

While most organizations are familiar with protecting against network vulnerabilities with a layer 3 firewall, these traditional firewalls are not designed to prevent the latest application layer threats including SQL injection and Cross Site Scripting attacks. Operating at Layer 7, web application firewalls identify, understand and secure Web traffic. They also decrypt HTTPS traffic to ensure that no attacks are smuggled inside an encrypted channel.

The steps required to secure the Web infrastructure against the latest threats with the help of web application firewalls include:

- Choosing the network deployment for a web application firewall
- Applying default security policies
- Monitoring events in passive configuration
- Fine-tuning policies
- Enabling active protection

Through these steps, organizations can protect their environments quickly even as applications evolve and newer versions of the applications become available.

Choosing a Deployment Model

The Barracuda Web Application Firewall supports three different deployment modes to meet both the varied needs of your network and the operational needs of your organization.

- **Reverse proxy.** The reverse proxy configuration accepts traffic on virtual IP addresses and proxies the traffic to a private network behind the appliance. This configuration is the most secure configuration but generally involves changing the IP addresses of backend servers. This deployment model offers the most comprehensive security and application delivery options.
- **Bridge-path.** In Bridge-path configuration the Barracuda Web Application Firewall sits inline between the network firewall and the Web servers and does not require any changes to the IP addresses of the servers. The Barracuda Web Application Firewall intercepts and inspects all traffic to the Web servers and forwards only valid traffic. The system includes a hardware fail-safe mechanism that provides a direct path to the backend servers, allowing the appliance to be moved out of the data path if required.
- **One-armed proxy.** This is a flexible deployment option in which traffic can be selectively routed through the Barracuda Web Application Firewall while remaining traffic can be sent directly to the backend server. This approach is preferred for scenarios in which the administrator wants to retain direct access to the server in case the server is hosting other services such as an email server in addition to the Web server. The disadvantage of one-armed proxy is that both request and response traffic traverses over a single NIC.

Table 1: Summary of deployment modes

Scenario	Preferred deployment option	Details
Enforce maximum security	Reverse Proxy	Creates an isolated network for the Web servers.
Load balance multiple Web servers while securing the Web application	Reverse Proxy	Provides load balancing and other traffic management features
Deploy quickly without any IP change	Bridge-path	Intercepts traffic based on the IP address of the Web server
Use a load balancer to route partial traffic for security inspection	One-armed	The Web Application Firewall is treated as a server for the load balancer.
Maintain direct access to the physical server for non Web Server based traffic	One-armed	Only Web traffic passes through the Barracuda Web Application Firewall - all remaining traffic goes directly to the server
High availability for deployed applications	Any	All deployment options are available in an active / passive cluster
Fail safe option	Bridge-path	In case the Barracuda Web Application Firewall needs to be shut down, the fail safe option simply connects the WAN to the LAN

Once the Barracuda Web Application Firewall has been deployed on the network, services have to be configured on to the appliance to provide information about the Web servers that are to be secured.

Applying Default Security Policies

The Barracuda Web Application Firewall provides robust default security to protect your Web applications. Default policies include:

- Parameter attack pattern filtering to prevent SQL injection, OS command injection, directory traversal, cross-site scripting (XSS), and other common Web application vulnerabilities
- Digital signing or encryption of cookies to prevent session tampering
- Suppression of server errors to cloak the information about the Web application, such as information about the Web server being used or an SQL error that occurred
- Blocking access to files with extensions like .bak or .old
- Request limits to enforce incoming data size for requests, headers and cookies
- Cookie replay protection to ensure cookies are submitted from the same client to which they were originally sent.

By applying default security policies, organizations can achieve a powerful level of base security independent of application specifics.

Monitoring in Passive Mode

Once the administrator configures a service, or Web application, on the Barracuda Web Application Firewall, the service begins utilizing the default security policies in passive mode. Passive mode enables the Barracuda Web Application Firewall to simply inspect traffic and report on security violations without

blocking any traffic. The advantage of passive monitoring is that the administrator can preview available protection without affecting production traffic. All policy violations observed are captured in the Web firewall logs on the Web Application Firewall. With passive mode, administrators can inspect logs to observe the benefits of protection, identify potential issues with broad-based rules and to determine if the appliance is appropriately sized for their needs.

Fine-Tuning Policies

The Barracuda Web Application Firewall presents the Policy Tuner feature which integrates with the Web firewall logs to create exceptions or to tune existing security policies. The Policy Tuner utilizes the data captured in the Web Firewall logs to generate relevant exceptions such as increasing the allowed parameter size in a form field. In addition, the Web site profiles can be utilized to define granular rules to protect critical portions of applications such as order forms. The profiles are also used to create exemptions on a per-URL or per-form parameter basis.

Setting Active Protection

Once policies have been fine tuned, the administrator can switch the Web application running in passive mode into active protection mode. This blocks all traffic that violates configured security policies. In the event that the backend application changes, the administrator can review the logs to see if additional configuration tuning is required for the newer parts of the Web application. This tuning can be easily achieved with the help of the Policy Tuner.

In addition to the basic security setup, the administrator should also consider setting up the following:

- **Administrative Accounts.** Create an account for each administrator managing the Barracuda Web Application Firewall. Audit logs can then be used more effectively to track the configuration changes applied by an administrator.
- **Alerts.** Receive information, via SNMP or email, about critical system events.
- **Backup and Logs.** Back up the system configuration regularly to keep a history of changes. All the logs should also be automatically exported out to a Syslog server or an FTP server on a regular basis.

The Barracuda Web Application Firewall with its default security policies provides a significant security blanket for all Web applications. These policies can be further tuned for even higher levels of security. With its flexible deployment modes, the Barracuda Web Application Firewall secures Web content hosted in very simple to very complex networks and offers the most compelling solution for organizations looking to secure their Web infrastructure.

For questions about the Barracuda Web Application Firewall, please visit <http://www.barracuda.com/waf> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.