How To Configure Secure Browsing For An HTTPS Service

Secure browsing can be enabled ONLY for HTTPS Services.

Overview

The Barracuda Web Application Firewall integrates with armored browsers to mitigate risks from malware infected clients. Key loggers and cache miners on client desktops and laptops can introduce risks such as session hijacking, credential theft and leakage of sensitive information. By using armored browsers, sensitive web applications such as Net-banking applications or trading platforms can push a layer of security onto the client side to protect applications from infected hosts.

Armored browsers reduce client-side risk by providing a temporary layer around a browser connecting to a secured website. The website administrator defines a specific security policy to protect sensitive data from theft and data leakage. When the browser is closed, the browser leaves no data remnants.

Currently, the Barracuda Web Application Firewall integrates with Quaresso Protect On Q (PoQ) armored browser, which is based on the Microsoft Internet Explorer and is available only on Windows operating systems.

Components of Secure Browsing

The secure browsing environment includes the following components:

- Armored Browser
- Credential Server
- Session Validator
- Credential Manager

Armored Browser

The armored browser is a temporary browser created on a client machine when it attempts to access a website enforcing secure browsing. The browser is instantiated remotely by the Credential Server component.

The armored browser protects the website from client-side weaknesses by providing a temporary security layer around the browser. The Credential Server controls the browser settings. All temporary files are cleared when the browser is closed.

Credential Server

A credential server is a server side component which downloads to clients the secured browser instance, and validates incoming requests.

You can configure credential servers on the **WEBSITES > Secure Browsing > Credential Servers** section. For more information, see Adding a Credential Server.

Session Validator

The Session Validator ensures that access to the secured web applications is via a secured browser instance with a valid session ID.

The Session Validator is deployed either as a module on the server or integrated with a reverse proxy deployed in front of the web server.

The Barracuda Web Application Firewall acts as the Session Validator. The administrators need to configure a secure browsing policy and associate it with the website that needs to be secured. The **WEBSITES > Secure Browsing**, **Add Secure Browsing Policy** enables you to define custom access rule and associate with your website. For more information, see Adding a Secure Browsing Policy.

Credential Manager

The Credential Manager is used to configure the Credential Servers.

How Secure Browsing Works

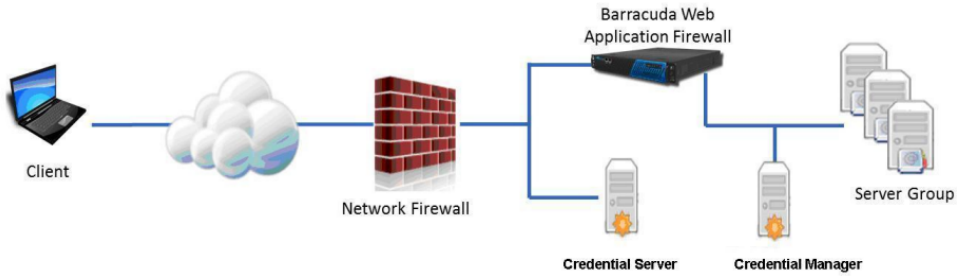
An HTTPS Service is protected by configuring secure browsing using the following steps:

1. A user attempts to access a protected website using their normal browser.
2. The Barracuda Web Application Firewall intercepts the request and checks if the request contains an armored browser specific header or not.
3. If not, the user is redirected to a credential server to download the armored browser. Once the download is complete, a new browser session is launched through which the user is allowed to access the protected website.
4. If the request is from an armored browser session, then the Barracuda Web Application Firewall checks for the armored browser specific header, and validates with the credential server.
5. If the credential server acknowledges that the header is valid, the client is allowed to access the protected website. If not, the request is blocked.

Configuring Secure Browsing

To enable secure browsing for an HTTPS Service through the Barracuda Web Application Firewall, do the following:

- Add a Credential Server
- Add a Secure Browsing Policy



Adding a Credential Server

The Barracuda Web Application Firewall uses the configured credential server to verify the armored browser is being used to access the service. A service should be associated with only one credential server.

Steps to add a credential server:

1. Go to the **WEBSITES > Secure Browsing** page.
2. In the **Credential Servers** section, click **Add Credential Server**. The **Add Credential Server** window appears, specify values for the following fields:
    1. **Name** – Enter a name for the credential server.
    2. **Armored Browser Type** – Select the armored browser type from the list.
    3. **Server Name /IP Address** – Enter the name or IP address of the Credential Server to be used for

protecting web applications.

4. **Server Port** – Enter the port number of the Credential Server.
5. **Policy Name** – Specify the Policy Name defined on the Credential Server.
6. **Cache Valid Sessions** – Set to *Yes* if you wish Barracuda Web Application Firewall to cache the session state information to validate subsequent requests from the client.
7. **Cache Expiry (Seconds)** – Specify the duration of time (in seconds) to store the cached session state information to validate the requests after which the session information is re-validated against the Credential Server
8. **Redirect URL** – Specify the URL where you want to redirect a user who accesses the protected web application from a normal browser. If not specified, the Barracuda Web Application Firewall redirects the user to the Credential Server.

3. Click **Add** to add the credential server.

Adding a Secure Browsing Policy

To add a secure browsing policy and associate it with the HTTPS Service, do the following:

1. Go to the **WEBSITES > Secure Browsing** page.
2. In the **Add Secure Browsing Policy** section, specify values for the following fields:
    1. **Policy Name** – Enter a name for the armored browsing policy.
    2. **Service** – Select the Service from the list for which you desire secure browsing.
    3. **Host Match** – Enter a host name to be compared to the host in the request. This can be either a specific host match or a wildcard host match with a single “* “ anywhere in the host name. For example, `*.example.com`, any request matching this host is required to authenticate before accessing this page.
    4. **URL Match** – Enter a URL to be compared to the URL in the request. The URL should start with a "/" and can have at most one " * " anywhere in the URL. For example, `/netbanking.html`, indicates any request matching this URL is required to authenticate before accessing this page. A value of “/*” means that the access control rule (ACL) applies for all URLs in that domain.
    5. **Credential Server** – Select the credential server to verify the armored browser session.
3. Click **Add** to associate the secure browsing policy with the service.

Figures