Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

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

Web Security Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of This Guide

This supplemental deployment guide introduces the Web Security solutions.

It explains the requirements that were considered when building the Cisco Smart Business Architecture (SBA) for Government design and introduces each of the products that were selected.

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- 100-1000 connected employees
- Up to 20 branches with approximately 25 employees each
- Hosts their own web services, either locally or co-located
- IT workers with a CCNA® certification or equivalent experience

The reader may be looking for any or all of the following:

- To understand the benefits of deploying Web security
- To understand more about the Cisco Web Security solution
- To deploy Web usage control
- Web content filtering to minimize productivity loss and liability exposure for their agency
- Web content filtering to reduce malware incursion
- Reduce cost by optimizing Web bandwidth usage and improve employee productivity
- The assurance of a tested solution

Related Documents

Before reading this guide

BN — Foundation Design Overview

BN — Foundation Deployment Guide

BN — Foundation Configuration Files Guide

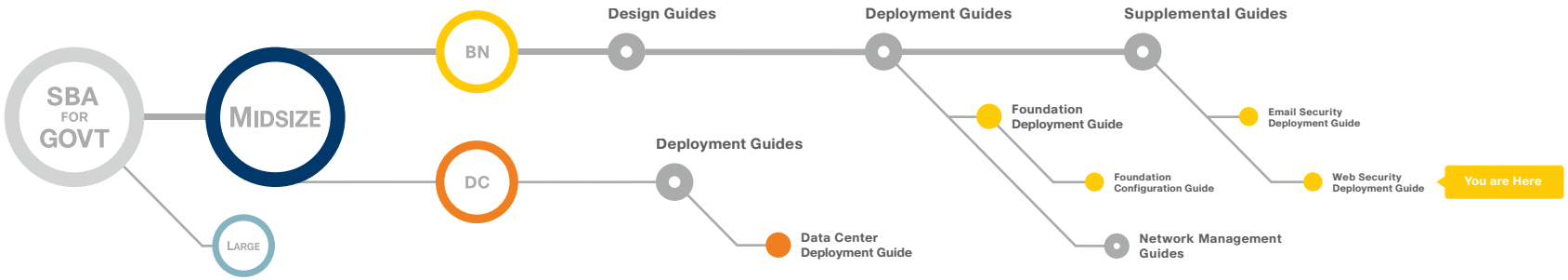


Table of Contents

Introduction

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

By deploying the Cisco SBA, your agency can gain:

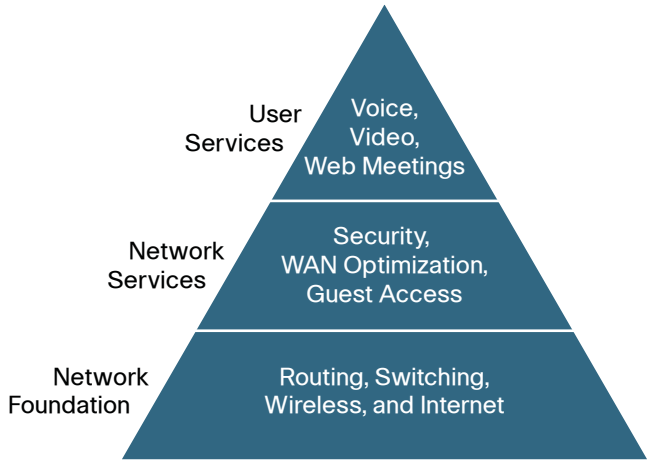
- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 branches
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- Ease of use: A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- Cost-effective: Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- Flexibility and scalability: As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- Reuse: We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.

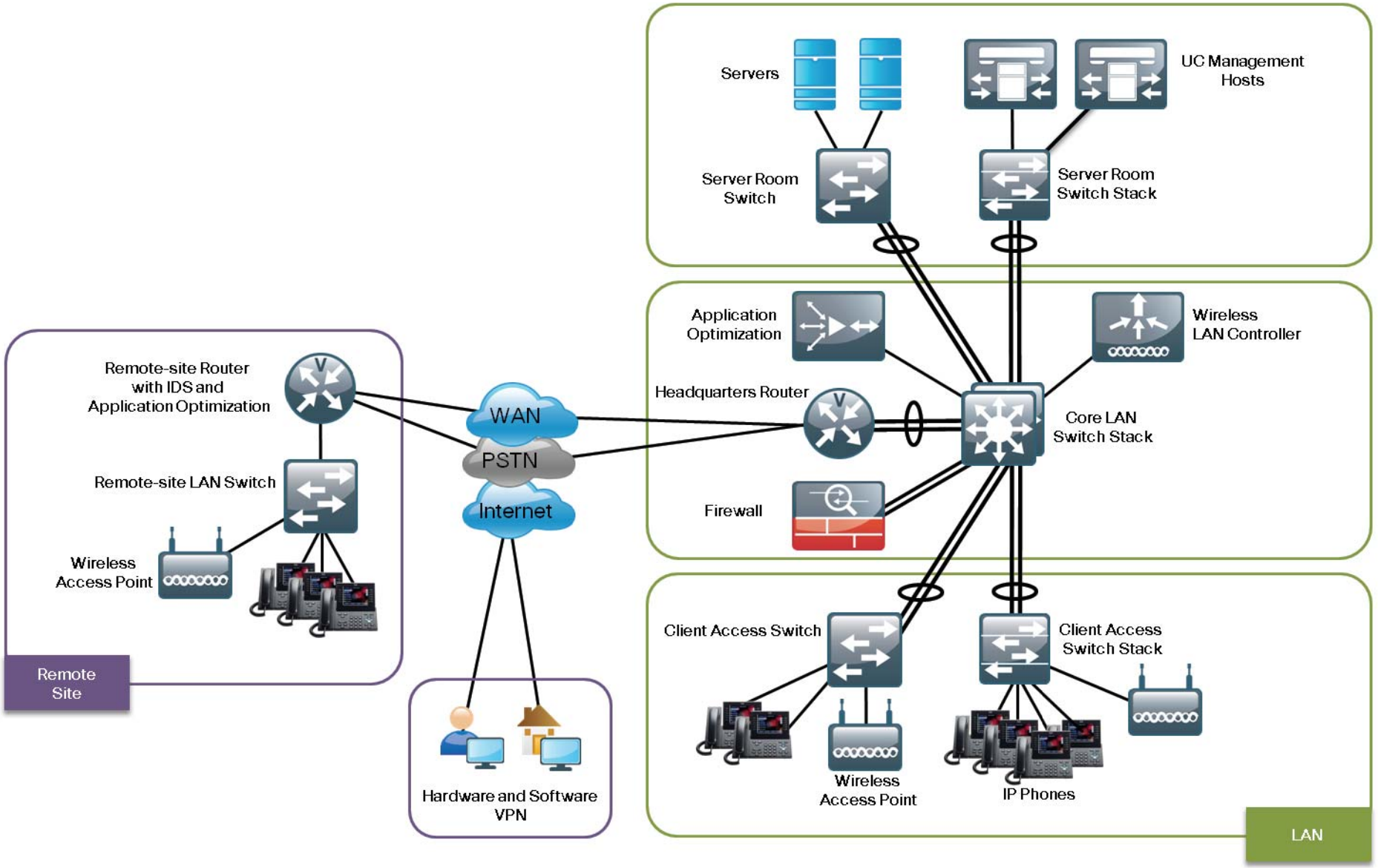
Figure 1. SBA Model



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- Network Foundation: A network that supports the architecture
- Network Services: Features that operate in the background to improve and enable the user experience without direct user awareness
- User Services: Applications with which a user interacts directly

Figure 2. Network Baseline Architecture



Web Security Basics

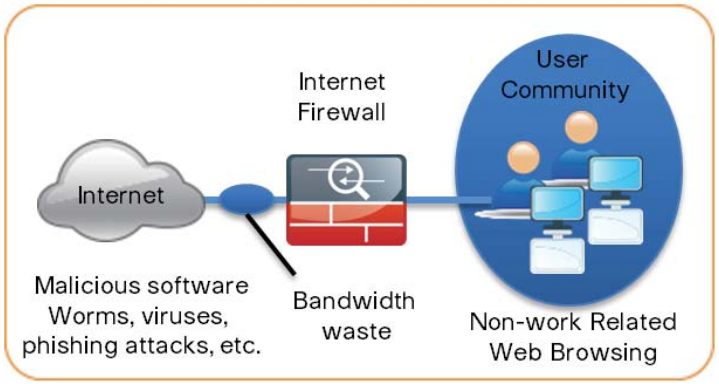
Agency Overview

Web access offers great rewards for agencies, as well as great risks.

Offering employee Web access creates two substantial risks:

- The cost of employee productivity loss browsing and bandwidth consumption.
- Threats from malicious software which can cause data leakage and liability exposure resulting from employees' access of unsavory content.

Figure 3. Reasons for Deploying WSA

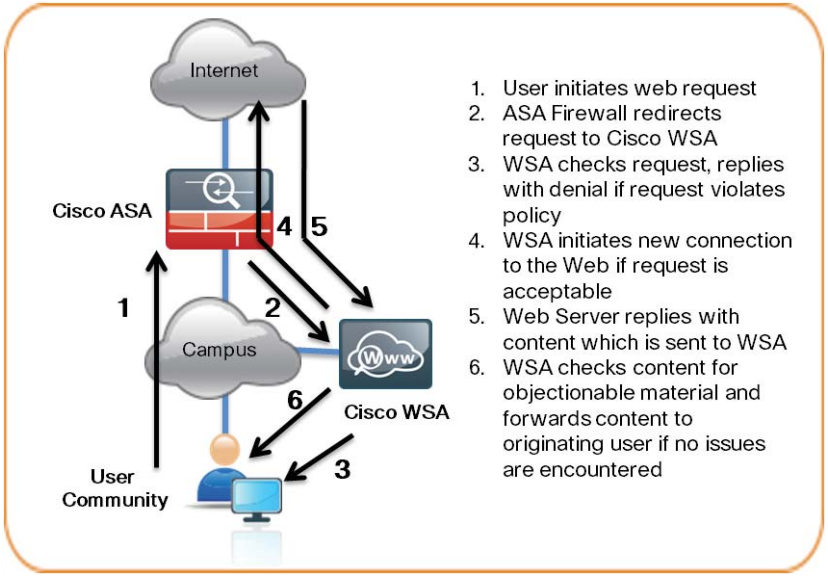


The proliferation of user-created content combined with the sheer volume of hosts on the Internet that are distributing compromised or malicious content as a result of inattention to update requirements or lax security configuration makes employees' Web access a risky proposition (Figure 3). The dynamic nature of the content on the Web makes it a tremendous challenge to maintain an up-to-date perspective of the threat profile of the whole Internet. Human-operated and worm-infested computers constantly scan the Internet in search of Web servers that they can infect in order to continue propagating their contagion to the greater Web-surfing populace.

