



Barracuda Web Application Firewall Best Practices Guide

Barracuda Web Application Firewall Best Practices Guide 1.0

Table of Contents

Introduction	2
Deployment Considerations	3
Deploy in Proxy mode, preferably as a Full-Reverse Proxy	3
Cluster for High Availability (HA) and redundancy	3
Barracuda Web Application Firewall System Configurations	4
Configure Administrator Email Notifications	4
Configure External Logging Systems	4
Configure SNMP Traps for Health Monitoring	4
Configure System Time	4
Configuring Access to the Barracuda Web Application Firewall	5
Resetting the Factory Admin Password	5
Securing Network Access	5
<i>Use a Separate Management network</i>	5
<i>Use HTTPS-Only for management access</i>	5
Controlling and restricting access	6
<i>Defining and Assigning Roles</i>	6
<i>Restrict IP Access</i>	6
General Web Application Security Recommendation	7
Always use HTTPS When Possible	7
Use Positive and Negative Security Models	7
<i>Negative Security Model</i>	7
<i>Positive Security Model</i>	7
<i>Combining Positive and Negative Security Models</i>	8
Enable Authentication, Authorization and Access Control (AAA)	8
<i>Set Up Authentication Services</i>	8
<i>Configure Authorization Rules</i>	8
Engage in Application Tuning Before Deployment	9
<i>Passive Mode</i>	9
<i>Exception Profiling</i>	9
Recommended Security Policy Settings	10
Predefined Security Policies	10
Custom Security Policies	10
<i>Set Cookie Tamper-Proof Mode to 'Encrypted'</i>	10
<i>Use Secure Cookies</i>	10
<i>Change Cookie Encryption Key Periodically</i>	11
<i>Check Incoming Requests</i>	11
<i>Validate User Input</i>	11
<i>Enable Server Cloaking</i>	12
<i>Enforcing Client Browser Versions</i>	12
Glossary of Terminology	13

Introduction

The goal of this document is to provide administrators with common best practice considerations as they are configuring their Barracuda Web Application Firewall to ensure the highest level of security and availability. This guide is to be used in conjunction with the Barracuda Web Application Firewall Administrator's Guide and Barracuda Web Application Firewall Online help, which document in depth on how to configure Barracuda.

Barracuda Web Application Firewall Best Practices Guide 1.0

Deployment Considerations

The Barracuda Web Application Firewall can be deployed in 3-modes:

Proxy Mode	
Full Reverse Proxy	In full reverse proxy mode, the Barracuda Web Application Firewall is deployed in-line, using both the physical ports (WAN and LAN) of the device. This is the recommended configuration as it provides the best security.
One-Arm Proxy	Deployed in One-armed proxy mode, incoming and outgoing network traffic to the Application Firewall passes through the WAN port. Virtual IP addresses of the services on the Web Application Firewall and backend real server IPs are on the same subnet. A high level of security is achieved with this configuration, but a network firewall is recommended to restrict direct access to the backend servers.
Bridge Mode	
Bridge Path	Deployed as an in-line Bridge Path, the Barracuda Web Application Firewall uses the same address for the VIP and back-end server, so data is passed through to the Web Application, including potential attacks, even as the security checks are performed. This configuration does not require changes to the existing network infrastructure but the WAN and LAN need to be on a different switch.

Deploy in Proxy mode, preferably as a Full-Reverse Proxy.

Full-Reverse Proxy is the industry accepted best practice and is inherently more secure than bridge mode deployments. Proxy mode deployments give administrators the ability to protect against critical attacks like session spoofing, CSRF that cannot be adequately protected by traditional Bridge Mode deployments. Key capabilities of Barracuda Web Application Firewall Proxy deployments that are not available in Bridge Mode architectures include:

- InstantSSL that converts an HTTP site to HTTPS without any code changes

In addition, proxy deployments enable application acceleration capabilities including:

- Real Server Load Balancing
- SSL Offloading
- TCP Pooling
- Content routing
- Caching
- Compression

Cluster for High Availability (HA) and redundancy

Due to the 24/7 nature of web traffic, it is important that any deployments in line with the data path have added redundancy. Barracuda Web Application Firewalls configured in HA clusters and will automatically synchronize security and network configurations between the clusters to provide seamless failover in response to disruptions.

