CHAPTER 3

Configuring the Infrastructure

This chapter provides an overview of the configuration used in testing to validate the functionality of the Cisco WSA. This chapter is not intended to provide step-by-step procedures to configure the Cisco WSA because of the variability in network architectures and the potential impact on device configuration. However, this chapter discusses specific items related to FactoryTalk applications, their interaction with the Cisco WSA, and the steps required to help ensure that they will interoperate with the Cisco WSA and efficiently complete their functions.

Cisco Web Security Appliance

System Setup Wizard

From an out-of-box state, the most efficient way to complete the setup of the Cisco WSA is to use the System Setup Wizard. While this design guide does not describe in detail the System Setup Wizard, it does provide important information to be aware of during this phase of Cisco WSA deployment. Important items from the System Setup Wizard that affect the functionality of the Cisco WSA and FactoryTalk Applications are defined in the sections following Table 3-1.

Table 3-1 Network and System Settings

Property	Description
Default System Hostname	The system hostname is the fully-qualified hostname used to identify the appliance in the following areas: • Command line interface (CLI) • System alerts • End-user notification and acknowledgment pages • When forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.
DNS Server(s)	• Use the Internet's Root DNS Servers—You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network. **Note**: Internet root DNS servers will not resolve local host names. If you need the appliance to perform this action, you must use a local DNS server or add the appropriate static entries to the local DNS using the CLI. • Use these DNS Servers—Provide the address(es) for the local DNS server(s) that the appliance can use to resolve host names.
NTP Server	The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet. The default is time.sco.cisco.com.
Time Zone	Provide time-zone information for location of the appliance; affects time stamps in message headers and log files.
Appliance Mode of Operation	• Standard—Used for standard on-premise policy enforcement. • Cloud Web Security Connector—Used primarily to direct traffic to the Cloud Web Security service from Cisco for policy enforcement and threat defense. • Hybrid Web Security—Used in conjunction with the Cloud Web Security service from Cisco for cloud and on-premise policy enforcement and threat defense.

Network and Network Context

Note When you use the Web Security Appliance in a network that contains another proxy server, it is recommended that you place the Web Security Appliance downstream from the proxy server, closer to the clients. A system with multiple proxies was not tested and validated as a part of this design guide.

Table 3-2 Network and System Settings

Property	Description
Is there another web proxy on your network?	Is there another proxy on your network such that traffic must pass through it? Will it be upstream of the Web Security Appliance? If yes for both points, select the checkbox. This allows you to create a proxy group for one upstream proxy. You can add more upstream proxies later. This was not tested or validated as a part of this design guide.
Proxy group name	A name used to identify the proxy group on the appliance.
Address	The hostname or IP address of the upstream proxy server.
Port	The port number of the upstream proxy server.

Network and Network Interfaces and Wiring

You can use the host name specified here when connecting to the appliance management interface (or in browser proxy settings if M1 [Management] is used for proxy data), but you must register it in your organization’s DNS.

Table 3-3 Network and Network Interfaces and Wiring

Setting	Description
Ethernet port	(Optional) **Check Use M1 port for management only** if you want to use a separate port for data traffic. If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. You must also define different routes for management and data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic. You can enable and configure the P1 port only in the System Setup Wizard. If you want to enable the P2 interface, you must do this after finishing the System Setup Wizard.
IP Address and Netmask	The IP address and network mask to use when managing the Web Security appliance on this network interface.
Hostname	The host name to use when managing the Web Security appliance on this network interface.

Network and Routes for Management and Data Traffic

Note If you enable “Use M1 port for management only”, this configuration section will have separate configuration options for management and data traffic; otherwise one joint configuration section will be shown.

Table 3-4 Network and Routes for Management and Data Traffic

Property	Description
Default Gateway	The default gateway IP address to use for traffic through the Management and Data interfaces.
Static Routes Table	Optional static routes for management and data traffic. Multiple routes can be added. • Name—A name used to identify the static route. • Internal Network—The IPv4 address for this route's destination on the network. • Internal Gateway—The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Network and Transparent Connection Settings

Note By default, the Cloud Connector is deployed in transparent mode, which requires a connection to a Layer 4 switch or a version 2 WCCP router. The version 2 WCCP router was tested and validated as a part of this design guide.

Table 3-5 Network and Transparent Connection Settings

Property	Description
Layer 4 Switch or No Device	Specifies that the Web Security appliance is connected to a Layer 4 switch for transparent redirection or that no transparent redirection device is used and clients will explicitly forward requests to the appliance.
WCCP v2 Router	Specifies that the Web Security Appliance is connected to a version 2 WCCP-capable router. If you connect the appliance to a version 2 WCCP router, you must create at least one WCCP service. You can enable the standard service on this screen or after the System Setup Wizard is finished, where you can also create multiple dynamic services. When you enable the standard service, you can also enable router security and enter a passphrase. The passphrase used here must be used on all appliances and WCCP routers within the same service group. A standard service type (also known as the "web-cache" service) is assigned a fixed ID of zero, a fixed redirection method (by destination port), and a fixed destination port of 80. A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options.

Security and Security Settings

Table 3-6 Security and Security Settings

Option	Description
Global Policy Default Action	Specifies whether to block or monitor all web traffic by default after the System Setup Wizard completes. You can change this behavior later by editing the Protocols and User Agents settings for the Global Access Policy. The default setting is to monitor traffic.
Layer 4 Traffic Monitor	Specifies whether the Layer 4 Traffic Monitor should monitor or block suspected malware by default after the System Setup Wizard completes. You can change this behavior later. The default setting is to monitor traffic.

Table 3-6 Security and Security Settings

Option	Description
Acceptable Use Controls	Specifies whether to enable Acceptable Use Controls. If enabled, Acceptable Use Controls allow you to configure policies based on URL filtering. They also provide application visibility and control, and related options such as safe search enforcement. The default setting is enabled.
Reputation Filtering	Specifies whether to enable Web Reputation filtering for the Global Policy Group. Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. The default setting is enabled.
Malware and Spyware Scanning	Specifies whether to enable malware and spyware scanning using Webroot, McAfee, or Sophos. The default setting is that all three options are enabled. Most security services will be automatically enabled/disabled to match the services normally available for cloud policies. Similarly, policy-related defaults will not be applicable. At least one scanning option must be enabled. If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware. You can further configure malware scanning after you finish the System Setup Wizard.
Cisco Data Security Filtering	Specifies whether to enable Cisco Data Security Filters. If enabled, the Cisco Data Security Filters evaluate data leaving the network and allow you to create Cisco Data Security Policies to block particular types of upload requests. The default setting is enabled.

Interface Configuration

The Cisco WSA that was tested and validated was configured in a dual-homed type of architecture (Figure 3-1). Overall three interfaces and IP addresses were dedicated to the device:

- M1 Interface and IP address

  This is intended for management of the Cisco WSA only and should be out-of-band.

- P1 Interface and IP address

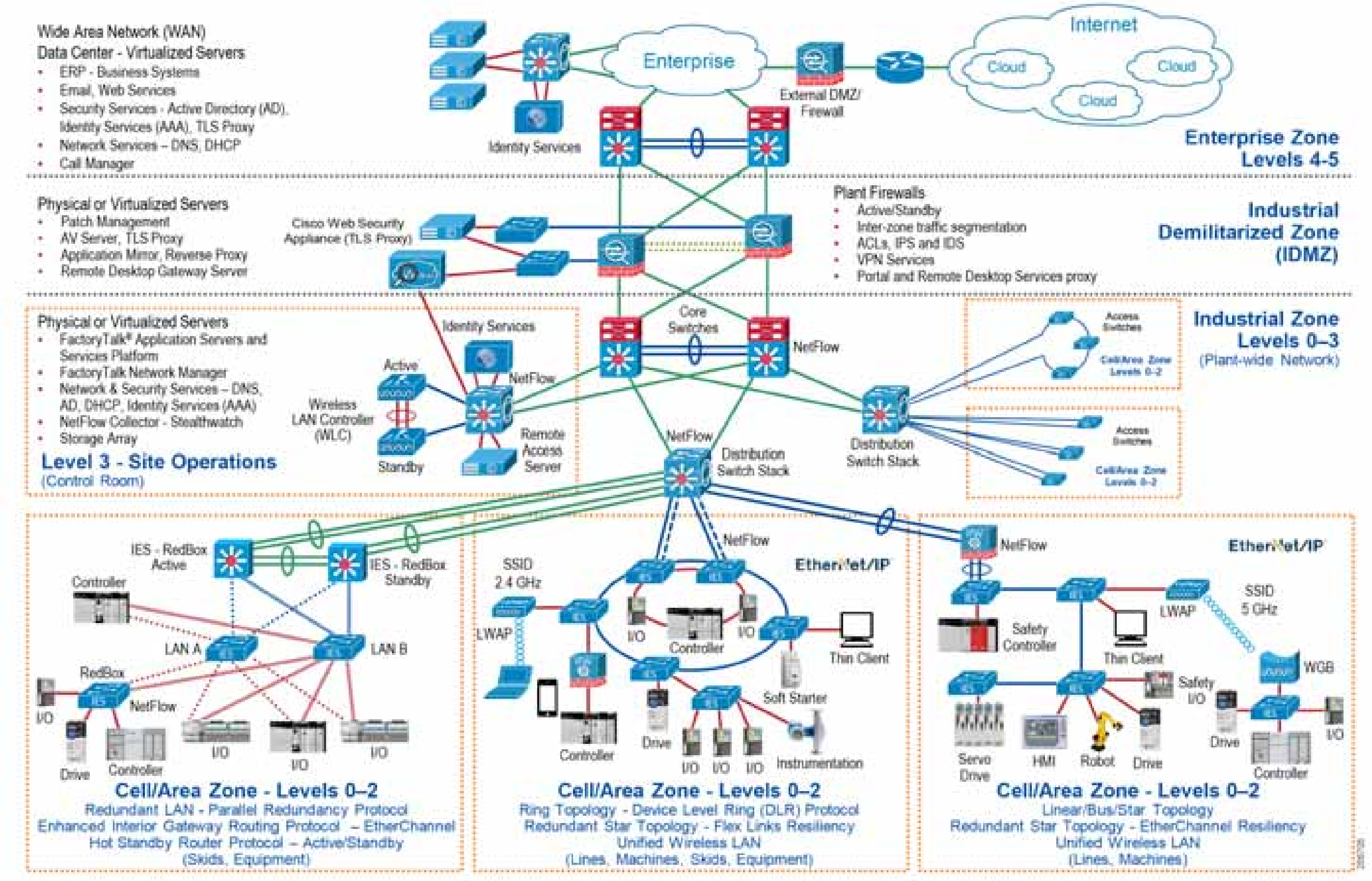
  This interface resides in the same subnet as the firewall interface in the Industrial Zone and should be Layer 2 accessible from the IDMZ firewall. All WCCP traffic is forwarded to this interface.