Technology Overview

This Cisco Web Security Appliance (WSA) is a Web proxy that works with other Cisco network components to monitor and control outbound requests for Web content and scrubs return traffic for unwanted or malicious content (Figure 4).

Figure 4. Logical Traffic Flow Using WSA



Cisco Web Security Appliance (WSA) is deployed on a network using one or more interfaces that are used to forward requests and responses. Traffic can be directed to the WSA using either explicit proxies configured on the end host, or using a network protocol like WCCP running on an inline device like the perimeter firewall or router.

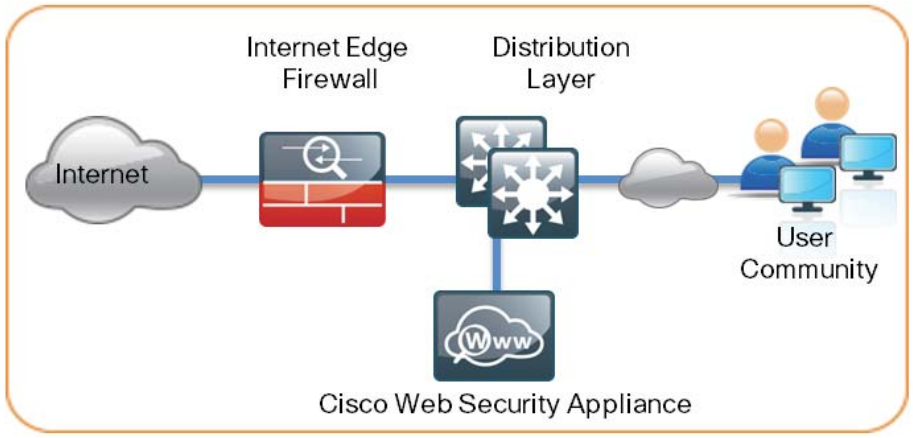
Cisco WSA uses several mechanisms to apply Web Security and Content Control.

- It begins with basic URL filtering with category-based Cisco IronPort Web Usage Controls, based on an active database comprising the analysis of sites in 190 countries in 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' Cisco security appliances that choose to participate in the Cisco SenderBase® network.

- If no details of the website or its content are known, the 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.

In the SBA Midsize architecture Cisco WSA is connected by one interface to the Cisco Adaptive Security Appliance's (ASA) inside network. In the SBA design, the Cisco WSA is con¬nected to the highly available distribution switch on the same VLAN as the inside interface of the ASA. The Cisco ASA redirects connections using the Web Cache Control Protocol (WCCP) to the WSA.

Figure 5. Web Security Deployment in the Borderless Network



Notes

Deploying the Cisco Web Security Appliance

This section details the processes you need to complete to deploy the Cisco Web Security Appliance (WSA), including:

- Preparing for WSA Deployment
- Completing the Basic Deployment
- Enabling Security Services
- Deploying WCCP
- Deploying HTTPS
- Enabling Authentication
- Maintaining the WSA

Process

Preparing for WSA Deployment

1. Plan the WSA Installation

Procedure 1 Plan the WSA Installation

Step 1: Determine how Web traffic will be sent to the WSA. This is often perceived as the most challenging portion of the WSA integration since it involves devices outside the WSA.

Since the WSA is not deployed in an inline manner where it would sit between the client and the website the client is trying to access, an alternative method to divert or redirect Web traffic to the WSA must be used. There are two possible methods to accomplish this redirection of traffic to the WSA.

Explicit Proxy Deployment

An Explicit Proxy deployment is when a client proxy-aware application, like a mature Web browser, has a configuration area within for proxy settings to declare and use a proxy, like the WSA. This method is typically combined with a Firewall restricting Web traffic that does not originate from the WSA's IP to prevent users from circumventing Web policy controls and accessing the Internet directly. From an operational standpoint, this method introduces the least amount of complications as proxy-aware applications understand what a proxy is and work with the proxy to provide the client with the requested service as opposed to the next method, which tricks the applications into using a proxy. However, from a deployment standpoint, it presents surface-level challenges as to how an administrator will configure every client with WSA proxy settings.

Explicit proxy is a good way to test the configuration of the WSA as you deploy it, as explicit mode does not depend on anything else in the network to function.

Reader Tip

There are protocols such as WPAD and PAC scripts along with tools such as Microsoft Group and System policy controls within Microsoft Active Directory (AD) to make deploying this method simpler, but this is beyond the scope of this document.

Transparent Proxy Deployment

The other deployment option is a Transparent Proxy deployment, where all port 80 (and possibly port 443) traffic is redirected to the WSA by another network device at some network choke point. This is easily accomplished using the Cisco ASA firewall (or possibly any other network device that supports WCCP v2 redirection) and is the method used in this Deployment Guide.

Tech Tip

If your user test base is small, you can manually configure each client easily without affecting your entire network, skipping the WCCP portion of this Deployment Guide.

In any case, it is always possible to use both options at the same time (explicit and transparent proxy) on the same WSA.

Step 2: Determine what type of physical topology will be used.

The WSA has 6 gigabit interfaces:

- 2 management interfaces labeled M1 and M2
- 2 traffic monitor interfaces labeled T1 and T2
- 2 proxy data interfaces labeled P1 and P2.

For this deployment guide, the WSA will combine management and proxy services onto the management interface and will not use any other interfaces. This is the most common method because it simplifies the deployment by eliminating routing complexity and only requires one IP address for the WSA.

Process

Completing Basic Deployment

1. Initial Setup with Out-of-Band Configuration
2. Initial Configuration with the Setup Wizard
3. Configure System Updates
4. Configure Feature Keys

In order to complete the basic deployment, complete the initial setup, including the out-of-band configuration as necessary. Then configure the system and feature keys, both of which require the WSA to have HTTP/S Internet access.

Procedure 1 Setup with Out-of-Band Configuration

This procedure is only required if a PC cannot be connected directly to the WSA to perform the System Setup Wizard and need to change the default IP information to allow remote network access.

Step 1: To change the default network settings via a serial console port, connect using a standard null modem cable with the terminal emulator settings of 8-1-none 9600 baud.

Step 2: Once connected and logged in, run "**interfaceconfig**" and "**setgateway**" to change the basic network settings. Issue the command "**commit**" to have your changes saved and placed into the running configuration.

Step 3: Enter a hostname. This configured hostname for the WSA needs to be fully resolvable forwards/reverse as well as in short form within your DNS system. It is important to enter this information correctly.

Step 4: Enter the following text at the command line:

```
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]> 192.168.31.240
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.0
Hostname:
[ironport.example.com]> websec1.cisco.local
Do you want to enable FTP on this interface? [Y]>
Which port do you want to use for FTP? [21]>
Do you want to enable SSH on this interface? [Y]>
Which port do you want to use for SSH?
[22]>
Do you want to enable HTTP on this interface? [Y]>
Which port do you want to use for HTTP?
[8080]>
Do you want to enable HTTPS on this interface? [Y]>
Which port do you want to use for HTTPS?
[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]>
Both HTTP and HTTPS are enabled for this interface, should
HTTP requests redirect to the secure service? [Y]>

Currently configured interfaces:
1. Management (192.168.31.240/24 on Management: websec1.cisco.
local)
```

```
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
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 Gatetway
2. Data Default Gateway
[]> 1
Enter new default gateway:
[ ]> 192.168.31.1
ironport.example.com> commit
Please enter some comments describing your changes:
[]> basic setup
```

Step 5: After configuring, you should be able to ping devices on the network, assuming appropriate network access has been created (on the firewall if needed). This is the WSA pinging its default gateway:

```
websec1.cisco.local> ping 192.168.31.1
Press Ctrl-C to stop.
PING 192.168.31.1 (192.168.31.1): 56 data bytes
64 bytes from 192.168.31.1: icmp_seq=0 ttl=255 time=0.678 ms
64 bytes from 192.168.31.1: icmp_seq=1 ttl=255 time=0.524 ms
64 bytes from 192.168.31.1: icmp_seq=2 ttl=255 time=0.522 ms
^C
--- 192.168.31.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.522/0.575/0.678/0.073 ms
```

Procedure 2 Initial Configuration with Setup Wizard

If the install procedures allow a PC to connect directly to the WSA via its default IP, then use the System Setup Wizard. It is best to only perform the minimal configuration through the System Setup Wizard as possible, leaving the most advanced configurations to their respective sections in the UI. Therefore, this procedure covers only the basic network settings, DNS information, time settings, and username/password information.

Tech Tip

If the installation procedures require the WSA to be rack mounted in a remote room and initial configuration to be performed remotely using an out-of-band connection such as serial, preconfigure the WSA with basic network settings explained in Procedure 1 before performing this procedure.

Step 1: Access the WSA's Graphical User Interface (GUI) through a Web browser.

The default username and password is admin / ironport.

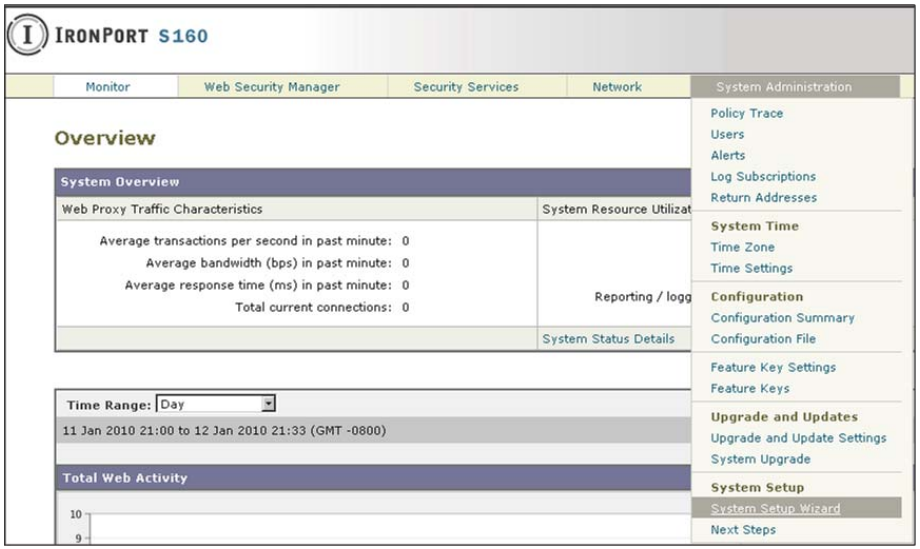
Step 2: If the WSA's default network settings have not been changed, then prepare to connect the WSA directly with your PC by plugging into the WSA's M1 NIC and configuring your PC with an IP in the 192.168.42.x network range (all the NICs on the WSA are all gigabit so a cross-over cable is not necessary), or put them both on the same network (Layer 2 connectivity). The default WSA IP address is 192.168.42.42.