Barracuda Web Application Firewall System Configurations

Barracuda Web Application Firewall system settings should be configured properly to ensure consistency of events, logs, alerts and security across an organizations infrastructure.

Configure Administrator Email Notifications

The Barracuda Web Application Firewall sends email alerts in response to system and threat alerts. To set the administrator email:

1. Go to *Basic > Administration*
2. Enter the administrative email address and the mail server configuration information in the *Email Notifications* box on near the bottom of the page.
3. Click *Save Changes*.

Barracuda Networks highly recommends that administrators configure the administrator email account on the account to receive important notifications.

Configure External Logging Systems

The Barracuda Web Application Firewall stores four types of logs:

Firewall Logs	Logs all actions/events on the Barracuda Web Application Firewall. These logs help the administrator analyze traffic for suspicious activity and fine tune the security settings
Access Logs	Logs all Web traffic activities. These logs provide information about the Web site traffic and performance.
Audit Logs	Logs all administration and configuration activities. This information assists in audits
System Logs	Logs system events.

Logs are stored in a circular queue and are overwritten once the logs file reaches the maximum size. Log data can be exported using FTP to an external storage system for archival or exported using syslog to a Security Information and Event Management (SIEM) for analysis and storage. Barracuda Web Application Firewalls supports syslog exports to popular SIEM tools including ArcSight, Splunk, Q1Labs QRadar, RSA enVision, Symantec SIEM, eIQ Networks SecureVue and TriGeo SIM. To set up an external FTP or syslog server, go to *Advanced > Export Logs*.

Barracuda highly recommends that administrators set up an external storage or SIEM system to store log data.

Configure SNMP Traps for Health Monitoring

In addition to email alerts, Barracuda Web Application Firewalls can send traps to notify administrators of system alerts. SNMP Traps can be configured on the *Basic > Administration* page. Documentation of MIB definitions can be found at <https://<waf-ip-address>/Barracuda-BWS-MIB.txt> or by clicking on the "Help" Tab next to SNMP Manager section of the *Basic > Administration*.

Barracuda recommends configuring SNMP Traps if a SNMP monitoring tool available in the network.

Configure System Time

By default, the Barracuda Web Application Firewall will synchronize Time with the Barracuda Networks NTP server. It is recommended that administrators configure the Barracuda Web Application Firewall to use the organization's NTP server to ensure time synchronization across the organization's servers:

1. Go to *Advanced > System Configuration*
2. Enter NTP server IP in the *NTP Server Settings* box
3. Click "Add" button

It is possible to designate more than one NTP servers. When multiple servers are defined, NTP uses the server whose time is most accurate based on various factors like the time variation and distance to the server.

Configuring Access to the Barracuda Web Application Firewall

The Barracuda Web Application Firewall is a critical component of an organizations security infrastructure and any access to the Barracuda Web Application Firewall should be strictly controlled.

Resetting the Factory Admin Password

The Web Application Firewall ships with an Admin user account that has full administrative privileges and cannot be deleted from the system.

Barracuda strongly recommends that administrators change the default Admin password to a strong password.

The Barracuda Web Application Firewall does not enforce any rules on passwords, but general best practice guidelines recommend:

- Password lengths of more than 12 characters
- Use randomly generated passwords where feasible
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links, or biographical information
- Include numbers, and symbols in passwords
- If the system recognizes case as significant, use capital and lower-case letters

Securing Network Access

Network access to the Web Application Firewall should be controlled and limited. Recommended best practices include:

Use a Separate Management Network

Setting up a separate management network separates administrative traffic from WAN and LAN traffic. This physically ensures that only users with access to the management network can access the administrative interface on the Web Application Firewall. To set this up:

1. Use the MGMT port on the Web Application Firewall to connect to the management domain.
2. Login into the Web Application Firewall
3. Go to *Basic > IP Configuration*
4. Configure the Management IP Configuration section of the page and select "Yes" on for "Allow administration access".
5. Save the configuration

Test to see if you can reach the console using the management network. Once you have confirmed you can reach the Web Application Firewall, log back into the Web Application Firewall.