- P2 Interface and IP address

  This interface resides in the IDMZ and is the internet facing interface of the Cisco WSA. Once traffic has been analyzed and approved, it is sent via P2.

Once the three interfaces are configured and defined, routing tables for each interface can be configured to ensure that the desired connectivity is achieved. Typically, a default route on the P2 or IDMZ interface is used to help ensure that cloud and web traffic can reach its destination on the internet.

Figure 3-1 Cisco WSA Network Architecture

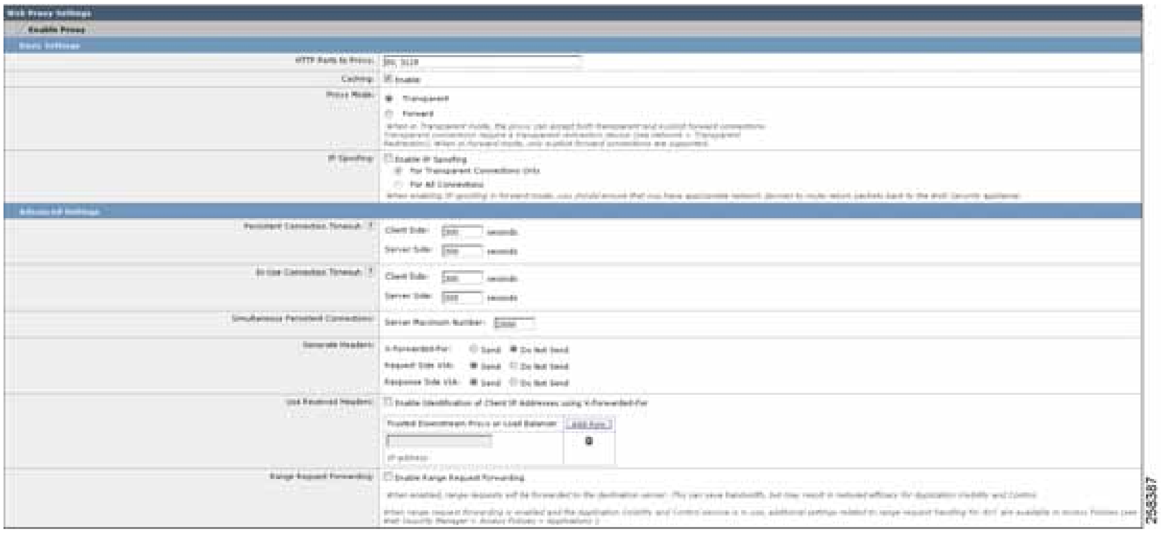

Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Cisco Web Security Appliance (TLS Proxy)
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
FactoryTalk Network Manager
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
NetFlow Collector - Stealthwatch
Storage Array
Level 3 - Site Operations
(Control Room)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
NetFlow
Remote Access Server
Core Switches
NetFlow
NetFlow
Distribution Switch Stack
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0-2
Access Switches
Cell/Area Zone Levels 0-2
Industrial Zone Levels 0–3
(Plant-wide Network)
IES - RedBox Active
IES - RedBox Standby
Controller
LAN A
LAN B
RedBox
NetFlow
I/O
Drive
Controller
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Redundant LAN - Parallel Redundancy Protocol
Enhanced Interior Gateway Routing Protocol – EtherChannel
Hot Standby Router Protocol – Active/Standby
(Skids, Equipment)
SSID 2.4 GHz
LWAP
NetFlow
EtherNet/IP
I/O
Controller
I/O
Thin Client
Controller
Drive
Soft Starter
I/O I/O I/O
Instrumentation
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
NetFlow
EtherNet/IP
Safety Controller
LWAP
SSID 5 GHz
Thin Client
Safety I/O
WGB
Servo Drive
HMI
Robot
Drive
Drive
Controller
I/O
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Redundant Star Topology - EtherChannel Resiliency
Unified Wireless LAN
(Lines, Machines)

Web Proxy Configuration

The configuration of the proxy stays in a mostly default state and can be accessed and viewed by navigating to **Security Services**->**Web Proxy**. The HTTP ports that are to be proxied by the Cisco WSA can be defined in the configuration. Additionally, a proxy mode must be selected depending on the type of deployment that will be used with the Cisco WSA. The types of deployment, Transparent and Forward, were defined and discussed in Chapter 2, "CPwE Cloud Connectivity Design Considerations." Transparent and Forward proxy modes were both tested and validated, however there is a difference in the overall configuration of the network and end devices between the two proxy modes. This chapter focuses on Transparent Mode configuration, but notes which configurations are not required for Forward Mode deployments. Figure 3-2 shows the Web Proxy Settings that were used during testing.

Caching is a feature that is typically used to attempt to reduce traffic and resources used on the network by saving a version of the webpage and providing it to clients. For testing and validation purposes, the caching feature was enabled but is not required.

Figure 3-2 Web Proxy Settings



Web Proxy Settings

☑ Enable Proxy

Basic Settings

HTTP Ports to Proxy: 80, 3128

Caching: ☑ Enable

Proxy Mode: ● Transparent ○ Forward
[illegible]

IP Spoofing: □ Enable IP Spoofing
● For Transparent Connections Only
○ For All Connections
[illegible]

Advanced Settings

Persistent Connection Timeout: Client Side: 300 seconds Server Side: 300 seconds

In-Use Connection Timeout: Client Side: 300 seconds Server Side: 300 seconds

Simultaneous Persistent Connections: Server Maximum Number: 2000

Generate Headers:
X-Forwarded-For: ○ Send ● Do Not Send
Request Side VIA: ● Send ○ Do Not Send
Response Side VIA: ● Send ○ Do Not Send

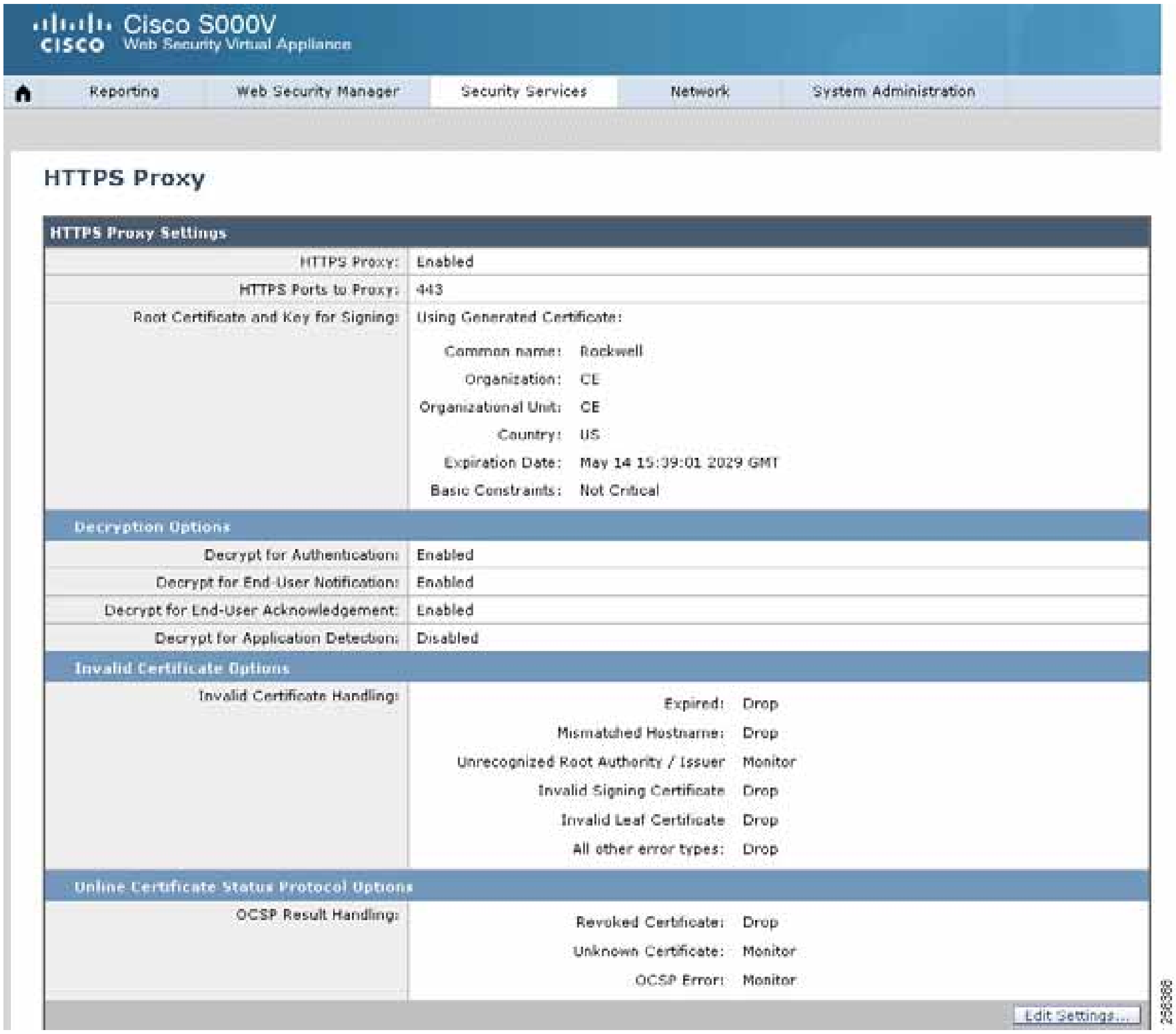
Use Received Headers: □ Enable Identification of Client IP Addresses using X-Forwarded-For
Trusted Downstream Proxy or Load Balancer | Add Row
IP address

Range Request Forwarding: □ Enable Range Request Forwarding
[illegible]
[illegible]

HTTPS Proxy Configuration

The HTTPS proxy feature is a separate configuration that is required for use with most cloud applications. This configuration is located under **Security Services**->**HTTPS Proxy**. Once this feature is enabled, a port (443 by default) must be entered to inform the Cisco WSA which HTTPS traffic to proxy. This value should remain 443 as shown in Figure 3-3 unless a solution is being implemented that changes the HTTPS traffic default port.