Step 3: Access the WSA's GUI by opening a browser and browsing to the WSA via https, the address of the WSA, and port 8443: https://192.168.42.42:8443.

If you are unable to connect, ping the WSA's address to test connectivity. A ping failure could indicate a problem either on the PC, network, routing, or that the WSA's IP address has been changed. Another good way to troubleshoot is by connecting to the WSA's serial port.

Step 4: After logging in, the System Setup Wizard should immediately start walking you through the initial system setup. If not, or if you would like to start over with a clean install, you can access the wizard by clicking **System Administration > System Setup Wizard** (Figure 6).

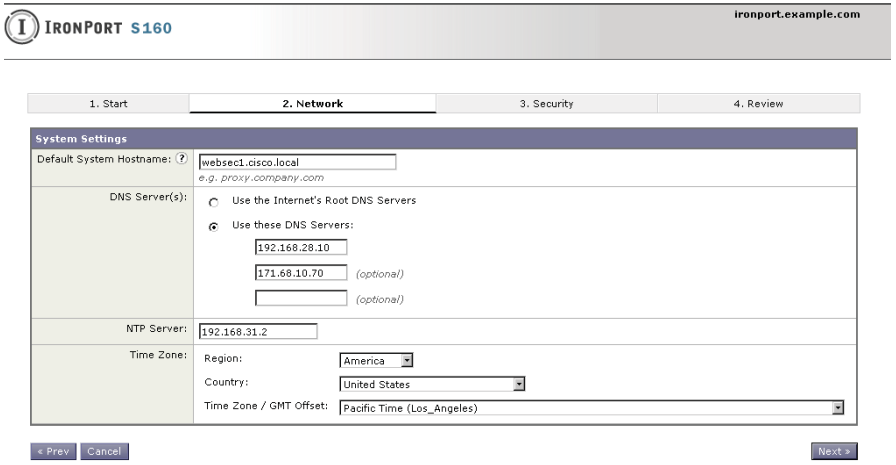
Figure 6. System Setup Wizard



Step 5: Read the license and accept, then select the **Begin Setup** button.

Step 6: The Network System Settings panel sets up DNS and time. NTP is used because effective security practices require a constant time reference throughout a network (Figure 7).

Figure 7. Network System Settings



Tech Tip

Though not needed in this deployment, Network Context will let you set up additional upstream proxies.

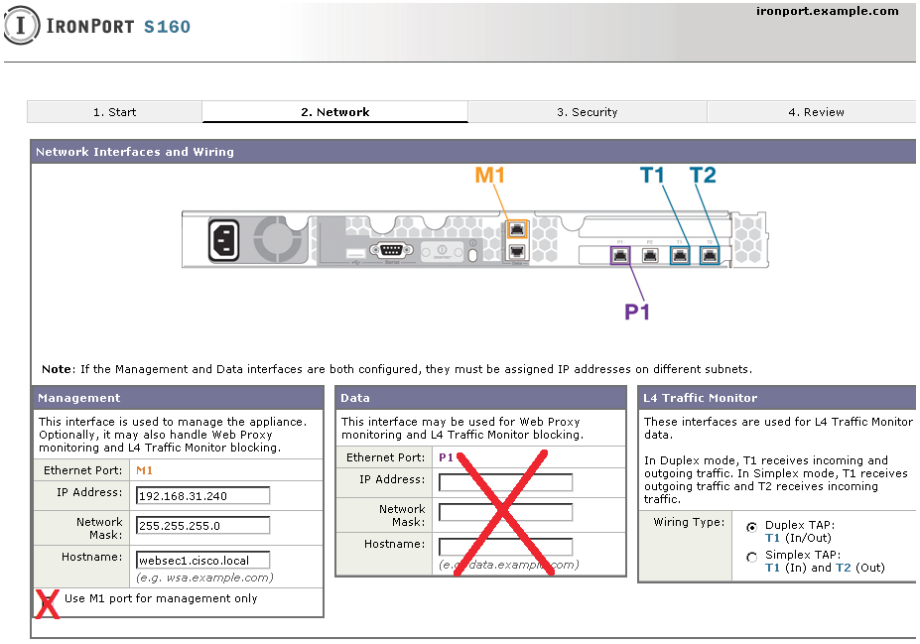
Step 7: Network Interfaces and Wiring sets up which ports will be used and what IP addresses are used on each port (Figure 8).

This deployment uses M1 for both management and proxy services.

Input the IP address, netmask, and hostname as shown.

Do not check the "Use M1 for Management only" box and do not use interface P1.

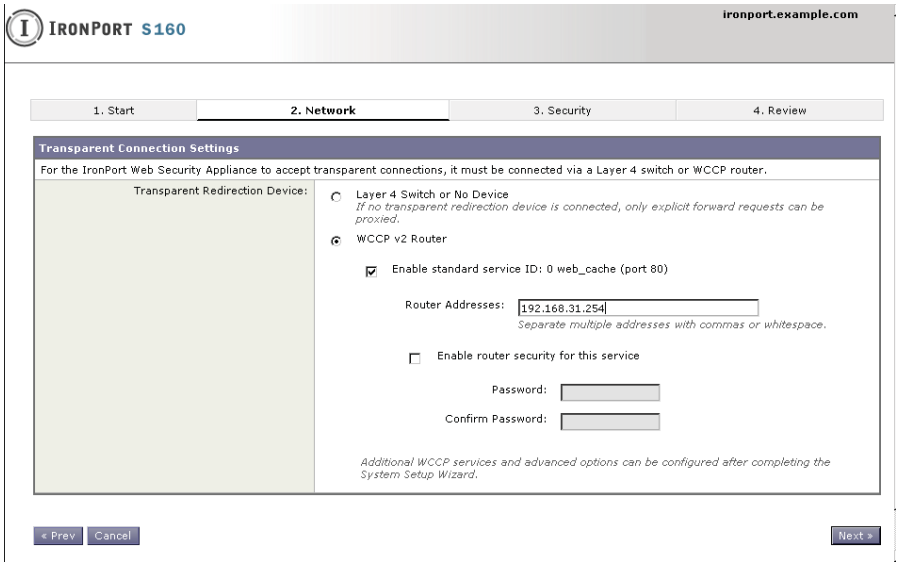
Figure 8. Network Interfaces and Wiring



Step 8: Routes for Management and Data Traffic (not shown here) displays the current Gateway information and allows entry of any static routes that might be needed. In this deployment, the only data displayed here is the gateway information you entered at the CLI earlier. Click **Next**.

Step 9: Transparent Connection Settings is where the WCCP configuration is defined. Only an HTTP service is built by default. Skip this for now by clicking **Next**. You will modify this later to redirect HTTPS as well (Figure 9).

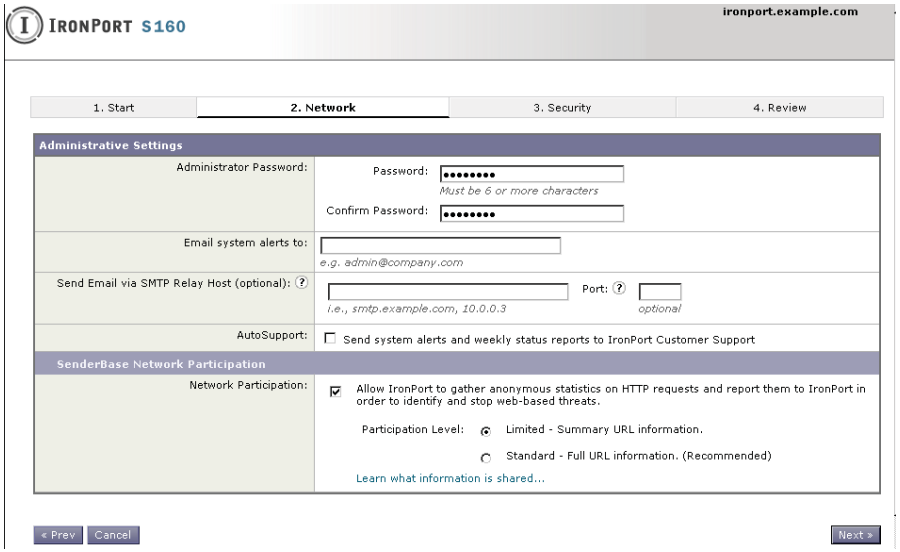
Figure 9. Transparent Connection Settings



Step 10: Administrative Settings is where the admin password can be set up. It is also where SenderBase Network Participation is defined. This is how the administrator controls if data is fed back into SenderBase and if so, what type of data (Figure 10).

Enter the Administrator Password for the appliance. Click **Next**.