1. Go to *Basic > IP Configuration*
2. Select "No" on the "Allow administration access" on WAN IP section
3. Select "No" on the "Allow administration access" on LAN IP section
4. Save the changes

Use HTTPS-Only for management access

1. Login to the Web Application Firewall using HTTPS
2. Go to *Advanced > Secure Administration*
3. Change HTTPS/SSL Access Only to Yes

Controlling and Restricting Access

Defining and Assigning Roles

Access to the Barracuda management interface should be guided by the principle of *least privilege*. User roles ideally should be well-defined and should be limited to the minimal amount required to perform their job functionality.

The Barracuda Web Application Firewall ships with eight predefined roles representing the most common user roles used to administer the Web Application Firewall:

Role	Description
Admin	This is the super administrator role. The default 'admin' user is assigned this role. This role has the privilege to perform all system operations. An admin is responsible for creating and assigning roles.
Audit-Manager	User assigned to this role can perform auditing tasks. This role has the privilege to view logs, but is exempted from exporting logs. The role's responsibility is: <ul style="list-style-type: none"> • View logs • Generate reports
Certificate-Manager	User assigned to this role can perform certificate management tasks. The role's responsibility include: <ul style="list-style-type: none"> • Uploading certificates • Creating certificates • Uploading trusted certificates
Guest	User assigned to this role can view all configurations, but is exempted from modifying the configuration.
Monitoring-Manager	User assigned to this role can monitor system activities. The role's responsibility include: <ul style="list-style-type: none"> • View logs • Configuring email notifications • Exporting System logs, Application Logs and FTP access Logs • Generating and scheduling reports
Network-Manager	User assigned to this role can perform network related operations. The role's responsibility include: <ul style="list-style-type: none"> • Advanced IP configuration • Configuring SNAT and ACL's • Network troubleshooting
Policy-Manager	User assigned to this role can manage security policies on the Web Application Firewall.
Service-Manager	User assigned to this role can manage services on the Web Application Firewall.

Beyond the predefined roles, the Barracuda Web Application Firewall gives administrators fine grain access control capabilities to create custom roles that best represent what is needed for their teams. Administrators can create their own custom role using under the *Advanced > Admin Access Control* tab.

Always assign the least amount of privileges required when creating new users.

Restrict IP Access

In addition to creating a management network and fine grained user roles for access control, it is recommended that administrators restrict IP access on the management network to a limited subnet. This ensures that only a small set of users utilizing designated devices can access the management console of the Barracuda Web Application Firewall.

NOTE: Be careful when setting up the IP subnet of the management network. Incorrect configurations can lock out access to the Barracuda Web Application Firewall. If locked out, administrators will need to access the Barracuda Web Application Firewall via the serial console.

General Web Application Security Recommendation

Always use HTTPS When Possible

Barracuda recommends usage of HTTPS for all Web applications that uses cookies to store information on the client or requires user input. Using HTTPS ensures that applications are secure from man-in-the-middle attacks where attackers attempt to eavesdrop (or spoof) the traffic communication between the client and server. Man-in-the-middle attacks are common when using unsecure WI-FI hotspots available at coffee shops, libraries or when using any other public, unsecure networks. HTTPS reduces the risk of eavesdropping by negotiating a stateful, encrypted connection using a handshake protocol. Barracuda Web Application Firewalls provide a number of minimally invasive ways to enable HTTPS without impacting web server performance or requiring application code change:

- **If you are concerned about Web Server performance**, Barracuda Web Application Firewalls can offload SSL traffic. When deployed as a reverse proxy, the Barracuda Web Application Firewall can perform HTTPS encryption on behalf of the web server when communicating with client browsers. Since all traffic terminates on the Barracuda Web Application firewall, backend traffic with the Barracuda Web Application Firewall can continue using HTTP resulting and thereby not adding additional encryption burdens on the web server.
- **If your web application is not written for HTTPS**, Barracuda Web Application Firewalls provides an innovative feature called InstantSSL that transforms plain vanilla HTTP sites into secure HTTPS sites without requiring any application changes. This solves the obstacle of having to rewrite applications to support HTTPS by offloading the transformation to the Barracuda Web Application Firewall.
- **If clients have bookmarked or continue to use the HTTP site**, the Barracuda Web Application firewall can seamlessly redirect the clients to the HTTPS site.

Use Positive and Negative Security Models

For maximum security and ease of use, it is recommended that organizations configure both negative and positive security rules in a Security Policy.