Figure 3-3 HTTPS Proxy Settings



HTTPS Proxy

HTTPS Proxy Settings

HTTPS Proxy: Enabled
HTTPS Ports to Proxy: 443
Root Certificate and Key for Signing: Using Generated Certificate:
Common name: Rockwell
Organization: CE
Organizational Unit: CE
Country: US
Expiration Date: May 14 15:39:01 2029 GMT
Basic Constraints: Not Critical

Decryption Options

Decrypt for Authentication: Enabled
Decrypt for End-User Notification: Enabled
Decrypt for End-User Acknowledgement: Enabled
Decrypt for Application Detection: Disabled

Invalid Certificate Options

Invalid Certificate Handling:
Expired: Drop
Mismatched Hostname: Drop
Unrecognized Root Authority / Issuer Monitor
Invalid Signing Certificate Drop
Invalid Leaf Certificate Drop
All other error types: Drop

Online Certificate Status Protocol Options

OCSP Result Handling:
Revoked Certificate: Drop
Unknown Certificate: Monitor
OCSP Error: Monitor

Additional configuration relating to the HTTPS proxy includes decryption options and certificate related options.

Decryption options include those shown in Table 3-7, which are left in the default state for testing and validation.

Table 3-7 Decryption Options

Decryption Option	Description
Decrypt for Authentication	For users who have not been authenticated before this HTTPS transaction, allow decryption for authentication.
Decrypt for End-User Notification	Allow decryption so that AsyncOS can display the end user notification. Note: If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”.

Table 3-7 Decryption Options (continued)

Decryption Option	Description
Decrypt for End-User Acknowledgment	For users who have not acknowledged the web proxy before this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment.
Decrypt for Application Detection	Enhances the ability of AsyncOS to detect HTTPS applications.

Certificate Configuration Options

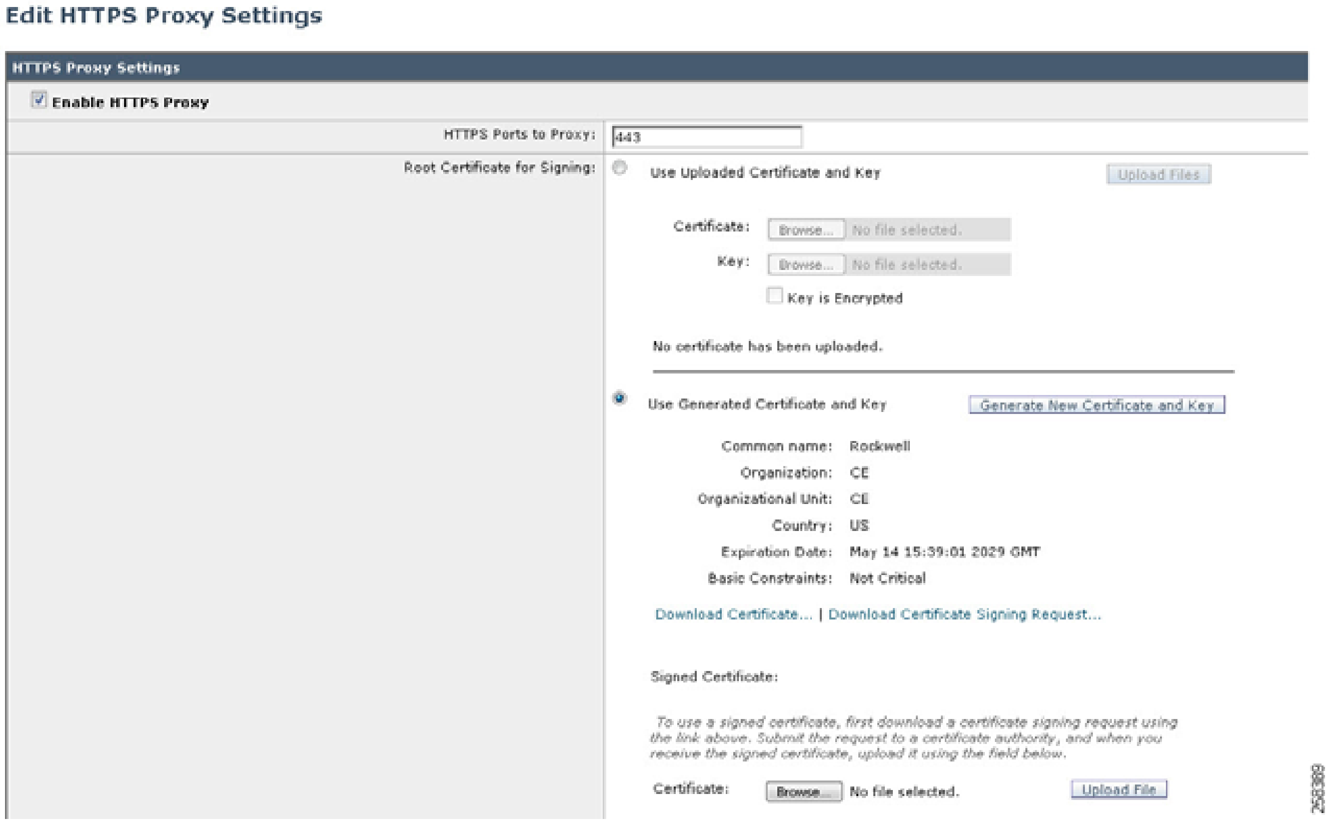
There are two parts to the certificate configuration options, including **Invalid Certificate** and **Online Certificate Status Protocol** (OSCP). These options can generally be uniformly applied to most architectures, but some are application-dependent. If internal or not well-known certificate authorities (CA) are in use (such as Rockwell Automation CA), the **Unrecognized Root Authority/Issuer** option needs to be set to **Monitor** instead of **Drop**. During the testing and validations outlined in this design guide, these options remained set to **Monitor**. OSCP is an internet protocol used for obtaining the revocation (validity) status of X.509 digital certificates and is defined in RFC 6960.

Since cloud applications and most web traffic typically use TLS or other forms of encrypted traffic to send data, the Cisco WSA must act as a man-in-the-middle (MiTM) to allow for the decryption, inspection, and re-encryption of traffic passing through it. To allow for this MiTM process to take place, the Cisco WSA must have a valid certificate to present to a requesting client, which must be trusted by that client. This can be a self-signed certificate generated by the Cisco WSA or from another certificate authority (CA). During the HTTPS Proxy configuration, the certificate that the Cisco WSA presents to the client is configured using either method. For testing and validation, a certificate generated by the Cisco WSA (self-signed) was used to decrypt traffic.

This is completed by using the **Generate New Certificate and Key** process located in the configuration section. Some information is then provided, such as common name, organization and expiration date and entered into the certificate in case a requesting user must verify. This information is shown in Figure 3-4.

After the certificate has been generated, the **Download Certificate** link can be used to download and distribute the certificate. The usage of this certificate is described in Windows Certificates, which describes the configuration of the EWS machines.

Figure 3-4 Certificate Details



Edit HTTPS Proxy Settings

HTTPS Proxy Settings

☑ Enable HTTPS Proxy

HTTPS Ports to Proxy: 443

Root Certificate for Signing:

○ Use Uploaded Certificate and Key

Certificate: No file selected.

Key: No file selected.

□ Key is Encrypted

No certificate has been uploaded.

● Use Generated Certificate and Key

Common name: Rockwell
Organization: CE
Organizational Unit: CE
Country: US
Expiration Date: May 14 15:39:01 2029 GMT
Basic Constraints: Not Critical

Download Certificate... | Download Certificate Signing Request...

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

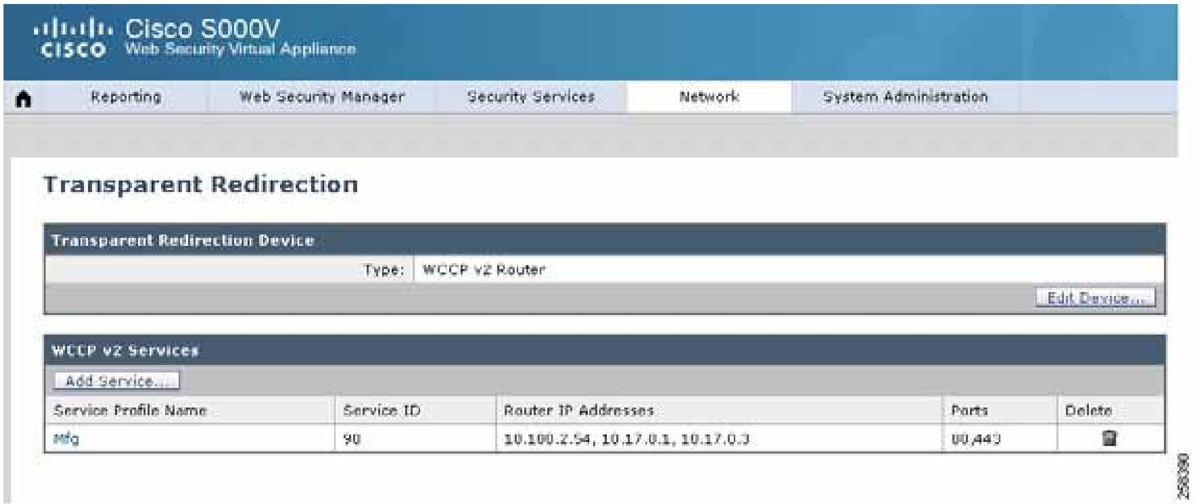
Certificate: No file selected.