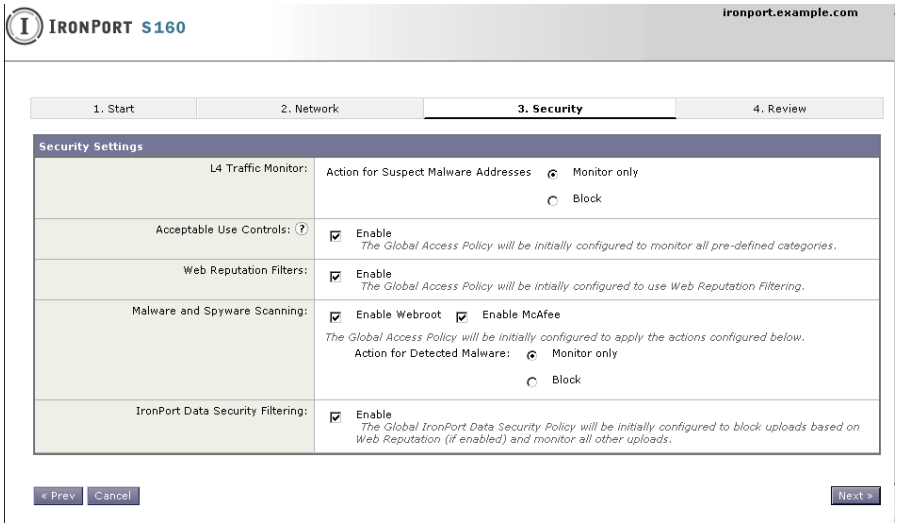
Figure 10. Administrative Settings



Step 11: The Security Settings page defines the security policy for the appliance and what actions will be taken for the different security features. The default configuration is fairly common as it leaves the appliance in Monitor only mode for Malware and Spyware Scanning (Figure 11).

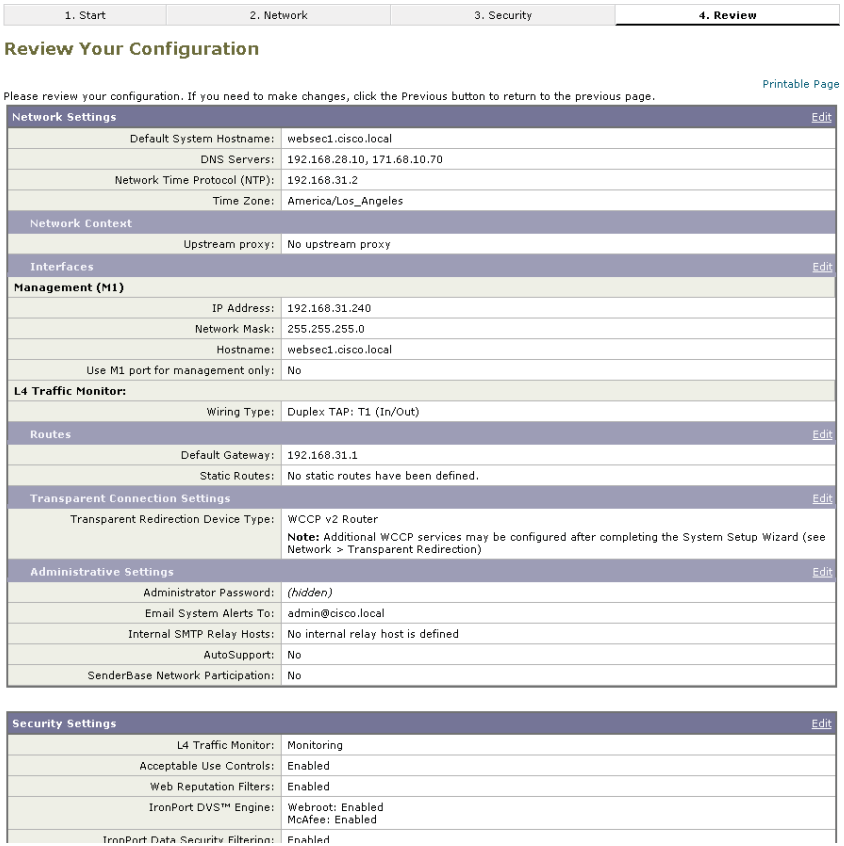
Press **Next** as no changes are required.

Figure 11. Security Settings



Step 12: Review your configuration to ensure it is correct before applying it (Figure 12). Then select the **Install this Configuration** button.

Figure 12. Review



Step 13: After installation, a reconnect will be needed if the IP address is changed from default. If you changed your laptop address to connect to the WSA, you will need to change it back to an appropriate setting in your network to reconnect to the WSA.

Procedure 3 Configure System Updates

If newer software versions are available, they should be selected and installed. In general, all upgrades should be installed. Each upgrade will usually require a reboot of the appliance, so it can take some time.

Step 1: To upgrade the code on the appliance, select the **System Administration-> System Upgrade** button. This will display the current software version.

Step 2: Select the **Available Updates** button to see what newer updates are available.

It is also possible to upgrade from the console. Run the upgrade command until the following message appears, indicating no new upgrades are available:

```
websec1.cisco.local> upgrade
No available upgrades.
```

Procedure 4 Configure Feature Keys

Step 1: Access **System Administration> Feature Keys**. This section is where the license keys for the different features on the box are displayed.

Step 2: To check to see whether your box has any licenses that are not currently enabled, select the **Check for New Keys** button. This will instruct the WSA to make a connection to the license service and 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, that there will be missing feature keys. Figure 13 shows what an evaluation appliance feature key display might look like:

Figure 13. Feature Keys

Feature Keys

Feature Keys for Serial Number: 00219BFC150B-62PKTH1

Description	Status	Time Remaining	Expiration Date
IronPort Web Proxy & DVS™ Engine	Active	27 days	Sun Mar 7 09:37:48 2010
IronPort L4 Traffic Monitor	Active	27 days	Sun Mar 7 09:37:55 2010
IronPort Web Reputation Filters	Active	264 days	Fri Oct 29 19:14:54 2010
Cisco IronPort Web Usage Controls	Active	27 days	Sun Mar 7 09:40:17 2010
IronPort URL Filtering	Active	264 days	Fri Oct 29 19:14:54 2010
McAfee	Active	264 days	Fri Oct 29 19:14:54 2010
IronPort HTTPS Proxy	Active	27 days	Sun Mar 7 09:37:21 2010
Webroot	Active	264 days	Fri Oct 29 19:14:54 2010

Pending Activation

No feature key activations are pending.

Check for New Keys

Note that some of the keys have less than 30 days remaining. This indicates a possible Evaluation Appliance. A user-purchased box will have approximately one or more years of remaining time.

Also note that the keys include one labeled "Cisco IronPort Web Usage Controls." This is a feature that was added to the appliance in some of the most recent software release versions, and if your box came with code that was before this feature was added, you will not have a key for it.

Step 3: If your appliance is missing keys or the duration of the keys is not correct, please contact your trusted Partner or Cisco reseller to resolve the issue. Please have your appliance serial number handy (at the top of the Feature Key page).

Process

Enabling Security Services

1. Turn on Web Usage Controls
2. Test the WSA
3. Configure Logging
4. Set up Custom URL Categories
5. Define Access Policiies
6. Define Web Reputation and Anti-Malware Settings

Procedure 1 Turn on Web Usage Controls

The first step in actually enabling security services on the box is to turn on the Web usage controls.

Step 1: Access **Security Services > Acceptable Use Controls**.

Step 2: Select the **Edit Global Settings** button.

Step 3: Change the "Ironport URL Filters" to "Cisco Ironport Web Usage Controls".

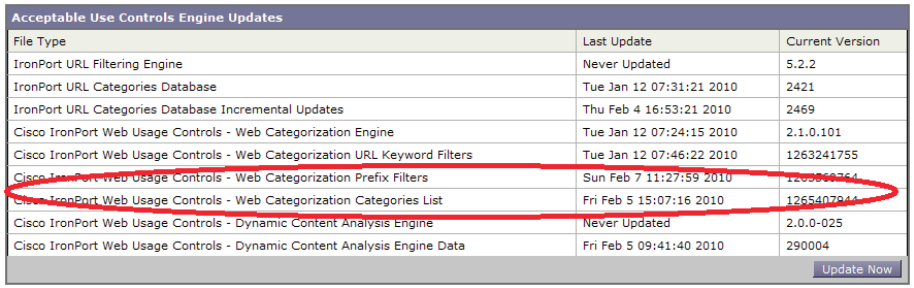
Step 4: Select the **Enable Dynamic Content Analysis Engine** button.

Step 5: Submit and then commit the changes.

Step 6: On the Acceptable Use Controls main page are listed the Acceptable Use Controls Engine Updates.

Select the **Update Now** button and wait until the page reports back success. Ensure that at least some of the controls have an update that is current or very nearly so. Due to randomness of update schedules, it is impossible to know when updates will come out for each section. The Web Prefix Filters and the Web Categories List tend to get updated fairly often and are good bets for recent update histories (Figure 14).

Figure 14. Engine Updates



Acceptable Use Controls Engine Updates

File Type	Last Update	Current Version
IronPort URL Filtering Engine	Never Updated	5.2.2
IronPort URL Categories Database	Tue Jan 12 07:31:21 2010	2421
IronPort URL Categories Database Incremental Updates	Thu Feb 4 16:53:21 2010	2469
Cisco IronPort Web Usage Controls - Web Categorization Engine	Tue Jan 12 07:24:15 2010	2.1.0.101
Cisco IronPort Web Usage Controls - Web Categorization URL Keyword Filters	Tue Jan 12 07:46:22 2010	1263241755
Cisco IronPort Web Usage Controls - Web Categorization Prefix Filters	Sun Feb 7 11:27:59 2010	1265560764
Cisco IronPort Web Usage Controls - Web Categorization Categories List	Fri Feb 5 15:07:16 2010	1265407944
Cisco IronPort Web Usage Controls - Dynamic Content Analysis Engine	Never Updated	2.0.0-025
Cisco IronPort Web Usage Controls - Dynamic Content Analysis Engine Data	Fri Feb 5 09:41:40 2010	290004

Update Now

Procedure 2 Test the WSA

The WSA can now be tested for functionality.

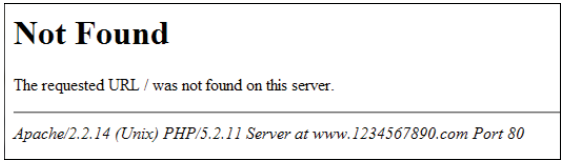
Step 1: Set up a client on the inside of the network with the WSA as the explicit proxy in the Web browser of your choice.

Step 2: Use the IP address of the WSA as the proxy and set the port to 3128.

Step 3: You will test two different addresses, one that is resolvable externally, for instance www.cisco.com, which should return without issue. This proves the client has Internet access, hopefully going through the WSA. The other address should be something not resolvable externally, like www.1234567890.com. This request should return an error from the WSA, not the browser; proving the WSA is serving content.

Firefox will return an error like the one below (Figure X).

Figure 15. Browser Error



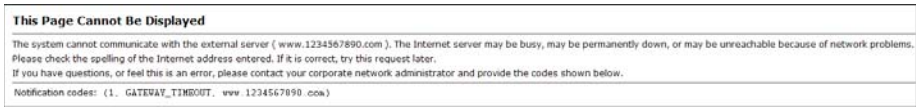
Not Found

The requested URL / was not found on this server.