Negative Security Model

Negative security policies are easy to deploy and protect against known exploits. The Attack patterns defined in the Barracuda Web Application Firewall can be found under *Advanced > View Internal Patterns*. In addition to Barracuda defined patterns, administrators can define their own custom patterns that can be used in the negative security model in a custom Security Policy for a particular Web application. Custom patterns can be added in *Advanced > Libraries*.

The weakness of negative security is that by definition negative security can block *known* attack patterns that it can identify. It cannot guard against zero-day or unknown exploits. This is true for all security products and all security vendors. Barracuda Networks minimizes the risk of zero-day exploits by continually updating Attack Patterns, Virus definitions, and other patterns used by the Barracuda Web Application Firewall through Energized Updates. This ensures that the Barracuda Web Application Firewall can defend against the latest vulnerabilities. However it is still important to include a positive security model to protect against the unknown unknowns.

Positive Security Model

Positive security policies are much more secure in that it explicitly defines what can be done on the system and blocks the rest that do not match conform to what is predefined. Barracuda Web Application Firewalls can categorize every URL and input data to define explicitly what user input is allowed for a given web page. Administrators can build detailed whitelists in the Barracuda Web Application Firewall in the *Websites > Web Site Profile* menu. The Adaptive Profiling capability of the Barracuda Web Application firewall automates the process by sampling traffic over a given period of time and auto-generates profiles based on observed input. This can be configured under the *Websites > Adaptive Profiling* menu and turned on using the *Start Learning* button under *Websites > Web Site Profile*.

The limitation of positive security models is that it requires administrators to predefine all acceptable behavior and inputs. This means that every URL and every parameter must be categorized and configured. Moreover any changes to the web application will require additional tuning ensure that the positive security model is up to date. Applications today are constantly changing and unless you are deploying a static information only web site, it is often impractical to use only a positive security as the constant need to tune the application makes it difficult to deploy the security policy in a timely fashion, even when using automated learning tools like *Adaptive Profiling*.

Combining Positive and Negative Security Models

In most practical deployments, both negative and positive security policies are used in conjunction to provide security without burdening the organization with never-ending tuning and profiling. While most web applications have different requirements, there are best practices and rule-of-thumbs that can be used to configure a Positive-Negative security model in the Barracuda Web Application Firewall:

- **Configure Default policy or a Custom Security Policy to set Global Values for a Service.** The Barracuda Web Application Firewall security policies enable administrators to set global values on request limits, URL parameters, and other input values of what is allowed.
- **Use Adaptive Profiling to build URL and input profiles on high value pages.** Certain areas of web applications like online shopping carts or address update pages are extremely important and should be profiled so that administrators explicitly define what inputs can be entered into each field. This limits the scope of valid entries and prevents any deviations that may introduce vulnerabilities.
- **Stay up to date on Energized Updates and Firmware Updates.** Barracuda Networks continually adds new pattern definitions and anti-virus signatures to the Web Application Firewall. Ensuring that Web Application Firewall receives the latest updates is important in keeping the negative security definitions effective.

Enable Authentication, Authorization and Access Control (AAA)

Barracuda Networks strongly recommends the use of AAA capabilities. Most interactive websites require user and session management to enforce access control so that users cannot access accounts and or URL locations that are not explicitly granted. Even the most basic websites that do not handle user input often have administrative portions of the website that should be locked down. Barracuda Web Application Firewall has extensive AAA capabilities that can extend traditional application delivery capabilities to support comprehensive Identity and Access Management (IAM) ranging from simple application authentication and authorization up to more granular, full-featured Single Sign-On (SSO). At a minimum, it is recommended that administrators configure basic AAA settings:

Set Up Authentication Services

Barracuda Web Application Firewall support of number of authentication services that can be used to identify and authorize users to web resources on backend web servers. Supported services include:

- LDAP
- RADIUS
- RSA SecurID (for two-factor authentication)
- CA Siteminder (for Single Sign On)
- Client Certificates

Client certificate authentication can be configured under *Access Control > Client Certificates*. All other authentication methods can be configured under *Access Control > Authentication Services* menu.

If your organization does not support any of the authentication services, the Barracuda Web Application Firewall has the ability to acts as an authentication gateway. It is possible to define user accounts and groups locally on the Barracuda Web Application Firewall to use for authentication and authorization. To define your own user groups, go to *Access Control > Local User/Groups*.