Once the certificate has been exported/downloaded or the signing request had been completed, the certificate will be used on individual client computers or devices.

Redirection Configuration

When using transparent redirection on the Cisco WSA, a method must be used to send web traffic from the infrastructure to the Cisco WSA. Typical redirection methods were described in Chapter 2, “CPwE Cloud Connectivity Design Considerations.” For testing and validation, the WCCP v2 router redirection method was selected as shown in Figure 3-5.

Figure 3-5 Redirection Type



Transparent Redirection

Transparent Redirection Device

Type: WCCP v2 Router

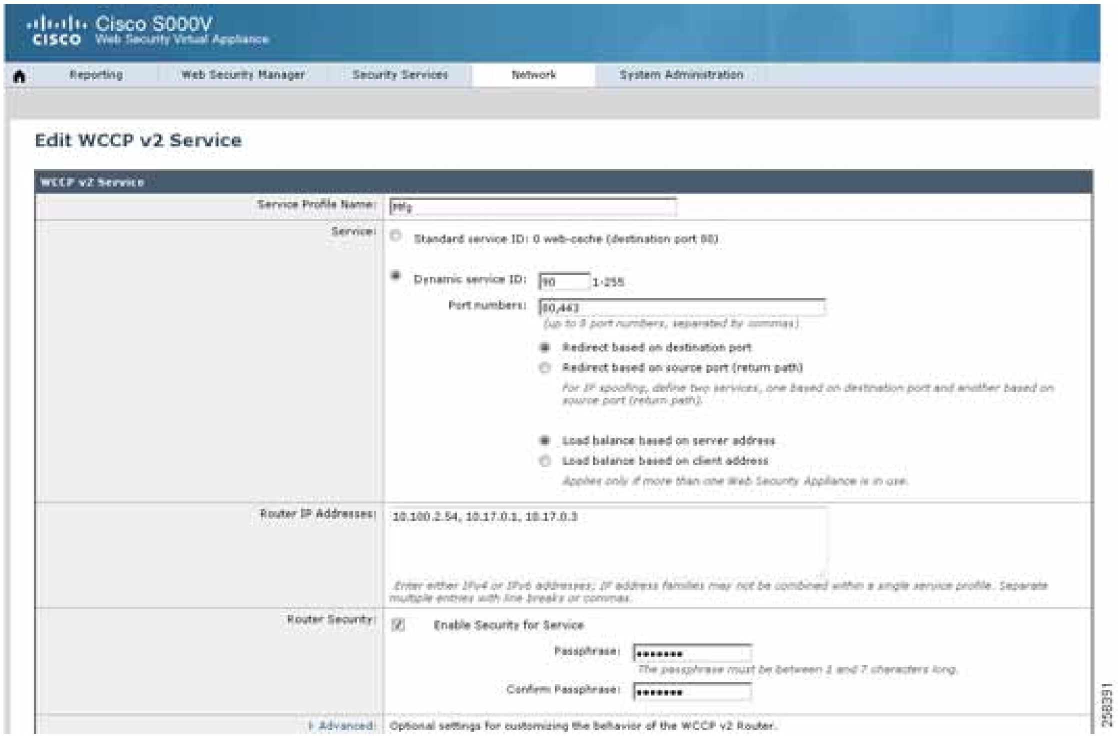
WCCP v2 Services

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
Mfg	90	10.100.2.54, 10.17.0.1, 10.17.0.3	80,443	🗑

Once the WCCP v2 redirection method has been selected, the WCCP v2 services must be defined. These services, described in Chapter 2, “CPwE Cloud Connectivity Design Considerations,” allow for the group of WCCP v2 devices to send specific traffic types to the Cisco WSA. In our test case, a custom service ID of 90 was used to define both HTTP (Port 80) and HTTPS (Port 443) traffic. This service ID is then used throughout the infrastructure devices to allow for adjacency between the infrastructure and the Cisco WSA.

The configuration of the WCCP v2 services has several items that must be defined as shown in Figure 3-6.

Figure 3-6 WCCP Service Profile



Edit WCCP v2 Service

WCCP v2 Service

Service Profile Name: Mfg

Service: ○ Standard service ID: 0 web-cache (destination port 80)

● Dynamic service ID: 90 1-255

Port numbers: 80,443

(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: 10.100.2.54, 10.17.0.1, 10.17.0.3

Enter either IPv4 or IPv6 addresses; IP address families may not be combined within a single service profile. Separate multiple entries with line breaks or commas.

Router Security: ☑ Enable Security for Service

Passphrase: ••••••••

The passphrase must be between 1 and 7 characters long.

Confirm Passphrase: ••••••••

▹ Advanced: Optional settings for customizing the behavior of the WCCP v2 Router.

- The WCCP v2 service must have a service profile name. This name is for organizational purposes on the Cisco WSA and is not shared across additional infrastructure devices.
- The dynamic service ID was selected for the Service, as mentioned above, which allows the user to define the port numbers (up to eight) that will be used for the WCCP v2 redirection. Additional ports can be added to the service ID if needed. This is used on additional devices through the infrastructure and is shown in a Cisco ASA configuration in Cisco Adaptive Security Device Manager (ASDM) Configuration.
- The Router IP Addresses define the WCCP v2 devices, such as routers, switches, and firewalls that exist in the infrastructure. These devices are responsible for forwarding target web traffic defined by the service ID to the Cisco WSA.

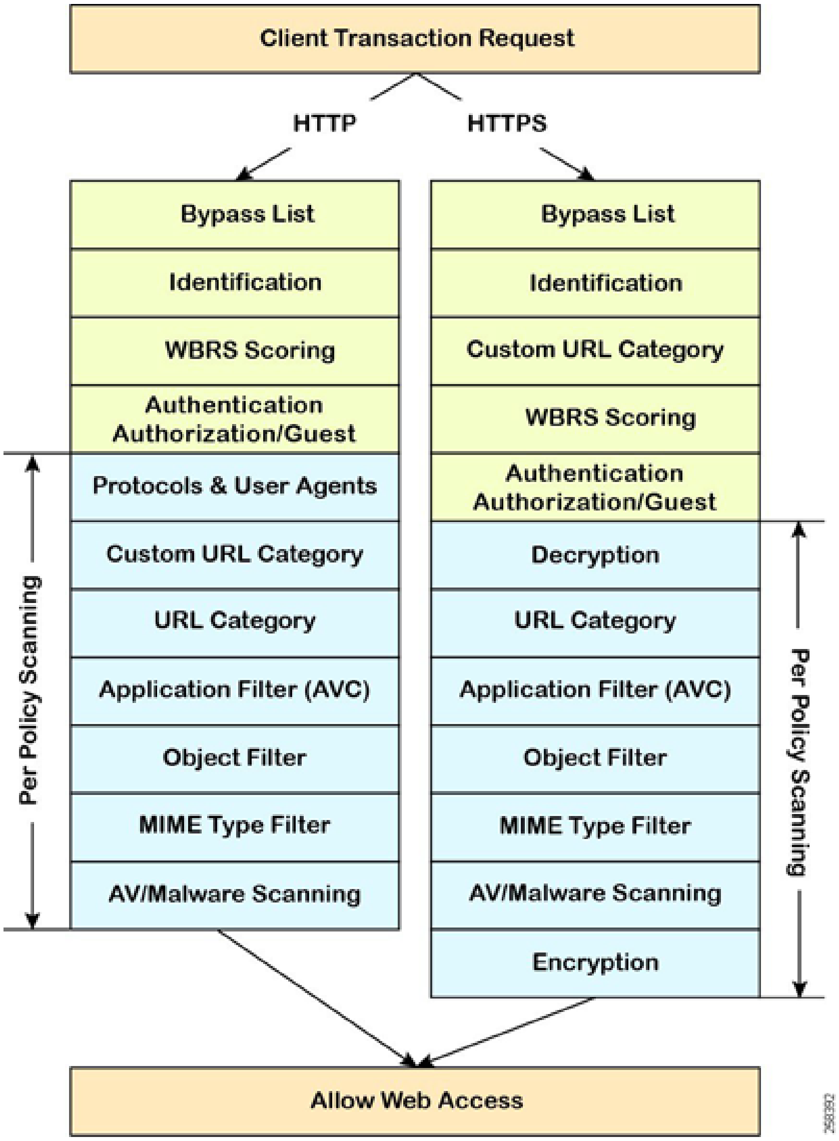
Cisco WSA Rule Configuration

Once web traffic (HTTP or HTTPS) is received by the Cisco WSA, policies and rules exist to restrict, decrypt, monitor, or pass-through the traffic. The purpose and definition of each of these actions is defined in Table 3-8. Additionally, Figure 3-6 defines the logical flow of data as well as the various lists and technologies that are processed during the flow of traffic.

Table 3-8 Web Traffic Action

Option	Description
Monitor	Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.
Drop	The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.
Pass through	The appliance passes through the connection between the client and the server without inspecting the traffic content. However, with a standard pass-through policy, the WSA does check the validity of the requested server by initiating an HTTPS handshake with the server. This validity check includes server certificate validation. If the server fails the check, the transaction is blocked. You can skip validation checks for specific sites by configuring policies that incorporate custom categories, which include these sites, thereby indicating that these sites are trustworthy-these sites are passed through without validity checks. Exercise care when configuring policies that allow validity checks to be skipped.
Decrypt	The appliance allows the connection, but inspects the traffic content. It decrypts the traffic and applies access policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying access policies, you can scan the traffic for malware.

Figure 3-7 Cisco WSA Logical Flow



A few items shown in Figure 3-7 are defined below; not all items are defined since some were not used or did not affect the testing and validation:

- Bypass List
  - This is used for applications or web traffic that may have issues being sent to a proxy or if there is a specific application that would not need to be inspected by the Cisco WSA. Items that are within the Bypass List are allowed through the Cisco WSA without additional examination.
- Custom URL Category
  - Custom URL Categories are used to websites that may not be well-known enough to fall into one of the existing pre-defined URL Categories. The Rockwell Automations website falls under the Business and Industry category and does not require a Custom URL category.

