Executive Summary

Web 2.0, collaboration, and mobility technologies are redefining how, when, and where business gets done. This helps enterprises boost productivity, increase business agility, and enable greater collaboration among employees, customers, and partners. The old model, one in which security was a means of locking down access, has been replaced with one of enablement, which allows people to collaborate more freely.

Organizations depend on authentication, authorization, and accounting to enable collaboration while retaining the ability to provide privilege-based access, control non-productive activities, and keep a user activity trail.

The Cisco® IronPort S-Series Web Security Appliance helps enterprises secure and control web traffic by offering a fast web proxy, URL filters, multiple layers of malware defense, antimalware scanning engines, multiprotocol support, and comprehensive management and reporting. The Cisco IronPort® Web Security Appliance supports a wide range of authentication mechanisms, giving enterprises a greater degree of control over their web traffic. But with this support comes a complexity that can overwhelm an IT administrator, making it difficult to identify what functions should be used under what circumstances.

This white paper takes a scenario-based approach to help you identify the capabilities that you need, and it also explains how those functions work. You can then refer to the Cisco IronPort AsyncOS® for Web User Guide 6.0 to make the required configuration changes to enable the functions you need.

This paper contains the following topics:

- Introduction to authentication, authorization, and accounting
- Supported authentication protocols
- Authentication scenarios
- Authorization scenarios
- Accounting scenarios
Introduction

This section introduces the concepts of authentication, authorization, and accounting.

- **Authentication.** Authentication is a mechanism by which one entity establishes its identity to another entity. The entities that are typically involved are clients and servers. User agents such as browsers and FTP clients are examples of clients. Proxies and origin servers are examples of servers. Authentication is achieved in a transaction where a client presents its credentials to the server and if the credentials are verified successfully, then authentication succeeds. Usernames and passwords, one-time tokens, and client certificates are some examples of credentials used today.

- **Authorization.** Authorization is the process of verifying that an authenticated subject has the authority to perform a certain operation. Authority is based on the subject’s privileges. For example, does the authenticated user John Doe have privileges to access the third-floor printer at this time of the day?

- **Accounting.** Accounting refers to a record of the transactions performed by a subject. This can be achieved with access logs and error logs.

Authentication Protocols

This section describes the authentication protocols that are supported in the Cisco IronPort Web Security Appliance.

**Lightweight Directory Access Protocol (LDAP)**

The Cisco IronPort Web Security Appliance supports authentication using standard and secure LDAP versions 2 and 3. Secure LDAP requires version 3. A wide variety of LDAP servers are supported, including OpenLDAP, Sun ONE Directory Server, and Active Directory (AD). Although you can define multiple LDAP authentication realms in the Cisco IronPort Web Security Appliance, the appliance supports only a basic authentication scheme for LDAP.

Refer to the *Cisco IronPort AsyncOS for Web User Guide* for a detailed description of LDAP configuration options.

**LDAP Authentication Flow**

1. Request for http://www.ironport.com
2. WSA sends auth dialog to client
3. Client sends auth credentials to WSA
4. WSA sends credentials to LDAP server
5. LDAP server validates credentials and sends response to WSA
6. WSA sends response to client
NT LAN Manager (NTLM)
The Cisco IronPort Web Security Appliance supports Active Directory 2000, 2003 (Cisco IronPort Web Security Appliance 5.6 and above), and 2008 (Cisco IronPort Web Security Appliance 6.0 and above). It also supports both the Basic and NTLMSSP schemes for NTLM authentication. The NTLMSSP authentication scheme enables single sign-on because the user credentials are retrieved directly from the host machine and the user is never prompted to provide authentication credentials. The Cisco IronPort Web Security Appliance uses a challenge-response mechanism between the client and the Active Directory server to authenticate users.

To configure an NTLM authentication realm on the Cisco IronPort Web Security Appliance, the appliance must join an Active Directory domain. If this AD domain has a trust relationship with other AD domains, users belonging to those domains can also be authenticated. You may specify up to three Active Directory servers for failover.

Refer to the Cisco IronPort AsyncOS for Web User Guide for a detailed description of NTLM configuration options.

NTLMSSP Authentication Flow

Authentication Scenarios
This section describes how authentication features of the Cisco IronPort Web Security Appliance can be used in real-world scenarios.

How does the Cisco IronPort Web Security Appliance track user credentials?
Once the user has authenticated successfully, the Cisco IronPort Web Security Appliance associates the transactions with the user using authentication “surrogates.” Two authentication surrogates are supported: IP addresses and cookies. You can also configure the Cisco IronPort Web Security Appliance to not use any surrogate when authenticating users. The scenarios to choose the surrogates and the associated functions are described below.