For all interactive Web Applications, Barracuda recommends organizations to configure at least authentication service.

Configure Authorization Rules

Administrators can control which users or groups can access what portions of any Web application after setting up an Authentication Service. Administrators should analyze the Web application and determine the access rights of the various roles in the application. For example, it is common for organizations to have:

- General information Web pages accessible to anyone
- Administrative pages accessible only to administrators of the application
- Customer and/or Partner sections that are accessible to only users of a particular group

It is important to define granular access control rules to only allow users with the right credentials and roles to access the different areas of the website. For example, the Barracuda Web Application Firewall to configure granular authorization rules to:

- Only allow administrators to browse <http://www.example.com/admin/> section.
- Only allow admins and partners to log into the partner portal at <http://www.example.com/partner/>
- Allow all access to the corporate landing page at <http://www.example.com>

All of the rules can managed under *Access Control > Authorization*.

It is highly recommended that authorization rules should be configured for pertinent sections of the Web Application.

Engage in Application Tuning Before Deployment

The Barracuda Web Application Firewall is the easiest to use and quickest to deployment Web Application Firewall solution. However as with all security products, there is often a period of time required to deploy and tune the solution to avoid false positives. Barracuda Networks has made this process as simple as possible by providing important tools to simplify and automate the tuning of security policies.

Passive Mode

Barracuda Web Application Firewalls can be deployed in Passive-mode where the Web Application Firewall applies the selected Security Policy in Log Only mode to the service. This allows traffic to pass without interruptions while logging possible violations in the Firewall logs.

These logs are stored under *Basic > Web Firewall Logs* and should be used to analyze Security Policy violations. Violations will be flagged in red and administrators can look at the details of why that request was flagged. If a false positive is detected in the Web Firewall Logs, it is possible to issue by clicking on the "Fix" hyperlink on the log entry and the Barracuda Web Application Firewall will modify the Security Policy configuration to prevent future false positives.

Barracuda recommends that prior to deploying any Security Policy to use Passive Mode on QA or Production traffic to tune the policy based on live traffic.

Exception Profiling

The concept of "Exception Profiling" in the Barracuda Web Application Firewall is to apply a set of heuristics on the "violations" generated by clients, and either recommend or auto create exceptions to the policies existing on the Barracuda Web Application Firewall, so as to minimize the false positives by providing a mechanism to adjust the originally created policies. The controls for enabling and configuration exception profiling can be found on the *Advanced > Exception Profiling* page.

Security policies that incur a large number of false positives can indicate a mismatch between Security Policy rules and application traffic. The Barracuda Web Application Firewall will flag and make exception recommendations based on the threshold configured on Exception Profiling tool. If it is determined that the result is a false positive, administrators can accept the recommendation and create an exception for that particular pattern for that specific page. Once accepted, the exception pattern can be found under the *Websites > Web Site Profile* as a URL entry. This ensures that the exception is applied only to that particular URL and not globally to the security policy. For global changes, administrators must add the exception pattern at the Security Policy level under the *Security Policies* tab.

Before the deployment of any new or modified Security Policy, it is recommended that organizations engage in a round of Exception Profiling.

Recommended Security Policy Settings

Barracuda Web Application Firewall approach to security is to provide the highest level of security while still be easily configurable.

Predefined Security Policies

Barracuda Web Application Firewalls ship with four predefined security policies. These include:

Default	Baseline security policy that protects web applications from the most common attacks. All new services start with Default policy.
OWA	Security policy for Outlook Web Access (OWA)
Sharepoint	Security policy for Microsoft Sharepoint
Oracle	Security policy for Oracle applications

The predefined security policies represent some of the most common applications used by organizations and are preconfigured by Barracuda Networks to enforce the most common security settings applicable to the application.

Custom Security Policies

Administrators can build custom security policies that best enforce the necessary security configurations for that application. All custom security policies start the same settings as predefined factory *Default* security policy. This provides administrators with a baseline security configuration to build upon. For custom security policies, Barracuda Networks recommends:

Set Cookie Tamper-Proof Mode to 'Encrypted'

HTTP Cookies are used by website for authentication, storing site preferences, shopping cart contents, identifying server-based session, or anything else that can be accomplished through storing text data. Because cookies are stored on the client web browser, they can be easily manipulated by attackers to fool web servers, steal sessions, and/or other malicious activity.