    - All transactions resulting in unmatched categories are reported on the **Reporting** -> **URL Categories** page as uncategorized URLs. Many uncategorized URLs are generated from requests to websites within the internal network. Cisco, Panduit, and Rockwell Automation recommend using custom URL categories to group internal URLs and allow all requests to internal websites.

- Web Reputation Score (WBRS) Scoring
    - WBRS is an innovative method that analyzes the behavior and characteristics of a web server and provides the latest defense in the fight against spam, viruses, phishing, and spyware threats.
    - WBRS uses real-time analysis on a vast, diverse, and global dataset in order to detect URLs that contain some form of malware. It is a critical part of the Cisco security database, which helps protect from blended threats from email or web traffic.
    - WBRS differs from a traditional URL blacklist or whitelist because it analyzes a broad set of data and produces a highly granular score of -10 to +10, instead of the binary good or bad categorizations of most malware detection applications. This granular score offers administrators increased flexibility; different security policies can be implemented based on different WBRS scoring ranges.
- Decryption Policies
    - Decryption policies define the handling of HTTPS traffic within the web proxy:
        - When to decrypt HTTPS traffic.
        - How to handle requests that use invalid or revoked security certificates.
    - You can create decryption policies to handle HTTPS traffic in the following ways:
        - Pass through encrypted traffic.
        - Decrypt traffic and apply the content-based access policies defined for HTTP traffic. This also makes malware scanning possible.
        - Drop the HTTPS connection.
        - Monitor the request (take no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decrypt action.
- URL Category
    - The category that a URL falls into is determined by a filtering categories database. The Web Security Appliance collects information and maintains a separate database for each URL filtering engine. The filtering categories databases periodically receive updates from the Cisco update server.
    - The URL categories database includes many different factors and sources of data internal to Cisco and from the internet.

Decryption Policy

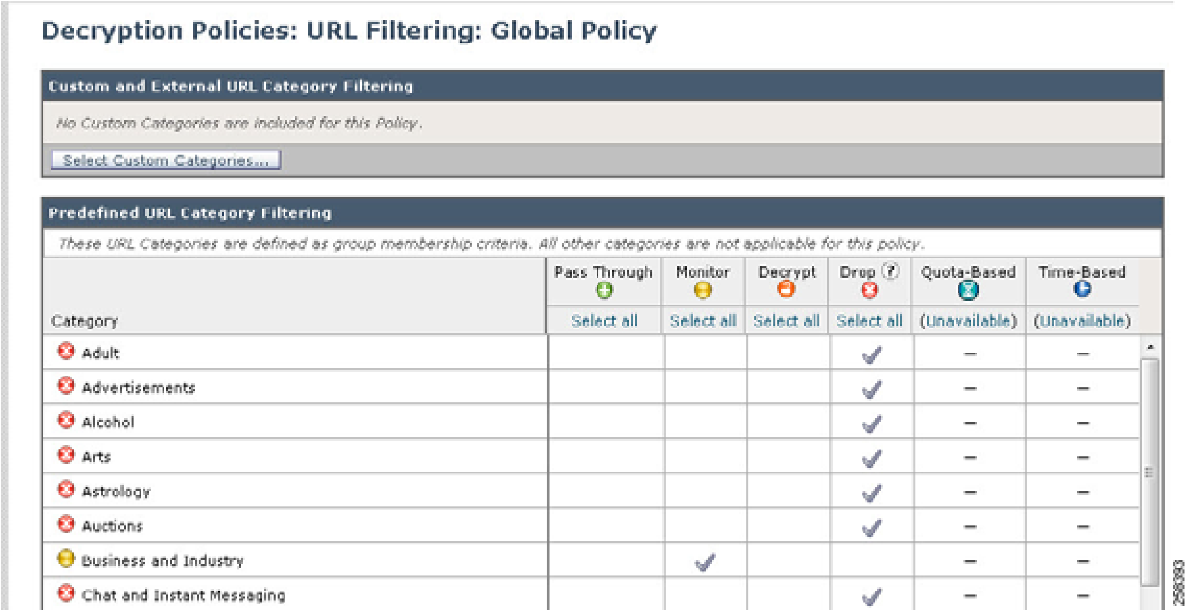
The decryption policy configuration of the Cisco WSA is dependent on the types of applications and software that may be sending HTTP and HTTPS traffic throughout the infrastructure. For testing and validation, the focus was to help ensure that Rockwell Automation software and applications continued to function while the proxy was in place and providing inspection. Based on the testing of current offerings that offer cloud connectivity by Rockwell Automation, the following software was tested:

- FactoryTalk AssetCentre
    - Lifecycle status information
- FactoryTalk Activation Manager
    - Activation retrieval, renewal, and rehosting

- ControlFLASH Plus
  - Lifecycle status information
  - Firmware and release notes downloads

The Rockwell Automation software mentioned above reaches out to rockwellautomation.com as the primary domain name for all requests. The rockwellautomation.com domain name is a known good domain name and is categorized under the Business and Industry URL category. Any subdomain such as api.rockwellautomation.com would also fall under this URL category. For minimal access the following decryption policy can be set to Decrypt, Monitor, or Pass-Through as shown in Figure 3-8.

Figure 3-8 Decryption Policy



Decryption Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this 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	Quota-Based	Time-Based
	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult				✓	–	–
Advertisements				✓	–	–
Alcohol				✓	–	–
Arts				✓	–	–
Astrology				✓	–	–
Auctions				✓	–	–
Business and Industry		✓			–	–
Chat and Instant Messaging				✓	–	–

Infrastructure Device WCCP v2 Configuration

In the previous sections WCCP v2 was described as the method of redirection that would be used for HTTP and HTTPS traffic within the infrastructure. For Cisco IOS devices, the configuration for WCCP v2 is standard, but specific device documentation should be cross-referenced with the configurations outlined in this design guide. The configuration for WCCP v2 in this section is shown both from Command Line Interface (CLI) as well as Cisco ASDM. This generally will allow the application of WCCP v2 redirection to Cisco ASA and route and switch devices. This allows the user to have multiple choices where redirection could be applied depending on network architecture and traffic flow.

For WCCP, the device chooses the highest reachable IP address configured on an interface and uses that as the router ID. This is the same process that Open Shortest Path First (OSPF) follows for the router ID. When the device redirects packets to the proxy the device sources the redirect from the router ID IP address (even if it is sourced out another interface) and encapsulates the packet in a GRE header.

The GRE connection is unidirectional. The device encapsulates redirected packets in GRE and sends them to the proxy. The device does not process any GRE-encapsulated responses from the proxy. The proxy must communicate directly to the inside host.

Command Line Interface Configuration

Note If using WCCP on a Cisco ASA, the commands below should exlude **ip**. For example, **ip wccp web-cache** on the Cisco ASA would be **wccp web-cache**.

Issue the following commands:

Step 1 enable

Enable privileged EXEC mode. Enter your password if prompted.

```
Device> enable
```

Step 2 configure terminal

Enters global configuration mode.

```
Device# configure terminal
```

Step 3 ip wccp version {1 | 2 }

Specifies which version of WCCP to configure on a device. WCCPv2 is the default running version.

```
Device(config)# ip wccp version 2
```

Step 4 ip wccp {web-cache | service-number} [group-address multicast-address] [redirect-list access-list] [group-list access-list] [password password [0 | 7]]

Specifies a web-cache or dynamic service to enable on a device, specifies the IP multicast address used by the service group (optional), specifies any access lists to use, specifies whether to use MD5 authentication, and enables the WCCP service.

- During testing the service-number used was 90.
- A redirect list is recommended and is described below.

Note The password length must not exceed eight characters.

```
Device(config)# ip wccp 90 password rockwell
```

Step 5 interface type number

Targets an interface number for which the web cache service will run and enters interface configuration mode.

```
Device(config)# interface Gigabitethernet 0/0
```

Step 6 ip wccp {web-cache | service-number} redirect {in}

Enables packet redirection on an outbound or inbound interface using WCCP. As indicated by the **out** and **in** keyword options, redirection can be specified for outbound interfaces or inbound interfaces.

```
Device(config-if)# ip wccp 90 redirect in
```

Step 7 exit

Exits interface configuration mode.

```
Device(config-if)# exit
```

Step 8 interface type number

Targets an interface number on which to exclude traffic for redirection and enters interface configuration mode.

```
Device(config)# interface GigabitEthernet 0/2/0
```

Step 9 ip wccp redirect exclude in

(Optional) Excludes traffic on the specified interface from redirection.

```
Device(config-if)# ip wccp redirect exclude in
```

Redirect Access-List

The redirect access-list allows you to control which traffic should be redirected and is used with the **ip wccp** command. It is recommended to add deny statements to the redirect list for RFC 1918 addresses such as 10.0.0./8, 172.16.0.0/12, and 192.168.0.0/16 to help ensure that local traffic is not forwarded to the proxy. The following example shows how to redirect traffic only from subnet 10.1.1.0:

```
device(config)# ip access-list extended 100
device(config-ext-nacl)# permit ip 10.1.1.0 255.255.255.0 any
device(config-ext-nacl)# exit
device(config)# ip wccp web-cache redirect-list 100
device(config)# interface vlan 40
device(config-if)# ip wccp 90 redirect in
```