Refer to the Cisco IronPort AsyncOS for Web User Guide for information configuring authentication surrogates.
COOKIE SURROGATES

Scenario 1: Environments that do not have an IP address for user mapping, for example, in Citrix environments.

Scenario 2: Organizations that use Dynamic Host Configuration Protocol (DHCP) extensively. Therefore, the same machine may get assigned different IPs at different times.

In both the above scenarios, tracking users with an IP address will not work well, so you need to use cookies.

A cookie surrogate can be used as a session or a persistent cookie. Session cookies are valid only for a particular browser session. For a new session of a browser, the cookie becomes invalid and the client is authenticated again. Persistent cookies are valid until they time out, and they survive browser restarts. As long as the persistent cookie is valid, the user is not authenticated across browser sessions.

The figure below illustrates how cookie-based surrogates work in both explicit forward mode and transparent mode (applicable to Cisco IronPort AsyncOS 6.0 and later).

Cookie-Based Surrogates

The advantage of using cookies is that authentication stays with the browser rather than the user name or IP. Because of this, cookies are considered safer than IP address surrogates. One disadvantage of using cookies is that they do not work for applications that do not support cookies, such as browsers where cookies are disabled or FTP clients.

IP ADDRESS SURROGATES

Scenario 1: Organizations or customers that do not use cookies in their environment because of concerns about invasion of privacy. Some organizations have a corporate policy against cookie usage.

Scenario 2: Organizations or customers that interact with many HTTPS websites where cookie-based surrogates do not work.

Scenario 3: Organizations that need authentication for custom applications that do not support cookies.
In all the above scenarios, it is recommended to use IP address surrogates. Authentication requests are tracked using the client IP address. While an entry of the client IP address is available in the authentication cache of the Cisco IronPort Web Security Appliance, the client is not authenticated again.

**IP-Based Surrogates**

An advantage of IP address surrogates is that they work with HTTPS requests. Also, IP address surrogates work with all applications, including those that do not support cookies. A disadvantage of IP address surrogates is that the authentication remains with the IP address and not the user. If a different user logs in on the same IP address, the user is considered authenticated.

**AUTHENTICATION WITHOUT ANY SURROGATES**

The web proxy does not use any surrogate to keep track of users, and it authenticates the user for every new TCP connection. This option is available only in explicit forward mode.

The Cisco IronPort Web Security Appliance uses a time-to-live (TTL) for the authentication credentials so that the user is not prompted for the credentials again for a specified period of time.

**How can user credentials be sent securely from the client to the Web Security Appliance?**

**Scenario:** Organizations that do not want to send user credentials in clear text from the client to the web proxy, since this can be perceived as a security hole.

When a client makes a connection to the Cisco IronPort Web Security Appliance and sends authentication credentials, the credentials are sent in clear text and can be easily captured via packet capture. However, you can configure the Cisco IronPort Web Security Appliance so that clients can send credentials securely. This is called “credential encryption” in Cisco IronPort AsyncOS 6.0 and later. When credential encryption is used, IP or cookie surrogates must be configured. Credential encryption works both in explicit forward and transparent mode.
In order to establish a secure connection between the client and the Cisco IronPort Web Security Appliance, either a default or custom HTTPS certificate and private key are installed in the Cisco IronPort Web Security Appliance.

Refer to the Cisco IronPort AsyncOS for Web User Guide for more information on configuring credential encryption.

How can authentication be used with other proxies?

Scenario: Organizations that need the Cisco IronPort Web Security Appliance to work with their existing proxies. The existing proxies may be used as upstream proxies and may have authentication enabled.

Upstream proxies may be deployed in an organization’s environment for various reasons. The following list shows the different combinations of deploying a Cisco IronPort Web Security Appliance with an upstream proxy.

<table>
<thead>
<tr>
<th>Deployment Mode</th>
<th>Cisco IronPort Web Security Appliance</th>
<th>Upstream Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both in explicit forward mode</td>
<td>Client authenticates only once, if only the Cisco IronPort Web Security Appliance or only upstream proxy require authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client authenticates twice if both the Cisco IronPort Web Security Appliance and upstream proxy require authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Client may not require authentication if it is in a single sign-on environment</td>
<td></td>
</tr>
<tr>
<td>Cisco IronPort Web Security Appliance in explicit forward mode and upstream proxy in transparent mode</td>
<td>Recommended to be configured for authentication</td>
<td>Not recommended to be configured for authentication, since client is not aware of the existence of this proxy</td>
</tr>
<tr>
<td>Both in transparent mode</td>
<td>Can be configured for authentication even though client is not aware of the web proxy</td>
<td>Not recommended to be configured for authentication, since client is not aware of the existence of this proxy</td>
</tr>
<tr>
<td>Cisco IronPort Web Security Appliance in transparent mode and upstream proxy in explicit forward mode</td>
<td>Not recommended to be configured for authentication, since client is not aware of the Cisco IronPort Web Security Appliance</td>
<td>Recommended to be configured for authentication</td>
</tr>
</tbody>
</table>
What is authentication at the origin server?
Some origin servers on the Internet require users to authenticate before they can be granted access. Cisco IronPort Web Security Appliance authentication does not interfere with authentication at the origin server. In such cases, the HTTP headers show two levels of authentication: one for proxy authentication and another for origin server authentication. Proxy authentication is processed first, followed by origin server authentication.