Barracuda Web Application Firewall configured in proxy-mode provides administrators the ability to encrypt or sign cookies on behalf of the backend web servers:

- **Encrypting cookies** renders cookie content unreadable
- **Signing cookies** attaches a signature to prevent tampering but is still readable by the client browser

Some web applications use JavaScript or other client side scripting language to manipulate data stored in cookies. In this situation, it may be difficult to enforce a policy of using encrypting cookies without a redesign of the web application. In this situation, it is possible to use signed cookies to guard against cookie tampering on the client side but this will leave cookie content exposed in plain text.

To set cookie security mode:

1. Go to *Security Policy > Cookie Security*
2. Click on "Encrypted" (or "Signed") option next to the *Tamper Proof Mode*
3. Click "Save Changes"

Barracuda Networks recommends using Signed Cookies over HTTPS to protect against man-in-the-middle attacks and to protect against cookie tampering on the client side.

Use Secure Cookies

Cookies carry session information which should be exchanged between the client and the server using secure connection. When a cookie is sent to the browser, the browser will return the cookie to the server on HTTP or HTTPS connection. If 'Secure cookie' setting is enabled the browsers will send the cookie only on secured HTTPS connection.

1. Go to *Security Policy > Cookie Security*
2. Click on "Yes" option next to "Secure Cookie" field
3. Click "Save Changes"

Barracuda Networks recommends enable Secure Cookie to protect against man-in-the-middle cookie theft or cookie sniffing.

Change Cookie Encryption Key Periodically

If you are using cookie encryption it is important to rotate encryption key on a period basis to ensure maximum security. The Barracuda Web Application Firewall allows administrators to generate and manage cookie encryption keys store on the Web Application Firewall. Generated keys are valid for 3 months and the Barracuda Web Application Firewall will generate a warning message when the expiration date is reached.

To generate and install a new key:

1. Go to *Advanced > System Configuration*
2. Click the Generate button next to *Generate New Cookie Encryption Key*.
3. A window with a new encryption key will open
4. Copy the *New Cookie Encryption Key* in the new window into the *Cookie Encryption Key* field in the original window.
5. Copy the *New Cookie Encryption Key Expiry Date* in the new window into the *Cookie Encryption Key Expiry Date* field in the original window.
6. Click *Save Changes*

Barracuda recommends that cookie encryption key be changed EVERY month.

Check Incoming Requests

Block unwanted HTTP methods: Web servers support all the methods defined by in HTTP. Normally applications do not use all the available methods and making them available to the external world may open up security holes.

It is a good practice to restrict access to only GET and POST methods. If some part of the application uses some other HTTP method then that should be configured as an exception. To block unwanted HTTP methods go to:

Restrict number of input parameters and content length: Normal applications have an average of 20 parameters that are submitted to a form. The average number should be configured as the Max Parameter settings in the Security Policy. Any form that requires a larger number of parameters should be configured as an exception. Additionally the maximum content length should be restricted to represent the type of traffic you are expecting. For example, if you have website that has minimal form input fields, then it may be prudent to reduce the maximum content length to a lower value than the default value of 32kb.

To restrict number of input parameters and content length:

1. Go to *Security Policy > URL Protection*
2. Enter new value in "Max Parameters" field
3. Enter new value in "Max Content Length" field
4. Click "Save Changes"

Validate User Input

All parameters being submitted to the applications should be inspected to ensure that attacks are not being injected via form based inputs. Some best practices include:

Deny characters that are used to create attack strings: Administrators can set Meta-characters to block on the *Security Policy > Parameter Protection* page under the *Denied Metacharacters* field. In general it is best to deny characters like ESC, *, or any other characters used in scripting that are not necessary for the form entry page.

Check file uploads: If your Web application allows users to upload files to the web server, it is necessary to limit permissible file types. This reduces the risk of Trojans, root kit, or any other forms of malware from being uploaded onto your system. To limit file types go to *Security Policy > Parameter Protection* and modify the *File Upload Extension* field to only allow predefined file types. Additionally Virus Scanning can be enabled on models 660 and above under *Website > Advanced Security*.

