Introduction to the Product and the Release

This chapter contains the following sections:

Introduction to the Web Security Appliance

The Cisco Web Security Appliance intercepts and monitors Internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other Internet-based threats.

What's New in AsyncOS 11.0

Feature	Description
Cisco Defense Orchestrator Integration	You can connect your appliances with Cisco Defense Orchestrator and analyze security policy configuration of your appliances to identify and resolve policy inconsistencies, model policy changes to validate their impact, and orchestrate policy changes to achieve consistency and maintain clarity in security posture. The Cisco Defense Orchestrator is a cloud-based platform that helps network operations staff establish and maintain an end-to-end security posture by managing security policies across Cisco security devices. See Connect the Appliance to Cisco Defense Orchestrator for more information.
Simplified appliance registration on CTA	You can use the **CTA Template** option to automatically select fields and criteria required to send W3C logs to the Cisco Cognitive Threat Analytics (CTA) system. See Configuring CTA-specific Custom W3C Logs for more information.

Feature	Description
Secondary DNS servers	You can now specify secondary DNS servers to resolve host name queries not resolved by the primary name servers. You can also set priority levels for the servers. The secondary DNS servers receive host name queries when the primary DNS servers return the following errors: • No Error, no answer section received. • Server failed to complete request, no answer section. • Name Error, no answer section received. • Function not implemented. • Server Refused to Answer Query. See Editing DNS Settings for more information.
`supportrequest` command enhancement	You can send a set of system and configuration information to be attached to the service request automatically, if you specify the service request number in the optional step while using the `supportrequest` command. See Web Security Appliance CLI Commands for more information.
Virtual Appliance Enhancement	Virtual appliances can now be deployed on Microsoft Hyper-V version 5.0. See the Cisco Content Security Virtual Appliance Installation Guide, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Related Topics

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

Using the Appliance Web Interface

Web Interface Browser Requirements

To access the web interface, your browser must support and be enabled to accept JavaScript and cookies. It must be able to render HTML pages containing Cascading Style Sheets (CSS).

The Cisco Web Security Appliance follows the Target Environments set by YUI: http://yuilibrary.com/yui/environments/

Your session automatically times out after 30 minutes of inactivity.

Some buttons and links in the web interface cause additional windows to open. Therefore, you may need to configure the browser's pop-up blocking settings in order to use the web interface.

Note Only use one browser window or tab at a time to edit the appliance configuration. Also, do not edit the appliance using the web interface and the CLI at the same time. Editing the appliance from multiple places concurrently results in unexpected behavior and is not supported.

Enabling Access to the Web Interface on Virtual Appliances

By default, the HTTP and HTTPS interfaces are not enabled on virtual appliances. To enable these protocols, you must use the command-line interface.

Step 1 Access the command-line interface. See Accessing the Command Line Interface.

Step 2 Run the `interfaceconfig` command.

Pressing Enter at a prompt accepts the default value.

Look for the prompts for HTTP and HTTPS and enable the protocol(s) that you will use.

Accessing the Appliance Web Interface

If you are using a virtual appliance, see Enabling Access to the Web Interface on Virtual Appliances , on page 3.

Step 1 Open a browser and enter the IP address (or hostname) of the Web Security appliance. If the appliance has not been previously configured, use the default settings:

```
https://192.168.42.42:8443
```

-or-

```
http://192.168.42.42:8080
```

where `192.168.42.42` is the default IP address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for `HTTPS`.

Otherwise, if the appliance is currently configured, use the IP address (or host name) of the M1 port.

Note You must use a port number when connecting to the appliance (by default, port `8080`). Failing to specify a port number when accessing the web interface results in a default port 80, Proxy Unlicensed error page.

Step 2 When the appliance login screen appears, enter your user name and passphrase to access the appliance.

By default, the appliance ships with the following user name and passphrase:

- User name: **admin**
- Passphrase: **ironport**

If this is the first time you have logged in with the default **admin** user name, you will be prompted to immediately change the passphrase.

Step 3 To view a listing of recent appliance access attempts, both successes and failures, for your user name, click the recent-activity icon (**i** or **!** for success or failure respectively) in front of the “Logged in as” entry in the upper right corner of the application window.

Committing Changes in the Web Interface

Step 1 Click the **Commit Changes** button.

Step 2 Enter comments in the Comment field if you choose.

Step 3 Click **Commit Changes**.

Note You can make multiple configuration changes before you commit all of them.

Clearing Changes in the Web Interface

Step 1 Click the **Commit Changes** button.

Step 2 Click **Abandon Changes**.

Supported Languages

AsyncOS can display its GUI and CLI in any of the following languages:

- German
- English
- Spanish
- French
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Chinese
- Taiwanese

The Cisco SensorBase Network

The Cisco SensorBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. SensorBase provides Cisco with an assessment of reliability for known Internet domains. The Web Security appliance uses the SensorBase data feeds to improve the accuracy of Web Reputation Scores.

SensorBase Benefits and Privacy

Participating in the Cisco SensorBase Network means that Cisco collects data and shares that information with the SensorBase threat management database. This data includes information about request attributes and how the appliance handles requests.

Cisco recognizes the importance of maintaining your privacy, and does not collect or use personal or confidential information such as usernames and passphrases. Additionally, the file names and URL attributes that follow the hostname are obfuscated to ensure confidentiality. When it comes to decrypted HTTPS transactions, the SensorBase Network only receives the IP address, web reputation score, and URL category of the server name in the certificate.

If you agree to participate in the SensorBase Network, data sent from your appliance is transferred securely using HTTPS. Sharing data improves Cisco's ability to react to web-based threats and protect your corporate environment from malicious activity.

Enabling Participation in The Cisco SensorBase Network

Note Standard SensorBase Network Participation is enabled by default during system setup.

Step 1 Choose **Security Services > SensorBase**.

Step 2 Verify that SensorBase Network Participation is enabled.

When it is disabled, none of the data that the appliance collects is sent back to the SensorBase Network servers.

Step 3 In the Participation Level section, choose one of the following levels:

- **Limited.** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
- **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a more robust database, and continually improves the integrity of Web Reputation Scores.

Step 4 In the AnyConnect Network Participation field, choose whether or not to include information collected from clients that connect to the Web Security appliance using Cisco AnyConnect Client.

AnyConnect Clients send their web traffic to the appliance using the Secure Mobility feature.

Step 5 In the Excluded Domains and IP Addresses field, optionally enter any domains or IP addresses to exclude from traffic sent to the SensorBase servers.

Step 6 Submit and commit your changes.