How does the Cisco IronPort Web Security Appliance effectively fail over and fail back to other authentication servers?

**Scenario:** When authentication is enabled and an organization’s Internet traffic is very high, the amounts of authentication requests that are sent tend to be very high as well. This can result in a heavy load on authentication servers, and requires failover capabilities.

The Cisco IronPort Web Security Appliance allows administrators to define and add multiple authentication servers. In Cisco IronPort AsyncOS 6.0 and later, the Cisco IronPort Web Security Appliance supports up to three Active Directory or LDAP servers in a single authentication realm. This is useful for the scenario mentioned above, where an organization can add multiple authentication servers to enable failover capability. The Cisco IronPort Web Security Appliance connects to the authentication server that is first in the list of servers mentioned in the realm. This ensures a low latency.

Failover is the ability to seamlessly switch to redundant servers upon failure of primarily active servers. When an active server serving requests to a client fails or shuts down abruptly, any subsequent requests are tried on the redundant servers one at a time until a connection is successfully established. Once a connection is successfully established, this server caters to all subsequent requests until another failure of the server. The user experience is not hindered and the user is not aware that failover has occurred.

Failback is the ability to seamlessly start using the primary server once the primary server comes back up again. To achieve this, the health-monitoring program of the appliance periodically tests connectivity to the primary server. If the primary server is up, the appliance fails back to the primary server.

How can a guest user be provided access?

**Scenario:** Organizations that want to provide guests with restricted Internet access instead of blocking all access. Examples of guests are visitors, partners, contractors, part-time students, and a new hire until she gets an account in the user directory.

Use the guest access feature in Cisco IronPort AsyncOS 6.0 and later to address this scenario. The feature is enabled via the Identity page using a checkbox labeled “Support Guest privileges for users failing authentication.” After you enable guest access in the Identity group, you can use the guest identity to create access, routing, or decryption policies for guests.

When a request hits an identity group that applies to guests, the user is prompted to authenticate. If the user credentials are invalid, the user falls in a guest access policy. You can log the guest user in the access logs by either the user name as entered by the end user, or by the IP address. Each guest user name/IP address is prefixed by “[Unauthenticated].”

Refer to the *Cisco IronPort AsyncOS for Web User Guide* for information on configuring guest access.
How can a user re-authenticate?

Scenario 1: Shared environments such as hospitals, universities, and libraries where users browse the Internet using shared workstations. Every time a new user accesses the shared resource, the user must be asked to authenticate.

Scenario 2: Environments where a user may have multiple roles in the organization, such as an engineer and a manager, and the user needs different levels of access for each role. As an engineer, when the user tries to access a resource that needs manager privileges, the user must be prompted for re-authentication.

In Cisco IronPort AsyncOS 6.0 and later, the re-authentication feature provides a mechanism for a user to authenticate again upon encountering a blocked page based on restrictive URL filtering in access policies. Re-authentication is not triggered for resources blocked by web reputation scores or malware scanning verdicts. Also, if the client is using an identity with no authentication required, then the user is not prompted for re-authentication and is presented with a block page.

Refer to the Cisco IronPort AsyncOS for Web User Guide for information on configuring the re-authentication feature.

How can I determine membership if a member is not part of a group object?

Scenario: Organizations that have organized their directory structures such that users are not part of any group, or the group object does not have the information about the user.

Group information of a user may be stored in different ways in an LDAP server. For example, users can be grouped by group object or by user object.

Cisco IronPort AsyncOS 6.0 and later support options to fetch user group information using either user object or group object in the LDAP server.

Refer to the Cisco IronPort AsyncOS for Web User Guide for information on configuring this feature.

Authorization Scenarios

This section describes how using authorization with a Cisco IronPort Web Security Appliance can be used to enforce acceptable use policies.

Scenario 1: Organizations that want to control access to individuals based on their identity or role. For example, they want to grant more restricted access to an engineer than a vice president.