Apache/2.2.14 (Unix) PHP/5.2.11 Server at www.1234567890.com Port 80

The WSA will return an error like the one below (Figure 16).

Figure 16. WSA Error



This Page Cannot Be Displayed

The system cannot communicate with the external server (www.1234567890.com). The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.
Please check the spelling of the Internet address entered. If it is correct, try this request later.
If you have questions, or feel this is an error, please contact your corporate network administrator and provide the codes shown below.

Notification codes: (1, GATEWAY_TIMEOUT, www.1234567890.com)

Procedure 3 Configure Logging

To monitor Web Usage, the appliance stores client access data for a relatively short duration, rotating logs for space reasons.

Tech Tip

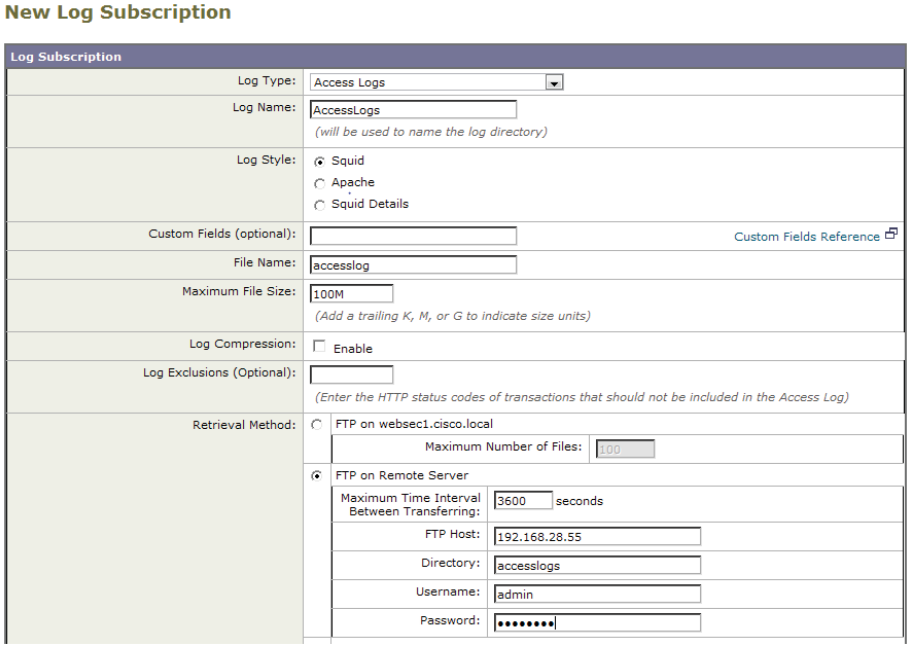
If you require long-term compliance reporting, look into the Cisco software solution called Sawmill for IronPort. This software is either an add-on for the larger installations or comes bundled in the package for smaller purchases. This guide does not cover the installation or use of the Sawmill product. Refer to the Sawmill product literature.

Step 1: For the Sawmill reporting product to work, the WSA needs to send its logs to an FTP server where the Sawmill product can access them. For this deployment, we assume you have an FTP server already deployed and configured.

Apply the configuration to move the log access logs (Figure 17) off the WSA to your ftp server:

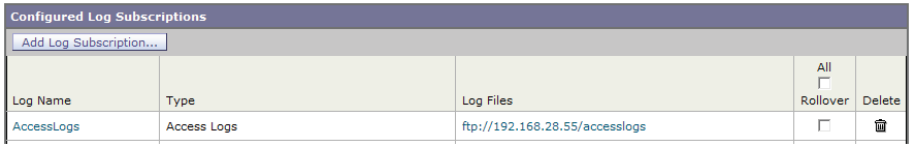
```
System Administration -> Log Subscriptions
   Add Log Subscription
```

Figure 17. Log Subscriptions



Step 2: Verify that your subscription looks like the information below (Figure 18).

Figure 18. Configured Subscriptions



Procedure 4 Set Up Custom URL Categories

Now set up the standard custom URL categories that most administrators find necessary to implement their desired URL filtering.

Step 1: Access **Web Security Manager > Custom URL Categories**.

Step 2: Select **Add Custom Category**

Step 3: Add four placeholders for the four different action exceptions that you might want to put URLs into. To do this, create four different Custom URL Categories starting with one titled "Block List".

You will have to enter a placeholder URL (block.com) because you cannot create a category and have it be empty. Once you find a URL you wish to block and add it to each list, you can delete the placeholder (Figure 19).

Figure 19. Adding Custom Category

Step 4: Now create three more lists using these three titles: Monitor List, Warn List, and Allow List. You should end up with an ordered list of custom categories.

Step 5: Commit Changes.

Procedure 5 Define Access Policies

Now that you have created the Custom Categories, enable them for use and define actions for each. This is where you will implement your web acceptable use policy as defined by your agency's Acceptable Use Policy, which can include the category of the URL (adult, sports, streaming media), the action desired (monitor, warn, or block), and whether a time-based factor is involved.

Step 1: Access **Web Security Manager > Access Policies**.

Step 2: Click on the link beneath URL Categories header.

Step 3: Click the **Include** button for each of the four custom categories (Figure 20) you created earlier and change each action to match the category (change Block List to have the Block action, Monitor List to Monitor, etc.).

Figure 20. Custom Category Actions

Access Policies: URL Categories: Global Policy

Custom URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

	Redirect	Allow	Monitor	Warn	Block	Time-Based
View: Included Categories Only | **All Categories**	Select all	Select all	Select all	Select all	Select all	(Unavailable)
Block List [Exclude]					✓	–
Monitor List [Exclude]			✓			–
Warn List [Exclude]				✓		–
Allow List [Exclude]		✓				–

Step 4: For testing purposes, change one of the predefined categories to Block to allow us to test the deployment (Figure 21). For example, change Gambling from Monitor to Block.

You will also use this section to implement your agency's Web access policy for acceptable use.

Figure 21. Figure 21. URL Category Actions

Freeware and Shareware	✓			–
Gambling			✓	–
Games	✓			–

Step 5: Commit all changes.

Step 6: To test these changes using the browser which is explicitly pointing to the WSA Appliance, try browsing to www.gambling.com.

The WSA should return the message shown in Figure 22.

Figure 22. Blocked Website

This Page Cannot Be Displayed

Based on your corporate access policies, access to this web site (http://www.gambling.com/) has 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.

Notification codes: (1, WEBCAT, BLOCK-WEBCAT, 0x0000062a, 1265572921.083, AAAEGQAAAAAAAAAAAlv8AEP8AAABAAAAAAAAAAQ==, http://www.gambling.com/)

Procedure 6 Define Reputation & Anti-Malware Settings

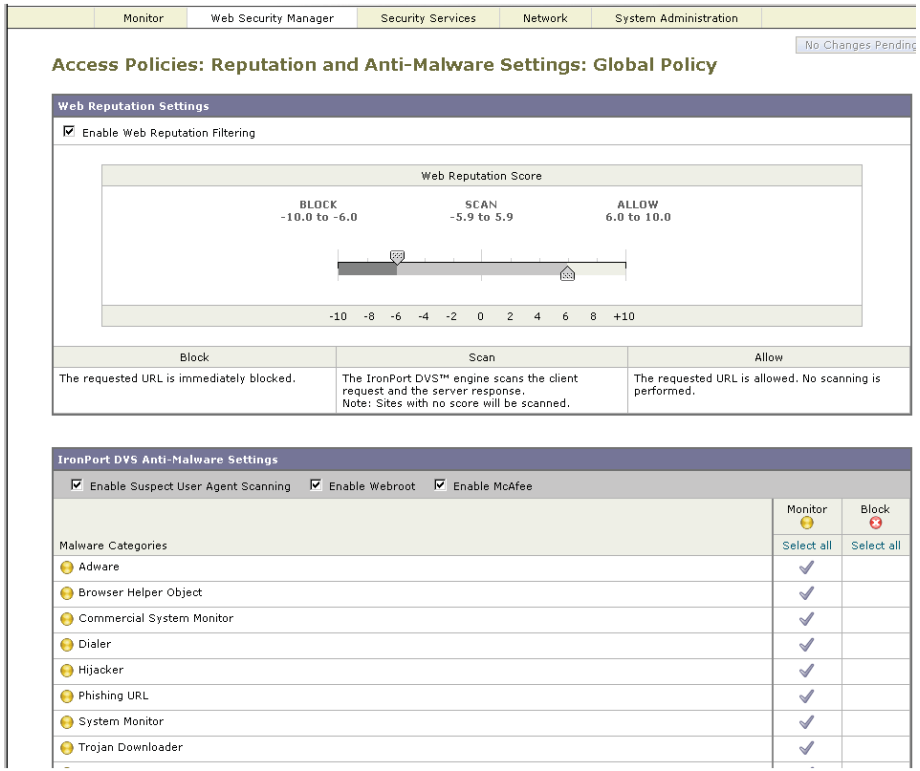
Reputation can range from –10 as the worst to +10 being completely trustworthy.

- By default, websites having a –6 or worse reputation are automatically blocked preventing possibly infected content from being brought back into the network from such sites.
- Sites with reputations between –5.9 and +5.9 trigger the WSA to scan the client request and the server response using the Cisco IronPort DVS Engine which looks for attacks like phishing, malware, viruses, and worms. By default, the security policy is not set up to block these if detected. This page (Figure 23) is where those changes would be implemented if your agency's security policy requires it.
- URLs with a reputation score higher than 6.0 are passed without scanning by default.

Step 1: Navigate to **Web Security Manager >Access Policies** and click on the link called **enabled** underneath the Web Reputation header.

This takes you to the area where Web Reputation and Anti Malware settings can be changed.