Group-List Access-List

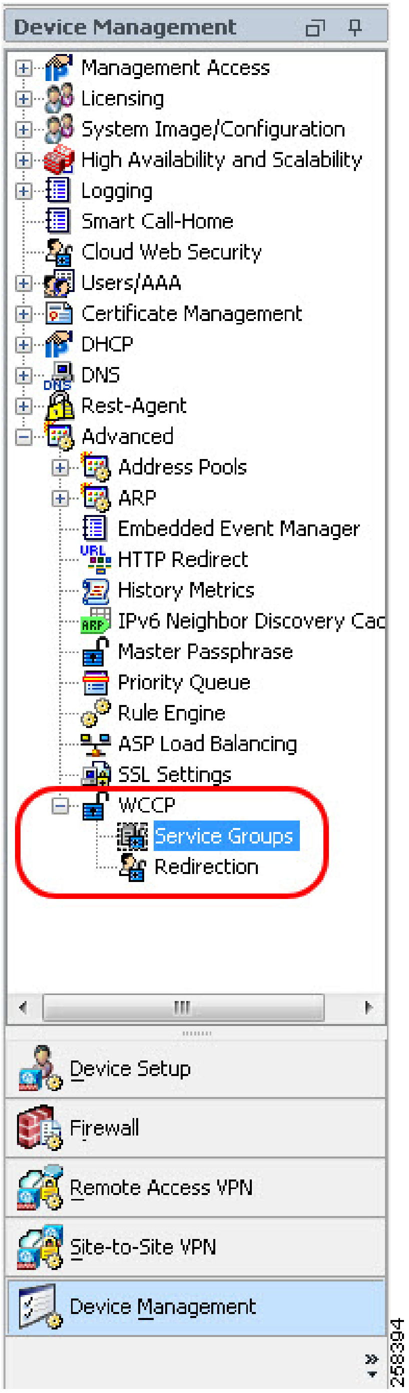
To achieve better security, you can use a standard access-list to notify the redirecting device about the IP addresses that are valid addresses for the Cisco WSA attempting to register with the current device. The following example shows a standard access-list configuration session where the access-list number is 10 for some sample hosts. When this access-list is applied to the **ip wccp** command, only proxies that are listed in the access-list will be added to the group.

```
device(config)# access-list 10 permit host 11.1.1.1
device(config)# access-list 10 permit host 11.1.1.2
device(config)# access-list 10 permit host 11.1.1.3
device(config)# ip wccp 90 group-list 10
```

Cisco Adaptive Security Device Manager (ASDM) Configuration

Step 1 Choose **Configuration**->**Device Management**->**Advanced**->**WCCP**->**Service Groups** (Figure 3-9).

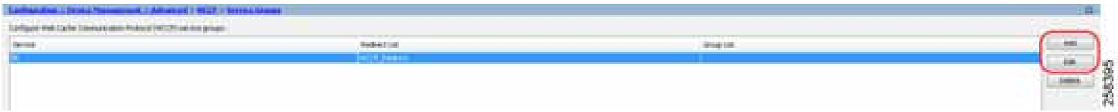
Figure 3-9 ASDM Menu



Step 2 Do any of the following (Figure 3-10):

- To add a new service group, click **Add**.
- To edit a service group, select it and click **Edit**.

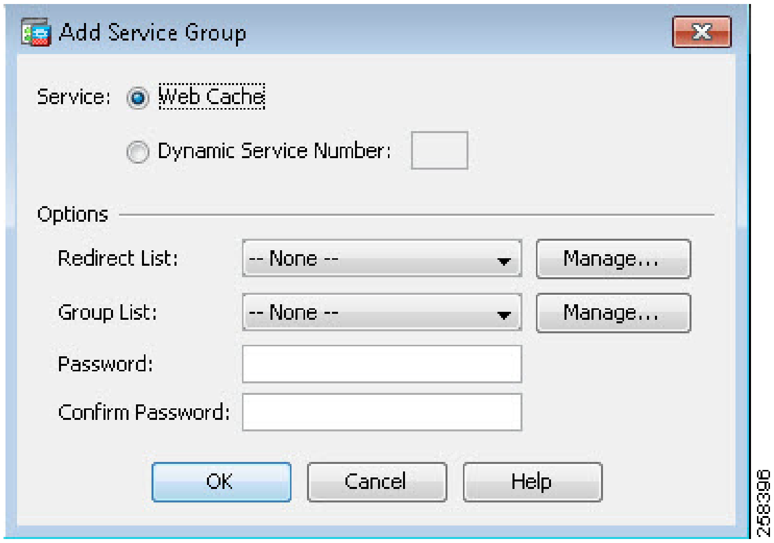
Figure 3-10 WCCP Service Group



Step 3 In the Add/Edit Service Group dialog box, configure the following options (Figure 3-11).

- Service—The type of service, one of:
  - Web Cache—The standard service, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the WCCP-enabled device. This exludes TCP port 443 HTTPS traffic.
  - Dynamic Service Number—The Cisco WSA device defines the services associated with this dynamic service number (0-254); on the ASA, you are simply associating the number with this group. For testing and validation, the dynamic service number of 90 was used.
- Redirect List—(Optional) An ACL whose permit entries define the traffic that should be redirected for this service. Click **Manage** to create new ACLs or to view the contents of an ACL.
- Group List—(Optional) An ACL whose permit entries define the WCCP-enabled devices that can provide this service.
- Password, Confirm Password—(Optional) A password up to seven characters long, which is used for MD5 authentication for messages received from the service group. You must configure the same password on the Cisco WSA.

Figure 3-11 Add Service Group



Add Service Group

Service: ● Web Cache

○ Dynamic Service Number:

Options

Redirect List: -- None --

Group List: -- None --

Password:

Confirm Password:

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes.

Configure WCCP Packet Redirection

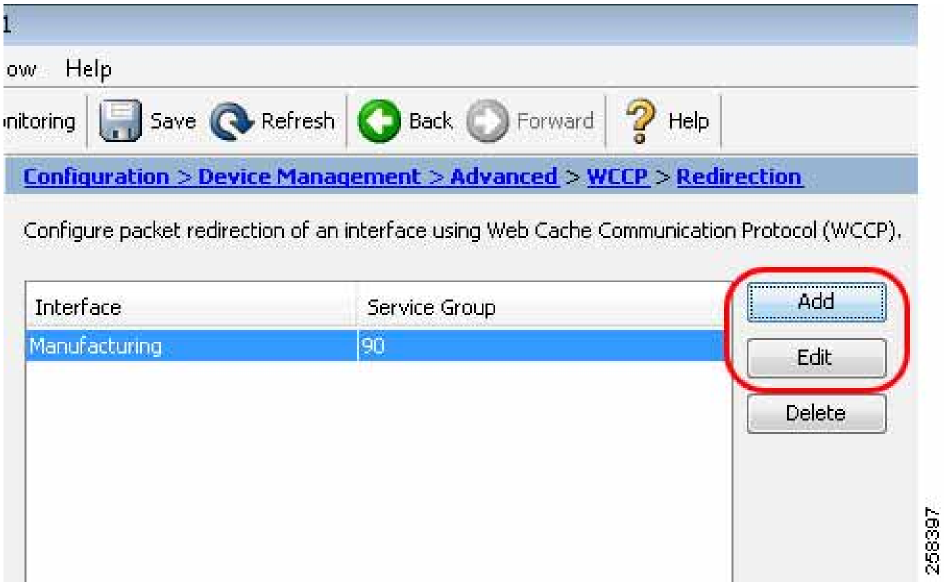
To configure packet redirection on the ingress of an interface using WCCP, perform the following steps:

Step 1 Choose **Configuration**->**Device Management**->**Advanced**->**WCCP**->**Redirection**.

Step 2 Do any of the following (Figure 3-12):

- To add redirection for an interface and service group, click **Add**.
- To edit redirection for an interface and service group, select it and click **Edit**.

Figure 3-12 WCCP Redirection



Configuration > Device Management > Advanced > WCCP > Redirection

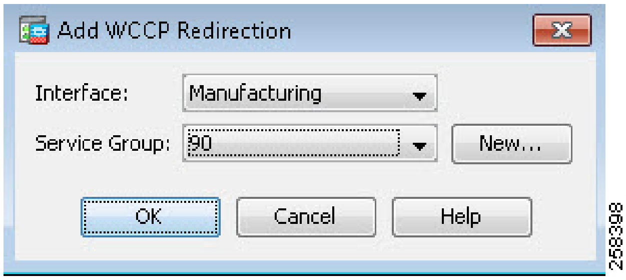
Configure packet redirection of an interface using Web Cache Communication Protocol (WCCP).

Interface	Service Group
Manufacturing	90

Step 3 In the Add/Edit WCCP Redirection dialog box, configure the following options (Figure 3-13):

- Interface—The interface whose inbound traffic you want to redirect to the WCCP-enabled device.
- Service Group—The WCCP service group for which you are redirecting traffic. Click **New** if you need to create a group.

Figure 3-13 WCCP Redirection Interface



Interface: Manufacturing

Service Group: 90

Step 4 Click **OK**.

Step 5 Click **Apply** to save your changes. Be sure to save the startup configuration once complete.

Workstation Configuration

With the Cisco WSA and WCCP v2 configuration complete, the workstations that are intended to use the proxy must be configured. Depending on the proxy configuration, transparent or explicit, the configuration varies slightly. However, both methods still require the importation of certificates generated by the Cisco WSA.

This section focuses on the Windows Operating System (Windows 7) and its associated web browsers and certificate stores. Once the certificate has been imported, a trust is created between the workstation and the Cisco WSA.

No workstation configuration besides the importation of the certificates is needed to help ensure the success of the transparent proxy deployment. With this in mind, there is no subsection listed for Transparent Redirection.

