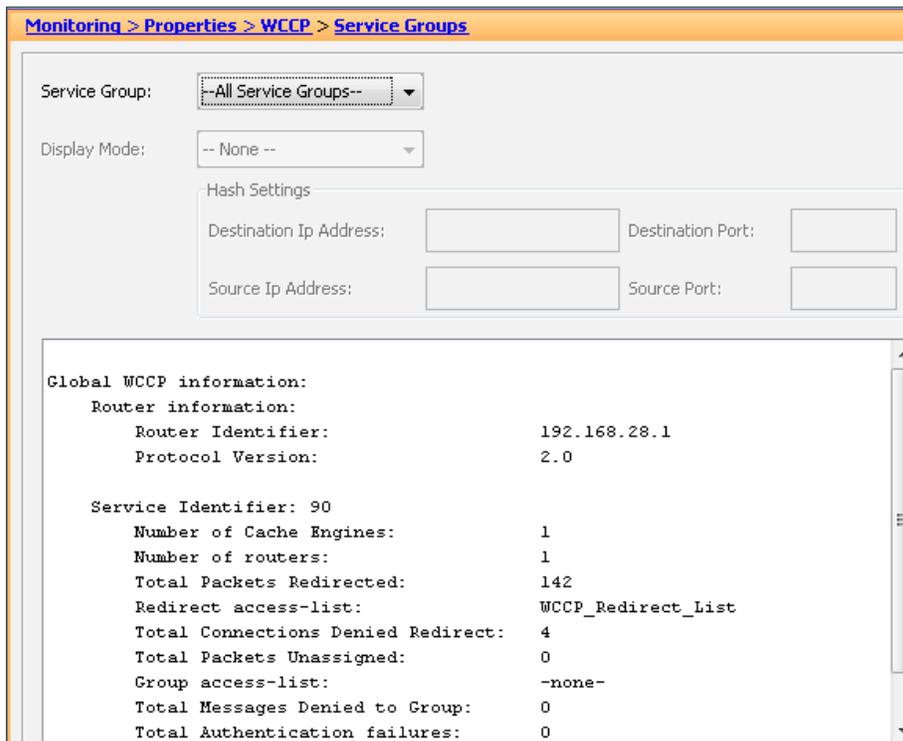
Step 23: If you want to test the configuration, use a browser that is not already configured to go to the appliance as an explicit proxy (or remove the explicit proxy settings), and test to the following sites:

- 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 24: 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.



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 15 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 16, "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)**

Add Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID: Track IP Address:

SLA ID: Target Interface:

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

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

Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: Both IPv4 only IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
inside	0.0.0.0	0.0.0.0	10.4.24.1	255	Tunneled
outside-16	0.0.0.0	0.0.0.0	172.16.130.126		Tracked ID - 1 Address - 172.18.1.1 Interface - outside-16
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 16 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**.

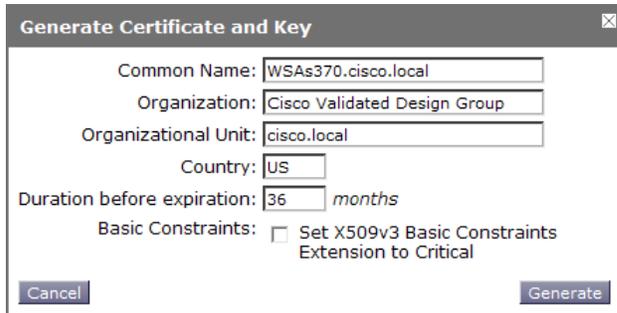
Step 2: On the HTTPS Proxy License Agreement page, click **Accept**.

Tech Tip

You need to generate a certificate for Cisco WSA to use on the client side of the proxy connection. Generating a self-signed certificate causes the client browser to warn about the certificate for each connection to an HTTPS website. To avoid this, upload a certificate that was issued from an organization's trusted certificate authority to the appliance. If the clients already have the trusted root certificate loaded on their machines, the HTTPS proxy does not generate errors related to unknown certificate authority.

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:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: Set X509v3 Basic Constraints Extension to Critical

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.

The screenshot shows the 'HTTPS Proxy Settings' configuration page. The 'Invalid Certificate Handling' section is expanded, displaying a table with the following data:

Certificate Error	Drop	Decrypt	Monitor
Expired	Select all	Select all	Select all
Mismatched Hostname			Select all
Unrecognized Root Authority			Select all
All other error types			Select all

Below the table, a note states: "No end-user notification will be provided for dropped HTTPS connections. Use this setting with caution. If the connection is not dropped, an equivalent certificate will be generated."

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 about using certificates as part of the Cisco WSA HTTPS proxy mechanism, see the *Cisco WSA End-User Guides* at http://www.cisco.com/en/US/products/ps10164/products_user_guide_list.html, or consult a trusted partner or Cisco sales representative.