Figure 23. Web Reputation and Anti-Malware Settings



Process

Deploying WCCP

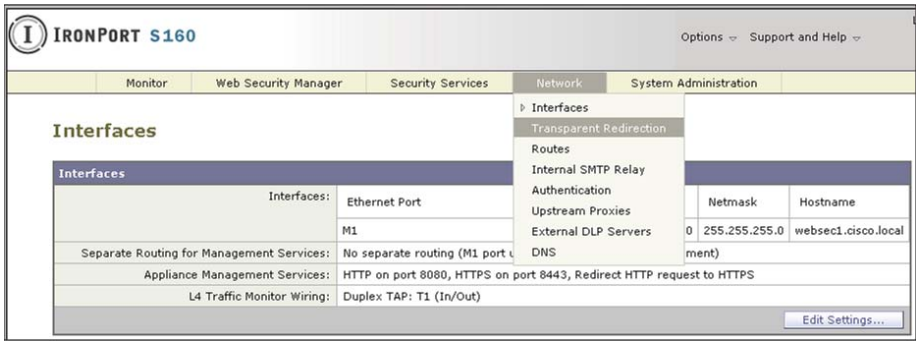
1. Configure WCCP on the WSA
2. Configure WCCP on the Firewall
3. Test Configuration

Procedure 1 Configure WCCP on the WSA

Now that the WSA is working and applying an access policy for HTTP traffic, implement WCCP on the WSA and the ASA firewall to allow the WSA to begin to receive traffic directly from the ASA instead of having browsers configured to use the WSA as an explicit proxy.

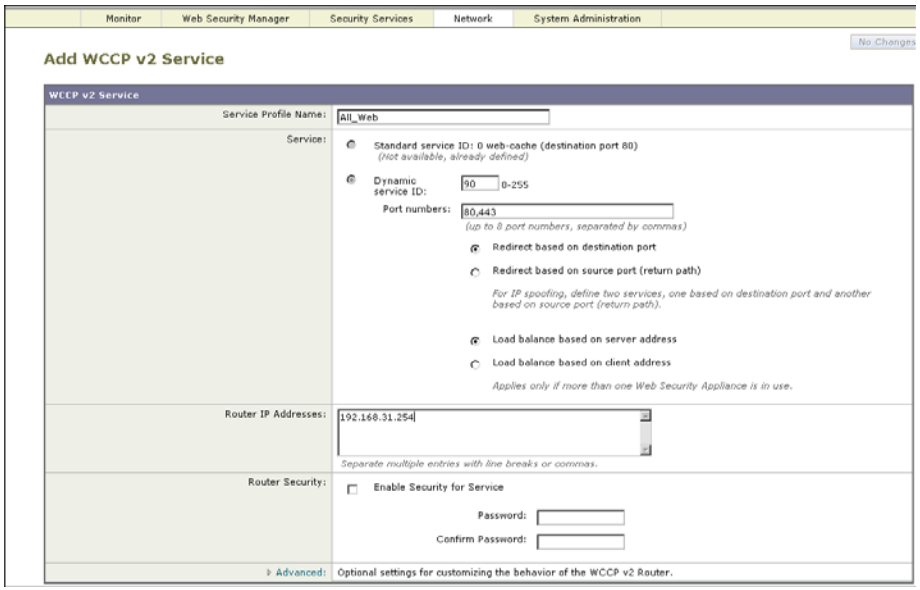
Step 1: To configure WCCP on the WSA, click on **Network->Transparent Redirection**.

Figure 24. Transparent Redirection



Step 2: The policy that was defined in the Setup wizard defines policy "web_cache" with Service ID 0 to send port 80 traffic to the WSA. In order to send both port 80 traffic and port 443 (HTTPS), create a new policy. The new policy will redirect both port 80 and 443 (Figure 25) and be labeled using the Dynamic Service ID of '90'.

Figure 25. Adding a New WCCP Redirect Policy



Step 3: Click the top right button to commit your changes.

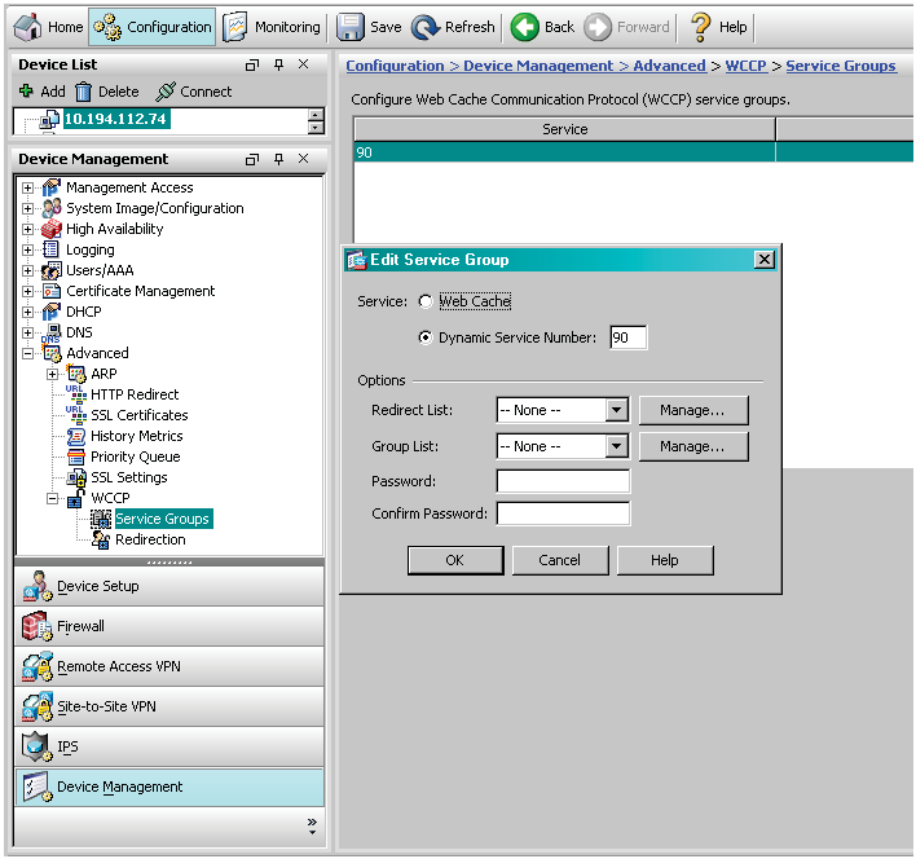
Procedure 2 Configure WCCP on the Firewall

Now configure the ASA Firewall on the Internet Edge to redirect http and https traffic to the WSA.

Step 1: Bring up ASDM on the Firewall and go to **Configuration > Device Management > Advanced > WCCP**.

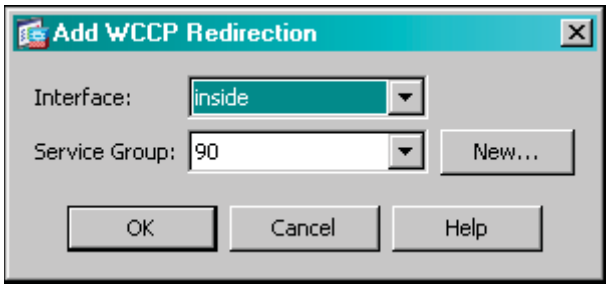
Step 2: Under Service Groups, build a new service group using the Dynamic Service ID of 90 that we defined on the WSA (Figure 26).

Figure 26. Configuring WCCP Redirect on the ASA Firewall



Step 3: Under Redirection, create a policy to add the redirect for the Inside Interface using service group 90 (Figure X).

Figure 27. Enabling the WCCP Policy on the ASA Inside Interface



Tech Tip

Until the HTTPS service is configured on the WSA, doing the above configuration will block HTTPS traffic going through the network. Leave the policy on the ASA for just port 80 until after HTTPS inspection is configured if the WSA deployment is live with real traffic.

Procedure 3 Test Configuration

Step 1: Use a browser that is not already configured to go to the appliance as an explicit proxy (or remove the explicit proxy settings).

Step 2: Test to a resolvable allowed address (like www.cisco.com).

Step 3: Test to a resolvable blocked address (like www.gambling.com).

Step 4: To check that WCCP redirection is working, in ASDM, navigate to **Monitoring > Properties > WCCP > Service Groups**.

Step 5: Verify that the status window shows the router ID as 192.168.31.254 and the number of cache engines is '1' (one), which is the Cisco WSA appliance. If things are working correctly and redirections are occurring, the Total Packets Redirected counter will be increasing.

Process

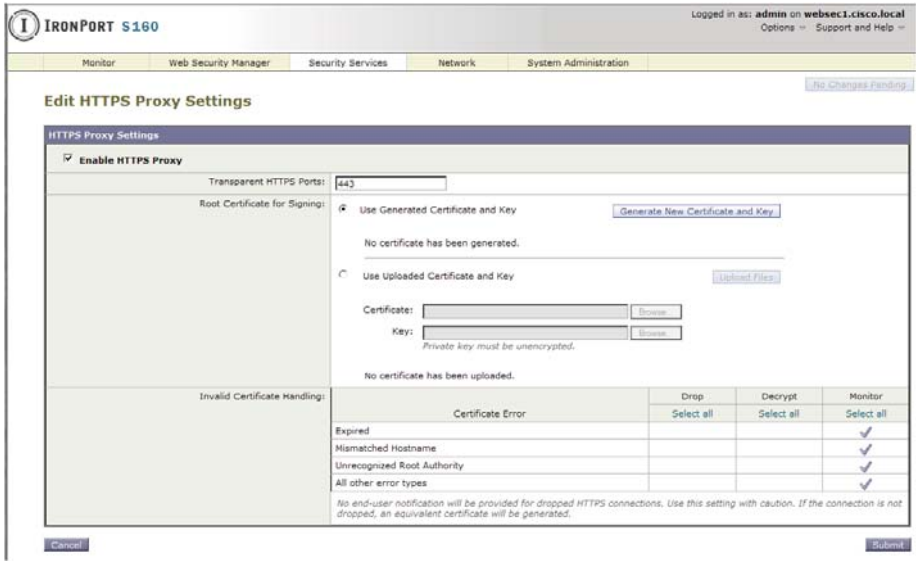
Deploying HTTPS

1. Set Up the HTTPS Proxy Connections
2. Configure HTTPS Proxy Policies

Procedure 1 Set Up the HTTPS Proxy Connections

Step 1: Enable the feature. **Access Security Services > HTTPS Proxy** and then select the **Enable and Edit Settings** button (Figure 28).

Figure 28. Edit HTTPS Proxy Settings



Step 2: This is where you will define the ports you wish to proxy HTTPS on (the default is only on TCP 443).

Step 3: Generate a certificate for the WSA to use on the client side of the proxy connection.