When a request is received from a client, an identity is assigned to the request based on one or more criteria, such as subnet, ports, authentication realms, and so on. The policies that are based on this identity determine the user’s authorization—in other words, the privileges to access the Internet. These could be access, routing, data security, external DLP, or decryption policies.

Scenario 2: Organizations that want to restrict access to specific browsers.

A policy can be defined such that users who access the Internet cannot use a specific browser. For example, an organization may not want users to use Firefox 2.
Scenario 3: Organizations that want to restrict certain protocols for authenticated users.
A policy can be defined such that after authentication succeeds, certain protocols are not allowed for the authenticated users. For example, an organization may not want to allow certain authenticated users, such as software programmers, to use FTP.

Scenario 4: Organizations that want to restrict authenticated users for a certain time range.
A policy can be defined such that after authentication succeeds, the authenticated users get access to the Internet for a certain period of time. For example, an organization may want to allow access to shopping websites only after business hours.

Accounting Scenarios
This section describes how Cisco IronPort Web Security Appliance log files can be used for accounting purposes.

Scenario: Organizations that want to track, monitor, or audit transactions of their employees. The head of the IT department wants to present data to senior management on how the network resources are being used.

Access logs and authentication logs are used to achieve accounting of user actions.

- **Access logs** provide descriptive information about each user transaction. Access log entries provide information on how the appliance handled each transaction. Information about the authenticated user is also available in the access log. Following is an example of an entry in the access log.

  123253620.642 922 172.28.5.206 TCP_MISS/200 24520 GET http://www.ironport.com/ HTTP/1.1 gtuser5@LDAP DIRECT/www.ironport.com text/html DEFAULT_CASE-MySubnetAccessPolicy-MySubnetIdentity-DefaultRouting<Comp,ns,0,-,-,-,-,0,-,-,-,-,-> "-"

  Refer to the *Cisco IronPort AsyncOS for Web User Guide* for details on access log fields.

- **Authentication logs** are used to provide information for authentication transactions. They are primarily used to provide information about authentication decisions or failure or success. Following is an example of an entry in the authentication log.


There are five log levels that are available for access logs and authentication logs: Critical, Warning, Information, Debug, and Trace. The default log level is Information.

In the Cisco IronPort Web Security Appliance monitor dashboard, reports for client web activity can also be used for accounting. The “Top client by total web activity” bar chart shows total transactions for a user. The “Top clients by transactions blocked” bar chart shows the number of transactions that were blocked for a user. This gives a picture of the user’s activity. The “Client details” table gives a summary and also details on the bandwidth saved, high-risk transactions blocked by URL category, web reputation score, and malware.

Refer to the *Cisco IronPort AsyncOS for Web User Guide* for details on the Monitor page.
Conclusion

As Internet usage continues to increase, authentication and authorization are critical for the enterprise to gain the desired visibility into (and apply the necessary control over) web transactions. Managing authentication and authorization can be challenging because each enterprise has unique environments including user directories, the way the groups are set up, browsers, policies on cookie usage, and more. A secure web gateway should be flexible enough to fit into diverse environments, yet able to provide granular controls based on user identity.

As explained in this paper, the Cisco IronPort S-Series Web Security Appliance provides authentication, authorization, and accounting capabilities that provide that flexibility—making it an ideal choice to fit diverse enterprise needs.

If you require additional help make the required configuration changes to enable the functions you need, please contact your Cisco Systems Engineer.

Appendix

The following section summarizes the different authentication features that are available in the Cisco IronPort Web Security Appliance.

- **Authentication surrogates.** IP, cookie, and no surrogates. This feature can be used to associate one or more transactions with a user. Two forms of objects are used to achieve this association: IP addresses and cookies. See Section 7.1 for more details.

- **Secure client authentication.** This feature can be used to ensure that a transaction between the client and the web proxy is secure so that user credentials are not exposed. See Section 7.2 for more details.

- **Upstream proxies.** This feature highlights how authentication in the Cisco IronPort Web Security Appliance should be set up if upstream proxies are deployed in the network. See Section 7.3 for more details.

- **Origin server authentication.** This feature highlights how the Cisco IronPort Web Security Appliance evaluates multiple authentication requests via HTTP headers. See Section 7.4 for more details.

- **Failover and failback.** This feature highlights how the Cisco IronPort Web Security Appliance handles authentication requests when authentication servers fail over and fail back. See Section 7.5 for more details.

- **Failed authentication.** This feature can be used to provide minimal Internet access to users who are not part of the organization. See Section 7.6 for more details.

- **Re-authentication.** This feature can be used to generate levels of authentication for URL categories. See Section 7.7 for more details.