Windows Certificates

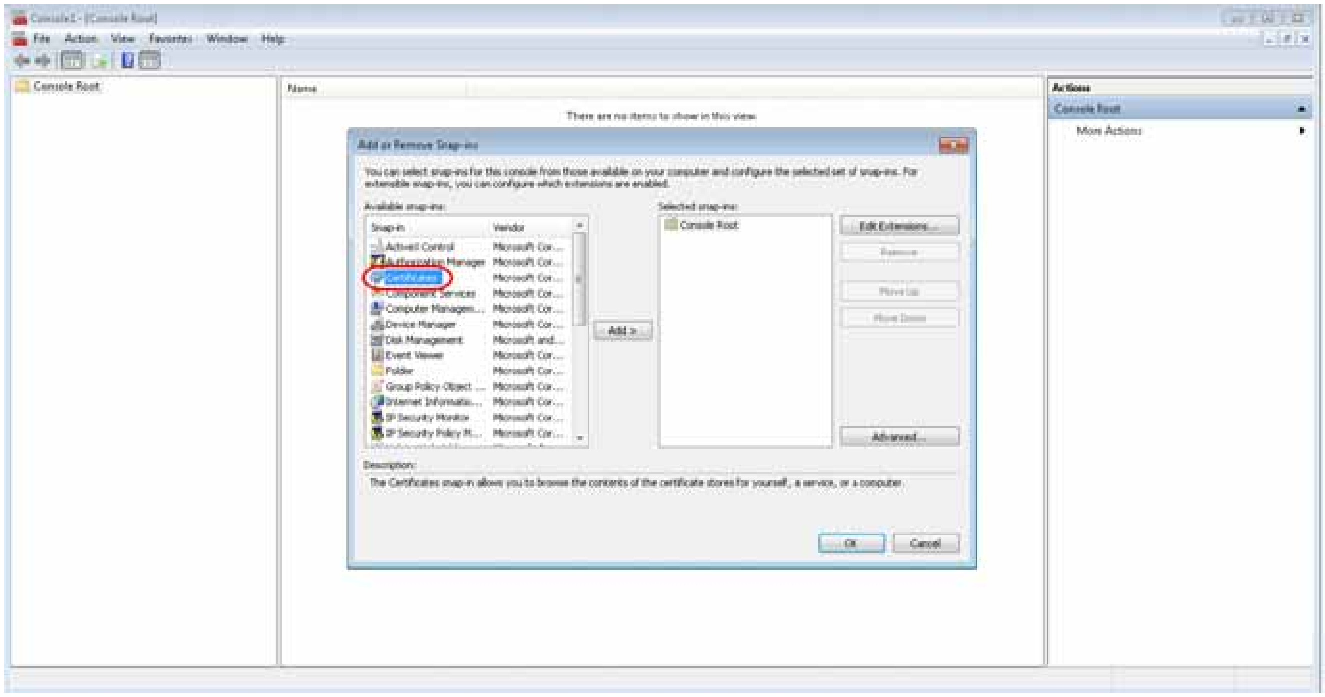
As previously mentioned, the Cisco WSA providing TLS proxy services must have the ability to decrypt the data coming from the application or EWS. To provide this service, a certificate that is used (generated by the Cisco WSA or a root CA) on the Cisco WSA must be stored on each EWS that wishes to send traffic to the cloud through the Cisco WSAs TLS proxy service. Based on testing and validation it is recommended to add the Cisco WSA certificate to each pertinent web browser and the Microsoft certificate store. This can be accomplished manually or through Group Policy; for testing this was completed manually.

Step 1 **Start**-> **Run**. Type **MMC.exe**.

Step 2 Click **File**->**Add/Remote Snap-in**.

Step 3 In the Available snap-ins list, click **Certificates** and click **Add** (Figure 3-14).

Figure 3-14 Add or Remove Snap-ins



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

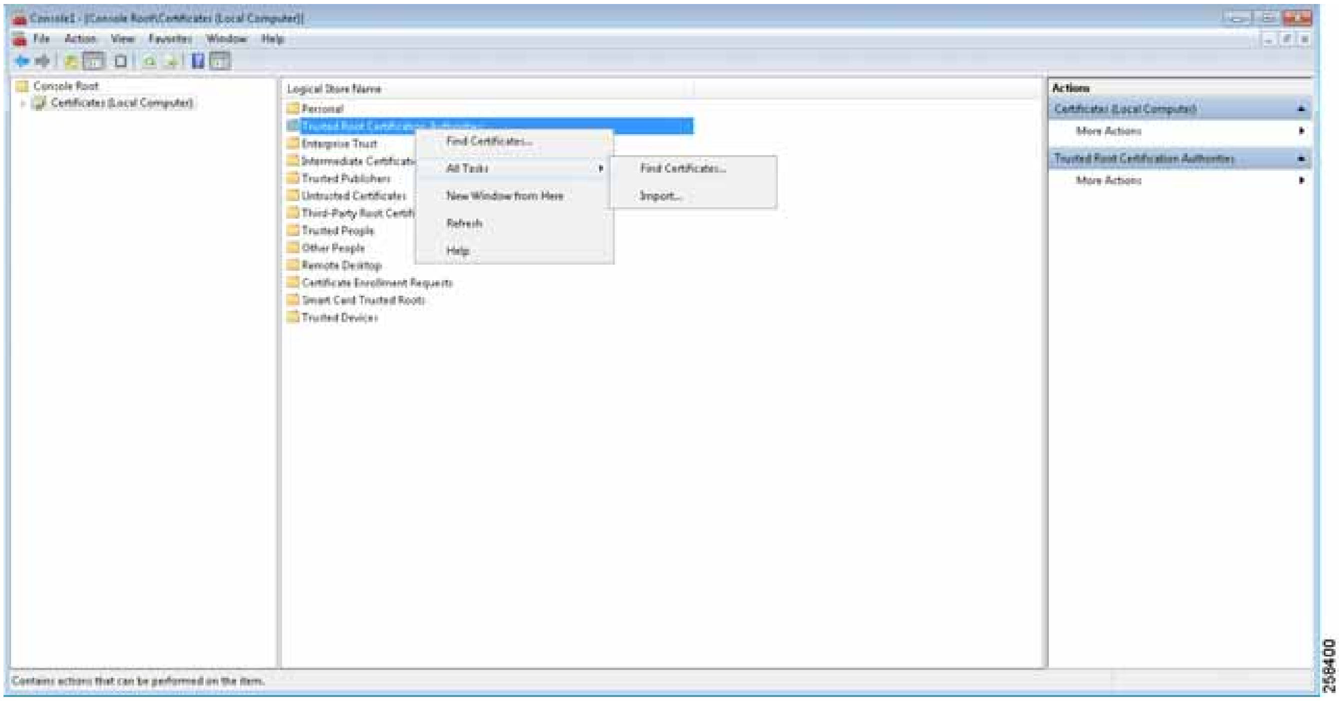
Step 4 Depending on security posture and how the application is being used, select **My User Account**, **Computer Account**, or **Service Account** and click **Next**.

Generally, for a single user computer, **My User Account** is the acceptable choice.

Step 5 Once finished, click **OK**.

Step 6 In the MMC window, click **Certificates** then right-click **Trusted Root Certification Authorities**->**All Tasks**->**Import…** (Figure 3-15).

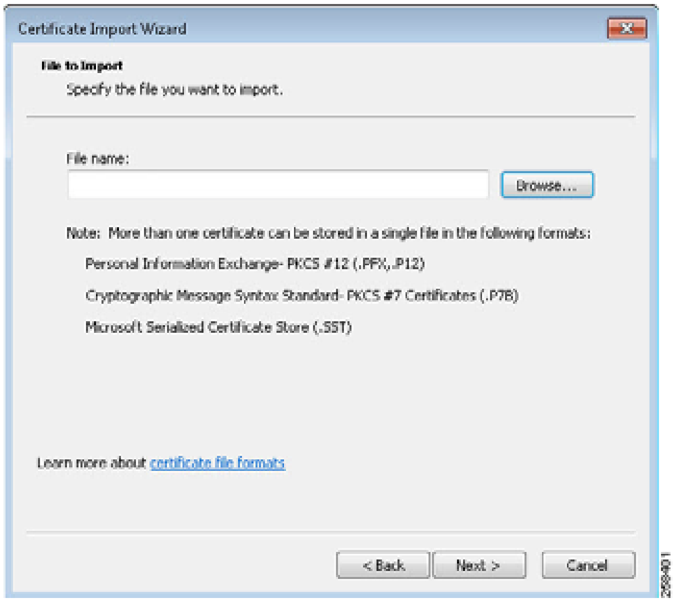
Figure 3-15 All Tasks->Import



This opens the Certificate Import Wizard where the certificate downloaded from the Cisco WSA in the previous section should be selected.

Step 7 Once the wizard is launched, click **Next** for the first prompt and then the **File to Import** window displays prompting for a file name (Figure 3-16).

Figure 3-16 Certificate Import Wizard


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

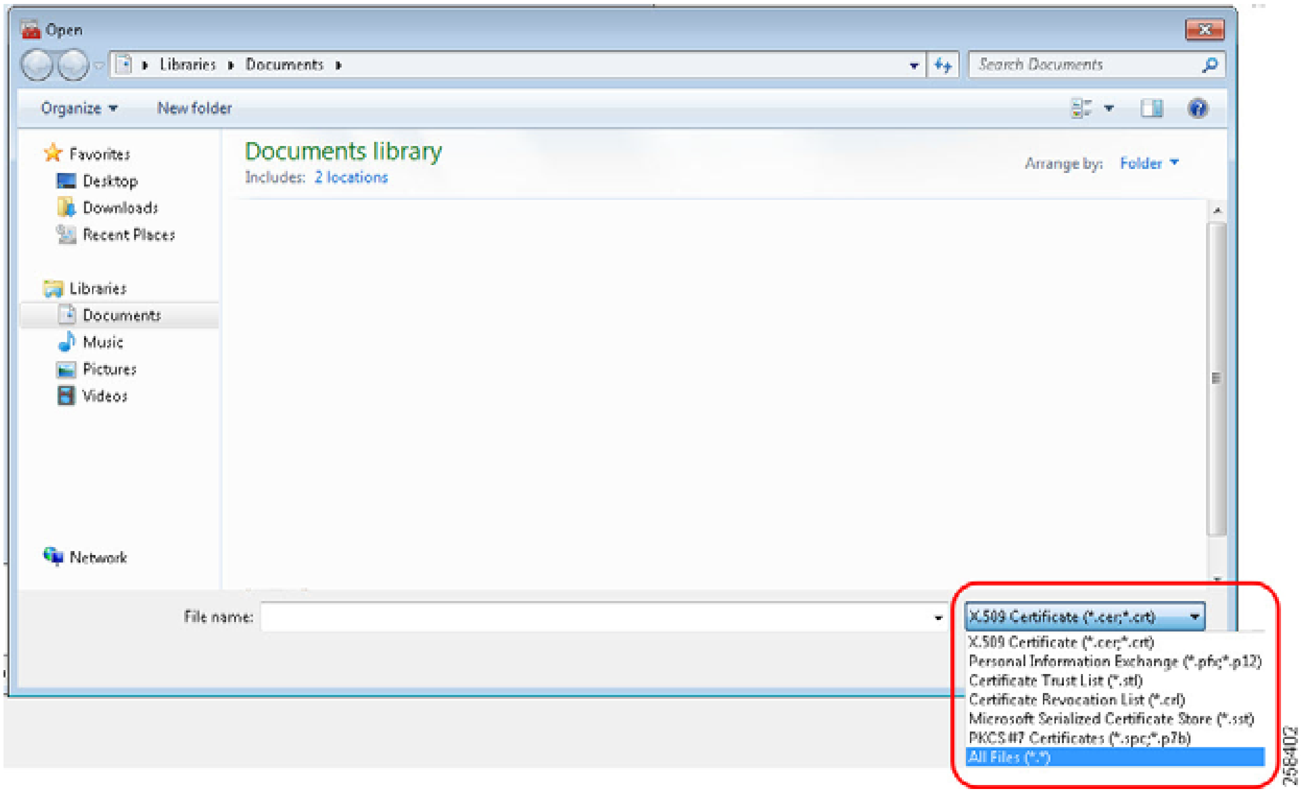
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

When browsing for the certificate using this method, it is important to note that the certificate that was downloaded from the Cisco WSA is a .pem file extension. By default, the browse feature in the certificate import wizard is looking for X.509. To locate the .pem certificate from the Cisco WSA, the file type in the browse window must be adjusted and set to **All files** (*.*) (Figure 3-17).

