Additional Configurations

The following topics describe some additional features that you can configure in your appliance. See the online help or user guide for your AsyncOS release for complete details.

User Policies

Use the web interface to create policies that define which users can access which web resources as necessary.

- Identify Users—Choose **Web Security Manager** > **Identities** to define groups of users that can access the Internet.
- Define Access Policies—Choose **Web Security Manager** > **Access Policies** to control user access to the Internet by configuring which objects and applications to allow or block, which URL categories to monitor or block, and web reputation and anti-malware settings.

You can also define several other policy types to enforce your organization's acceptable use policies by controlling access to the Internet. For example, you can define policies for decrypting HTTPS transactions and other polices that control upload requests.

For information about configuring policies on the Cisco Web Security Appliance appliance, see the "Working with Policies" chapter in the *AsyncOS for Cisco Web Security Appliances User Guide*.

Reporting

You can view statistics about blocked and monitored web traffic on your network by viewing reports available in the web interface. You can view reports about the top URL categories blocked, client activity, system status, and more.

More Information

There are other features that you may want to configure for your Cisco Web Security Appliance. For more information about configuring feature keys, end user notifications, logging, and for details about other available

web security appliance features, see the Cisco Web Security Appliance S196, S396, S696, and S696F documentation.