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

Success — The Custom URL Category "Pass Through List" was added

Custom URL Categories

Add Custom Category...

Order	Category
1	Block List
2	Monitor List
3	Warn List
4	Allow List
5	Drop List
6	Decrypt List
7	Pass Through 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 [X]

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**.

Category	Pass Through	Monitor	Decrypt	Drop	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)
Drop list				<input checked="" type="checkbox"/>	—
Decrypt List			<input checked="" type="checkbox"/>		—
Pass through list	<input checked="" type="checkbox"/>				—

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**.

Category	Pass Through	Monitor	Decrypt	Drop	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)
Finance	<input checked="" type="checkbox"/>				—
Freeware and Shareware		<input checked="" type="checkbox"/>			—
Gambling				<input checked="" type="checkbox"/>	—

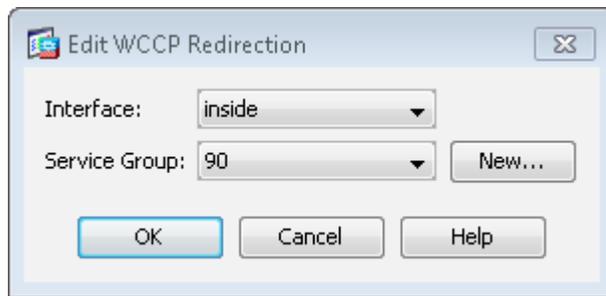
Step 23: Click **Commit Changes**.

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**.



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 17 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: From the **Authentication Server Type and Scheme** drop-down select **Active Directory**

Step 3: Specify the **Active Directory Server** and the **Active Directory Domain**, and then click **Join Domain**.

The screenshot shows the 'Add Realm' configuration window. The 'Authentication Realm' section has 'Realm Name' set to 'WSA Authentication' and 'Authentication Server Type and Scheme(s)' set to 'Active Directory (Kerberos, NTLMSSP or Basic Authentication)'. The 'Active Directory Authentication' section includes 'Active Directory Server' (with IP '10.4.48.10' entered), 'Active Directory Account' (with domain 'cisco.local' and location 'Computers' entered), and a 'Join Domain...' button. The 'Active Directory agent' section has 'Enable Transparent User Identification using Active Directory agent' checked. The 'Network Security' section has 'Client Signing Required' checked. A 'Test Current Settings' section at the bottom has a 'Start Test' button.

Step 4: 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**.

The screenshot shows the 'Computer Account Credentials' dialog box. It contains the text: 'Enter login credentials to create a computer account on your Active Directory server. These credentials are used once and will not be stored.' Below this, there are two input fields: 'Username' with 'administrator' entered and 'Password' with masked characters. At the bottom, there are 'Cancel' and 'Create Account' buttons.



Tech Tip

The DNS entries for the server must be added, and the server must have successfully joined the AD domain before proceeding.

Step 5: On the Add Realm page, click **Start Test**. This tests the NTLM connection to the Active Directory domain.

Step 6: In the Test Authentication Realm Settings box, monitor the results.



Step 7: When the test is completed successfully, click **Submit**, and then click **Commit Changes**.

Step 8: 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 9: Navigate to **Web Security Manager > Identities**, and then click **Add Identity**.

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

Step 10: On the Add Identity page, in the **Name** box, enter **Exempt Subnets**.

Identities: Add Identity

Identity Settings	
<input checked="" type="checkbox"/> Enable Identity	
Name: ?	<input type="text" value="Exempt Subnets"/> <small>(e.g. my IT policy)</small>
Description:	<input type="text" value="Subnets that are exempt from user authentication."/>
Insert Above:	1 (Global Policy)
Membership Definition	
<small>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</small>	
Define Members by Subnet:	<input type="text" value="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"/> <small>(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)</small>
Define Members by Protocol:	<input checked="" type="radio"/> All protocols <input type="radio"/> HTTP/HTTPS Only ? <input type="radio"/> Native FTP Only
Define Members by Authentication:	<input type="text" value="No Authentication"/> <small>This option may not be valid if any preceding Identity requires authentication on all subnets.</small>
Advanced <small>Define additional group membership criteria.</small>	

Step 11: In the **Define Members by Subnet** box, enter the subnet(s) that you want to allow to access the Internet without authentication.

Step 12: In the **Define Members by Authentication** list, choose **No Authentication**, and then click **Submit**.

i Tech Tip

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 13: On the **Identities** page, click **Add Identity**.

Step 14: On the **Add Identity** page, in the **Name** box, enter **Exempt User Agents**, and then click **Advanced**.

Step 15: In the **Advanced** section, next to **User Agents**, click **None Selected**.

Step 16: On the **Membership by User Agent** page, Under **Common User Agents** click **Others**.

Step 17: Under **Others**, select **Microsoft Windows Update** and **Adobe Acrobat Updater**.

i 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.