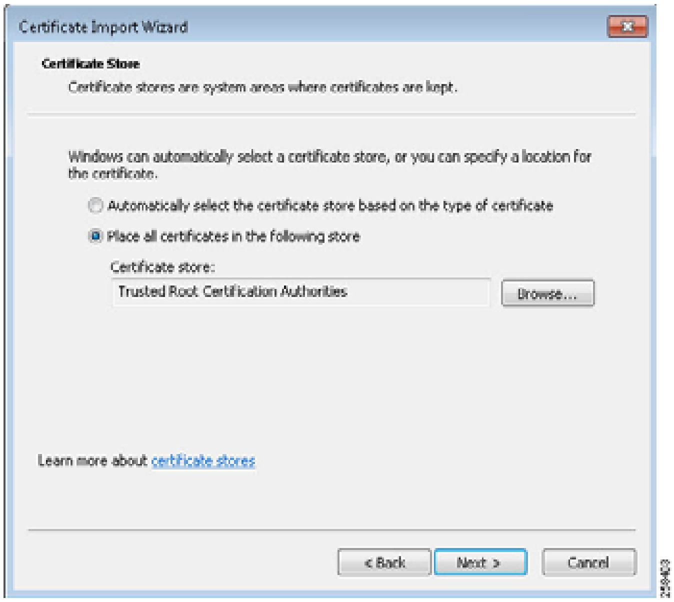
Figure 3-17 Select Certificate


Open
Libraries ▸ Documents ▸
Search Documents
Organize ▾
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Network
Documents library
Includes: 2 locations
Arrange by: Folder ▾
File name:
X.509 Certificate (*.cer;*.crt)
X.509 Certificate (*.cer;*.crt)
Personal Information Exchange (*.pfx;*.p12)
Certificate Trust List (*.stl)
Certificate Revocation List (*.crl)
Microsoft Serialized Certificate Store (*.sst)
PKCS #7 Certificates (*.spc;*.p7b)
All Files (*.*)
258402

Step 8 Once the certificate has been selected, click **Next** to display the **Certificate Store** screen (Figure 3-18).

Step 9 On this screen ensure that the **Place all certificates in the following store** is set to **Trusted Root Certification Authorities**, then click **Next**.

Figure 3-18 Certificate Store


Certificate Import Wizard
Browse...
Learn more about certificate stores
< Back
Next >
Cancel
258403

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

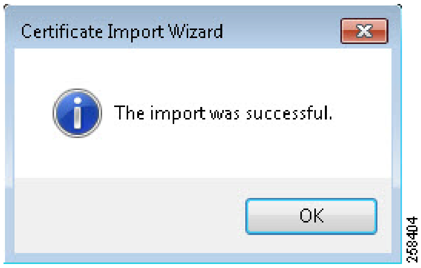
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Step 10 Verify the settings on the final screen and click **Finish**.

A window displays indicating that the import was successful (Figure 3-19).

Figure 3-19 Successful Import



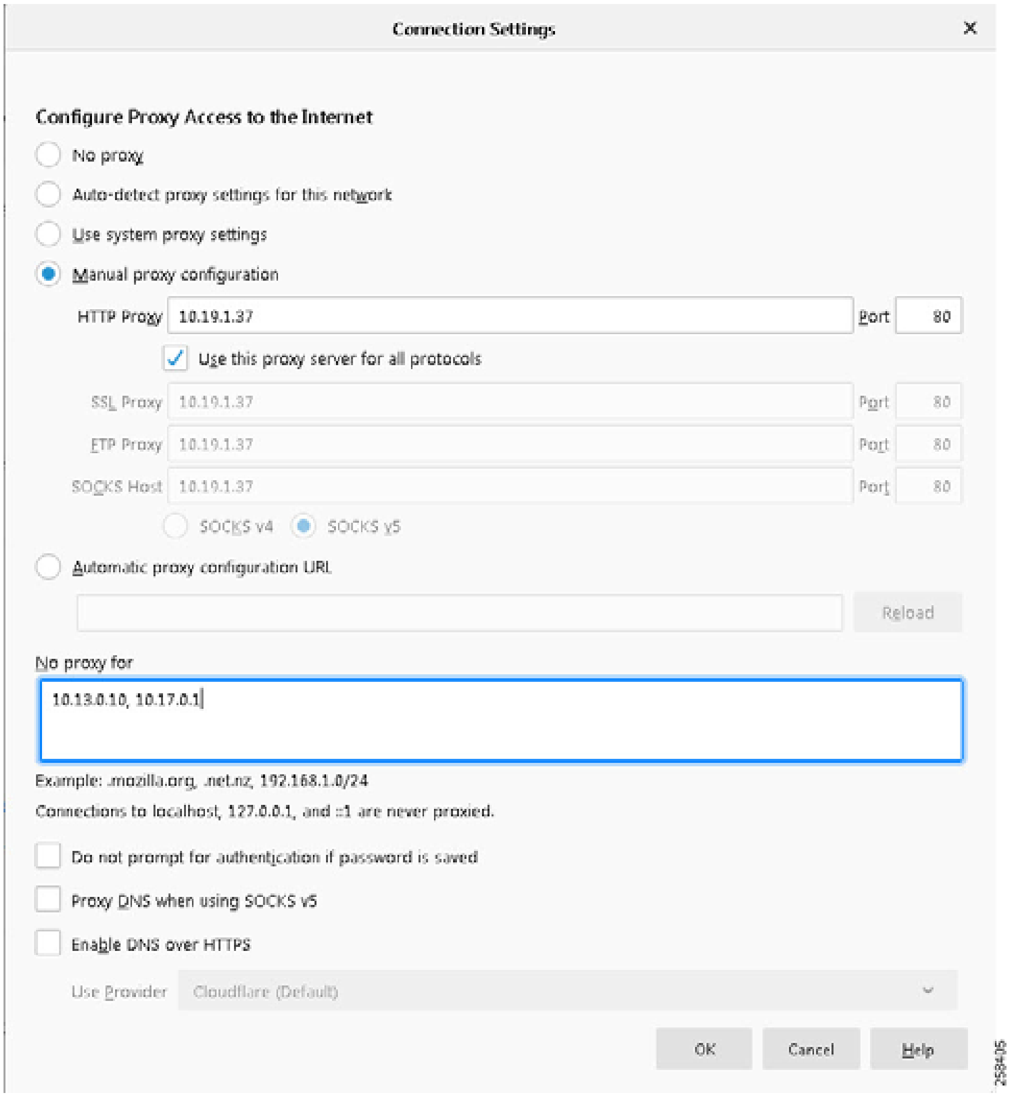
The import was successful.

Note It is also required that each web browser in use in the system (including Internet Explorer, even if not used for browsing) also has the same certificate imported into the browser as a certificate authority. Because there are various web browsers with different interfaces, this design guide does not detail the process.

Explicit Redirection

Explicit redirection of web traffic follows similar setup requirements as the WCCP transparent redirection method. The explicit redirection method does not require the dual-homed approach that was described in Interface Configuration. Explicit redirection only requires a single interface (besides management) and can exist solely in the IDMZ. The certificate must be imported to the various locations as descried in Windows Certificates. The biggest difference between the two redirection methods is that the explicit redirection requires the user to configure each web browser to explicitly redirect to the Cisco WSA proxy. As with the certificate importation, each browser has a different method to access the proxy settings and each browser is required to be set up to point to the Cisco WSA. The example below of the proxy configuration was taken from FireFox (Figure 3-20).

Figure 3-20 FireFox Connection Settings



Connection Settings ×

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 10.19.1.37 Port 80

☑ Use this proxy server for all protocols

SSL Proxy 10.19.1.37 Port 80

FTP Proxy 10.19.1.37 Port 80

SOCKS Host 10.19.1.37 Port 80

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

10.13.0.10, 10.17.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

□ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

Some important items to note in the above configuration:

- These settings could be applied via Group Policy if applicable, however, this is not detailed in this design guide.
- The **HTTP Proxy** field is where the IP address of the Cisco WSA is entered and the **Port** field is the expected port for that protocol.
- The checkbox **Use this proxy server for all protocols** is used to ensure that the address is consistent for HTTP and SSL/HTTPS. The correct port is applied based on protocol and what is shown in the **Port** field has no bearing.

- The **No proxy for field** is required for any applications that use HTTP traffic as their form of communication. Any servers or devices that the computer would communicate with via HTTP or HTTPS should be listed here. In most circumstances, entering the subnet addresses with the mask of the local network is sufficient. Ideally the proxy should only be used for traffic that is moving from a trusted to an untrusted network. When addresses are not defined in the **No proxy for field**, even basic web traffic like attempting HTTP to an Allen-Bradly 1756-EN2TR would be sent to the proxy and would not reach the end device. Even services such as the interaction between FactoryTalk AssetCentre server and FactoryTalk AssetCentre client use HTTP traffic. It is important to understand the traffic usage in the network before deploying explicit proxying.