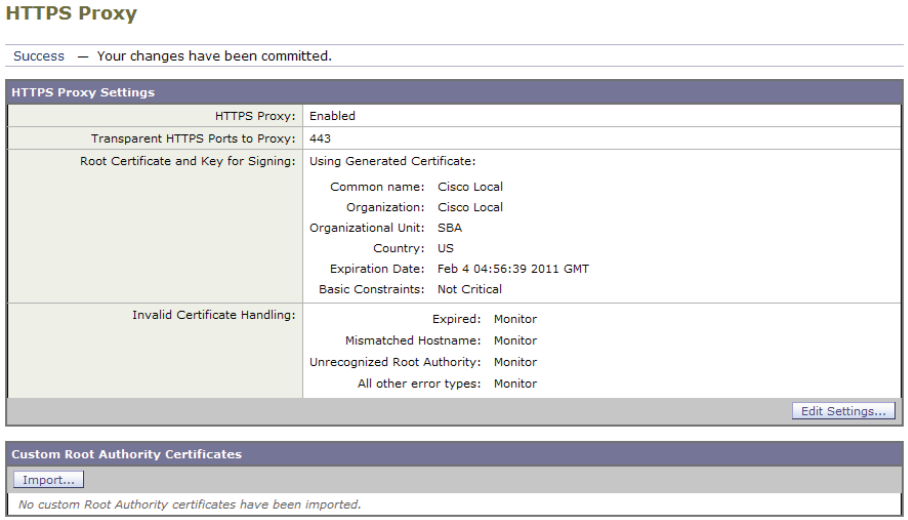
Option A: Generating a certificate typically means the client browser will complain about the certificate for each connection to an HTTPS website. To avoid this, you can upload a certificate file and its matching private key file to the appliance if you have a certificate that is trusted in your organiza¬tion. If users already have this certificate loaded on their machines, the HTTPS proxy will not generate errors related to Unknown Certificate Authority.

Option B: Instead of adding an agency root certificate to the WSA, another option is to inform users in the agency to accept the root certificate supplied by the WSA as a trusted source.

Also on the WSA HTTPS Proxy Settings page, you can configure what the WSA is supposed to do when the server it is connecting to has an invalid certificate. The choices, depending on what the certificate error was, can range from dropping the connection, decrypting it, or monitoring it.

Step 4: After defining your policy, submit and then commit your changes.

Figure 29. HTTPS Proxy Settings



Reader Tip

For more information about using certificates as part of the WSA HTTPS Proxy mechanism, please consult the WSA User Guide, your trusted Partner or Cisco Sales Representative.

Procedure 2 Configure HTTPS Proxy Policies

The second step for HTTPS proxy configuration is to configure policies around HTTPS proxy.

Step 1: Access **Web Security Manager -> Custom URLs**.

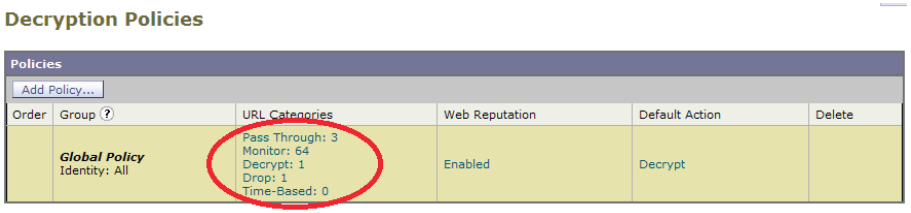
Step 2: As before, add three new Custom Categories, including Drop List, Decrypt List, and Pass Through List

Step 3: Commit the changes.

Step 4: Go to **Web Security Manager -> Decryption Policies**.

Step 5: Select the link below the URL categories header to get to the URL Categories menu (Figure 30).

Figure 30. Link to Decryption Policies: URL Categories



Step 6: You will see all the custom categories you have created. DO NOT include the ones previously created for HTTP. Only include the three new entries. Then change their action to correspond with their name: Drop List to have the action Drop, etc. At the end, it should look like this:

Figure 31. Decryption Policies: URL Categories

Decryption Policies: URL Categories: Global Policy

Custom URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

View: Included Categories Only | **All Categories**		Pass Through	Monitor	Decrypt	Drop	Time-Based
		Select all	Select all	Select all	Select all	(Unavailable)
~~Block List~~	[Include]					–
~~Monitor List~~	[Include]					–
~~Warn List~~	[Include]					–
~~Allow List~~	[Include]					–
Drop List	[Exclude]				✓	–
Decrypt List	[Exclude]			✓		–
Pass Through List	[Exclude]	✓				–

Step 7: The Predefined URL Categories at the bottom of the page allow you to create and enforce policy around how the WSA handles specific types of websites with relation to decryption. Some agencies have strict policies about not decrypting healthcare or financial websites and potentially other categories as well. The Categories on this page allow you to enforce that policy on the WSA (Figure 32).

Figure 32. Defining HTTPS Decryption Policy

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Pass Through	Monitor	Decrypt	Drop	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)
Adult		✓			–
Advertisements		✓			–
Alcohol and Tobacco		✓			–
Arts and Entertainment		✓			–
Business and Industry		✓			–
Cheating and Plagiarism		✓			–
Child Porn		✓			–
Computer Security		✓			–
Computers and Internet		✓			–
Cults		✓			–
Dating		✓			–
Dining and Drinking		✓			–
Education		✓			–
File Transfer Services		✓			–
Filter Avoidance		✓			–
Finance	✓				–
Freeware and Shareware		✓			–
Gambling		✓			–
Games		✓			–
Government and Law		✓			–
Hacking		✓			–
Hate Speech		✓			–
Health and Nutrition	✓				–

Step 8: To test your new configuration, you will need to set up categories for Web pages that you know are encrypted (HTTPS) and then use those URLs in the testing process. Because you have to know whether the site uses HTTPS or not for all pages, it is easier to use Custom Categories for a specific Web page that you do know is HTTPS and put the address into the Drop List.

Step 9: When you try to access that site, the WSA should drop the connection.

Process

Enabling Authentication

1. Set Up Authentication
2. Configure Identity Groups

Authentication is the act of confirming the identity of a user. When you enable authentication, the WSA verifies the identity of clients on the network before allowing them to connect to a destination server. By using authentication in the WSA, you can:

- Set up different Web access policies by user or group membership against a central user directory.
- Enable user tracking, so that when a user violates an acceptable use policy, the WSA can match up the user with the violation instead of just using an IP address.
- Enable compliance reporting.

The WSA supports two different authentication protocols: Lightweight directory access protocol (LDAP) and NT LAN Manager (NTLM). Because most agencies will have an AD server, they will be using NTLM. Single Sign-On (SSO) is also only available when using NTLM.

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

Partial list of applications:

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

Tech Tip

If applications need to access a particular URL, you can cre¬ate an Identity based on a custom User Agent category that does not require authentication. When this is done, the client application will not be asked for authentication.

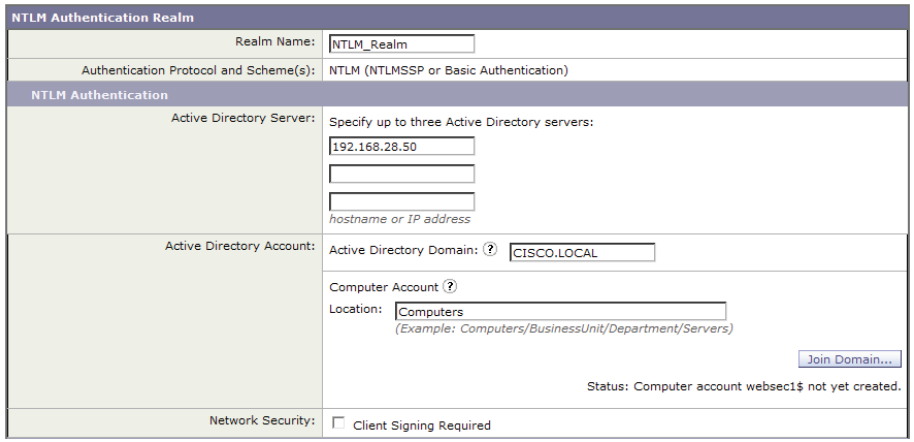
For agencies that require authentication, please consult your trusted Cisco IronPort Partner or Reseller or your Cisco account team. They will be able to help you set up an authentication solution that meets your requirements while minimizing any possible complications.

Procedure 1 Set Up Authentication

Step 1: Build an Authentication Realm, which defines how Authentication is supposed to occur.

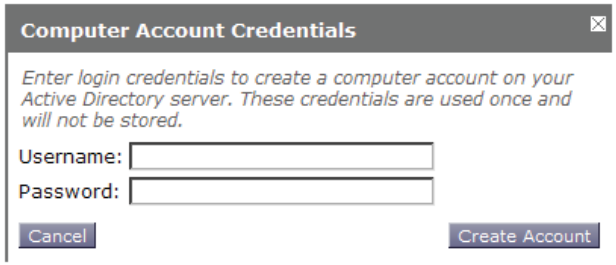
For this deployment, we built a Realm for NTLM authentication to our AD server. In the Realm definition, we specify the AD server and the AD domain (Figure 33).

Figure 33. Building an NTLM Authentication Realm



Step 2: Select the **Join Domain** button. When you do this, you will need an AD Domain Administrator present to enter a username and password with authority to create domain accounts for computers (Figure 34).

Figure 34. AD Administrative Domain Logon

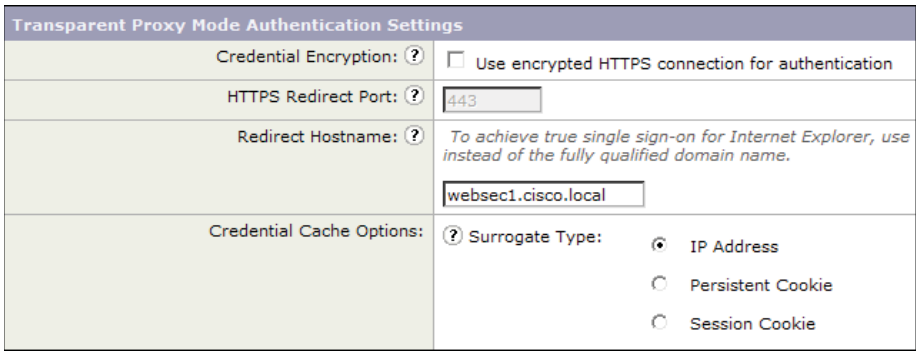


Step 3: Hit the **Start Test** button on the same page to test the NTLM connection to the AD domain.