Scan for Injection Patterns: Injection attacks are one of the most common forms of attack on Web applications. Barracuda Web Application Firewalls come with a number of predefined injection patterns to protect web applications against SQL Injection, OS injection, XSS and many other types of common injection patterns. These patterns will capture and protect against the vast majority of injection type attacks. However depending on the type of application, it may be necessary to create your patterns. This can be done by adding a new regular expression into the scanning libraries. To add your own custom signatures go to *Advanced > Libraries* and enter the new pattern under the *Attack Type* section.

Enable Server Cloaking

One of the first steps that any attackers performs when targeting a web application is to find out the details of the backend servers. Typically this is done by purposely sending a series of commands to obtain the HTTP headers and server error codes back from the targeted web servers. Clues gleaned from HTTP headers and error codes can then be used to figure out the OS, database, software, or other version information and targeted to exploit the specific weaknesses of the software stack.

Barracuda recommends that Server Cloaking be enabled for all Security Policies to suppress server information leakage from HTTP responses and HTTP headers. Some common headers to filter include:

Header	Description
Server	Server name information. Often includes HTTP server and underlying OS information
X-Powered-By	Specifies the technology (PHP, JBoss, e.g.) supporting the web application
X-AspNet-Version	Specifies the ASP.NET version used on the web server
X-Runtime	Can be used to identify web servers like nginx, Mongrel

To enable Server cloaking:

1. Go to *Security Policy > Cloaking*
2. Select *Policy Name* from menu list.
3. Set *Suppress Return Code* to "On". This will suppress HTTP errors and return a generic page.
4. Set *Filter Response Header* to "On". This will suppress all headers listed in the *Headers to Filter* list.
5. Add the headers to filter under *Headers to Filter*. Barracuda Web Application Firewalls are preconfigured to suppress, Server, X-AspNet-Version, X-Powered-By. You can add your own headers by entering the name and clicking *Add*.

Enforcing Client Browser Versions

Older web browsers do not contain the latest security functionality and security patches needed to secure communication between the client and the web servers. Consequently it is best practice to restrict client browser versions to prevent access via an insecure channel. For example, due to the numerous known vulnerabilities in Internet Explorer 6 (IE6), client access using IE6 should be restricted. To do so:

1. Go to *Security Policies > Global ACLs*
2. Select the policy to modify by choosing it in the *Policy Name* drop down menu.
3. Add a name to *URL ACL Name*
4. Enter */** in *URL match box*. This will enable the ACL rule on all URLs in that domain
5. In *Extended Match* field, click on the edit icon
 - In *Element Type* select *Header*
 - In *Element Name* select *User-Agent*
 - In *Operations* select *contains*
 - In *Value* add *MSIE 6.0*
6. Select *Redirect* from *Action*
7. Add a *Redirect URL*. You can point to a custom page with a message stating that IE6 is not supported.

It is possible to add any type of browser using the Global ACLs capabilities of the Barracuda Web Application Firewall. As a best practice, Barracuda Networks recommend administrators perform a risk-to-usability analysis and make decision on allow/ deny ACLs based on the results of the assessment.

Glossary of Terminology

Bridge Mode	
Bridge Path	Deployed as an in-line Bridge Path, the Barracuda Web Application Firewall uses the same address for the VIP and back-end server, so data is passed through to the Web Application, including potential attacks, even as the security checks are performed. This configuration does not require changes to the existing network infrastructure.
Proxy Mode	
Full Reverse Proxy	In full reverse proxy mode, the Barracuda Web Application Firewall is deployed in-line, using both the physical ports (WAN and LAN) of the device. This is the recommended configuration as it provides the best security.
One-Arm Proxy	Deployed in One-armed proxy mode, incoming and outgoing network traffic to the Application Firewall passes through the WAN port. A high level of security is achieved with this configuration, but because traffic is limited to the WAN port, network throughput is decreased.
Real Server	Identifies the server (IP address, port) that hosts the Web application that will be protected by the Barracuda Web Application Firewall.
Services	A user-designed entry point for controlled access to the Web site. A service sets the front-end interface (VIP) and a variety of possible controls (such as SSL encryption, authentication, load balancing, and caching policies) for the Web site.
Virtual IP address (VIP)	The user-defined IP address on which the Barracuda Web Application Firewall accepts traffic for a configured Web application. In a redundant configuration it is a virtual address that applies regardless of which Barracuda Web Application Firewall is managing the application at any given time.