Identities: Policy "Exempt User Agents": Membership by User Agent

Advanced Membership Definition: User Agents

Common User Agents:	<ul style="list-style-type: none">BrowsersOthers<ul style="list-style-type: none"><input checked="" type="checkbox"/> Microsoft Windows Update ^Windows-Update-Agent\$<input checked="" type="checkbox"/> Adobe Acrobat Updater Adobe Update Manager Acrobat SOAP
Custom User Agents:	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div> <p><small>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.</small></p> <p style="text-align: right;">Example User Agent Patterns</p>
Match User Agents:	<input checked="" type="radio"/> Match the selected user agent definitions <input type="radio"/> Match all except the selected user agent definitions

Cancel Done

Step 18: In the **Custom User Agents** box, enter any application that uses HTTP and is failing authentication, and then click **Done**.

i Tech Tip

If it is not possible to enter the application that is failing, then a specific custom URL category can be built and then used in the **Advanced** tab for URL categories.

Step 19: On the Identities: Add Identity page, click **Submit**.

Step 20: 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 21: On the Identity Policies: Global Group page, in the **Identification and Authentication** list, choose **Authenticate Users**.

Identity Policies: Global Group

Settings for Global Policy

Identification and Authentication:

Select a Realm or Sequence:

Select a Scheme:
Scheme setting applies to HTTP/HTTPS only.

If a user fails authentication: Support Guest privileges ?

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Authentication Surrogates: ?

HTTP/HTTPS: IP Address
 Persistent Cookie
 Session Cookie
 Apply same surrogate settings to explicit forward requests

If this option is not selected, no surrogates will be used with HTTP/HTTPS explicit forward requests, and NTLM credential caching will not be available to these requests. In addition, re-authentication will not be available for Kerberos.

Native FTP: No Surrogate
 IP Address

This setting will apply to explicit forward Native FTP requests. For transparent Native FTP requests using authentication, IP address surrogate is always used.

Step 22: In the **Select a Realm or Sequence** list, choose **All Realms**.

Step 23: In the **Select a Scheme** list, choose **Use NTLMSSP or Basic**, and then click **Submit**.

Step 24: Click **Commit Changes**.

Step 25: 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.

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 Cisco ASA. 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.



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

In the following table, to determine the part number for a Cisco Web Security Premium Subscription license, use the values that you need for the term and quantity components of the part number. For example, if you need a license with a 1-year term for 5300 users, the part number would be WSA-WSP-1Y-S8.

Functional Area	Product Description	Part Numbers	Software
Web Security Appliance	WSA S370 Web Security Appliance with Software	WSA-S370-K9	AsyncOS 8.0.5-075
Web Security Virtual Appliance	Cisco Web Security Premium Subscription License	WSA-WSP-[term]-[quantity]	AsyncOS 8.0.5-075
	Term Based Subscription License - 1 year	term = 1Y	
	Term Based Subscription License - 3 year	term = 3Y	
	Term Based Subscription License - 5 year	term = 5Y	
	Quantity Based Subscription License - User Band S1 (100-199 Users)	quantity = S1	
	Quantity Based Subscription License - User Band S2 (200-499 Users)	quantity = S2	
	Quantity Based Subscription License - User Band S3 (500-999 Users)	quantity = S3	
	Quantity Based Subscription License - User Band S4 (1000-1999 Users)	quantity = S4	
	Quantity Based Subscription License - User Band S5 (2000-2999 Users)	quantity = S5	
	Quantity Based Subscription License - User Band S6 (3000-3999 Users)	quantity = S6	
	Quantity Based Subscription License - User Band S7 (4000-4999 Users)	quantity = S7	
	Quantity Based Subscription License - User Band S8 (5000-9999 Users)	quantity = S8	
	Quantity Based Subscription License - User Band S9 (10,000-19,999 Users)	quantity = S9	
	Quantity Based Subscription License - User Band S10 (20,000-49,999 Users)	quantity = S10	
	Quantity Based Subscription License - User Band S11 (50,000-99,999 Users)	quantity = S11	
Quantity Based Subscription License - User Band S12 (100,000-249,999 Users)	quantity = S12		
Quantity Based Subscription License - User Band S13 (250,000-499,999 Users)	quantity = S13		
Quantity Based Subscription License - User Band S14 (500,000-999,999 Users)	quantity = S14		
Quantity Based Subscription License - User Band S15 (More than 1,000,000 Users)	quantity = S15		

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.1(5) IPS 7.1(8p2)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	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	7.1(6)

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	15.1(1)SY IP Services feature set
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/ DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/ DFC4	WS-X6824-SFP-2T	
	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	
Modular Distribution Layer Switch	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services feature set
	Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500E 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500E 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 feature set
	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	

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We validated the deployment of Cisco WSA as a virtual appliance (vWSA).
- We upgraded Cisco WSA software to 8.0.5-075.
- We improved usability of procedures for configuring firewall policy rules

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. USERS 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.

© 2014 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)