Step 4: On the Authentication main page, select the **Edit Global Settings** button.

Step 5: Change the **Credential Cache Option > Surrogate Type** to "IP Address" (Figure 35).

Figure 35. Transparent Mode Authentication Settings



Step 6: Click **Submit** and commit changes.

Procedure 2 Configure Identity Groups

The next step in setting up Authentication is to configure identity groups, which are based on the identity of the client or the transaction itself.

Step 1: Access **Web Security Manager > Identities** and click **Add Identity**.

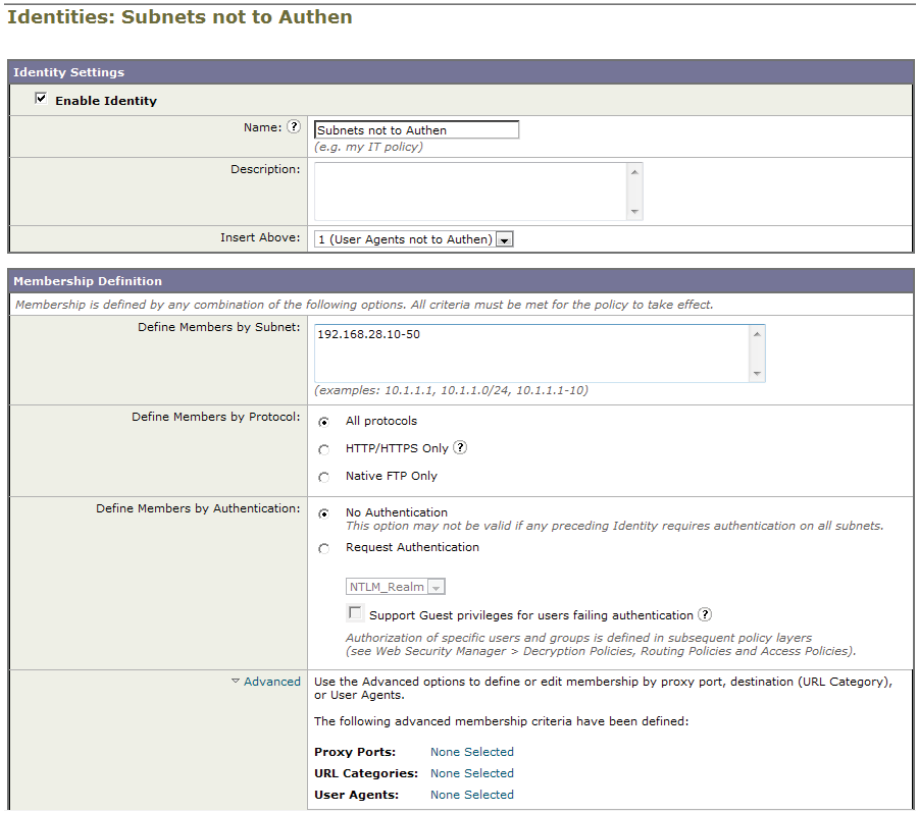
Step 2: Start by adding two sample identities: "Subnets not to Authen" and "User Agents not to Authen." (Figure 36)

If the need arises to build an Identity around subnets, just insert the client IP address or range or subnet that you do not want to have to authenticate to access the Internet.

Tech Tip

This action defeats the purpose of running authentication for that IP address and that all log information from the WSA will never have authentication data from employees using that IP address. But it might be required in certain cases and is given here as an example of how to change the operational policy of the WSA.

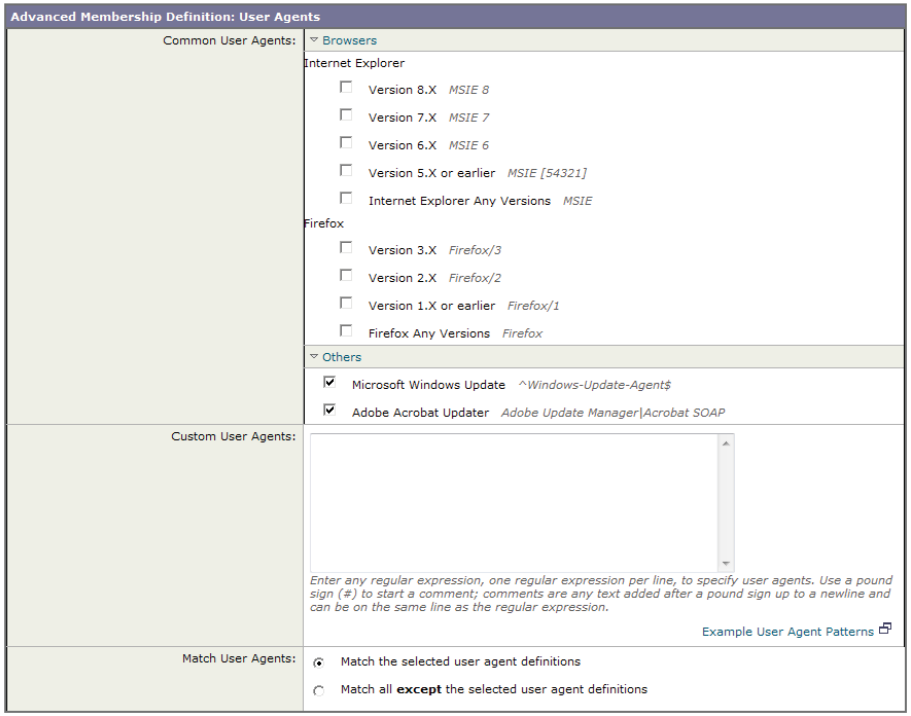
Figure 36. Example Identity: “Subnets not to Authen”



Step 3: Now build an identity for User Agents. In this case, select the **Advanced** tab for User Agents

Step 4: Select Microsoft Windows Update and Adobe Acrobat Updater agent types. Selecting these agents means that when connections over HTTP with those User Agents in the HTTP Header are seen, no authentication will be requested. Custom User Agents can be defined for any application that uses HTTP and is failing authentication. If that is not possible, then a specific custom URL category can be built and then used in the “Advanced” tab for URL Categories.

Figure 37. Example Identity: “User Agents not to Authen”



Step 5: Now that you have built an Identity for “User Agents not to Authenticate” and know how to build an identity for subnets not to authenticate, you have completed the Authentication section. Now test the deployment to insure 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 your needs or requirements.

Process

Maintaining the WSA

1. Monitor the WSA
2. Troubleshoot the WSA

Once deployment is complete, use the following two procedures to maintain the WSA.

Procedure 1 Monitor the WSA

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

Tech Tip

Because the appliance itself only stores data for a limited amount of time, you need to install separate software from Sawmill to allow for long-term storage and reporting of events from the WSA.

Please consult your Cisco Account Team or your trusted Partner for more information on Sawmill and long-term reporting.

Procedure 2 Troubleshoot the WSA

Step 1: To determine why the WSA took the action it did on a Web connection to a specific site from a specific user, run the Trace tool under **System Administration >Policy Trace**.

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

Reader Tip

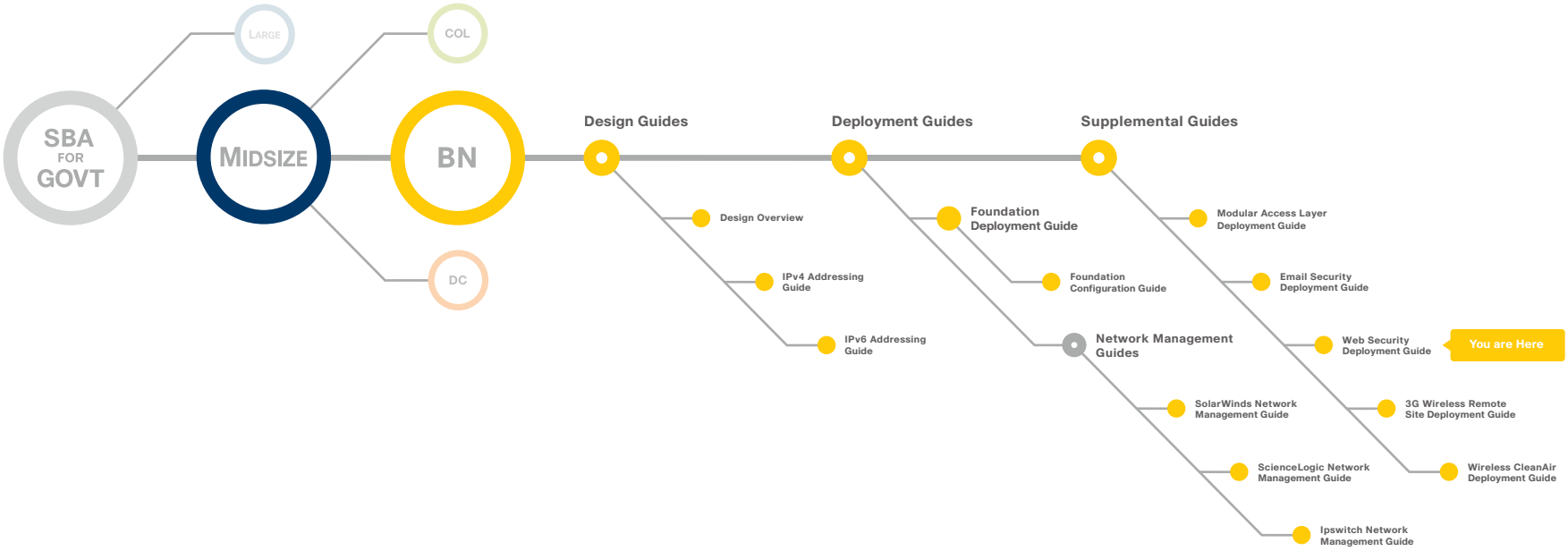
To learn more about Cisco SBA, visit:
http://www.cisco.com/go/smartarchitecture or
http://www.cisco.com/go/partner/smartarchitecture

Appendix A: Product Part Numbers

The following products and software version have been validated for the Cisco SBA:

Functional Area	Product	Part Numbers	Software Version
Internet Edge	Cisco Ironport S160 Web Security Appliance	S160-BUN-R-NA	6.3.1-025

Appendix B:
SBA for Midsize Agencies Document System



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.**

C07-641132-00 12/10